Manual básico de:

GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

AMÉRICA LATINA Y CARIBE

Proyecto :AMPARO

Lacnic

Rambla República de México 6125

Montevideo C.P. 11400

Uruguay

Phone: + 598 2604 2222

ISBN: 978 - 9974 - 98 - 741 - 8

Edición 201

Acerca de Amparo

Antecedentes

Internet se ha convertido en una herramienta crucial tanto para las compañías como para los individuos. Toda clase de transacciones sociales y económicas están migrando a la red global de manera cada vez más trivial y casi automática. Desafortunadamente la creciente virtualización de la economía y de la sociedad también trae aparejados desafíos significativos. Spam, acceso indebido a datos confidenciales y robo son solo algunos de los daños cometidos por criminales y terroristas contra organizaciones e instituciones, particularmente en aquellas situadas en países sin capacidad institucional para protegerse.

Dada esta realidad, resulta muy importante para las organizaciones y también para los proveedores de acceso Internet, contar con mecanismos para evitar y contener actividades abusivas que permiten generar los problemas referidos.

Para contrarrestar estos problemas, uno de los mecanismos utilizados cada vez con mayor frecuencia, es el de contar con un grupo que a su nivel (empresa, servicio, país) tenga la capacidad de tratar los incidentes de seguridad de red. Estos grupos son comúnmente denominados Equipos de Respuesta a Incidentes de Seguridad de Computadores o en Inglés Computer Security Incident Response Team (CSIRT).

Objetivos

Este proyecto busca aumentar la capacidad de prevención y de respuesta a incidentes de seguridad informática en la región de América Latina y el Caribe a través de:

1. El desarrollo de actividades de investigación aplicada que apoyen los procesos y prioridades regionales promoviendo un ambiente adecuado y sinérgico que contribuya significativamente a resolver los principales aspectos de la problemática de seguridad informática en América Latina y el Caribe;
2. La promoción de la creación de CSIRT`s a nivel de grandes organizaciones del sector público y privado de los diferentes países de la región. Esto implica, sensibilizar a los

actores relevantes con capacidad de incidir en la problemática de seguridad en Internet, sobre la necesidad de generar acciones inmediatas para su consideración, entre las que se encuentra, la creación de marcos normativos, estructuras organizativas de coordinación y respuesta. Puntos de contacto nacionales y la promoción sistemática de la investigación en la temática;

3. La construcción de una plataforma regional de capacitación de expertos en Seguridad Informática que alimente las distintas organizaciones relacionadas con esta problemática en los distintos sectores de la sociedad en nuestros países;

4. La contribución al análisis sobre los posibles modelos e impactos de la constitución de un CSIRT Regional que potencie a las iniciativas en cada país, provea y mantenga las mejores prácticas y genere una red de confianza para el intercambio de información, frente a la ocurrencia de incidentes.

Resultados esperados

- Una agenda regional de prioridades de investigación en Seguridad Informática.
- Creación de materiales para la capacitación de expertos en Creación y Operación de CSIRT`s.
- Realización de Talleres regionales.
- Realización de un Taller regional para Instructores.
- Un curso para Creación y Operación de CSIRT`s.
- Expertos capacitados en Creación y Operación de CSIRT`s.
- Expertos capacitados en metodologías y herramientas para la operación de CSIRT`s.
- Capacitación de Instructores regionales en Creación y Operación de CSIRT`s
- Creación de redes de profesionales de referencia para el intercambio de información sobre mejores prácticas y actualización CSIRT`s
- Financiación de proyectos de investigación sobre problemáticas de Seguridad.
- Sistematización, publicación y difusión de las mejores prácticas en materia de Seguridad Informática.

- Estudio sobre posibles modelos, necesidades financieras e impactos de la implantación de un CSIRT Regional (LAC-Cert).

Acerca del Manual:

El presente manual ha sido desarrollado en el marco de las actividades del Proyecto AMPARO, una iniciativa de LACNIC con el apoyo de IDRC de Canadá.

El proceso de creación del mismo ha implicado un gran esfuerzo por parte de un equipo de expertos en el manejo de incidentes de seguridad, académicos de diversos países de la región, de alto reconocimiento nacional e internacional y personal de LACNIC, e IDRC, con los que nos ha tocado vivir esta primera fase del Proyecto.

A todos ellos un inmenso agradecimiento, porque han hecho posible la creación del primer Manual de Gestión de Incidentes de Seguridad Informática, que será puesto a consideración de la comunidad técnica de América Latina y el Caribe.

El material que se ha desarrollado consta del presente Manual, varios Talleres de simulación de casos, presentaciones y otros documentos, los que serán sometidos de ahora en más a un proceso de mejora continua, en el cual esperamos una alta participación e involucramiento de los excelentes técnicos de seguridad que la Región dispone.

Asimismo el Proyecto AMPARO, en conjunto con muchas otras organizaciones que se han acercado a colaborar, realizará una serie de Talleres de Entrenamiento Regionales, en los que éste conjunto documental será la base de difusión para los instructores expertos en gestión de incidentes. Estamos plenamente convencidos que tenemos por delante un gran desafío aún, que es la difusión del contenido desarrollado, a las personas que lo necesitan, aquellas que diariamente están gestionando incidentes de seguridad en las organizaciones de la región.

Finalmente es necesario también agradecer el gran apoyo recibido por parte del personal de LACNIC, que ha sido fundamental.

Msc. Ing. Eduardo Carozo Blusmztein, CIS

Autores del “Manual básico de Gestión de Incidentes de Seguridad Informática”

Ing. Rubén Aquino Luna, MEXICO

Ing. José Luis Chávez Cortez, GUATEMALA

Ing. Leonardo Vidal, URUGUAY

Ing. Lorena Ferreyro, ARGENTINA

Ec. Araí Alvez Bou, URUGUAY

Msc. Ing. Eduardo Carozo, URUGUAY

Autores de los “Talleres de Gestión de Incidentes”

Ing. Gastón Franco, ARGENTINA

Ing. Carlos Martinez, URUGUAY

Ing. Alejandro Hevia, CHILE

Ing. Felipe Troncoso, CHILE

Dr. Jeimy Cano, COLOMBIA

Ing. Andres Almanza, COLOMBIA

Integrantes del Steering Committe del Proyecto AMPARO

Dr. Ing. Cristine Hoeppers, BRASIL

Ing. Patricia Prandini, ARGENTINA

Ing. Indira Moreno, MEXICO

Ing. José Luis Chávez Cortez, GUATEMALA

Dr. Ing. Alejandro Hevia, CHILE

Ing. Pablo Carretino, ARGENTINA

Dr. Jeimy Cano, COLOMBIA

Revisión Histórica

Nombre	Fecha	Descripción de la Revisión	Versión
José Luis Chávez Cortez	16/09/2009	Versión Inicial – Capítulo I	1.0
Rubén Aquino Luna	Dic/2009	Versión Inicial – Capítulo II	1.0
Leonardo Vidal	28/11/2009	Versión Inicial – Capítulo III	1.0
Lorena Ferreyro	Oct-/2009	Versión Inicial – Capítulo IV	1.0
Araí Alvez Bou	27/11/2019	Versión Inicial – Capítulo IV – Sección 4.2	1.0
José Luis Chávez Cortez	7/03/10	Integración Inicial	1.1
Rubén Aquino Luna	9/03/10	Revisión del contenido y su indización en el documento.	1.1
Leonardo Vidal	9/03/10	Revisión del contenido y su indización en el documento.	1.1
Lorena Ferreyro	9/03/10	Revisión del contenido y su indización en el documento.	1.1
Araí Alvez Bou	9/03/10	Revisión del contenido y su indización en el documento.	1.1
Eduardo Carozo	17/03/10	Revisión sobre la integración final del documento.	1.1
Eduardo Carozo	26/07/12	Revisión sobre la integración final del documento	1.2
Rebeca Pilco Vivanco	31/01/2015	Revisión y Actualización de contenido y estructura del documento	1.3

Índice General

CAPíTULO 1

Lineamientos y Acciones recomendadas para la formación de un Centro de Respuesta a Incidentes de Seguridad Informática

1. Lineamientos y acciones recomendadas para la formación de un Centro de Respuesta a Incidentes de Seguridad Informática

1.1. Recomendaciones organizacionales y normativas para la integración de un Centro de Respuesta a Incidentes de Seguridad Informática en la organización

1.1.1 Introducción

A continuación se presenta un marco de información que tiene total vinculación con el proceso organizacional y normativo para la integración de un CSIRT en una organización.

Inicia con la descripción de la información básica que se debe conocer sobre un CSIRT, aplicaciones e infraestructura a tomar en cuenta, recomendaciones de posibles escenarios de inserción dentro de la organización y definiciones de las políticas de seguridad informática.

Puesto que es vital que cada miembro de una comunidad sea capaz de entender lo que es razonable esperar de su equipo, un CSIRT debe dejar claro que pertenece a su comunidad, definir los servicios que el equipo ofrece, cómo y dónde reportar incidentes y publicar sus políticas y procedimientos de operación.

Adicionalmente, se detalla la información que debe incluirse en un documento base que será utilizado por el CSIRT para comunicar información relevantes a sus integrantes.

Es preciso enfatizar que sin la participación activa de los usuarios, la eficacia de los servicios de un CSIRT puede ser disminuida considerablemente.

Muchos incidentes de seguridad informática se originan fuera de los límites de la comunidad local y afectan a los sitios en el interior, otros se originan dentro de la comunidad local y afectan usuarios en el exterior. A menudo, el manejo de incidentes de seguridad requerirá varios sitios y un CSIRT para la resolución de casos que requieran este nivel de colaboración. Las comunidades necesitan saber exactamente cómo su CSIRT estará trabajando con otros CSIRT's y organizaciones fuera de sus comunidades, y qué información será compartida.

El resto de esta sección describe el conjunto de temas y cuestiones que un CSIRT necesita elaborar para sus integrantes. Sin embargo, no se trata de especificar la respuesta "correcta" a cualquier área de un tema.

1.1.2 Información inicial

1.1.2.1 ¿Qué es un Centro de Respuesta de Incidentes de Seguridad Informática?

Para los propósitos de este documento, un Centro de Respuesta a incidentes de Seguridad Informática (CSIRT) es un equipo que ejecuta, coordina y apoya la respuesta a incidentes de seguridad que involucran a los sitios dentro de una comunidad definida.

Cualquier grupo que se autodenomina un CSIRT debe reaccionar a incidentes de seguridad reportados así como a las amenazas informáticas de “su” comunidad.

1.1.2.2 Nombre del centro de respuesta

No hay algún requisito respecto de cómo debe nombrarse a un centro de respuesta a incidentes. En realidad un centro de respuesta puede tener cualquier nombre. El reconocimiento de los centros de respuesta que existen en la actualidad se ha dado más bien a través de la reputación que han logrado por el trabajo que realizan.

Si bien no existen requisitos para el nombre de un centro de respuesta a incidentes de seguridad, hay algunos de uso frecuente que seguramente alguna vez hemos visto, particularmente siglas en inglés como las siguientes:

- IRT - Incident Response Team
- CSIRT - Computer Security Incident Response Team
- CIRT - Computer Incident Response Team
- CIRC - Computer Incident Response Capability
- SIRT - Security Incident Response Team
- SERT - Security Emergency Response Team
- CERT - Computer Emergency Response Team

De esta lista, quizá los más frecuentes sean los dos primeros y el ultimó. Éste último, sin embargo, es un nombre que sólo puede usarse con el permiso del Software Engineering Institute (SEI) de la Universidad de Carnegie Mellon, en Estados Unidos.

1.1.2.3 Relaciones entre diferentes CSIRT's

En algunos casos, un CSIRT puede ser capaz de operar eficazmente por sí mismo y en estrecha colaboración con sus integrantes. Pero, también es probable que en algunos incidentes que se reporten a un CSIRT participen partes externas a él, esto significa que el equipo tendrá que interactuar con otros CSIRT's y sitios fuera de su comunidad.

La colaboración entre los CSIRT's incluye desde: solicitar a los otros equipos asesoramiento en la resolución de determinado incidente, difundir el conocimiento de los problemas y trabajar en cooperación para resolver un incidente de seguridad que afectan a uno o más comunidades de los CSIRT's.

Al establecer relaciones de apoyo de tales interacciones, el CSIRT debe decidir qué tipo de acuerdos deben existir entre ellos para compartir información, salvaguardar la información, si esta relación puede ser divulgada, y si es así a quién.

Tome en cuenta que hay una diferencia entre un acuerdo o convenio, en el que los CSIRT's implicados estén de acuerdo para trabajar juntos y compartir la información y la cooperación simple, en la que un CSIRT (o cualquier otra organización) simplemente pide ayuda o consejo a otro contacto de CSIRT. Aunque el establecimiento de estas relaciones es muy importante y afectan a la capacidad de un CSIRT en apoyo de su comunidad corresponde a los grupos implicados decidir sobre los detalles específicos.

Está fuera del alcance de este documento el hacer recomendaciones para este proceso.

1.1.2.4 ¿Qué se protege con un CSIRT?

Un equipo de respuesta debe tener como objetivo proteger infraestructuras críticas de la información, en base al segmento de servicio al que esté destinado deberá ser su alcance para cubrir requerimientos de protección sobre los servicios que brinda. El CSIRT debe brindar servicios de seguridad a las infraestructuras críticas de su segmento.

Las infraestructuras críticas en un país están distribuidas en grandes sectores, los cuales pueden ser:

- Agricultura.
- Energía.
- Transporte.

- Industrias.
- Servicios Postales.
- Suministros de Agua.
- Salud Pública.
- Telecomunicaciones.
- Banca / Finanzas.
- Gobierno.
- Educación

Mientras que las infraestructuras de información están segmentadas de la siguiente manera:

- Internet: servicios Web, Hosting, correo electrónico, DNS, etc.
- *Hardware: servidores, estaciones de trabajo, equipos de red.*
- *Software: sistemas operativos, aplicaciones, utilitarios.*
- *Sistemas de Control: SCADA, PCS/DCS.*

1.1.3 Beneficios de la implementación de un CSIRT

Un Centro de Respuesta a Incidentes de Seguridad Informática tiene como beneficio principal la capacidad que le brindará a su comunidad en proveer un servicio en el manejo de una respuesta rápida que permita contener un incidente de seguridad informática, y según sea el caso el poder posibilitar la recuperación del daño causado por el mismo. Las relaciones o alianzas con pares que tenga el centro así como el acceso compartido a estrategias de respuesta y alertas tempranas hacen más efectiva su operación.

También contribuyen en procesos de aseguramiento de sistemas, identificación de vulnerabilidades hasta la detección de incidentes.

A continuación se listan algunos de los beneficios que se obtiene al implementar un CSIRT:

- Convertirse en un punto de contacto confiable dentro de la comunidad para el manejo de incidentes de seguridad informática.
- Promueve un desarrollo en el uso de infraestructura tecnológica basado en buenas y mejores prácticas para la adecuada coordinación de la respuesta a incidentes de seguridad informática.
- Un punto especializado y asesor para la protección de las distintas actividades informáticas de los sectores que conforman su comunidad objetivo.

- Brinda información sobre vulnerabilidades y las asocia con sus respectivas recomendaciones para la su mitigación y/o control.
- Provee servicios de publicación de información eficaz con la finalidad de socializar la cultura de seguridad informática.
- Participa y comparte experiencias con equipos similares y proveedores de servicios de seguridad informática para su promoción y actualización, así como para el establecimiento de mejores estrategias para el manejo de incidentes de seguridad informática.
- Administra puntos de contacto con otros CSIRT para respaldar las distintas estrategias de seguridad informática en un sentido más global.
- Apoya a otras instituciones que lo requieran a desarrollar capacidades propias para el manejo de incidentes así como la implantación de buenas y mejores prácticas de seguridad informática.
- Posee un equipo conformado por personal especializado, en constante proceso de actualización con la intención de brindar servicios de soporte informático con un alto nivel de eficacia y eficiencia a los distintos requerimientos que la comunidad demande de su respectivo CSIRT.
- Promueve y desarrolla materiales de concientización, educación y entrenamiento en variedad de temas de seguridad informática.

1.1.4 Análisis FODA para un CSIRT

Es necesario realizar un proceso de análisis que evalué si las medidas adoptadas son relevantes, si están fuera o dentro de la organización así mismo, si provee un valor positivo o negativo.

Para poder analizar la situación ante la creación de un CSIRT se presenta el siguiente análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas) que apoya la conformación de un cuadro situacional que nos permite obtener un diagnóstico preciso que apoye en el proceso de toma de decisiones acordes con los objetivos y políticas de un CSIRT.

Tabla 1: Análisis FODA General para un CSIRT.

ANÁLISIS FODA GENERAL PARA UN CSIRT	
ELEMENTO	**DESCRIPCIÓN**
FORTALEZAS	• Posee el respaldo de la organización que lo hospeda así como el recorrido que la misma tenga en la comunidad a la que pertenece. • Un punto focal para la notificación y tratamiento de incidentes de seguridad. • Disponibilidad de personal técnico calificado y actualizado. • Dado el conocimiento que posee su personal, el CSIRT es relevante para el proceso de educación para la seguridad y prevención de incidentes.
OPORTUNIDADES	• Desarrollo de relaciones comerciales de largo plazo con los clientes. • Búsqueda de alianzas con terceros que complementen los servicios en el mercado objetivo. • Gran necesidad de coordinación de incidentes de seguridad informática. • Proyecto de interés general para todos los sectores de la sociedad. • No existe una centralización en la medición y seguimiento de la seguridad informática en el segmento de servicio.
DEBILIDADES	• Experiencia. • Reconocimiento del trabajo del nuevo CSIRT. • Los sectores público y privado no tienen la prioridad ni la costumbre de asesorarse por un ente especializado en temas de seguridad informática. • Infraestructura TIC débil. • Incipiente regulación de servicios informáticos.
AMENAZAS	• Desaceleración de la economía mundial y local. • Rápida obsolescencia de los equipos informáticos. • Competidores ya establecidos en el mercado de la seguridad informática.

	• Respaldo financiero limitado. • Bajos incidentes de seguridad informática pueden desembocar en dificultar el auto sostenimiento del CSIRT.

1.1.5 Creación de un Presupuesto Preliminar de Inversión y Funcionamiento

Es un presupuesto que deberá ser ajustado de acuerdo con las validaciones que se realicen al modelo de la comunidad objetivo que atenderá. Usualmente los rubros se proyectan para un mínimo de un año y cubre los siguientes puntos:

- **Presupuesto de Inversión**: comprende todo el cuadro de adquisición de equipos que permitan asegurar el proceso productivo y ampliar la cobertura del mercado. Los principales componentes considerados para el presupuesto de Inversión son:
    - **Estudios y Diseños**: los costos incluyen las evaluaciones de riesgos y vulnerabilidades de seguridad de la información, que permitan prevenir la acción de los incidentes y crear una línea base para el desarrollo de los servicios y el monitoreo de la seguridad de la información en las entidades atendidas.
    - **Plataforma Tecnológica**: incluye el hardware y software requerido para garantizar la operación y la seguridad de la información propia del CSIRT así como la necesaria para la prestación de los servicios ofrecidos. Comprende los siguientes rubros: Hardware, Software, Servicios de Seguridad, Mantenimiento y Reparaciones, Desarrollo Web, Tecnologías de Seguridad de la Red y de la Información, Gestión de Equipos de Seguridad, Monitoreo de Equipos de Seguridad, Correlación de Equipos de Seguridad, Protección a los Sistemas.
    - **Mobiliario**.
    - **Seguros de Equipos e Infraestructura**.
- **Presupuesto de Funcionamiento**: tiene que ver con la razón principal de la entidad CSIRT. Los componentes son:
    - **Costo de Personal**: debe de diseñarse en base a la estructura organizacional del CSIRT con salarios acordes al mercado laboral y los perfiles requeridos. Los pro-

bables elementos son los siguientes: Director, Directores, Jefes de Grupo, Profesionales Certificados en Seguridad, Equipo Base, Personal Administrativo. También es importante proyectar las prestaciones de ley respectivas.

- **Reclutamiento**: asume la contratación de un tercero para el proceso de búsqueda y reclutamiento del personal del CSIRT.
- **Entrenamiento y Capacitación**: costos asociados con la preparación técnica del personal para un mejor desempeño en la operación.
- **Operación**: Costos estimados asociados a la operación diaria del CSIRT en la prestación de los servicios ofrecidos tales como: Logística para conferencias y talleres, Costos de Presentación, Suscripciones a Medios Especializados, Traducciones, Elaboración de Talleres, Publicaciones, Publicidad y Materiales Informativos, Viáticos.
- **Infraestructura**: alquiler de establecimiento, servicios públicos, mantenimiento.
- **Impuestos de Ley**: impuestos municipales, impuestos fiscales, registro de comercio, etc. Es importante detallar todos los impuestos que apliquen.
- **Costo Variable Adicional**: Auditorías de Seguridad, Configuración y Mantenimiento de la Seguridad, Análisis de Riesgos, Planificación de la continuidad de la operación y recuperación tras un desastre, Recopilación de Pruebas Forenses, Respuesta a Incidentes In Situ, Evaluación de Productos.

- **Presupuesto de Ventas de Servicios**: se estima con base en tarifas y comportamientos esperados del mercado y considerando la operación del CSIRT durante el año de operación.
  - **Venta de Servicios**: Cursos de Capacitación, Auditorías de Seguridad, Configuración y Mantenimiento de la Seguridad Informática, Análisis de Riesgos, Planificación de la Continuidad de la Operación y Recuperación tras un Desastre, Recopilación de Pruebas Forenses, Respuesta a Incidentes In Situ, Evaluación de Productos.

1.1.6 Servicios

1.1.6.1 Servicios de un CSIRT

Un CSIRT puede realizar funciones proactivas, reactivas y de investigación para ayudar a proteger y asegurar los bienes críticos de una organización o de una comunidad. No hay un grupo de funciones o servicios estándares que pueda ofrecer un CSIRT. Cada equipo elige sus servicios basados en las necesidades de su área de cobertura de servicio.

Para detallar esto se presenta la siguiente tabla:

Tabla 2: Servicios CSIRT.

Servicio	Procesos

Servicios Reactivos	• Servicio de alertas.
	• Gestión de incidentes.
	  ○ Análisis de incidentes.
	  ○ Respuesta a incidentes en sitio.
	  ○ Soporte de respuesta a incidentes.
	  ○ Coordinación de respuesta a incidentes.
	• Gestión de vulnerabilidades.
	  ○ Análisis de vulnerabilidades.
	  ○ Respuesta a vulnerabilidades.
	  ○ Coordinación de respuesta a vulnerabilidades.
	• Gestión de Artefactos (*****).
	  ○ Análisis.
	  ○ Respuesta.
	  ○ Coordinación de la respuesta.

Servicios Proactivos	• Comunicados. • Vigilancia tecnológica. • Auditorías de seguridad o evaluaciones. • Configuración y mantenimiento de seguridad, herramientas y aplicaciones e infraestructura.

	• Desarrollo de herramientas de seguridad. • Servicios de detección de intrusos. • Difusión de información relacionada con la seguridad.
Calidad de los servicios de gestión de la seguridad	• Análisis de riesgos. • Continuidad de negocio y plan de recuperación de desastres. • Consultoría de seguridad. • Sensibilización en seguridad. • Educación / Entrenamiento. • Evaluación de productos o certificación.

(*****) *Artefacto*: herramientas, programas o porciones de código utilizadas por los atacantes para lograr vulnerar la seguridad de un sistema.

Debe tener en cuenta que algunos servicios tienen tanto un aspecto reactivo como proactivo. Por ejemplo, la gestión de vulnerabilidades puede realizarse en respuesta al descubrimiento de una vulnerabilidad que está siendo activamente explotada. Pero también puede hacerse proactivamente revisando y testeando código para determinar dónde hay vulnerabilidades, por lo tanto los problemas pueden ser reparados antes de que sean ampliamente conocidos o explotados.

Algunos equipos pueden ofrecer muchos servicios de esta lista, otros pueden tener capacidad para proveer algunos pocos; aún otros equipos pueden compartir la responsabilidad de proveer estos servicios con otras partes de la organización de la que dependen, o pueden tercerizar algunos servicios para respuesta a un incidente o contratar a un proveedor de servicios de gestión de la seguridad, pero es conveniente que cuando un CSIRT está recién formado, se enfoque de manera principal en el servicio de respuesta a incidentes y algunos que puedan identificarse como necesarios y útiles para la operación del centro. A partir de proporcionar esos servicios de manera adecuada, el centro de respuesta podrá ir haciéndose presente en el ámbito de acción y generando confianza en la o las organizaciones en las que actúa y, a partir de ello, se pueden contemplar la implementación de otros servicios asociados.

El manejo de incidentes es en sí mismo es un servicio que puede incluir diversos aspectos: gestión de incidentes, atención en sitio, coordinación de equipos, cómputo forense, análisis de software malicioso, etc.

Si bien la tarea principal de un centro de respuesta a incidentes de seguridad de la información es esencialmente el manejo de incidentes, es realmente difícil que las actividades se limiten a esa tarea únicamente. Las razones para realizar actividades adicionales a la respuesta a incidentes tienen que ver con el entorno del centro de respuesta y con las necesidades que se van observando durante la operación del mismo. Sobre el primer caso, es frecuente que en la organización se observe al centro de respuesta también como una entidad de consulta y asesoría, debido a que sabe cómo solucionar problemas sobre seguridad de la información. En el segundo caso, con la operación cotidiana de un centro de respuesta a incidentes de seguridad generalmente surge la necesidad de actuar en alguna o en las otras dos fases del ciclo de la seguridad de la información: prevención y detección.

La experiencia ha demostrado que cualquiera que sean los servicios que un CSIRT elige ofrecer, la organización de la que dependen o gerencia debe asegurar que el equipo tiene los recursos necesarios (gente, experiencia técnica, equipamiento e infraestructura) para proveer un servicio valioso para los miembros de la comunidad, o el CSIRT no tendrá éxito y sus destinatarios no informarán incidentes al equipo.

Además, como hay cambios constantes en la tecnología y el uso de Internet, pueden emerger otros servicios que necesiten ser provistos por un CSIRT. Esta lista de servicios por lo tanto necesitará evolucionar y cambiar con el transcurso del tiempo.

Entre las muchas actividades adicionales que puede proporcionar un CSIRT están:

1.1.6.1.1 Emisión de boletines y alertas de seguridad

Las actividades de prevención son importantes ya que contribuyen a evitar incidentes de seguridad informática derivados del desconocimiento de nuevas amenazas. De este modo, el centro de respuesta puede emitir boletines sobre nuevas vulnerabilidades en sistemas operativos, aplicaciones, etc., y las formas de mitigar los riesgos asociados a las vulnerabilidades. Es también importante que el centro de respuesta emita boletines y alertas relacionadas con la infraestructura de seguridad que aplica a la organización, de tal forma que no se confunda a la organización con información que podría ser innecesaria. Además de boletines y alertas sobre vulnerabilidades y amenazas, el centro de respuesta también puede emitir información sobre lecciones aprendidas de incidentes ocurridos dentro de la misma organización.

1.1.6.1.2 Análisis de vulnerabilidades

El personal del centro de respuesta a incidentes también puede apoyar con actividades de análisis de vulnerabilidades dentro de la organización, colaborando con actividades de auditoría o de pentest. Generalmente dentro del centro de respuesta a incidentes se cuenta con personal capacitado para esta actividad porque son habilidades que también se requieren en el manejo de incidentes. Debe tenerse en cuenta que no puede delegarse la responsabilidad principal del análisis de vulnerabilidades al personal de manejo de incidentes ya que su tarea principal es la respuesta a incidentes.

1.1.6.1.3 Detección de incidentes

El personal del centro de respuesta a incidentes también puede colaborar en actividades de detección de incidentes. Ya que el centro de respuesta es quien cuenta con información sobre los incidentes que ocurren en la organización, es útil que su personal participe en la definición de los mecanismos y dispositivos para la detección de incidentes. Esa misma participación y colaboración en la detección puede servir para dar una perspectiva al centro de respuesta sobre las amenazas cotidianas a la seguridad de la información de la organización.

1.1.6.1.4 Difusión y capacitación

Una labor muy importante de un centro de respuesta a incidentes en materia de prevención es el desarrollo de programas de capacitación y difusión sobre seguridad de la información. Estos programas deben realizarse de forma permanente pues es la forma más efectiva de lograr que los integrantes de la organización estén conscientes de las amenazas a la seguridad de su información y la de la organización y de las medidas para mitigar los riesgos asociados a las vulnerabilidades identificadas y también para que conozcan las medidas que deben tomarse ante alguna contingencia o incidente. Muchas veces el éxito en la respuesta y en la investigación de un incidente de seguridad de la información depende de la colaboración de todos los involucrados, por lo que no debe escatimarse en los programas de difusión y capacitación ya que también es a través de ellos como se logra de manera efectiva disminuir las posibilidades de que los incidentes se repitan.

1.1.6.1.5 Implementación de mejores prácticas

Al funcionar como una referencia en materia de seguridad de la información, un centro de respuesta puede actuar como consultor de organizaciones para la implementación de mejores prácticas que ayuden a mitigar los riesgos de seguridad a los que su información está expuesta.

En general, los servicios que proporcione un centro de respuesta dependen de los objetivos para los cuales fue creado y, por tanto, de su ámbito de acción.

1.1.6.1.6 Reporte, clasificación, asignación

Dos de las cosas más importantes para un equipo de respuesta a incidentes es la forma en que se reportarán los incidentes al centro de respuesta por parte de los usuarios y cómo el personal del centro de respuesta realizará la clasificación y asignación del incidente para atenderlo de manera adecuada.

La importancia de estas acciones radica en que definen cómo se maneja un incidente de acuerdo a las circunstancias en que éste ocurre y eso establece la prioridad que se le da al mismo y, por tanto, los recursos que se destinarán para el manejo. Es por ello que para un centro de respuesta a incidentes es fundamental definir la forma en que se realizarán éstas acciones iniciales. La eficacia y eficiencia del centro de respuesta dependen en gran medida de que los reportes se reciban de forma inmediata y se recolecte la información necesaria para determinar el tipo de incidentes de que se trata. Con esa información, el personal debe clasificar el incidente de acuerdo a los procedimientos que existan para ello y transferir el manejo del mismo a la persona indicada para atender el incidente de acuerdo a su tipo y prioridad.

El reporte de los incidentes al centro de respuesta puede hacerse a través de diversos medios, entre los más comunes están:

- Vía telefónica (posiblemente establecer una línea de atención 24x7 o un 01-800)
- Direcciones de correo electrónico específicas
- Formularios web
- De forma personal

Además de implementar los mecanismos para la recepción, clasificación y asignación de reportes de incidentes, es importante contar con un sistema para el seguimiento de los reportes de incidentes, que permita consultar en todo momento el status de cada incidente, su clasificación y, en general, todos los datos asociados a los reportes.

Contar con un sistema de estas características permite contar con información sobre la operación del centro de respuesta, se pueden definir métricas para el cumplimiento de los niveles de servicio establecidos con la organización y se pueden tomar decisiones de acuerdo al desarrollo del seguimiento de cada incidente. Al final de un período de tiempo, el sistema proporcionará información estadística muy valiosa para observar el comportamiento del servicio del centro de respuesta y para observar la evolución de las necesidades de los usuarios del mismo. Hay una diversidad de sistemas de seguimiento de reportes (tracking) que pueden servir para un centro de respuesta a incidentes.

La forma de operar el proceso de reporte, clasificación y asignación de incidentes es como una mesa de ayuda, por lo que debe capacitarse a una parte o todo el personal del centro de respuesta a incidentes sobre el proceso. Si bien puede parecer trivial, no debe soslayarse la importancia de la capacitación y actualización constante en este rubro si se pretende proporcionar un servicio adecuado y homogéneo para cara reporte que el centro de respuesta reciba.

Otra manera de cubrir el proceso inicial de reporte, clasificación y asignación de incidentes de seguridad es a través de algún centro de recepción o mesa de ayuda de un tercero, otra organización que se encargue del proceso y que una vez prestada la atención inicial transfiera el control del incidente al personal especializado del centro de respuesta. Si se toma esta alternativa, es muy importante tener en cuenta que el personal de la mesa de ayuda que se contrate será, de muchas formas, quien proporcione el primer nivel de servicio del centro de respuesta y por ello debe entender no sólo el proceso de reporte, clasificación y asignación, sino incluso la misión, los servicios e incluso la estructura del centro de respuesta.

1.1.6.2 Servicios informáticos de un CSIRT

Los servicios informáticos de un CSIRT deben estar acorde a la administración de la seguridad de la organización y deben dividir sus tareas en tres grupos relevantes:

- **Autenticación**: establecer las entidades que pueden tener acceso al universo de recursos de cómputo que posee un CSIRT.

- **Autorización**: es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.
- **Auditoría**: se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Los servicios informáticos para un CSIRT, y específicamente, la definición de los sistemas informáticos necesarios para su operación deben de ser consistentes con los métodos de protección que el CSIRT posea.

A continuación se listan los métodos de protección más comúnmente empleados dentro de una estructura CSIRT.

Tabla 3: Métodos comúnmente utilizados para la protección en un CSIRT.

Método	Descripción
Sistemas de Detección de Intrusos	Permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.
Sistemas Orientados a la Conexión de Red	Monitorean las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador.
Sistemas de Análisis de Vulnerabilidades	Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La "desventaja" de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.
Sistemas de Protección de Integridad de Información	Sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger.

Sistemas de Protección a la Privacidad de la Información	Herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades.

Resumiendo, un modelo de seguridad debe de estar formado por múltiples componentes o capas que pueden ser incorporadas a la organización CSIRT según vaya madurando en la implementación y aplicación de los métodos de protección mencionados. Puntualmente se brinda un listado de aplicaciones de software que entran dentro del esquema de los distintos métodos de protección y que son elementos fundamentales para operativizar los distintos servicios informáticos que posea un CSIRT.

1.1.6.3 Estableciendo medios de comunicación seguros

Una vez que una de las partes ha decidido compartir información con otro equipo, todas las partes implicadas necesitan garantizar canales de comunicación seguros.

Los objetivos de la comunicación segura son:

- Confidencialidad: ¿Puede alguien acceder al contenido de la comunicación?
- Integridad: ¿Puede alguien manipular el contenido de la comunicación?
- Autenticidad: ¿Estoy comunicado con la persona "correcta"?

Es muy fácil de enviar falsos e-mail, y no es difícil establecer una identidad falsa por teléfono. Las técnicas criptográficas, por ejemplo, PGP (Pretty Good Privacy) pueden proporcionar formas eficaces de asegurar el correo electrónico, además con el equipo correcto, también es posible garantizar la comunicación telefónica. Pero antes de utilizar estos mecanismos, ambas partes necesitan de la infraestructura "correcta", es decir, la preparación de antemano. La preparación más importante es garantizar la autenticidad de las claves criptográficas utilizadas en la comunicación segura:

- **Claves Públicas (PGP y PEM)**: debido a que son accesibles a través de Internet, las claves públicas deben ser autenticadas antes de ser utilizadas. PGP se basa en una "Red de Confianza" (donde los usuarios registran las claves de otros usuarios) y PEM se basa en una jerarquía (donde las autoridades de certificación firman las claves de los usuarios).

- **Claves Secretas (DES y PGP / cifrado convencional)**: debido a que estos deben conocer tanto al emisor y el receptor, las claves secretas deben ser cambiadas antes de la comunicación a través de un canal seguro.

La comunicación es fundamental en todos los aspectos de respuesta a incidentes. Un equipo puede apoyar de la mejor manera el uso de las técnicas antes mencionadas, reuniendo toda la información necesaria de una manera coherente. Requisitos específicos (tales como llamar a un número específico para comprobar la autenticidad de las claves) debe quedar claro desde el principio.

No está dentro del alcance de esta sección el resolver los problemas técnicos y administrativos de las comunicaciones seguras. El punto es que los equipos de respuesta deben apoyar y utilizar un método que permita la comunicación entre ellos y sus integrantes (u otros equipos de respuesta). Cualquiera que sea el mecanismo, el nivel de protección que ofrece debe ser aceptable para la comunidad que lo utiliza.

1.1.6.4 Aplicaciones que apoyan la implementación de los servicios informáticos CSIRT

1.1.6.4.1 Sistema de Seguimiento de Incidentes

Denominado en inglés como issue tracking system, trouble ticket system o incident ticket system. Es un paquete de software que administra y mantiene listas de incidentes, conforme son requeridos. Los sistemas de este tipo son comúnmente usados en la central de llamadas de servicio al cliente de una organización para crear, actualizar y resolver incidentes reportados por usuarios, o inclusive incidentes reportados por otros empleados de la organización. Un sistema de seguimiento de incidencias también contiene una base de conocimiento que contiene información de cada cliente, soluciones a problemas comunes y otros datos relacionados. Un sistema de reportes de incidencias es similar a un Sistema de seguimiento de errores (bugtracker) y, en algunas ocasiones, una compañía de software puede tener ambos, y algunos bugtrackers pueden ser usados como un sistema de seguimiento de incidentes, y viceversa.

1.1.6.4.2 Correo Electrónico Seguro

El empleo de certificados personales de empresa le ayudará a asegurar sus comunicaciones a través del correo electrónico. Por un lado podrá firmar sus mensajes desde los clientes de correo de mayor uso en la actualidad, garantizando de esta manera su autenticidad (que el emisor del

mensaje es quien dice ser), integridad (que el contenido del mensaje no ha sido alterado) y no repudio (que no se podrá negar la autoría del mensaje). El proceso de firma de un e-mail se basa en la criptografía de clave pública o asimétrica y puede resumirse de la siguiente forma: el emisor creará un resumen a partir del propio mensaje (hash) y lo cifrará con su clave privada, este resumen será enviado junto con el mensaje original al receptor, el cual, al recibirlo, descifrará el hash recibido al tiempo que creará un nuevo resumen del mensaje que le llega. Si al comparar ambos hash éstos son idénticos la firma será válida. Este proceso, que en la teoría resulta algo complejo, se hace totalmente transparente al usuario a través de las aplicaciones de gestión de correo. Por otro lado, de manera alternativa o complementaria a la firma de un documento, a través de un certificado personal de empresa podremos cifrar el contenido de un mensaje, garantizando de esta manera la confidencialidad del mismo, ya que sólo el receptor del mensaje encriptado podrá desencriptarlo. El procedimiento de cifrado es inverso al de firma: el emisor cifrará el mensaje con la clave pública del receptor, por lo que éste será el único que podrá descifrarlo usando su clave privada (que sólo él conoce).

1.1.6.4.3 Sistemas de Comunicaciones Seguras

Existen varios sistemas de comunicaciones seguras en el mercado. Es importante saber qué tipo de seguridad brinda y es por ello que se brinda un listado que describe las características más importantes de cada uno:

- ✓ **SSH** (Secure Shell), stelnet: SSH y stelnet son programas que permite efectuar conexiones con sistemas remotos y mantener una conexión cifrada. Con esto evitamos, entre otras cosas, que las claves circulen por la red sin cifrar.
- ✓ **Cryptographic IP Encapsulation** (CIPE): CIPE cifra los datos a nivel de red. El viaje de los paquetes entre hosts se hace cifrado. A diferencia de SSH que cifra los datos por conexión, lo hace a nivel de socket. Así como una conexión lógica entre programas que se ejecutan en hosts diferentes, está cifrada. CIPE se puede usar en tunnelling para crear una Red Virtual Privada (VPN – Virtual Private Network). El cifrado a bajo nivel tiene la ventaja de poder hacer trabajar la red de forma transparente entre las dos redes conectadas en la RPV sin ningún cambio en el software de aplicación.
- ✓ **SSL**: o Secure Sockets Layer, proporciona los siguientes servicios:
  - Cifrado de datos: la información transferida, aunque caiga en manos de un atacante, será indescifrable, garantizando así la confidencialidad.

- Autenticación de servidores: el usuario puede asegurarse de la identidad del servidor al que se conecta y al que posiblemente envíe información personal confidencial.
- Integridad de mensajes: impide que modificaciones intencionadas o accidentales en la información pasen inadvertidas cuando viaja por el Internet.
- Opcionalmente, autenticación de cliente: permite al servidor conocer la identidad del usuario, con el fin de decidir si puede acceder a ciertas áreas protegidas.

1.1.6.4.4 Firewall

Es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Pueden ser implementados en hardware o software, o una combinación de ambos. Se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través de el, examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

1.1.6.4.5 Wrappers

Un Wrapper es un programa que controla el acceso a un segundo programa. El Wrapper literalmente cubre la identidad de este segundo programa, obteniendo con esto un más alto nivel de seguridad. Los Wrappers son usados dentro de la seguridad en sistemas UNIXs. Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento.

Los Wrappers son ampliamente utilizados, y han llegado a formar parte de herramientas de seguridad por las siguientes razones:

- ✓ Debido a que la seguridad lógica está concentrada en un solo programa, los Wrappers son fáciles y simples de validar.
- ✓ Debido a que el programa protegido se mantiene como una entidad separada, éste puede ser actualizado sin necesidad de cambiar el Wrapper.
- ✓ Debido a que los Wrappers llaman al programa protegido mediante llamadas estándar al sistema, se puede usar un solo Wrapper para controlar el acceso a diversos programas que se necesiten proteger.
- ✓ Permite un control de accesos exhaustivo de los servicios de comunicaciones, además de buena capacidad de Logs y auditorías de peticiones a dichos servicios, ya sean autorizados o no.

1.1.6.4.6 Listas de Control de Acceso

Las Listas de Control de Accesos (ACL) proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se les permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

1.1.6.4.7 HoneyPot

Es el software o conjunto de computadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los Honeypots pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al honeypot.

Algunos honeypots son programas que se limitan a simular sistemas operativos no existentes en la realidad y se les conoce como honeypots de baja interacción y son usados fundamentalmente como medida de seguridad. Otros sin embargo trabajan sobre sistemas operativos reales y son capaces de reunir mucha más información; sus fines suelen ser de investigación y se los conoce como honeypots de alta interacción.

Un tipo especial de honeypot de baja interacción son los sticky honeypots (honeypots pegajosos) cuya misión fundamental es la de reducir la velocidad de los ataques automatizados y los rastreos.

En el grupo de los honeypots de alta interacción nos encontramos también con los honeynet.

También se llama honeypot a un website o sala de Chat, que se ha creado para descubrir a otro tipo de usuarios con intenciones criminales.

1.1.6.4.8 Sistemas de Detección de Intrusos

Un sistema de detección de intrusos (IDS) es un componente más dentro del modelo de seguridad de una organización. Consiste en detectar actividades inapropiadas, incorrectas o anómalas desde el exterior–interior de un sistema informático.

Los sistemas de detección de intrusos pueden clasificarse, según su función y comportamiento en:

- ✓ Host–Based IDS: operan en un host para detectar actividad maliciosa en el mismo.
- ✓ Network–Based IDS: operan sobre los flujos de información intercambiados en una red.
- ✓ Knowledge–Based IDS: sistemas basados en Conocimiento.
- ✓ Behavior–Based IDS: sistemas basados en Comportamiento. Se asume que una intrusión puede ser detectada observando una desviación respecto del comportamiento normal o esperado de un usuario en el sistema.

La idea central de este tipo de detección es el hecho de que la actividad intrusiva es un conjunto de actividades anómalas. Si alguien consigue entrar de forma ilegal al sistema, no actuará como un usuario comprometido; su comportamiento se alejará del de un usuario normal.

Sin embargo en la mayoría de las ocasiones una actividad intrusiva resulta del agregado de otras actividades individuales que por sí solas no constituyen un comportamiento intrusivo de ningún tipo. Así las intrusiones pueden clasificarse en:

- ✓ **Intrusivas pero no anómalas**: denominados Falsos Negativos (el sistema erróneamente indica ausencia de intrusión). En este caso la actividad es intrusiva pero como no es anómala no es detectada. No son deseables, porque dan una falsa sensación de seguridad del sistema.

- ✓ **No intrusivas pero anómalas**: denominados Falsos Positivos (el sistema erróneamente indica la existencia de intrusión). En este caso la actividad es no intrusiva, pero como es anómala el sistema "decide" que es intrusiva. Deben intentar minimizarse, ya que en caso contrario se ignorarán los avisos del sistema, incluso cuando sean acertados.
- ✓ **No intrusiva ni anómala**: son Negativos Verdaderos, la actividad es no intrusiva y se indica como tal.
- ✓ **Intrusiva y anómala**: se denominan Positivos Verdaderos, la actividad es intrusiva y es detectada.

Los detectores de intrusiones anómalas requieren mucho gasto computacional, ya que se siguen normalmente varias métricas para determinar cuánto se aleja el usuario de lo que se considera comportamiento normal.

1.1.6.4.9 Call Back

Este procedimiento es utilizado para verificar la autenticidad de una llamada vía Modem. El usuario llama, se autentifica contra el sistema, se desconecta y luego el servidor se conecta al número que en teoría pertenece al usuario. La ventaja reside en que si un intruso desea hacerse pasar por el usuario, la llamada se devolverá al usuario legal y no al del intruso, siendo este desconectado. Como precaución adicional, el usuario deberá verificar que la llamada (retorno) proceda del número a donde llamó previamente.

1.1.6.4.10 Gestor de Contraseñas

Es un programa que se utiliza para almacenar una gran cantidad de parejas usuario/contraseña. La base de datos donde se guarda esta información está cifrada mediante una única clave (contraseña maestra o en inglés master password), de forma que el usuario sólo tenga que memorizar una clave para acceder a todas las demás. Esto facilita la administración de contraseñas y fomenta que los usuarios escojan claves complejas sin miedo a no ser capaces de recordarlas posteriormente.

1.1.6.4.11 Anti Sniffers

Esta técnica consiste en detectar Sniffers en el sistema. Generalmente estos programas se basan en verificar el estado de la tarjeta de red, para detectar el modo en el cual está actuando (recordar que un Sniffer la coloca en Modo Promiscuo) y el tráfico de datos en ella.

1.1.6.4.12 Herramientas Criptográficas

A continuación varios conceptos:

- **Criptografía**, palabra que etimológicamente proviene del griego Kriptos (Oculto) y Grafo (Escritura) y significa "arte de escribir con clave secreta o de un modo enigmático". Hace varios años dejó de ser un arte para convertirse en una técnica (o conjunto de ellas) que trata sobre la protección (ocultamiento ante personas no autorizadas) de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, Matemática Discreta, Teoría de los Grandes Números y la Complejidad Algorítmica. Es decir, la Criptografía es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es (mediante claves que sólo el emisor y el destinatario conocen), para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo. El mensaje cifrado recibe el nombre de Criptograma.
- **Criptoanálisis**: es el arte de estudiar los mensajes ilegibles, encriptados, para transformarlos en legibles sin conocer la clave, aunque el método de cifrado empleado siempre es conocido.
- **Criptosistema**: todo Criptosistema cumple la condición DK(EK(m)) = m es decir, que si se tiene un mensaje m, se cifra empleando la clave K y luego se descifra empleando la misma clave, se obtiene el mensaje original m. Existen dos tipos fundamentales de Criptosistemas utilizados para cifrar datos e información digital y ser enviados posteriormente por medios de transmisión libre.
    - **Simétricos o de clave privada**: se emplea la misma clave K para cifrar y descifrar, por lo tanto el emisor y el receptor deben poseer la clave. El mayor inconveniente que presentan es que se debe contar con un canal seguro para la transmisión de dicha clave.
    - **Asimétricos o de llave pública**: se emplea una doble clave conocidas como Kp (clave privada) y KP (clave Pública). Una de ellas es utilizada para

la transformación E de cifrado y la otra para el descifrado D. En muchos de los sistemas existentes estas clave son intercambiables, es decir que si empleamos una para cifrar se utiliza la otra para descifrar y viceversa.

- Entre los algoritmos utilizados se encuentran: Transposición, Cifrados Monoalfabéticos (Algoritmo de César y Sustitución General).

- **Algoritmos Simétricos**: La mayoría de los algoritmos simétricos actuales se apoyan en los conceptos de Confusión y Difusión, estos métodos consisten en ocultar la relación entre el texto plano, el texto cifrado y la clave (Confusión); y repartir la influencia de cada bit del mensaje original lo más posible entre el mensaje cifrado (Difusión). A continuación se listan algunos algoritmos:, Triple DES, Blowfish, RC5, IDEA, Rijndael (AES).

- **Algoritmos Asimétricos** (Llave Privada / Llave Pública): Su principal característica es que no se basa en una única clave sino en un par de ellas: una conocida (Pública) y otra Privada. Actualmente existen muchos algoritmos de este tipo pero han demostrado ser poco utilizables en la práctica ya sea por la longitud de las clave, la longitud del texto encriptado generado o su velocidad de cifrado extremadamente largos, un tipo de algoritmo asimétricos se presentan a continuación:

  - **RSA**: es el más empleado en la actualidad, sencillo de comprender e implementar, aunque la longitud de sus claves es bastante considerable (ha pasado desde sus 200 bits originales a 2048 actualmente).

  - **Curvas Elípticas (CEE):** la eficiencia de este algoritmo radica en la longitud reducida de las claves, lo cual permite su implementación en sistemas de bajos recursos como teléfonos celulares y Smart Cards.

- **Autentificación:** Se entiende por Autentificación cualquier método que permita garantizar alguna característica sobre un objeto dado.

  - **Firmas Digitales:** una firma digital se logra mediante una función Hash de resumen. Esta función se encarga de obtener una “muestra única” del mensaje original. Dicha muestra es más pequeña y es muy difícil encontrar otro mensaje que tenga la misma firma. Las funciones Hash están basadas en que un mensaje de longitud arbitraria se transforma en un mensaje de longitud constante dividiendo el mensaje en partes iguales, aplicando la función de transformación a cada parte y

sumando todos los resultados obtenidos. Actualmente se recomienda utilizar firmas de al menos 128 bits (38 dígitos) siendo 160 bits (48 dígitos) el valor más utilizado.

- **MD5:** el Message Diggest 5 procesa los mensajes de entrada en bloques de 512, y produce una salida de 128 bits.
- **SHA –** 2; tamaño de salida 512 bits

- **PGP** (Pretty Good Privacy): es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales. Utilizado correctamente, PGP puede proporcionar un gran nivel de seguridad. A diferencia de protocolos de seguridad como SSL, que sólo protege los datos en tránsito (es decir, mientras se transmiten a través de la red), PGP también puede utilizarse para proteger datos almacenados en discos, copias de seguridad, etc., PGP usa una función de 4 claves.
- **Estenografía**: consiste en ocultar en el interior de información aparentemente inocua, otro tipo de información (cifrada o no). El texto se envía como texto plano, pero entremezclado con mucha cantidad de "basura" que sirve de camuflaje al mensaje enviado. El método de recuperación y lectura sólo es conocido por el destinatario del mensaje y se conoce como "separar el grano de la paja". Los mensajes suelen ir ocultos entre archivos de sonido o imágenes y ser enormemente grandes por la cantidad extra de información enviada (a comparación del mensaje original).

1.1.6.4.13 Aplicaciones de aseguramiento de protocolos y servicios

Cuando se implementan aplicaciones informáticas se instalan servicios que están asociados a protocolos que permiten su funcionalidad bajo un ambiente determinado. Cada uno de los protocolos y servicios tienen su debilidad ya sea en su implementación o en su uso.

Ya que es necesaria la conectividad entre equipos, se ha de ofrecer los mínimos servicios necesarios para que todo funcione correctamente; esto choca frontalmente con las políticas de la mayoría de fabricantes y empresas, que por defecto mantienen la mayoría de servicios abiertos al instalar un equipo nuevo: es responsabilidad del administrador preocuparse de cerrar los que no sean estrictamente necesarios.

A continuación se brinda un listado de los protocolos y servicios comunes dentro de la implementación de una red informática: NetBIOS, ICMP, FINGER, POP, NTP, TFTP, SMTP, Servidores Web.

1.1.6.4.14 Otros Protocolos de Seguridad

- **SSH** (Secure Shell, en español: intérprete de órdenes segura): es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo. Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.
- **S/MIME:** El protocolo MIME Seguro fue propuesto por la empresa RSA y después de su aparición fue propuesto como estándar por la IETF pero por problemas de derechos y restricciones de patentes no pudo ser posible. Utiliza técnicas similares a PGP e incorpora certificados X.509. Aunque no cuente con el apoyo necesario para ser considerado un estándar, está implementado en muchos programas de correo electrónico. Tiene la ventaja sobre PGP, que al utilizar Autoridades de Certificación, es ideal para ser utilizado por empresas y para el comercio electrónico.
- **SOCKS**: En sus orígenes este protocolo fue aprobado por el IETF como un estándar para la autentificación ante un Firewalls. Actualmente, y combinado con SSL provee las bases para construir redes privadas virtuales (RPV) altamente seguras. Socks permite la conexión de equipos situados tras un Firewall. Inicialmente fue pensado para permitir el acceso desde una red interna a servicios disponibles en el exterior, sin embargo puede emplearse en sentido contrario, para el acceso desde el exterior de la organización (protegida con un Firewall). La conexión es validada por el sistema de autentificación y después el servidor Socks actúa de intermediario con la aplicación situada en el servidor destino. Socks actúa de “envoltura” sobre el protocolo UDP–TCP permitiendo que los equipos protegidos por el Firewall puedan conectarse a una red in-

segura, utilizando su propia dirección y devolviendo los resultados al cliente. Debe notarse que Socks sólo autentifica las conexiones pero no produce ningún tipo de cifrado de los datos por lo que se hace necesario combinarlo con algún algoritmo que si lo haga (SSH, SSL, PPTP, IPSec, etc.)

- **Kerberos**: es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura. Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro. Los mensajes de autenticación están protegidos para evitar escuchar secretamente (eavesdropping) y ataques de Replay (Ataques de Reinyección). Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza. Además, existen extensiones del protocolo para poder utilizar criptografía de clave asimétrica.

1.1.6.4.15 Redes Privadas Virtuales (RPV o VPN)

La tecnología de Redes Privadas Virtuales proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privado a través de una red insegura. Es decir que la red pública sólo proporciona la infraestructura para enviar los datos.

El objetivo fundamental de una VPN es proteger los datos durante la transmisión a través de la red, permitiendo el uso de redes públicas como si fueran privadas (virtualmente privadas). Esta protección previene el mal uso, modificación, uso no autorizado e interrupciones de acceso a la información mientras atraviesa los distintos segmentos de la red (o redes).

Una VPN no protege la información mientras está alojada en el origen, o cuando llega y se aloja en su destino. También puede dejar expuesto los datos durante alguno de los procesos de encriptación en la red (redes internas antes de la encriptación o redes externas después de la desencriptación). Una VPN solo protege los aspectos de protección en la comunicación, no protege la información alojada en el disco o impresa en pantalla.

1.1.6.4.16 Software Antivirus

Los antivirus nacieron como una herramienta simple cuyo objetivo fuera detectar y eliminar virus informáticos, con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, los antivirus han evolucionado hacia programas más avanzados que no sólo buscan

detectar un Virus informático, sino bloquear, desinfectar y prevenir una infección de los mismos, así como actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, etc.

El funcionamiento de un antivirus varía de uno a otro, aunque su comportamiento normal se basa en contar con una lista de virus conocidos y su formas de reconocerlos (las llamadas firmas o vacunas), y analizar contra esa lista los archivos almacenados o transmitidos desde y hacia un ordenador.

Adicionalmente, muchos de los antivirus actuales han incorporado funciones de detección proactiva, que no se basan en una lista de malware conocido, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuáles son potencialmente dañinas para el computador, con técnicas como Heurística, HIPS, etc.

Usualmente, un antivirus tiene un (o varios) componente residente en memoria que se encargan de analizar y verificar todos los archivos abiertos, creados, modificados, ejecutados y transmitidos en tiempo real, es decir, mientras el ordenador está en uso.

Asimismo, cuentan con un componente de análisis bajo demanda (los conocidos scanners, exploradores, etc.), y módulos de protección de correo electrónico, Internet, etc.

El objetivo primordial de cualquier antivirus actual es detectar la mayor cantidad de amenazas informáticas que puedan afectar un computador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección. Actualmente hay una gran mayoría de

antivirus pero no todos se asemejan al pretendido por todos, un antivirus eficaz en todos los sentidos.

1.1.6.4.17 Herramientas de análisis Forense

En la actualidad existen varias herramientas que sirven para realizar análisis forense informático sobre:

- Recuperación de evidencias en Discos Duros.
- Recuperación de contraseñas.
- Detección y recuperación de Virus, Troyanos y Spyware.
- Seguridad en el correo electrónico (Hoax).

- Análisis de redes P2P.
- Móviles y tarjetas SIM.
- Procesos en el computador del usuario.
- Anonimato.
- Investigación de información.

1.1.6.4.18 Voz sobre IP (VoIP)

Voz sobre Protocolo de Internet, también llamado Voz sobre IP, VozIP, VoIP (por sus siglas en inglés), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol). Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla (en forma digital o analógica) a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada).

Los Protocolos que son usados para llevar las señales de voz sobre la red IP son comúnmente referidos como protocolos de Voz sobre IP o protocolos IP. El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo redes de área local (LAN).

Es muy importante diferenciar entre Voz sobre IP (VoIP) y Telefonía sobre IP:

- VoIP es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite la transmisión de la voz sobre el protocolo IP.
- Telefonía sobre IP es el conjunto de nuevas funcionalidades de la telefonía, es decir, en lo que se convierte la telefonía tradicional debido a los servicios que finalmente se pueden llegar a ofrecer gracias a poder portar la voz sobre el protocolo IP en redes de datos.

1.2. Recomendaciones para la posible inserción del CSIRT en la organización y sus posibles modelos de relación

A continuación se dará una visión de qué tipo de estructura organizacional puede adoptar un CSIRT (debe de ser pertinente respecto a las servicios que brinda) así como de los posibles mapas relacionales con su organización.

Es muy importante tener claro los siguientes puntos:

- Crear la misión y visión
- Definir el segmento que se atenderá. (Comunidad)
- Canales de comunicación dentro de la organización y su dominio
- Seleccionar un modelo organizacional y servicios.
- Estructura dentro de la Organización: políticas, procesos y procedimientos

1.2.1 Modelos organizacionales para un CSIRT

Debe elegirse qué modelo organizacional se va a implementar. Dependiendo de la elección existe una sinergia natural de los servicios que se brindarán.

Obviamente el modelo que cada equipo tome en sus inicios podrá ser menor en alcance y cantidad, pero, dependiendo de la experiencia y madurez del equipo estos se podrán ir incrementando según sea la estrategia adoptada.

Los diferentes modelos existentes son:

- Equipo de Seguridad
- Equipo de Respuesta a Incidentes Centralizado
- Equipo de Respuesta a Incidentes Distribuido
- Equipo Coordinador

Nota: Información Completa de los diferentes modelos organizacionales se describe en el capítulo dos.

1.2.1.1 Tipos de estructuras organizacionales

Dentro de los distintos tipos de estructuras organizacionales definidos por los expertos se presentan a continuación los tipos que a criterio encajan para una organización CSIRT.

1.2.1.1.1 Modelo Funcional

Las actividades se agrupan por funciones comunes desde la base hasta la cima de la organización. Consolida el conocimiento y las habilidades humanas de actividades específicas con el fin de proporcionar una pericia o experiencia de mayor profundidad.

Es más efectiva cuando:

- Es necesaria una alta experiencia para lograr los objetivos organizativos.
- La organización necesita ser controlada y coordinada por medio de la jerarquía vertical.
- La eficiencia es importante.
- No se requiere mucha coordinación horizontal.

Estructura funcional con enlaces horizontales: para hacer frente a los retos actuales, las organizaciones complementan la jerarquía funcional vertical con vínculos horizontales.

Figura 1: Modelo de Organigrama Funcional.

Tabla 4: Fortalezas y Debilidades del Modelo Funcional.

MODELO FUNCIONAL	
FORTALEZAS	**DEBILIDADES**
• Permite economías de escala en los departamentos funcionales. • Permite el desarrollo de habilidades en profundidad. • Permite que la organización alcance sus objetivos funcionales. • Es mejor con uno o unos cuantos productos.	• Respuesta lenta a los cambios del entorno. • Puede hacer que las decisiones se acumulen en la parte superior, con sobrecarga de la jerarquía. • Conduce a una mala coordinación horizontal entre departamentos.

	• Da lugar a una menor innovación. • Implica un punto de vista limitado de las metas organizacionales.

1.2.1.1.2 Modelo Basado en el Producto

Se organiza de acuerdo a lo que se produce ya sean bienes o servicios; esta forma de organización es empleada en las grandes compañías donde cada unidad que maneja un producto se le denomina “divisiones” estos poseen subunidades necesarias para su operación.

Figura 2: Modelo de Organigrama basado en el Producto.

Tabla 5: Fortalezas y Debilidades del Modelo basado en el Producto.

MODELO BASADO EN EL PRODUCTO	
FORTALEZAS	**DEBILIDADES**
• Descentraliza la toma de decisiones. • Se utiliza en organizaciones grandes. • Rápida adaptación de unidades de trabajo.	• Reduce la oportunidad de utilizar equipo o personal especializado. • Entorpece la estandarización. • Coordinación deficiente entre líneas del producto.

• Permite que los problemas de coordinación e integración sean detectados lo más pronto posible y se les de una solución rápida. • Altamente recomendada para la implementación de cambios rápidos. • Se logra aislar los problemas concernientes a un producto respecto a los demás y evita que interfieran los problemas de una función con todos los productos. • Permite el empleo de equipo especializado para el manejo de materiales, así como de sistemas especializados de comunicaciones. • Satisfacción del Cliente.	• Se entorpece la comunicación entre especialistas, ya que ahora presentan sus servicios en diferentes unidades. • Los empleados de la organización se dividen en grupos y se encarga de la producción de un producto especifico, además cada grupo tiene un especialista para cada función y un gerente que es el responsable de supervisar el proceso que se lleva a cabo para la obtención del producto o servicio y además envía un reporte al director general de la organización acerca de la evolución de este proceso, este director general es el responsable de supervisar que cada gerente realice de forma adecuada su trabajo y fija las metas de la organización.

1.2.1.1.3 Basada en los clientes

El tipo particular de clientes que una organización busca alcanzar, puede también ser utilizada para agrupar empleados. La base de esta departamentalización está en el supuesto de que los clientes en cada conjunto tienen problemas y necesidades comunes que pueden ser resueltos teniendo especialistas departamentales para cada uno.

Aquí el cliente es el eje central, la organización se adapta y se subdivide agrupándose el personal para cumplir las funciones necesarias para satisfacer las necesidades de cada tipo de cliente.

Tabla 6: Fortalezas y Debilidades del Modelo basado en el Cliente.

MODELO BASADO EN EL CLIENTE	
FORTALEZAS	**DEBILIDADES**

• Mejora la adaptación a las necesidades del cliente. • Descentralización del proceso de decisión. • Mejor estandarización de productos. • Satisfacción del Cliente. • Gestión de nichos de negocio de la organización.	• Dificultad de coordinación con los departamentos organizados sobre otras bases, con una constante presión de los gerentes solicitando excepciones y tratamiento especial. • En ciertas ocasiones pueden reducirse o incrementarse ciertos tipos de clientes, ya sea por recesiones económicas donde los comercios minoristas tienden a disminuir y por el contrario se incrementan los muy pequeños negocios, esto requiere más vendedores pero disminuye el grado de eficiencia de los mismos.

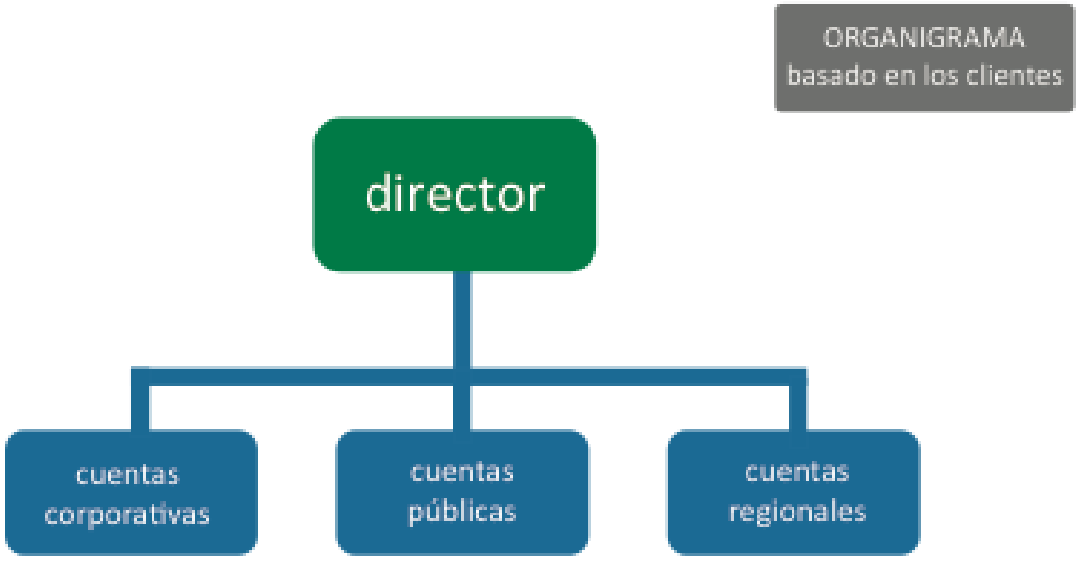


Figura 3: Modelo de Organigrama basado en el Cliente.

1.2.1.1.4 Híbrida

Esta estructura, reúne algunas de las características importantes de las estructuras anteriormente expuestas, la estructura de una organización puede ser de enfoque múltiple, ya que utiliza al mismo tiempo criterios de productos y función o producto y geografía.

Este tipo de estructuración es utilizada mayormente cuando las empresas crecen y tienen varios productos o mercados, es característico que las funciones principales para cada producto o mercado se descentralicen y se organicen en unidades específicas, además algunas funciones también se centralizan y localizan en oficinas centrales cuya función es relativamente estable y requiere economías de escala y especialización profunda. Cuando se combinan características de las estructuras funcionales y divisionales, las organizaciones pueden aprovechar las fortalezas de cada una y evitar alguna de sus debilidades.

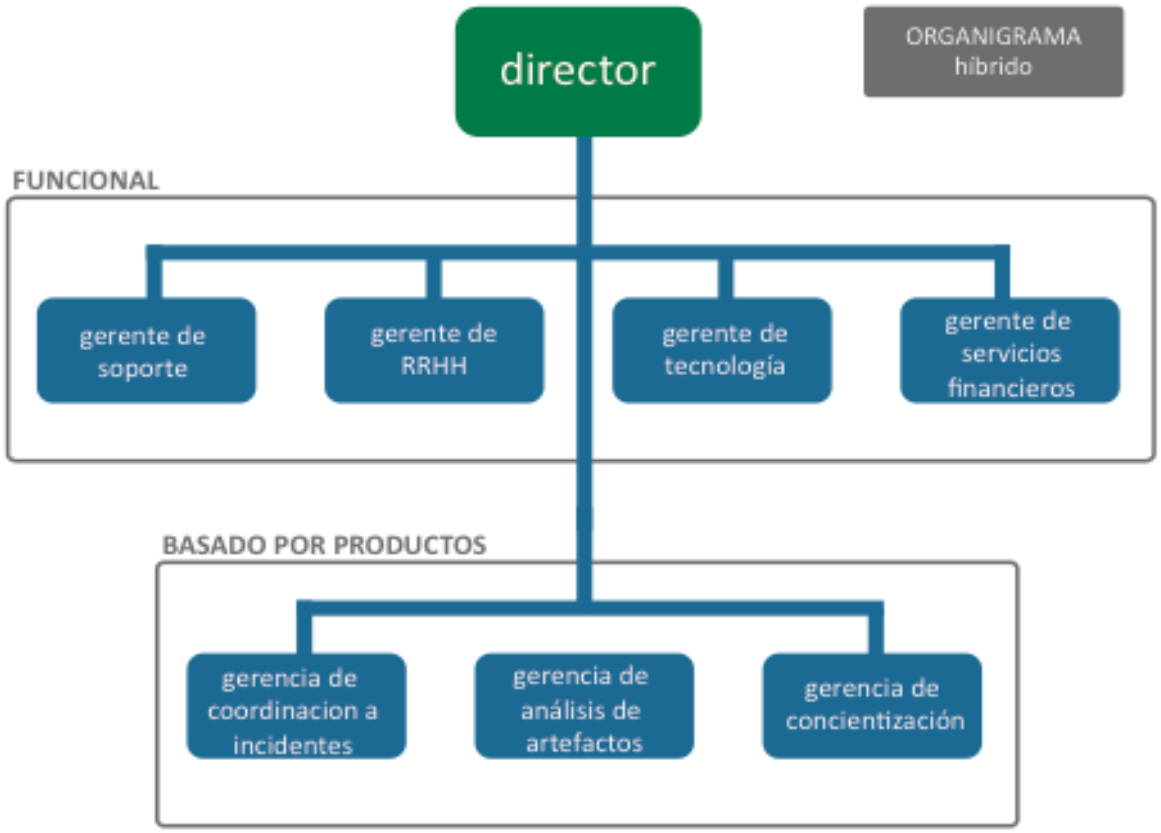


Figura 4: Modelo de Organigrama Híbrido

Tabla 7: Fortalezas y Debilidades del Modelo Híbrido.

MODELO HÍBRIDO	
FORTALEZAS	**DEBILIDADES**

• Coordinación entre y dentro de las líneas del producto. • Coincidencia de objetivos entre las divisiones y la central. • Eficiencia en los departamentos centralizados. • Adaptabilidad, coordinación en las divisiones.	• Se crean conflictos entre el personal corporativo y el divisional. • Altos costos Administrativos.

1.2.1.1.5 Matricial

Existen condiciones para la estructura matricial:

- ✓ Existe presión para compartir recursos escasos entre las líneas de producto.
- ✓ Existe presión ambiental con relación a dos o más resultados cruciales.
- ✓ El entorno de la organización es complejo e incierto. (Frecuentes cambios externos y alta interdependencia departamental. Alta necesidad de coordinación y procesamiento de información.)

La estructura formaliza los equipos horizontales junto con la tradicional jerarquía vertical. La estructura matricial es mejor cuando:

- ✓ La incertidumbre del entorno es alta.
- ✓ Los objetivos reflejan un requerimiento doble, como metas de producto y funcionales.
- ✓ Funciona mejor en organizaciones de tamaño mediano con pocas líneas de productos.

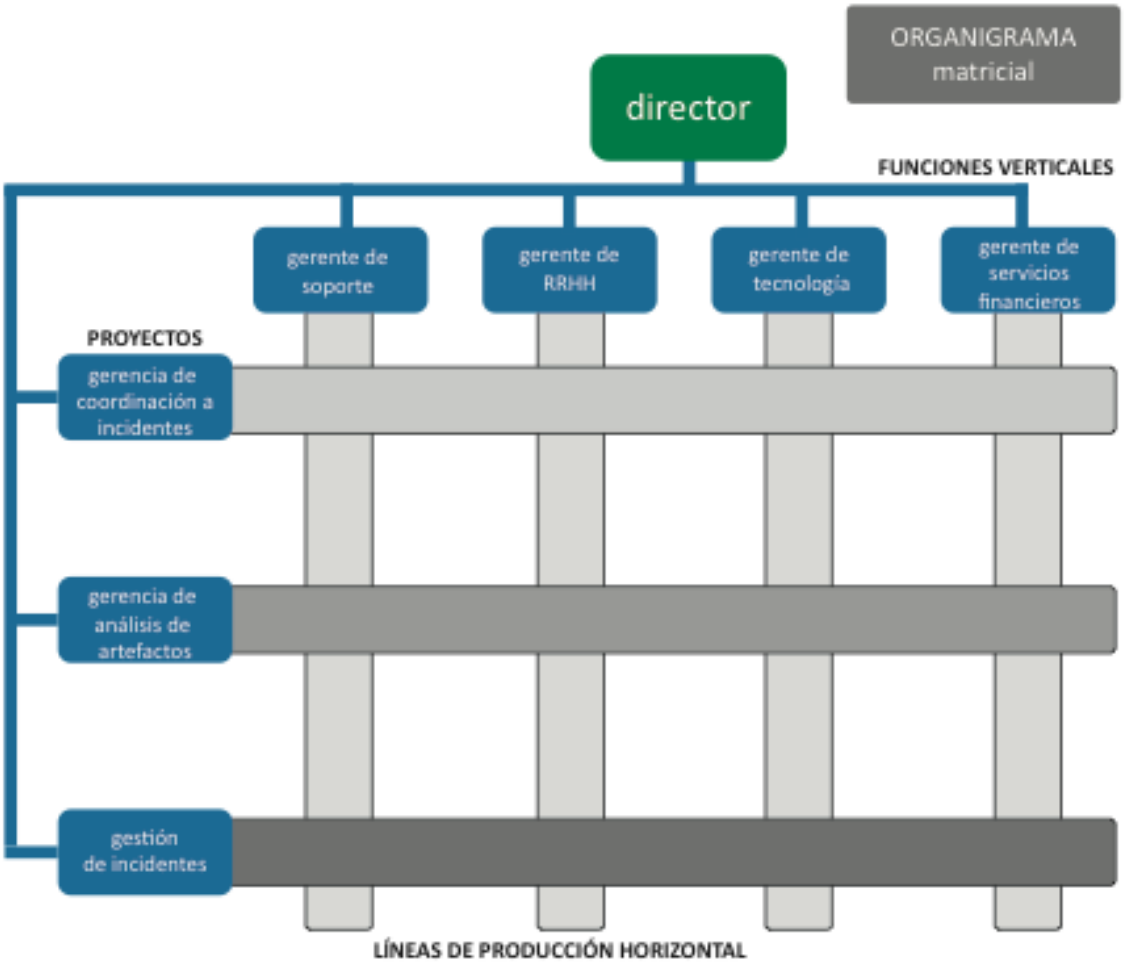


Figura 5: Modelo de Organigrama Matricial.

Tabla 8: Fortalezas y Debilidades del Modelo Matricial.

MODELO MATRICIAL	
FORTALEZAS	**DEBILIDADES**

• Logra la coordinación necesaria para satisfacer las demandas duales de los clientes. • Comparte flexiblemente los recursos humanos entre productos. • Adaptada para decisiones complejas y cambios frecuentes en un entorno inestable. • Proporciona oportunidades para el desarrollo de habilidades tanto funcionales como en productos. • Es más adecuada en organizaciones de tamaño mediano con productos múltiples. • Recursos Humanos compartidos.	• Somete a los participantes a la experiencia de una autoridad dual; esto puede ser frustrante y ocasionar confusión. • Implica que los participantes necesitan buenas habilidades interpersonales y mucha capacitación. • Consume tiempo; implica frecuentes reuniones y sesiones para la solución de conflictos. • No funcionará a menos que los participantes entiendan y adopten relaciones colegiadas en lugar de tipo vertical. • Requiere grandes esfuerzos para mantener el equilibrio de poder.

1.2.2 Políticas de Seguridad Informática

La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Estos riesgos que se enfrentan han llevado a que muchas empresas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

Las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la institución crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

1.2.2.1 Definición

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de lo que deseamos proteger y el porqué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios.

Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso limitaciones de los recursos y servicios informáticos.

1.2.2.2 Elementos

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la organización para lograr una visión conjunta de lo que se considera importante. Las políticas de seguridad informática deben considerar principalmente los siguientes elementos:

Tabla 9: Características que conforman una política.

Característica	Descripción
Alcance	Alcance de la política, incluyendo facilidades, sistemas y personal sobre la cual aplica.
Objetivo(s)	Objetivos de la política y descripción clara de los elementos involucrados en su definición.
Identificación de Roles	Las partes involucradas en la política deben de ser claramente identificados.
Responsabilidad	Deberes y responsabilidades de las partes identificadas deben de ser definidos.

Interacción	Describe la interacción apropiada entre las partes identificadas dentro de la política.
Procedimientos	Procedimientos esenciales pueden ser llamados, pero no deben ser explicados en detalle dentro de la política.
Relaciones	Identifica las relaciones entre la política, servicios y otras políticas existentes.
Mantenimiento	Describe las responsabilidades y guías para el mantenimiento y actualización de la política.
Sanciones	Definición de violaciones y sanciones por no cumplir con las políticas.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

1.2.2.3 Parámetros para su establecimiento

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- ✓ Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la organización.

- ✓ Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- ✓ Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos, bienes, y sus elementos de seguridad.
- ✓ Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos de su área.
- ✓ Monitorear periódicamente los procedimientos y operaciones de la organización, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- ✓ Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

1.2.2.4 Razones que impiden su aplicación

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

1.2.2.5 Políticas recomendadas

A continuación se listan las siguientes Políticas:

Tabla 10: Políticas recomendadas para la implementación de un CSIRT

Política	**Contenido Recomendado**
Política de Seguridad: son las directrices y objetivos generales de una organización relativos a la seguridad, expresados formalmente por la dirección general. Las políticas de seguridad deben de contemplar seis ele-	• Alcances. (facilidades, sistemas y personas.) • Objetivos. • Descripción de los elementos involucrados. • Responsabilidades.

mentos claves en la seguridad: disponibilidad, utilidad, integridad, autenticidad, confidencialidad y posesión.	• Requerimientos mínimos de seguridad en la configuración de los distintos sistemas. • Responsabilidades de los usuarios con respecto a la información a la que tienen acceso.
Política de Clasificación de Información: es la definición de los criterios de clasificación y acceso a la información.	• Introducción / Descripción. • Control de Acceso. • Identificación / Clasificación. • Interacciones de Terceros. • Destrucción y Disposición. • Seguridad Física. • Consideraciones especiales (información secreta).
Política Externa para el acceso de la Información: clasificación de criterios de acceso de entes externas a la organización para la utilización de la información que genera la organización.	• Definición de Accesos y Procesos apropiados para el acceso a la información. • Expedientes requeridos para el acceso. • Elaboración de informe para el acceso.
Política para la clasificación de los Datos: establecer cómo se clasificarán los datos dentro de la organización según los usuarios o entidades que la consuman.	• Introducción / Descripción. • Control de acceso. • Identificación / Clasificación. • Interacciones de Terceros. • Destrucción y Disposición. • Seguridad Física. • Consideraciones especiales (información secreta).
Política de Aislamiento de la Información: explica las clases de información que se pueden recopilar, su naturaleza y criterios de uso de la misma. Plasma excepciones de secreto sobre algunas de ellas.	• Descripción y aplicabilidad. • Definiciones. • Requisitos Específicos. • Información que se brindará al individuo. • El derecho individual del acceso a los datos.

	• El derecho individual de oponerse. • Acceso de datos personales a terceros. • Proceso de secreto y de seguridad. • Supervisión de actividades internas.
Política de Seguridad del Internet: es la descripción de los lineamientos de seguridad de acceso al Internet y su relación con la organización.	• Introducción. • Integridad de la información. • Secreto de la información. • Representaciones públicas. • Controles de accesos. • Uso personal. • Expectativas aislamiento de accesos. • Divulgación de problemas de la seguridad.
Política de Notificación de Incidentes: define los criterios permitidos y adecuados para el tratamiento de una notificación sobre un incidente reportado.	• Introducción / Descripción. • Control de acceso. • Identificación. • Clasificación de las notificaciones. • Interacciones con terceros. • Destrucción y Disposición. • Consideraciones especiales (información secreta).
Política de Tratamiento de Incidentes: hace referencia a la forma o los medios que se utilizan para el manejo de un incidente reportado.	• Introducción / Descripción. • Procedimiento. • Administración del riesgo. • Interacciones con terceros. • Reserva de información. • Consideraciones especiales (información secreta).

Política de Comunicación Externa: explica las normas para el manejo del intercambio de comunicación con entidades externas a la organización.	• Introducción / Descripción. • Control de acceso. • Identificación. • Clasificación de las notificaciones. • Interacciones con terceros. • Destrucción y Disposición. • Consideraciones especiales (información secreta).
Política de Entrenamiento y Capacitación: detalla los criterios de la organización en el manejo de los procesos de entrenamiento y capacitación del personal.	• Descripción. • Definiciones. • Procedimientos. • Reservas. • Consideraciones especiales.
Política de Tratamiento de Grandes Actividades: describe los criterios de la organización para el manejo de un evento que utilice una alta demanda de tiempo y recurso.	• Introducción / Descripción. • Procedimiento. • Administración del riesgo. • Interacciones con terceros. • Reserva de información. • Consideraciones especiales (información secreta).
Política de Error Humano: detalla las directrices o manejos que ejecutará la organización ante el eventual suceso de que un integrante del equipo comenta un error.	• Introducción / Descripción. • Consideraciones. • Factores implicados. • Reserva de información. • Consideraciones especiales (información secreta)
Política de Selección de Personal: define los criterios de la organización para la implementación del proceso de reclutamiento.	• Objetivos. • Descripción de los aspectos involucrados. • Proceso de reclutamiento.

	• Derechos, obligaciones y responsabilidades.
Política de Despido: define los criterios que aplica la organización cuando se da por finalizado unilateralmente un contrato laboral con un empleado.	• Descripción consistente respecto a los fines de la institución. • Definiciones. • Procedimiento. • Reservas. • Consideraciones especiales
Política de la Seguridad de la Computadora Personal: descripción de los criterios de aplicación de la seguridad informática sobre los computadores personales clasificados por su nivel de uso dentro de la organización.	• Descripción. • Uso en el negocio solamente. • Control de la configuración. • Control de acceso. • Virus. • Reserva. • Destrucción. • Documentación. • Seguridad Física.
Política de Uso del Correo Electrónico: establece los lineamientos de la utilización del correo electrónico de la organización.	• Objetivo. • Alcance. • Responsable. • Documentos asociados. • Definiciones. • Lineamientos del sistema de correo electrónico. • Condiciones de uso del correo electrónico.
Política de la Seguridad de la Red de Computadoras: establece los lineamientos de seguridad de todos los activos informáticos dentro de la red de computadoras. Brinda un nivel de detalle por cada dispositivo que se tenga en la red de computadoras de la organización.	• Propósito. • Alcance. • Política General. • Responsabilidades. • Control de acceso del sistema.

	• Uso de contraseñas. • Proceso de la conexión y del término de sesión. • Privilegios del sistema. • Establecimiento de accesos. • Virus Computacionales, Gusanos y Caballos de Troya. • Reserva de los datos y de los programas. • Cifrado. • Computadoras portátiles. • Impresiones en papel. • Aislamiento de accesos. • Registros y otras herramientas de la seguridad de los sistemas. • Manipulación de la información de la seguridad de la red. • Seguridad física del computador y su conectividad. • Excepciones. • Violaciones. • Glosario de términos.
Política de tele conmutación de la información: describe los lineamientos para el establecimiento de la comunicación por medio de equipos de telecomunicaciones.	• Control de ediciones. • Control de accesos. • Almacenamiento de datos y medios. • Medios de comunicación. • Administración del sistema. • Consideraciones del recorrido de los datos. • Seguridad física.
Política de uso de dispositivo móviles: descripción de los criterios de utilización de	• Control de ediciones y accesos. • Almacenamiento de datos y medios.

todos los dispositivos móviles que posea la organización.	• Medios de comunicación. • Administración del sistema. • Consideraciones del recorrido de los datos. • Seguridad física.
Política de la Seguridad de los equipos de Telecomunicaciones (Internos y Externos): dicta las normas de la organización para la aplicación de niveles de seguridad adecuados a los distintos dispositivos de telecomunicación internos y externos que sean de la organización.	• Descripción. • Uso en el negocio solamente. • Control de la configuración. • Control de acceso. • Fallas. • Reserva. • Destrucción. • Documentación. • Seguridad Física.

Para la definición de las políticas pueden existir diversidad de criterios e implementaciones según la organización CSIRT.

Para tener una visión más global en la implementación de políticas de una organización se presenta el estándar ISO 27002:2013, el mismo que está conformado por 14 dominios, 35 objetivos de control y 114 controles, un resumen de los dominios se presenta a continuación:

Tabla 11: ISO 27002:2013

Dominio	Observaciones
Políticas de Seguridad	Definir las directrices de la Dirección en seguridad de la información, incluye la definición y revisión de políticas.
Aspectos Organizativos de la Seguridad de la Información	Aspectos relativos a la gestión de la seguridad dentro de la organización, segregación de funciones, uso de dispositivos para movilidad y teletrabajo.
Seguridad ligada a los Recursos humanos	Considerar clausulas de confidencialidad, contratación de personal, etc.

Gestión de Activos	Inventario de activos y definición de sus mecanismos de control, así como etiquetado y clasificación de la información corporativa.
Control de Accesos	Definición y gestión de puntos de control de acceso a los recursos informáticos de la organización: contraseñas, seguridad perimetral, monitorización de accesos...
Cifrado	Controles criptográficos, gestión de llaves, etc.
Seguridad Física y Ambiental	Bajo este punto se engloban aspectos relativos a la seguridad física de los recintos donde se encuentran los diferentes recursos - incluyendo los humanos - de la organización y de los sistemas en sí, así como la definición de controles genéricos de seguridad.
Seguridad en las Operaciones	En este apartado se engloba aspectos de la seguridad relativos a la operación de los sistemas, protección para código malicioso, gestión de vulnerabilidades, gestión de copias de seguridad, etc.
Seguridad en las telecomunicaciones	Este apartado engloba aspectos de la seguridad en las telecomunicaciones, como los controles de red y el intercambio de software dentro de la organización.
Adquisición Desarrollo y Mantenimiento de los Sistemas de Información	Seguridad en el desarrollo y las aplicaciones, requisitos de seguridad de los sistemas de información, seguridad en los procesos de desarrollo de software, etc.
Relaciones con Terceros	Seguridad de la información en la relación con terceros, etc.
Gestión de Incidentes de Seguridad de la Información	Notificación de eventos de seguridad, valoración de eventos, respuesta a incidentes, etc.
Continuidad del Negocio	Definición de planes de continuidad, análisis de impacto, simulacros de catástrofes, etc.
Cumplimiento	Evidentemente, una política ha de cumplir con la normativa vigente en el país donde se aplica; si una organización se extiende a lo largo de diferentes países, su política tiene que ser coherente con la normativa del más restrictivo de ellos. En este apartado de la policía se establecen las relaciones con cada ley: derechos de propiedad intelectual,

	tratamiento de datos de carácter personal, exportación de cifrado, etc. junto a todos los aspectos relacionados con registros de eventos en los recursos (bitácoras) y su mantenimiento.

1.2.2.6 Publicando Políticas y Procedimientos CSIRT

Cada usuario que tiene acceso a un Equipo de Respuesta a Incidentes de Seguridad Cibernética debe saber tanto como sea posible sobre los servicios e interacciones de este equipo mucho antes de que él o ella en realidad los necesiten.

Una declaración clara de las políticas y procedimientos de un CSIRT ayuda al integrante a comprender la mejor manera de informar sobre los incidentes y qué apoyo esperar después. Las políticas y procedimientos deben proporcionar al usuario respuestas a preguntas como:

¿El CSIRT ayudará a resolver el incidente? ¿Va a proporcionar ayuda a evitar incidentes en el futuro?, claro que las expectativas, en particular de las limitaciones de los servicios prestados por un CSIRT, harán que la interacción sea más eficiente y efectiva.

Existen diferentes tipos de equipos de respuesta, algunos grupos son muy amplios (por ejemplo, CERT Centro de Coordinación de Internet), otros grupos más limitados (por ejemplo, DFN-CERT, CIAC), y otras tienen grupos muy restringidos (por ejemplo, equipos de respuesta comercial, equipos de respuesta corporativos). Independientemente del tipo de equipo de respuesta, la comunidad debe de apoyar el estar bien informados sobre las políticas y procedimientos de su equipo. Por lo tanto, es obligatorio que los equipos de respuesta publiquen esa información.

Un CSIRT debe comunicar toda la información necesaria acerca de sus políticas y servicios en una forma adecuada a las necesidades de sus integrantes. Es importante comprender que no todas las políticas y procedimientos deben ser accesibles al público. Por ejemplo, no es necesario entender el funcionamiento interno de un equipo con el fin de interactuar con él, como el conocer como reportar un incidente o recibir orientación sobre cómo analizar y asegurar uno de los sistemas.

Anteriormente algunos los equipos suministraban esta información una especie de Marco Operacional, otros proporcionaban una lista de Preguntas Frecuentes (FAQ), mientras que otros escribieron documentos para distribuirlos en conferencias de usuarios o boletines.

Se recomienda que cada CSIRT publique sus directrices y procedimientos en su propio servidor de información (por ejemplo, un servidor de World Wide Web). Esto permitirá a los integrantes acceder fácilmente a ella.

Las plantillas de información de un CSIRT facilitarán la distribución de información sobre la existencia del CSIRT y la información básica necesaria para acceder a ellos.

Independientemente de la fuente de la que se recupera la información, el usuario de la plantilla debe comprobar su autenticidad. Es altamente recomendable que esos documentos vitales sean protegidos por firmas digitales. Esto permitirá al usuario verificar que la plantilla fue de hecho publicada por el CSIRT y que no ha sido manipulada (se asume que el lector está familiarizado con el uso adecuado de las firmas digitales para determinar si un documento es auténtico).

1.3. Recomendaciones generales respecto de la infraestructura física necesaria en las etapas iniciales

Esta sección pretende brindar la información básica necesaria para la creación de un centro de cómputo que brindará los respectivos servicios tecnológicos de información para un CSIRT en formación.

Obviamente de acuerdo a la experiencia y el nivel de madurez en sus servicios se podrá escalar en cada uno de los puntos de acuerdo a cada uno de los servicios que estén implicados.

1.3.1 Recomendaciones de Seguridad Física y Ambiental

La instalación y ubicación física dentro de la organización depende de muchos factores, entre los que podemos citar: el servicio que se pretende obtener, el tamaño de la organización, las disponibilidades de espacio físico existente o planificado, etc.

Se comprende dentro del siguiente detalle la seguridad física y ambiental de las áreas, seguridad del equipo y controles generales.

Generalmente, la instalación física de un centro de cómputo exige tener en cuenta por lo menos los siguientes puntos:

1.3.1.1 Local Físico

Donde se analizará el espacio disponible, el acceso de equipos y personal, instalaciones de suministro eléctrico, acondicionamiento térmico y elementos de seguridad disponibles.

1.3.1.2 Espacio y Movilidad

Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o suelo falso, etc.

1.3.1.3 Tratamiento Acústico

Los equipos ruidosos como las impresoras con impacto, equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.

1.3.1.4 Ambiente Climático

En cuanto al ambiente climático, la temperatura de una oficina con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar comprendida entre el 45% y el 65%. En todos los lugares hay que contar con sistemas que renueven el aire periódicamente. No menos importante es el ambiente sonoro por lo que se recomienda no adquirir equipos que superen los 55 decibeles, sobre todo cuando trabajan muchas personas en un mismo espacio.

1.3.1.5 Instalación Eléctrica

El suministro eléctrico a un centro de cómputo, y en particular la alimentación de los equipos, debe hacerse bajo unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de baterías, etc.).

1.3.1.6 Picos y Ruidos Electromagnéticos

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

1.3.1.7 Cableado

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental. Es importante tener presente que el cableado posee varias categorías y el asesorarse cuál es la más indicada para el uso que se requiera es una parte vital del proceso de selección. Y por último aplicar procesos de certificación sobre el cableado instalado es altamente recomendable.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

- ✓ **Interferencia**: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
- ✓ **Corte del cable**: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
- ✓ **Años en el cable**: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos. Esto se puede hacer:

- ✓ Desviando o estableciendo una conexión no autorizada en la red: un sistema de administración y procedimiento de identificación de acceso adecuados hará difícil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.
- ✓ Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos.

- ✓ Luego, no hace falta penetrar en los cables físicamente para obtener los datos que transportan.

1.3.1.7.1 Cableado de Alto Nivel de Seguridad

Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreos de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

1.3.1.7.2 Pisos de Placas Extraíbles

Los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos pueden ser, en caso necesario, alojados en el espacio que, para tal fin se dispone en los pisos de placas extraíbles, debajo del mismo.

1.3.1.7.3 Sistema de Aire Acondicionado

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva. Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extintores de incendios, monitores y alarmas efectivas.

1.3.1.7.4 Emisiones Electromagnéticas

Desde hace tiempo se sospecha que las emisiones de muy baja frecuencia que generan algunos periféricos, son dañinas para el ser humano. Según recomendaciones científicas estas emisiones podrían reducirse mediante filtros adecuados al rango de las radiofrecuencias, siendo estas totalmente seguras para las personas. Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

1.3.1.8 Iluminación

El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos. Las oficinas mal iluminadas son la principal causa de la pérdida de la productividad en las organizaciones y de un gasto energético excesivo. Una iluminación deficiente provoca dolores de cabeza y perjudica a los ojos.

1.3.1.9 Seguridad Física del Local

Se estudiará el sistema contra incendios, teniendo en cuenta que los materiales sean incombustibles (pintura de las paredes, suelo, techo, mesas, estanterías, etc.). También se estudiará la protección contra inundaciones y otros peligros físicos que puedan afectar a la instalación y condiciones geográficas del lugar.

1.3.1.10 Próximos Pasos

Es inevitable el seguir creciendo sobre la base instalada y es allí donde se hace muy importante el no perder de vista que es necesario reforzar otros elementos para que apoyen la estrategia de escalabilidad y robustecimiento de la seguridad. A continuación se listan los elementos importantes que deben de ser tomados en cuenta según sea el caso:

1.3.1.10.1 Aseguramiento Contra Situaciones Hostiles

Robo de Equipo e Información, Fraude electrónico y Sabotaje.

1.3.1.10.2 Control de Accesos

Establecer control de accesos de personas y vehículos, implementación de detectores de metales, sistemas biométricos (emisión de calor, huella digital, verificación de voz, verificación de patrones oculares), verificación automática de firmas, seguridad con animales, protección electrónica (barreras infrarrojas y de microondas, detectores ultrasónicos, circuitos cerrados, sonorización y dispositivos luminosos).

1.3.1.11 Conclusiones

- Evaluar y controlar permanentemente la seguridad física del local es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organización.
- Tener controlado el ambiente y acceso físico permite:
    - Disminuir siniestros.
    - Trabajar mejor manteniendo la sensación de seguridad.
    - Descartar falsas hipótesis si se produjeran incidentes.
    - Tener los medios para luchar contra accidentes.
- Las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos; y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados.

Estas decisiones pueden variar desde el conocimiento de las áreas que recorren ciertas personas hasta el extremo donde pueden evacuar el local en caso de accidentes.

1.3.2 Recomendaciones sobre la arquitectura de redes de un CSIRT

En esta sección se brindan varias recomendaciones sobre: el ambiente físico, infraestructura de red, hardware, software, infraestructura de telecomunicaciones y cuatro diagramas que detallan posibles escenarios de implementación de una topología de red para un CSIRT según sean sus posibilidades y necesidades.

Es importante hacer mención que este detalle brinda un bosquejo bastante global de los elementos que tienen que ser tomados en cuenta para la implementación de una arquitectura de red para un CSIRT en particular.

1.3.2.1 Ambiente Físico

Las áreas relevantes a tratar dentro del ambiente físico son las siguientes:

- ✓ **Áreas Administrativas**: las áreas administrativas así como las salas de reuniones o apoyo podrán ser compartidas con el resto de la organización.

- ✓ **Áreas Operativas**: tales como salas de trabajo de los equipos técnicos, sala de servidores y sala de laboratorios son considerados ambientes críticos y deberán tener implementaciones de aspectos de seguridad física específica.

Es importante considerar dentro de todas las áreas físicas cuales pueden ser tomadas como críticas y cuáles no. Para los ambientes críticos deberán ser contempladas las siguientes características de seguridad:

- ✓ Ambiente aislado de otros departamentos.
- ✓ Segmentación del Circuito de Servicios: deben de estar separadas físicamente las redes de computadores así como el acceso hacia el Internet.
- ✓ Acceso restringido al ambiente de trabajo, teniendo puertas con mecanismos de seguridad como claves, botones magnéticos u otros recursos que permitan acceso restringido y forma de identificar y mantener almacenados los datos de acceso.
- ✓ Obedecer la política de seguridad de información del CSIRT y/u organización.

Se recomienda que el ambiente físico contemple ciertas características de seguridad, como:

- ✓ Que el acceso y permanencia en el local de terceras personas sea acompañado por integrantes del CSIRT.
- ✓ **Tener siempre a disposición medios de protección y prevención**: extintores, sensores de humo, rociadores, circuito interno de televisión, piso falso, paredes refractarias, caja fuerte para el almacenamiento de documentos secretos, sistema empresarial de almacenaje de copias de seguridad.

A continuación se listan las áreas físicas mínimas que se recomiendan para la implementación operativa de un CSIRT:

- ✓ Recepción.
- ✓ Oficina del Director.
- ✓ Cuarto de Seguridad. (Caja Fuerte)
- ✓ Sala de Reuniones.
- ✓ Sala de Archivos y Almacenamiento de Medios.
- ✓ Sala de Capacitación/Entrenamiento.

- ✓ Sala de Operaciones.
- ✓ Laboratorio.
- ✓ Sala de Servidores.

Obviamente dentro de una organización a la que pertenezca el CSIRT gozará del uso de áreas comunes a todos. (Espacios abiertos, jardines, corredores, sanitarios, áreas de parqueo de vehículos, etc.) De lo contrario, también tendrán que ser tomadas en cuenta dentro de su definición.

1.3.2.2 Infraestructura de Red

La infraestructura de la red de computadores del CSIRT debe estar separada de la infraestructura de la organización en que esté hospedada. El CSIRT debe tener una estructura propia de subredes y dominios. Red de la organización y red del CSIRT.

Se recomienda que el CSIRT tenga una estructura de red de computadores aislada, permitiendo implementar segmentos de redes con funciones específicas. Al menos deben de existir dos segmentos dentro de la red CSIRT:

- ✓ **Red para la operación en ambiente de producción**: para el almacenaje de los datos y ejecución de las tareas relativas a los servicios.
- ✓ **Red para tareas de laboratorio**: para la aplicación de pruebas y estudios.

Las redes que se conectan con el ambiente externo (Internet) deben de ser protegidas por medio de dispositivos de seguridad según su necesidad. (Firewall, Proxy, IDS, IPS, etc.)

1.3.2.3 Hardware

Para que un CSIRT pueda operar con todas sus posibilidades se hace necesario poseer equipos de uso general. En la siguiente tabla se listan los elementos necesarios a ser tomados en cuenta.

Tabla 12: Listado de equipos de hardware necesarios para un CSIRT

Equipo	Elementos
Equipos y medios de conectividad	• Routers. • Switches.

	• Cableado Estructurado. • Enlace con el Internet que cuente con: una velocidad adecuada, dirección IP válida / bloque de direcciones IP válidas. • Dispositivos de seguridad. (Antivirus, IDS, IPS) • Firewall. • Detección de Intrusos. • Correo electrónico, WEB, NTP, DNS. • Registro de bitácoras de sistemas. • Archivos. • Intranet. • Acceso Remoto (RPV). • Backup.
Estaciones de Trabajo y Equipos Portátiles	• Estaciones de trabajo. • Computadoras portátiles. • Accesorios: pen drive, CDs, DVDs, Discos Duros Externos, Herramientas, etc.
Equipos para la seguridad en ambiente físico	• Caja Fuerte a prueba de fuego para almacenar documentos y copias de seguridad. • Infraestructura de protección contra incendios. (Prevención, detección y alarma.) • Sistema de refrigeración y aire acondicionado compatible con las especificaciones de los equipos adquiridos. • Infraestructura de protección contra interrupciones en el suministro de energía eléctrica. (Estabilizadores, grupos de generadores compartidos con las instalaciones del órgano que acogerá al CSIRT.)
Otros	• Proyector multimedia portátil. • Impresora Multifuncional. (Impresora, fax y escáner.) • Dispositivos para la realización de copias de seguridad: grabadores de CD, DVD y Cintas Magnéticas. • Trituradora de papel.

	• Material de Oficina.

1.3.2.4 Software

Dentro de los tipos de software que debe utilizar una organización CSIRT se encuentran las siguientes recomendaciones:

- Que los sistemas operativos de los servidores, estaciones de trabajo y equipos portátiles utilicen software libre, siempre que esto sea posible.
- Procesos de aseguramiento de sistemas.
    - Aplicaciones y configuraciones de los equipos utilizados en la red operacional CSIRT que sigan un patrón y cumplan los siguientes requisitos:
        - Estar configurados en modo seguro.
        - Tengan instaladas las últimas actualizaciones y correcciones de seguridad.
        - Poseer sistemas de registro de eventos habilitados. (Bitácoras)
        - Sistemas de control del flujo de trabajo (Workflow) para el registro y seguimiento de incidentes.
        - Sistemas de información en la Web para recoger informaciones de incidentes y divulgación de alertas, recomendaciones y estadísticas.
        - Aplicativos de Firewall corporativo para las estaciones de trabajo y equipos portátiles.
        - Aplicativos para la detección y prevención de intrusos
        - Servicios de correo electrónico, Web, NTP y DNS.
        - Aplicativos de Criptografía y Firma Digital.
        - Aplicativos para uso en el Laboratorio. (Aplicativos para el análisis forense)
        - Utilización de programas de virtualización de servidores y estaciones de trabajo para usos internos y de laboratorio.

1.3.2.5 Infraestructura de Telecomunicaciones

A continuación se listan los componentes necesarios para la implementación de los servicios de un CSIRT:

- Conexión de Alta Velocidad con el Internet (Mínimo)
- PBX, extensiones y correo de voz.
- Equipo de FAX y telefonía móvil para hacer viable la operación 7x24.

1.3.2.6 Diagramas Sugeridos

1.3.2.6.1 Esquema Uno: Red Básica Segura

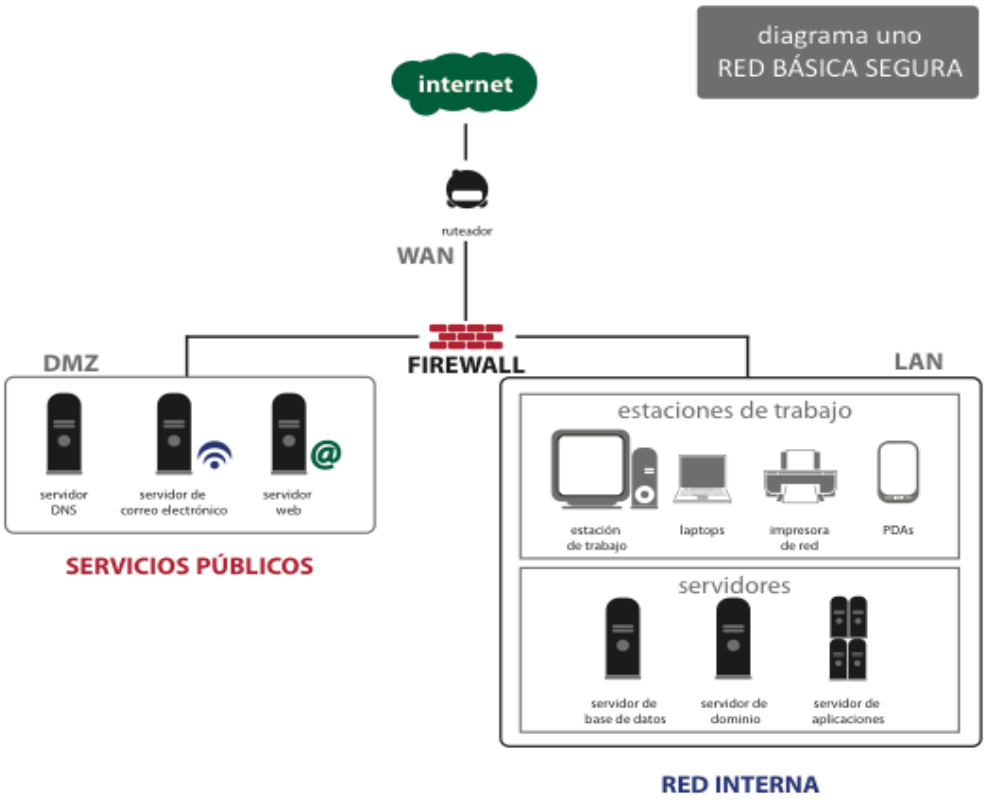


Figura 6: Diagrama Uno: Red Básica Segura.

Tabla 8: Fortalezas y Debilidades del Modelo Matricial.

MODELO MATRICIAL	
FORTALEZAS	**DEBILIDADES**
• Logra la coordinación necesaria para satisfacer las demandas duales de los clientes. • Comparte flexiblemente los recursos humanos entre productos. • Adaptada para decisiones complejas y cambios frecuentes en un entorno inestable. • Proporciona oportunidades para el desarrollo de habilidades tanto funcionales como en productos. • Es más adecuada en organizaciones de tamaño mediano con productos múltiples. • Recursos Humanos compartidos.	• Somete a los participantes a la experiencia de una autoridad dual; esto puede ser frustrante y ocasionar confusión. • Implica que los participantes necesitan buenas habilidades interpersonales y mucha capacitación. • Consume tiempo; implica frecuentes reuniones y sesiones para la solución de conflictos. • No funcionará a menos que los participantes entiendan y adopten relaciones colegiadas en lugar de tipo vertical. • Requiere grandes esfuerzos para mantener el equilibrio de poder.

1.3.2.6.2 Esquema Dos: Red Segura Redundante

Tabla 14: Detalles sobre un esquema de redes seguras redundantes

Detalles	Descripción
Características	• Esquema para brindar servicios reactivos. • Con redundancia de servidores. • Dos segmentos de red regulados por Firewalls. • Acceso a Internet mínimo de 2 Mbps.
Software	• Se puede utilizar software libre.

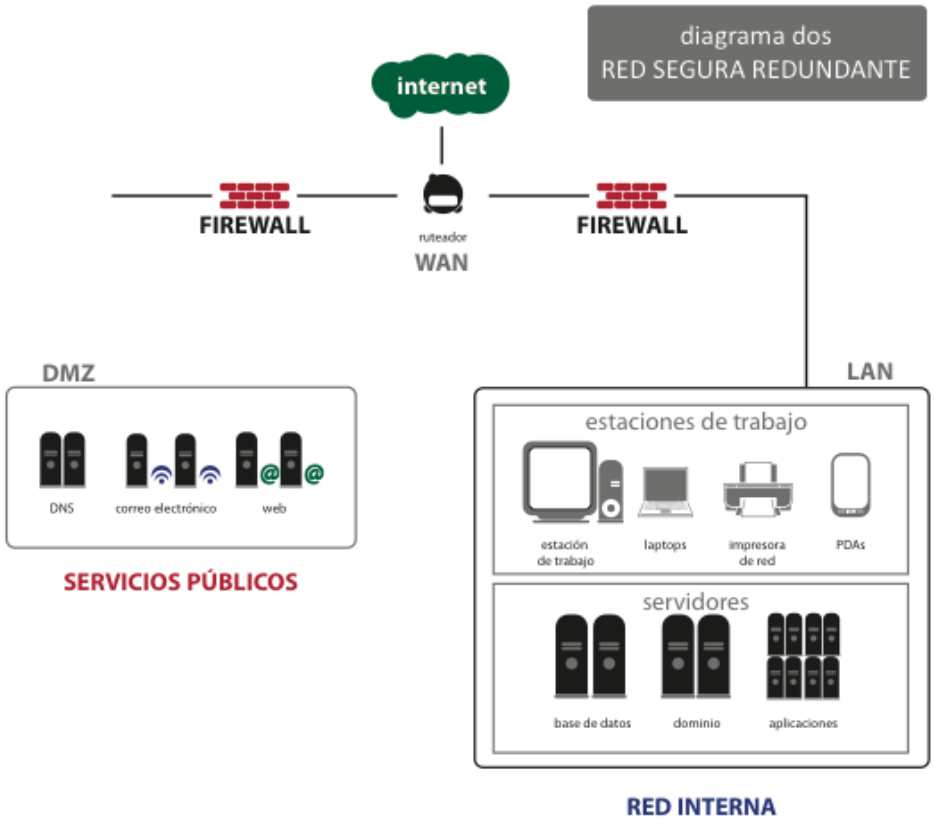


Figura 7: Diagrama Dos: Red Segura Redundante.

1.3.2.6.3 Esquema Tres: Red Segura Segmentada y Redundante

Tabla 15: Detalles sobre un esquema de redes seguras segmentadas y redundantes.

Detalles	Descripción
Características	• Esquema para brindar servicios reactivos y proactivos. • Sensores y servidor con Sistema de Detección de Intrusos (IDS). • Con redundancia de servidores. • Enlaces a Internet Redundantes. • Alta disponibilidad en los servicios. • Tres segmentos de red para servicios de la organización. • Una red especializada para pruebas. (Laboratorio de Pruebas) • Accesos entre segmentos regulados por varios Firewalls.

	• Acceso a Internet ○ Enlace principal a 8 Mbps. ○ Enlace secundario para pruebas a 2 Mbps.
Software	• Se puede utilizar software libre.

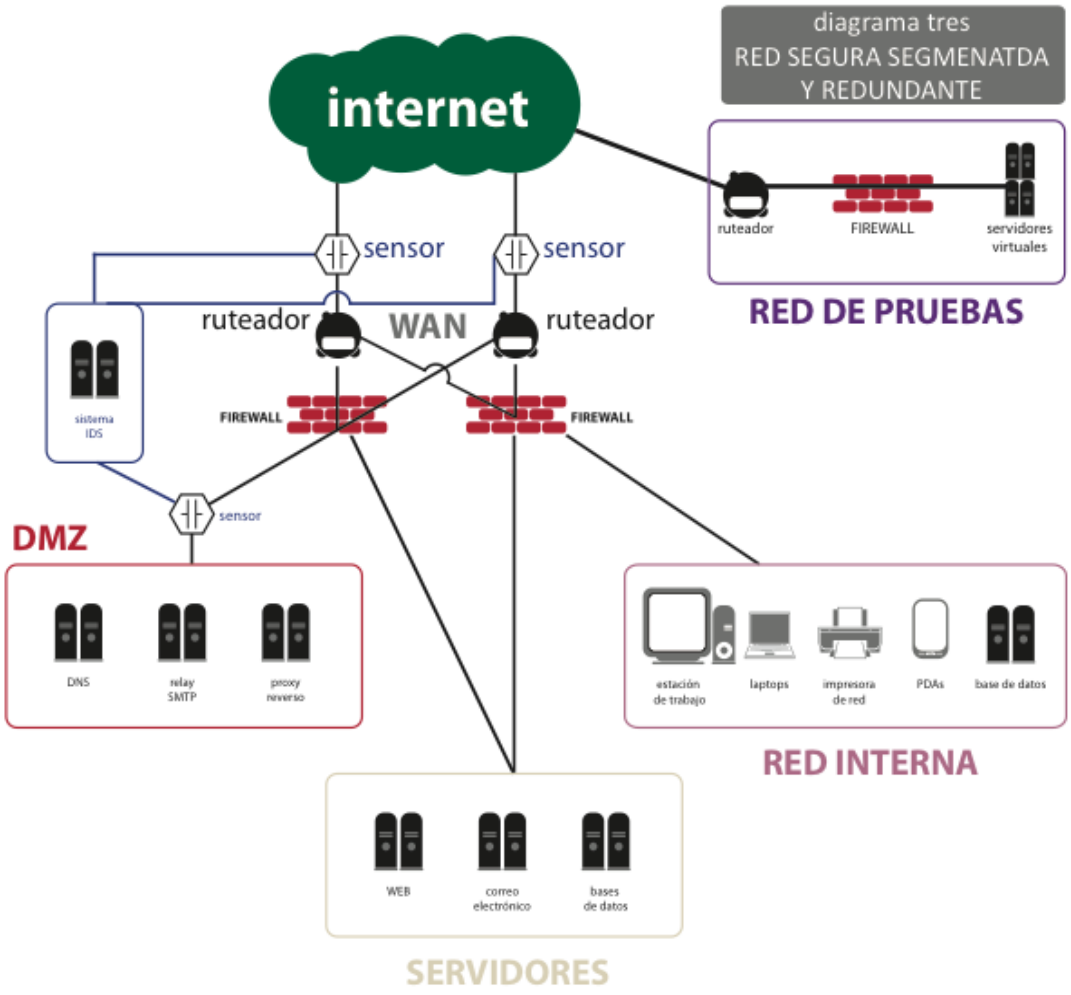


Figura 8: Diagrama Tres: Red Segura Segmentada y Redundante.

1.3.2.6.4 Esquema Cuatro: Red Segura Segmentada Separada de la Organización

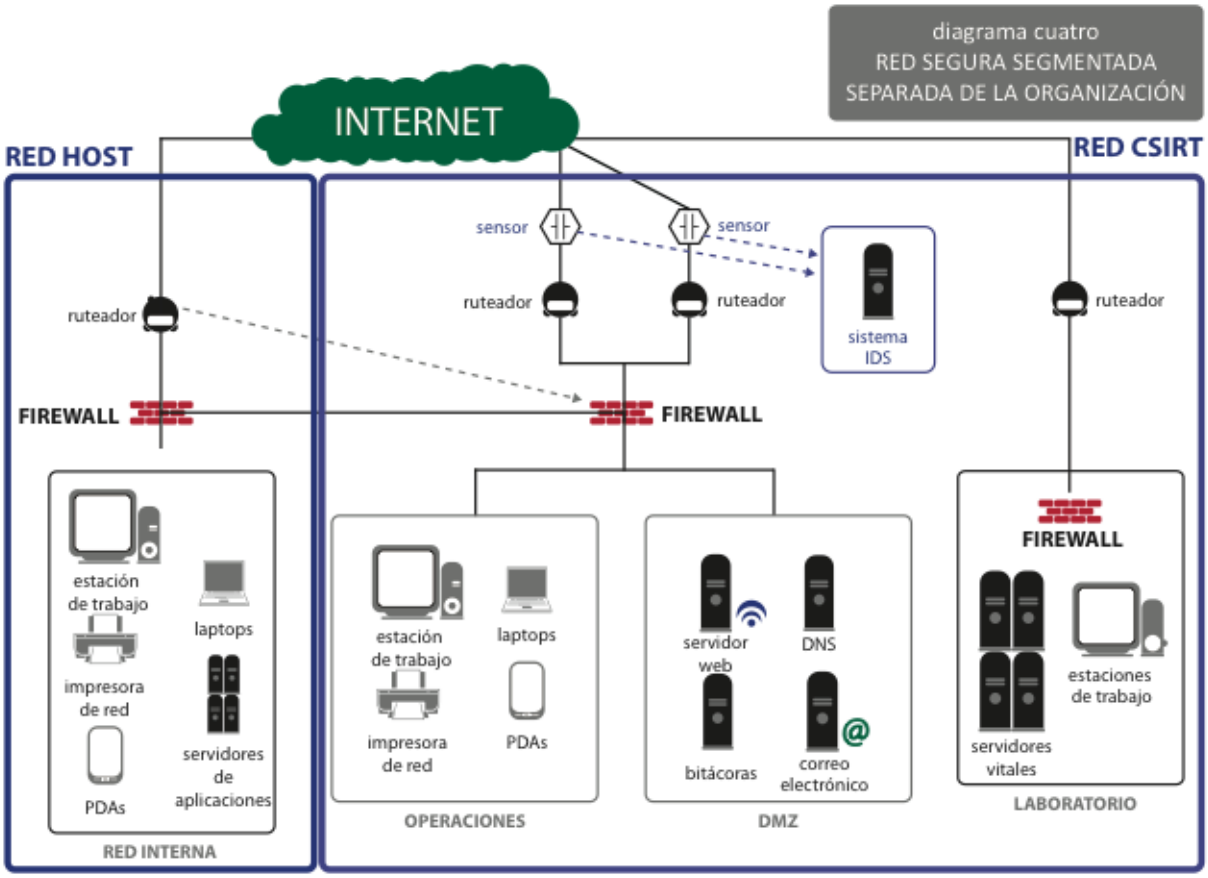


Figura 9: Diagrama Cuatro: Red Segura Segmentada separada de la Organización.

Tabla 16: Detalles sobre un esquema de red segmentada separada de la organización.

Detalles	**Descripción**
Características	• Esquema para brindar servicios reactivos y proactivos. • Separación física de la red CSIRT y de la organización. • Enlaces para el acceso al Internet redundantes para la red CSIRT. • Sensores y Servidor con Sistema de Detección de Intrusos (IDS). • Red aislada para Pruebas de laboratorio. • Tres redes diferentes.

	• Niveles de acceso internos regulado por los Firewalls entre la Organización y el CSIRT.
	• Acceso a Internet
	  ○ Enlace de la Organización: 2 Mbps.
	  ○ Enlaces redundantes CSIRT: 4 Mbps.
	  ○ Enlace para red de Laboratorio: 2 Mbps.

Software	• Se puede utilizar software libre.

1.4. Manejo de información, Procedimientos y Políticas

Es muy importante que las políticas y procedimientos de un equipo de respuesta sean publicados en su comunidad. En esta sección se listan todos los tipos de información que la comunidad necesita recibir de su equipo de respuesta. La forma de hacer llegar esta información a la comunidad difiere de un equipo a otro, así como el contenido de la información específica. El objetivo aquí es describir claramente los diversos tipos de información que un componente de la comunidad espera de su equipo de respuesta. Lo más importante es que un CSIRT tenga una política y que los que interactúan con el CSIRT sean capaces de obtenerla y entenderla.

Este esquema debe ser visto como una sugerencia. Cada equipo debe sentirse libre para incluir todo aquello que cree que es necesario para apoyar a su comunidad.

1.4.1 Descripción de Histórico de Actualización del Documento

Para esta sección inicial del documento se recomienda considerar los siguientes puntos:

- **Fecha de la última actualización:** esto debería ser suficiente para permitir que cualquier persona interesada evalué la vigencia del documento, si se considera conveniente y adecuado, podría ser oportuno versionar el documento.
- **Lista de distribución**: las listas de correo son un mecanismo conveniente para distribuir información actualizada a un gran número de usuarios. Un equipo puede decidir utilizar su propia lista o bien una ya existente para la notificación de cambios a los usuarios. La lista normalmente es integrada por grupos del CSIRT con los que se tienen interacciones

frecuentes. Las firmas digitales se deben utilizar para enviar mensajes de actualización entre CSIRT's.

- **Ubicación del documento**: la ubicación de un documento debe de ser accesible a través de los servicios de información en línea de cada equipo en particular. Los integrantes de cada grupo pueden fácilmente obtener más información sobre el equipo y comprobar si las actualizaciones son recientes. Esta versión en línea también debería ir acompañada de una firma digital que sería la autenticación del documento.

1.4.2 Información de Contacto

En esta segunda sección del documento debe describir los detalles completos de cómo ponerse en contacto con el CSIRT, esto puede ser muy diferente para los diferentes equipos. En algunos casos como ejemplo, podrían decidir no dar a conocer los nombres de los miembros de su equipo.

A continuación se listan la información que es recomendable detallar:

- Nombre del CSIRT.
- Dirección física (Ubicación).
- Dirección(es) de Correo(s) Electrónico(s).
- Zona horaria: esto es útil para la coordinación de los incidentes en el cual se cruzan zonas horarias.
- Número de teléfono y fax.
- Otras telecomunicaciones: algunos equipos pueden ofrecer comunicaciones de voz segura.
- Direcciones de correo electrónico
- Las claves públicas y el cifrado: el uso de técnicas específicas depende de la capacidad de los socios de comunicación para tener acceso a los programas, claves, etc. La información pertinente debe darse a manera de facilitar a los usuarios la habilitación del canal de comunicación cifrado respectivo cuando interactúe con el CSIRT.
- Miembros del equipo: información discrecional del grupo. (Si aplicase.)

- Horario de atención: el horario de funcionamiento semanal (8x5 o 7x24) y calendario de vacaciones deberá indicarse aquí.
- Información Adicional del Contacto: por ejemplo si existe un mail de contacto de uso general, contacto para reporte de incidentes, etc.

El nivel de detalle de esta información queda a criterio de cada grupo. Esto podría incluir diferentes contactos para diversos servicios, o podría ser una lista de servicios de información en línea. Si en algún caso existen procedimientos específicos para poder acceder a cierto servicio se recomienda que se detalle adecuadamente.

1.4.3 Descripción del CSIRT

Esta es la tercera sección del documento, en la que el CSIRT debe especificar lo que tiene que hacer y la autoridad bajo la cual lo hará. El documento debe incluir al menos los siguientes elementos:

- **Misión:** debe centrarse en las actividades principales del equipo. Con el fin de ser considerado un Equipo de Respuesta a Incidentes de Seguridad Informática, el equipo debe ser compatible con la presentación de informes de incidentes y el apoyo de sus integrantes frente a los sucesos. Los objetivos y propósitos de un equipo son especialmente importantes y requieren una definición clara y sin ambigüedades.
- **Comunidad:** una comunidad CSIRT puede ser determinada de varias maneras. La definición de la comunidad abarca un perímetro alrededor del grupo al que el equipo proporcionará el servicio, por ejemplo, podrían ser empleados de una empresa, suscriptores de pago, puede ser definida en términos de un enfoque tecnológico, como los usuarios de un sistema operativo determinado. Es importante que exista una sección de política del documento, la cual debe de explicar cómo serán tratadas las solicitudes fuera del perímetro definido.

  Si un CSIRT decide no revelar su comunidad, se debe explicar el razonamiento detrás de esta decisión. Por ejemplo, si se cobrasen servicios, el CSIRT no brindará una lista de sus clientes, sino que declarará que prestan un servicio a un gran grupo de clientes que se mantienen en secreto debido a los contratos y cláusulas de confidencialidad con sus clientes.

- **Organización Patrocinadora / Afiliación:** la organización patrocinadora, que autoriza las acciones del CSIRT, debe respaldar las distintas actividades del CSIRT. Sabiendo que esto ayudará a los usuarios a comprender los antecedentes y la puesta en marcha del CSIRT; es información vital para la construcción de confianza entre un componente y un CSIRT.

- **Autoridad:** esta sección puede variar mucho de un CSIRT a otro, basada en la relación entre el equipo y su comunidad. Mientras que una organización CSIRT dará su autoridad por la gestión de la organización, un comunidad CSIRT será apoyada y elegida por la comunidad, generalmente en un rol de asesoramiento. Un CSIRT puede o no tener la autoridad para intervenir en el funcionamiento de todos los sistemas dentro de su perímetro. Se debe identificar el alcance de su control, a diferencia del perímetro de su comunidad. Si otros CSIRT's operan jerárquicamente dentro de su perímetro, esto debe ser mencionado aquí, y los CSIRT's relacionados identificados. La divulgación de la autoridad de un equipo puede exponer a las reclamaciones de responsabilidad. Cada equipo debe buscar consejo legal sobre estos asuntos.

1.4.4 Políticas

La cuarta sección de este documento tiene por objetivo presentar las políticas implementadas por el CSIRT, como se había indicado anteriormente, es fundamental que los Equipos de Respuesta a Incidentes definan sus políticas y las comuniquen a su comunidad.

A continuación se presentan las siguientes:

- **Política de Tipos de Incidentes y Nivel de Apoyo**: en esta política deben listarse los tipos de incidentes que el equipo es capaz de hacer frente, y el nivel de apoyo que el equipo ofrecerá al momento de responder a cada tipo de incidente. El nivel de soporte puede cambiar dependiendo de factores tales como la carga de trabajo del equipo y la integridad de la información disponible. Estos factores deberían ser descritos y sus efectos deben ser explicados. Una lista de tipos de incidentes conocidos será incompleta con respecto a posibles futuros incidentes, así que un CSIRT también debería brindar algunos antecedentes "predeterminados" por el apoyo a tipos de incidentes no mencionados.

  El equipo debe indicar si va a actuar sobre la información que recibe y sus vulnerabilidades, mismas que crean oportunidades para futuros incidentes. Reaccionar sobre dicha

información, en nombre de sus integrantes es considerado como un servicio opcional de la política proactiva en lugar de una obligación de servicio básico para un CSIRT.

- **Política de Co-operación, Interacción y Divulgación de Información**: debe indicarse que los grupos relacionados con el CSIRT interactúan habitualmente Estas interacciones no están necesariamente relacionadas con el equipo de respuesta a incidentes de seguridad cibernética, pero se utilizan para facilitar una mejor cooperación en temas técnicos o de servicios. De ninguna manera se necesita detallar los acuerdos de cooperación entregados, el objetivo principal de esta sección es dar a los involucrados una comprensión básica de qué tipo de interacciones se han establecido y sus propósitos.

  La cooperación entre CSIRT's puede ser facilitada por el uso de un número único de asignación de etiquetas combinadas con los procedimientos de traspaso explícito. Esto reduce la posibilidad de malos entendidos, la duplicación de esfuerzos, asistencia en el seguimiento de incidentes y evitará "ciclos" en la comunicación.

  La presentación de informes y la política de divulgación deben dejar claro quiénes serán los destinatarios CSIRT de un informe en cada circunstancia. También debe tener en cuenta si el equipo se espera para operar a través de otro CSIRT o directamente con un miembro de otra comunidad sobre las cuestiones que se refieren específicamente a ese miembro.

  Los grupos relacionados a un CSIRT van a interactuar como se enumera a continuación:

  - **Equipos de Respuesta a Incidentes**: un CSIRT a menudo necesita interactuar con otros CSIRT's. Por ejemplo, un CSIRT dentro de una gran empresa puede tener que informar sobre los incidentes a un CSIRT nacional, y un CSIRT nacional deberá informar de los incidentes a CSIRT's nacionales en otros países para hacer frente a todos los sitios implicados en un ataque a gran escala. La colaboración entre CSIRT's puede conducir a la divulgación de la información. Los siguientes son ejemplos de esa comunicación, pero no pretende ser una lista exhaustiva:

    - Informe de incidentes dentro de la comunidad a otros equipos. Si se hace esto, el conocimiento de la información relacionada con el sitio puede ser del conocimiento público, accesible a todos, en particular la prensa.

- Manejo de incidentes que ocurren dentro de la comunidad, pero que informa fuera de ella (lo que implica que algunas informaciones ya han sido divulgadas fuera del sitio).
- Observaciones de información desde dentro de la comunidad que indica sospecha o incidentes confirmados fuera de él.
- Actuar sobre los informes de incidentes de fuera de la comunidad.
- Transmisión de información sobre vulnerabilidades a las empresas, para socios CSIRT o directamente a los sitios afectados que se encuentran dentro o fuera de la comunidad.
- Comentarios a las partes de la presentación de informes de incidentes o vulnerabilidades.
- El suministro de información de contactos relativos a los miembros de la comunidad, los miembros de otros grupos interesados, CSIRT's, o los organismos policiales.

- **Empresas**: algunas empresas tienen su propio CSIRT, pero otras no pueden. En tales casos, un CSIRT necesitará trabajar directamente con una empresa para proponer mejoras o modificaciones, para analizar el problema técnico o para poner a prueba las soluciones previstas. Las empresas desempeñan un papel especial en el manejo de un incidente si las vulnerabilidades de sus productos están involucradas en el incidente.
- **Los Organismos Policiales:** Estos incluyen la policía y otros organismos de investigación. CSIRT y usuarios deben ser sensibles a las leyes y reglamentos locales, los cuales pueden variar considerablemente en diferentes países. Un CSIRT puede asesorar sobre los detalles técnicos de los ataques o pedir asesoramiento sobre las consecuencias jurídicas de un incidente. Leyes y regulaciones locales pueden incluir la presentación de informes específicos y los requisitos de confidencialidad.
- **Prensa:** Un CSIRT puede ser abordado por la prensa para información y comentarios de vez en cuando. Una política explícita relativa a la divulgación a la prensa puede ser útil, particularmente para aclarar las expectativas de los integrantes de un CSIRT. La política de prensa suele ser muy sensible a los contactos d prensa.

- **Otros:** esto podría incluir actividades de investigación o de la relación con la organización patrocinadora.

El estado predeterminado de cualquier información relacionada con la seguridad que un equipo recibe por lo general será "confidencial", pero la adherencia rígida de esto hace que el equipo parezca ser “un agujero negro” de información. El cual puede reducir la probabilidad de que el equipo obtenga la cooperación de los clientes y de otras organizaciones. Se hace necesario definir la información que se debe de informar o divulgar, a quién, y cuándo.

Los diferentes equipos pueden estar sujetos a diferentes restricciones legales que requieren o restringen el acceso, especialmente si trabajan en las diferentes jurisdicciones. Además, pueden tener obligaciones de información impuestas por su organización patrocinadora. Cada equipo debe especificar estas restricciones, tanto para aclarar las expectativas de los usuarios y para informar a los otros equipos. Los conflictos de interés, en particular en materia comercial, también pueden limitar la divulgación de un equipo.

Un equipo normalmente recogerá las estadísticas. Si se distribuye la información estadística, la política de divulgación debe decirlo, y debe describir cómo obtener estas estadísticas.

- **Política de Comunicación y Autenticación**: se debe tener una política que describa los métodos de comunicación segura y verificable que se van a utilizar. Esto es necesario para la comunicación entre los CSIRT’s, y entre un CSIRT y sus integrantes. Se deben incluir las claves públicas para el adecuado establecimiento de comunicación segura junto con directrices sobre cómo utilizar esta información para comprobar la autenticidad y la forma de tratar la información dañada (por ejemplo, donde informar de este hecho)

  Por el momento, se recomienda que como mínimo cada CSIRT tenga (si es posible), una clave PGP disponible. Un equipo también puede utilizar otros mecanismos disponibles (por ejemplo, PEM, MOSS, S/MIME), de acuerdo a sus necesidades y las de sus integrantes. Obsérvese, sin embargo, que un CSIRT y los usuarios deben ser sensibles a las leyes y reglamentos locales. Algunos países no permiten el cifrado fuerte, o hacer cumplir las políticas específicas sobre el uso de la tecnología de cifrado. Además de cifrar la información sensible cuando sea posible, la correspondencia debe incluir la firma digital. (Tenga en cuenta que en la mayoría de los países, la protección de la autenticidad

mediante el uso de la firma digital no se ve afectado por las normas de encriptación existentes, o simplemente no existe.

Para la comunicación por teléfono o fax un CSIRT puede mantener en secreto los datos de autenticación de los socios con los que puedan tratar, el uso de una contraseña o frase puede ser un elemento definido previamente. Obviamente las claves secretas no deben ser publicadas, aunque se sepa de su existencia.

1.4.5 Servicios

Los servicios prestados por un CSIRT pueden dividirse en dos categorías: actividades en tiempo real directamente relacionados con la respuesta a incidentes, y actividades proactivas no en tiempo real, que soportan la tarea de respuesta a incidentes. La segunda categoría y parte de la primera categoría consisten en servicios que son opcionales en el sentido de que no todos los CSIRT los ofrecerán.

1.4.5.1 Respuesta a Incidentes

La respuesta a incidentes por lo general incluye la evaluación de los informes recibidos sobre incidentes (Evaluación de Incidentes) y el seguimiento de éstos con otros CSIRT's, proveedores de Internet y sitios (Coordinación de Incidentes). Un tercer nivel de servicios, ayuda a un sitio local para recuperarse de un incidente (Resolución de Incidentes), está compuesto por servicios típicamente opcionales, que no todos los CSIRT ofrecerán.

- **Informe de Evaluación de Incidentes (Triage)**: por lo general incluye:
  - **Informe de Evaluación**: la evaluación de los informes de incidentes, asignar prioridad a ellos, y relacionarlos a los incidentes en curso.
  - **Verificación**: ayuda a determinar si un incidente ha ocurrido realmente, así como su ámbito de aplicación.
- **Coordinación de Incidentes**: normalmente incluye:
  - **Categorización de la Información**: la categorización de los incidentes relacionados con la información (archivos de registro, información de contacto, etc.) con respecto a la política de divulgación de información.

- **Coordinación**: notificación a otras partes interesadas en una "necesidad de conocimiento", según la política de divulgación de la información.

- **Resolución de Incidentes**: Normalmente adicional u opcional, el servicio de resolución de incidentes incluye:
  - **Asistencia Técnica**: esto puede incluir el análisis de los sistemas comprometidos.
  - **Erradicación**: la eliminación de la causa de un incidente de seguridad (la vulnerabilidad explotada), y sus efectos (por ejemplo, la continuidad del acceso al sistema por un intruso).
  - **Recuperación**: ayuda en el restablecimiento de los sistemas afectados y los servicios a su estado antes del incidente de seguridad.

1.4.5.2 Actividades Proactivas

Normalmente opcional o adicional, los servicios proactivos podrían incluir:

- **El suministro de Información**: esto podría incluir un archivo de vulnerabilidades conocidas, parches o resoluciones de los problemas del pasado, o listas de correo de asesoramiento.
- **Herramientas de Seguridad**: puede incluir herramientas para la auditoria de la seguridad del sitio.
- **Educación y Entrenamiento**.
- **Evaluación de Productos**.
- **Auditoría de Seguridad de la Web y Consulta**.

1.4.5.3 Formas de Reporte de Incidentes

El uso de los formularios de reporte hace que sea más sencillo para los usuarios y los equipos hacer frente a incidentes. El usuario puede preparar respuestas a varias preguntas importantes antes de que él o ella entren en contacto con el equipo, y por lo tanto pueda venir bien preparado. El equipo recibe toda la información necesaria a la vez con el primer informe y se proceda de manera eficiente.

Dependiendo de los objetivos y los servicios de un CSIRT en particular, se pueden utilizar múltiples reportes, por ejemplo formularios de reporte para nuevas vulnerabilidades los mismos que puede ser diferentes a los reportes utilizados para el reporte de incidentes.

Es más eficaz proporcionar los reportes a través de los servicios de información en línea del equipo. La ubicación de los reportes debe indicarse en el documento de descripción del CSIRT

Los punteros exactos que se les debe dar en el documento de descripción de CSIRT, junto con las declaraciones acerca del uso adecuado, y las directrices sobre cuándo y cómo utilizar los formularios. Si por separado las direcciones de correo electrónico son compatibles con la forma basada en el informe, deben ser enumeradas aquí de nuevo.

1.4.6 Clausula

Aunque el documento de descripción CSIRT no constituye un contrato, la responsabilidad puede concebirse del resultado de las descripciones de los servicios y propósitos. Se recomienda la inclusión de una cláusula que aclare su función al finalizar el documento.

En situaciones en que la versión original de un documento debe ser traducido a otro idioma, la traducción debe llevar una advertencia y una referencia al documento original, ejemplo:

> *"Aunque tratamos de traducir con cuidado el documento original del alemán al Inglés, no podemos estar seguros de que el documentos exprese las mismas ideas en el mismo nivel de detalle y la corrección. En todos los casos, donde hay una diferencia entre las dos versiones, la versión alemana prevalecerá."*

El uso y la protección de cláusulas se ven afectadas por las leyes y regulaciones locales, de los cuales cada CSIRT debe ser cuidadoso. En caso de duda el CSIRT debe comprobar la declaración de la cláusula con un abogado.

1.5. Conclusiones

- La convergencia de los sistemas multiplica exponencialmente los problemas de seguridad planteados. El equilibro es difícil, el espectro a cubrir es amplio y, como dificultad extra, el campo de trabajo es intangible. Esto hace necesario desarrollar técnicas y/o adaptar las existentes de forma tal de circunscribir nuestro trabajo de conseguir información dentro de un marco de seguridad.

- Cuando se diseña un sistema se lo hace en base a su operatividad y/o funcionalidad dejando de lado la Seguridad. Será necesario establecer una pertenencia y correspondencia entre las técnicas adoptadas conformando un sistema de seguridad; y no procedimientos aislados que contribuyan al caos general existente. Esto sólo puede lograrse al integrar la seguridad desde el comienzo, desde el diseño, desde el desarrollo.
- Las tecnologías involucradas en estos procesos condicionan las técnicas empleadas, los tiempos condicionan esas tecnologías y, paradójicamente, las legislaciones deben adaptarse a los rápidos cambios producidos. Esto hace obligatorio no legislar sobre tecnologías actuales, sino sobre conceptos y abstracciones que podrán ser implementados con distintas tecnologías en el presente y el futuro. Es urgente legislar un marco legal adecuado, no solo que castigue a los culpables sino que desaliente acciones hostiles futuras.
- Algunos pocos métodos realmente novedosos de infiltración ponen en jaque los sistemas de seguridad. Aquí, se prueba la incapacidad de lograr 100% de seguridad, pero también es hora de probar que los riesgos, la amenaza, y por ende los daños pueden ser llevados a su mínima expresión. Muchas veces basta con restringir accesos a información no utilizada o que no corresponde a los fines planteados. Otras veces la capacitación será la mejor herramienta para disminuir drásticamente los daños.
- La seguridad es un estado mental, la seguridad perfecta requiere un nivel de perfección que realmente no existe, y de hecho dudo que algún día exista, pero los riesgos deben y pueden ser manejables.
- El costo en el que se incurre suele ser bajo comparado con aquellos luego de producido un daño. El desconocimiento y la falta de información son el principal inconveniente cuando se evalúa la inclusión de seguridad como parte de un sistema.
- El desarrollo de software es una “ciencia” imperfecta; y como tal es vulnerable. Es una realidad, la seguridad involucra manipulación de naturaleza humana. Hay que comprender que la seguridad consiste en tecnología y política, es decir que su combinación y su forma de utilización determina cuan seguros son los sistemas. El problema de la seguridad no puede ser resuelto por única vez, es decir que constituye un viaje permanente y no un destino.

CAPÍTULO 2

Tipologías de Centros de Respuestas

Resumen.

Se describen los modelos organizacionales existentes para centros de respuesta a incidentes de seguridad de la información con el objetivo de unificar la terminología y obtener conocimiento en las formas de organización más comúnmente utilizadas. Asimismo se describen las principales ventajas y desventajas de cada modelo y se señalan las situaciones a las que mejor se adapta cada uno.

2. Modelos organizacionales de centros de respuesta a incidentes

Al crear un Centro de Respuesta a Incidentes de Seguridad es fundamental decidir el modelo organizacional a utilizar. La respuesta efectiva ante incidentes depende de una planeación precisa del modo de operación del centro de respuesta.

Al planear un centro de respuesta a incidentes debe definirse la estructura que tendrá de acuerdo a los objetivos, visión y misión del mismo. Existen muchos factores que deben tomarse en cuenta para definir el modelo adecuado de centro de respuesta. Entre esos factores, algunos fundamentales son:

- El ámbito de acción u operación
- Misión del centro de respuesta
- Servicios que se pretende proporcionar
- Posición del centro de respuesta en la estructura organizacional
- Cuáles serán las obligaciones y la autoridad del centro de respuesta
- Infraestructura actual e infraestructura necesaria
- Financiamiento de la operación del centro de respuesta
- Estructura del Centro de Respuesta

La estructura de un Centro de Respuesta depende del alcance y ámbito de acción del mismo dentro de una organización. Es importante definir un modelo organizacional adecuado para el Centro de Respuesta, de tal forma que se contemplen todas las operaciones que se realizarán. Seleccionar adecuadamente un modelo permite establecer métodos adecuados para tareas y servicios que van desde cómo reportar un incidente por algún miembro de la organización hasta

la restauración de los servicios afectados por un incidente de seguridad, incluyendo todo lo que ello implica, como la forma de responder al incidente y el proceso para el análisis de la evidencia.

2.1. Modelos de referencia

La estructura organizacional de un centro de respuesta a incidentes define aspectos como la ubicación física del centro de respuesta, su lugar en la organización y en la circunscripción y los mecanismos de interacción con ellas.

Hay cuatro (tres en realidad) categorías principales en lo que se refiere a estructuras de un Centro de Respuesta:

2.1.1 Equipo de seguridad

Este es un modelo bajo el cual una organización responde a incidentes de seguridad con los recursos humanos y materiales existentes sin que exista un equipo o centro dedicado para la respuesta a incidentes. Esto generalmente significa que la respuesta a un incidente se realiza por parte de la persona que administra los dispositivos o recursos involucrados en él. De este modo, la respuesta a los incidentes de seguridad de la información es muy heterogénea ya que, aunque podría contarse con algún tipo de guías básicas, el éxito en la respuesta al incidente depende en gran medida de la capacidad y habilidades de administradores de sistemas, de red, desarrolladores, etc. Con este tipo de modelo es complicada la implementación de mejores prácticas en la respuesta a incidentes, la investigación y seguimiento coordinados. Hay también muy poca retroalimentación sobre un incidente y, por tanto, el aprendizaje para robustecer la seguridad de la información es muy limitado.

2.1.2 Equipo de respuesta a incidentes centralizado.

En este modelo, existe un único equipo de respuesta a incidentes que se encarga del manejo de todos los incidentes. Es un modelo adecuado para organizaciones pequeñas y para aquellas organizaciones grandes cuya infraestructura tecnológica no esté en sitios geográficamente distantes. El centro de respuesta centralizado es el único punto de contacto en toda la organización para la respuesta a incidentes y reportes de vulnerabilidades.

2.1.3 Equipos de respuesta a incidentes distribuido.

En este modelo, la organización cuenta con varios equipos de respuesta a incidentes. Todos los equipos conforman el centro de respuesta. Se crean o definen equipos de respuesta a incidentes para responder incidentes específicos. Los equipos pueden crearse de acuerdo a segmentos lógicos o físicos. En este caso, los equipos de respuesta pueden crearse por cada división de la organización o bien por unidades geográficas. Es importante que todos los equipos estén coordinados por una unidad central que permita garantizar que el servicio de respuesta a incidentes que proporciona cada uno de los equipos es consistente con el de todos los demás y con el que la organización ha definido. Establecer una entidad de coordinación centralizada también facilita el intercambio de información entre los distintos equipos de respuesta, lo cual es fundamental en este modelo ya que puede haber incidentes en que deban integrarse de manera coordinada más de uno de los equipos de respuesta. Claramente, este modelo es más adecuado para grandes organizaciones o bien para aquellas que cuentan con varias unidades en diversos sitios geográficos.

2.1.4 Equipo coordinador.

Este modelo organizacional de centros de respuesta se refiere a un centro de respuesta que trabaja con otros centros de respuesta. Esto es, se trata de un equipo que proporciona asesoría e información a otros equipos de otras entidades sobre las que no necesariamente ejerce autoridad directa. El centro de respuesta coordina y facilita el manejo de incidentes entre varias organizaciones, que pueden ser internas y/o externas, que pueden incluir divisiones o subsidiarias de una organización, entidades de un mismo gobierno, organizaciones pertenecientes a un mismo dominio o dentro de un estado o país. Su función principal es proporcionar análisis de incidentes y de vulnerabilidades, soporte y servicios de coordinación. Una actividad importante de este tipo de centros es la generación de guías, boletines, mejores prácticas, avisos sobre soluciones para mitigar el impacto de incidentes y sobre recuperación luego de la ocurrencia de alguno.

2.2. Centros de Respuesta Existentes

Cuando se planea la creación de un nuevo centro de respuesta, es muy útil echar un vistazo a los centros que ya existen y que han operado por algún tiempo en alguna parte del mundo. Es muy probable que el centro que se planea crear tengo algo o mucho en común con alguno o

algunos de los centros que existen en la actualidad y en cuyo modelo puede basarse la planeación.

Las ventajas de revisar la estructura de los grupos existentes son varias. Por un lado, se puede contactar al centro existente para conocer cómo se formó ese centro de respuesta y cómo opera en su ámbito de acción, cuáles fueron los principales obstáculos en la creación y consolidación del centro de respuesta y, por supuesto, cuál es el modelo y la estructura bajo los que funcionan. Por otra parte, hay muchos grupos de respuesta que pueden tener la disposición inclusive de apoyar, a través de proporcionar asesoría, la creación del nuevo centro de respuesta. El apoyo puede resultar muy valioso pues se trata de experiencias probadas. Es importante saber, sin embargo, que no podemos delegar la responsabilidad de la planeación y creación del centro de respuesta a incidentes en otra organización ya que, como se ha mencionado, el éxito en la operación del centro depende de cubrir de manera efectiva las necesidades particulares para las que está siendo creado.

2.3. La circunscripción del centro de respuesta

Un factor importante para elegir el modelo organizacional para un centro de respuesta a incidentes es definir la circunscripción en la que tendrá cobertura. Al definir la circunscripción quedará claro si el centro de respuesta proporcionará servicio a entidades externas o solamente a la organización dentro de la cual se constituye. Esta definición depende de los objetivos para los cuáles se crea el centro de respuesta y no necesariamente tiene que ver con el sector de la sociedad al que pertenece la organización en la que se crea el centro de respuesta. Una organización comercial puede crear un centro de respuesta para vender el servicio de respuesta a incidentes o bien para atender sus necesidades propias en la materia. Lo mismo ocurre en otros sectores, como el de gobierno e incluso el educativo.

Un segundo factor fundamental para elegir el modelo organizacional y que tiene también que ver con la definición de la circunscripción para el centro de respuesta es la cobertura geográfica que tendrá. Si todo se encuentra concentrado en una misma ubicación geográfica, puede optarse por un esquema centralizado, mientas que si la cobertura incluirá ubicaciones geográficas distintas, seguramente deberá optarse por un esquema distribuido.

2.4. Misión del centro de respuesta.

La misión del centro de respuesta es una definición breve, clara y precisa del propósito y de la función del centro de respuesta. Con la definición de la circunscripción y de la misión del centro de respuesta, pueden delinearse los servicios y el alcance que tendrá cada uno de ellos. Con todos estos elementos, se va conformando la elección del modelo organizacional adecuado para el centro de respuesta

2.5. Autoridad

De acuerdo a la ubicación en la estructura organizational del centro de respuesta a incidentes y de acuerdo a los objetivos y misión para los que haya sido creado, puede variar la forma en que ejerce autoridad sobre las diferentes áreas de la organización. Esencialmente hay tres tipos de autoridad que un centro de respuesta puede tener sobre su circunscripción:

- Autoridad total
- Autoridad compartida y
- No autoridad.

La diferencia entre los tres tipos de autoridad reside en la toma de decisiones. Si el centro de respuesta tiene **autoridad total**, por sí mismo y de acuerdo a las circunstancias de un incidente de seguridad puede tomar medidas para manejar el incidente. En este caso podría decidir la desconexión de dispositivos para recolectar evidencia, por ejemplo.

En el caso de **autoridad compartida**, el centro de respuesta es partícipe de las decisiones sobre el manejo de incidentes y las acciones que de él deriven. Si bien no toma la decisión por sí mismo como en el caso de autoridad total, sí tiene voto en la decisión.

Finalmente, es posible que el centro de respuesta **no tenga autoridad** sobre su circunscripción y que su función sea sugerir acciones para el manejo de incidentes, para que las autoridades correspondientes decidan si se llevan o no a cabo. Aún en este caso, la aportación del centro de respuesta puede resultar fundamental sugiriendo acciones y advirtiendo los riesgos para la información de la organización de no llevarlas a cabo.

El nivel de autoridad que tendrá el centro de respuesta es decisión de la administración y es importante que quede bien definido para evitar mensajes equivocados al interior de la organización que eventualmente pueden disminuir la credibilidad del centro de respuesta.

2.6. Personal del Centro de Respuesta

La respuesta a incidentes para una organización, independientemente del modelo que se utilice, debe estar a cargo de una sola persona de la organización. Aplica también esta recomendación para aquellas organizaciones que contratan con una entidad externa todo el servicio de manejo de incidentes. En tal caso, la persona dentro de la organización que está designada como responsable de la respuesta a incidentes se encarga de vigilar el cumplimiento del contrato por parte del proveedor. En los otros dos modelos, lo que se hace es designar a un jefe o administrador del equipo de respuesta a incidentes y a un responsable sustituto en caso de ausencia del primero.

El trabajo del administrador o jefe incluye una amplia variedad de tareas entre las que están incluidas las de actuar como un medio de enlace entre el centro de respuesta a incidentes y la dirección de la organización u otras unidades y equipos dentro de la misma. También es el punto de contacto en materia de respuesta a incidentes con entidades externas. Algo en lo que debe trabajar el jefe o administrador del centro de respuesta es en la comunicación necesaria al interior y exterior de la organización para evitar situaciones de crisis por la interacción del personal. Dentro de sus funciones también es muy importante la responsabilidad de que el centro de respuesta cuenta con el personal, recursos y habilidades necesarias para brindar el servicio.

Dentro de las características deseables del jefe o administrador de un centro de respuesta a incidentes de seguridad están también el dominio de aspectos técnicos y habilidades de comunicación, tanto hacia afuera del equipo como hacia adentro, con el fin de mantener relaciones de colaboración efectivas con otros grupos de respuesta y de mantener al interior un buen ambiente de trabajo dentro de un equipo que conozca sus responsabilidades y esté comprometido con la organización.

Dependiendo del tamaño del centro de respuesta, es probable que se requiera de un responsable técnico (CTO) que domine los aspectos técnicos del servicio de respuesta a incidentes y tenga la responsabilidad última sobre la calidad técnica del trabajo desarrollado por todo el equipo del centro de respuesta. Es importante destacar que esta posición no es la misma que la de líder de un incidente, quien se encarga de coordinar las actividades, recolectar información de quienes atienden directamente el incidente, y procurar la atención de las necesidades del personal involucrado en la atención del incidente.

El personal que se encarga de desarrollar las cuestiones técnicas para la respuesta a un incidente debe tener excelentes habilidades técnicas, ya que ese aspecto es fundamental para el éxito en el servicio debido a que ese dominio de los aspectos técnicos es lo que finalmente inspirará confianza al interior de la organización sobre el trabajo del centro de respuesta a incidentes.

La imprecisión en el dominio técnico puede minar la credibilidad de todo el centro de respuesta y el no contar con las habilidades técnicas suficientes puede eventualmente hacer que un incidente empeore. El centro de respuesta a incidentes debe contar con personal que domine la administración de sistemas, la administración de redes de datos, programación, soporte técnico, detección de intrusos, análisis de vulnerabilidades, análisis de malware de manera general y otros mecanismos con que la organización cuente dentro de su infraestructura.

Cada miembro del personal debe ser hábil para resolver problemas y eso regularmente se logra a través de la experiencia y la transferencia de conocimiento. No todos los miembros del personal deben ser expertos en cada tema, pero sí es conveniente que pada cada área de las mencionadas haya al menos una persona con las habilidades suficientes para proporcionar apoyo en algún incidente crítico que involucre su área.

Algo que puede ayudar a robustecer las habilidades del personal sin tanta experiencia es un plan y programas de transferencia de conocimientos continuos, contar con referencias técnicas suficientes como libros, revistas, etc. Promover la participación del personal en tareas que motiven su superación como la elaboración de material didáctico, participar en la instrucción de talleres, evaluar, integrar y desarrollar nuevas herramientas para ayudar a los administradores de sistemas, mejorar el servicio de respuesta a incidentes, etc.

En algunas circunstancias, podría haber rotación entre el personal que participa en la respuesta a incidentes con otras áreas de la organización o dentro del mismo centro de respuesta, de tal forma que los miembros del centro de respuesta conozcan las actividades de las otras áreas con las que se interactúa frecuentemente, sus problemas más frecuentes y su ambiente de trabajo, así como las actividades que realizan sus propios compañeros dentro del ambiente de trabajo. Si bien esto no siempre es posible, al menos debe procurarse la interacción y la retroalimentación sobre las actividades de la organización y del propio centro de respuesta.

Para el desarrollo de habilidades y conocimientos del personal, también puede acudirse al intercambio con expertos de otras entidades y promover la retroalimentación e intercambio de conocimientos con esas entidades.

Además de las habilidades técnicas, el personal del centro de respuesta a incidentes también es deseable que cuente con otras habilidades como capacidad para trabajar en equipo, habilidades de comunicación, facilidad para expresarse, habilidad para escribir informes técnicos, etc. Si bien no todos los miembros pueden contar con todas estas habilidades, es importante identificar quiénes son las personas que sí las tienen y contar con personas con alguna de las características mencionadas. Las habilidades de comunicación (hablar, expresarse, escribir) son particularmente importantes debido al trato que existe en la respuesta a incidentes con diversas personas como las víctimas de un incidente, directivos, administradores y eventualmente autoridades de procuración de justicia. En general, en un incidente, el personal del centro de respuesta requiere persona con las habilidades mencionadas para establecer el trato adecuado con los directivos de la organización, los usuarios y con el público en general. Las habilidades de comunicación son también importantes para evitar la revelación de información sobre la investigación antes de que ésta haya concluido a los involucrados sin que ello afecte el curso mismo de la investigación.

Respecto a la forma de contratación de empleados, los centros de respuesta pueden utilizar alguno de los siguientes tres modelos:

2.6.1 Empleados

En este caso, la misma organización es responsable de toda la respuesta a incidentes de seguridad. En este caso es mínimo el soporte técnico y administrativo de parte de organizaciones externas.

2.6.2 Parcialmente empleados

Bajo este modelo, la organización delega una parte de las tareas de respuesta a incidentes en organizaciones externas. Con frecuencia, se contrata y delega en una entidad externa el monitoreo de dispositivos de detección. Entonces, el proveedor de servicios de seguridad administrados identifica y analiza actividad sospechosa y reporta al equipo de respuesta de la organización cada uno de los incidentes detectados.

Otro esquema que se utiliza con frecuencia bajo este modelo es que el centro de respuesta de la organización proporcionar una respuesta a incidentes básica y cuenta con contratos con alguna o algunas entidades externas para responder a incidentes mayores. El contrato puede ser para actividades de cómputo forense, análisis avanzado de incidentes, contención y erradicación y mitigación de vulnerabilidades.

2.6.3 Outsourcing

La organización delega toda la responsabilidad de respuesta a incidentes, regularmente a una entidad que trabaja en sitio. Este modelo se usa con frecuencia cuando la organización requiere contar con un centro de respuesta pero no cuenta en su planta laboral con personal calificado para desempeñar esas actividades.

2.7. Selección del modelo de centro de respuesta

Hay algunos aspectos importantes que deben tomarse en cuenta cuando se define el modelo de un centro de respuesta, tanto para la estructura como para la forma de absorber o delegar responsabilidades en terceros.

Definir si se requiere la disponibilidad 24x7 del servicio de respuesta a incidentes. La decisión sobre la disponibilidad está en función de la criticidad de la infraestructura. Proporcionar un servicio 24x7 implica que haya personal disponible para atender los incidentes todo el tiempo y que se pueda contactar cuando se requiera o incluso que se requiera la presencia todo el tiempo de personal del centro de respuesta.

Aquellas organizaciones con limitaciones presupuestales o bien, aquellas en que la infraestructura a proteger no requiera de la presencia de tiempo completo del personal de respuesta a incidentes, podría establecer contratos de medio tiempo o lo que convenga, de acuerdo a sus necesidades. Lo importante en este caso es establecer medios de comunicación adecuados para poder atender con prontitud los incidentes. La atención directa e inicial del incidente podría recaer en el personal de soporte o help desk, entrenado adecuadamente para proporcionar la respuesta inicial y asesorado por el personal de respuesta a incidentes. De este modo, la investigación inicial y la recolección de información recaería en el personal de soporte o help desk, por lo que es fundamentan que cuente con la preparación para ello.

Un punto más que es importante considerar cuando se estructura un centro de respuesta a incidentes de seguridad es que las actividades de respuesta a incidentes pueden ser muy estresantes. Es importante reclutar al personal preparado técnicamente pero también preparado para trabajar bajo condiciones estresantes. Generalmente, es deseable personal con alguna experiencia para responder adecuadamente en situaciones de estrés.

El costo es también un factor fundamental al momento de definir el modelo de organización, sobre todo si se va a proporcionar un servicio con disponibilidad 24x7. Hay algunos aspectos

muy importantes que no deben soslayarse cuando se definen los costos de operación de un centro de respuesta:

2.7.1 Costos

El personal de respuesta a incidentes debe ser constantemente capacitado y actualizado en diversas áreas de las Tecnologías de la Información (TI). Además de conocer sobre diversos aspectos de TI, el personal de respuesta a incidentes también debe conocer y operar las herramientas propias de la actividad de investigación y recolección de evidencia sobre los incidentes. Otros costos que es importante tener en cuenta son los que se refieren a la seguridad física del área de trabajo del centro de respuesta y los medios y dispositivos de comunicación.

2.7.2 Experiencia del personal

El manejo de incidentes requiere conocimiento especializado y experiencia en diversas áreas de TI. Por esta razón es importante evaluar si se cuenta o se está dispuesto a contratar personal especializado en las cuestiones que se tienen que ver con los riesgos identificados en la organización. Al respecto, es posible que personal externo (Outsourcing) especializado en respuesta a incidentes cuente con mayor experiencia que el personal de la organización en áreas como la detección de intrusos, análisis de vulnerabilidades, pruebas de penetración, etc. Las organizaciones que proporcionan servicios de seguridad administrados regularmente cuentan con herramientas de correlación de eventos con información eventualmente de diversos clientes, lo que les ayuda en ocasiones a identificar más rápidamente una amenaza que a un cliente por sí mismo. Por el otro lado, seguramente el personal técnico de la misma organización conoce mejor el ambiente de operación de la infraestructura tecnológica y eso es un factor muy valioso al momento de manejar un incidente, ante la necesidad de actuar con eficiencia y eficacia al momento de identificar adecuadamente las amenazas y descartar por ejemplo los falsos positivos.

2.7.3 Estructura organizacional

Algunas organizaciones tienen en su estructura organizacional unidades (divisiones, departamentos, subdirecciones, etc.) que trabajan de manera independiente. En tales circunstancias, debe evaluarse la posibilidad de contar con un equipo de respuesta para cada una de esas unidades, regulada por un centro de respuesta centralizado que se encargaría de establecer la

comunicación entre los demás equipos y de la implementación de prácticas estándares para todos los equipos definir las políticas de los servicios.

Cuando se contrata a una organización externa, ya sea parcial o totalmente para la respuesta a incidentes es necesario tomar en cuenta algunos aspectos importantes:

La calidad del trabajo, tanto actual como futura. Cuando se contrata a un tercero para hacer la función del manejo y respuesta a incidentes, es conveniente evaluar no sólo la calidad del servicio que pueda proporcionar en la actualidad, sino los planes y programas de mejora continua de esa organización. Si se va a contratar el servicio de respuesta a incidentes de esta manera, es conveniente establecer también acuerdos para vigilar la calidad del trabajo de la organización que se está contratando.

2.7.4 División de responsabilidades

Si se contrata a una entidad externa para el manejo de incidentes, es importante definir las responsabilidades y la autoridad sobre la operación de la infraestructura tecnológica de la organización. Generalmente no es deseable que una entidad externa sea quien finalmente tome decisiones sobre la operación tecnológica de la organización. Así, por ejemplo, cuando ocurre un incidente con algún servidor, es probable que el centro de respuesta a incidentes decida que lo que hay que hacer es desconectarlo de red. Sin embargo, seguramente la decisión sobre parar o no las operaciones es algo que debe caer en la responsabilidad de la propia organización. Este tipo de definiciones resultan de particular importancia cuando se contrata a un tercero para llevar a cabo toda la operación del manejo y respuesta a incidentes.

2.7.5 Protección de información confidencial

Es importante definir, en un contrato con una entidad externa que provea el servicio de manejo de incidentes, la información a la que tendrá acceso y cómo tendrá acceso. De acuerdo a la clasificación de la información dentro de una organizaciones deben establecerse controles específicos para que el proveedor del servicio pueda acceder a determinada información o bien, cómo deberá proporcionar la información sobre un incidente de tal manera que alguien dentro de la organización con los privilegios necesario para el manejo de información sensible o confidencial sea quien pueda dar seguimiento a una investigación a partir de la información proporcionada por el prestador del servicio de manejo de incidentes.

2.7.6 Falta de conocimiento específico sobre la organización

El conocimiento detallado sobre la operación y estructura de la organización es fundamental para un análisis preciso y para establecer la prioridad de los incidentes. Para que la operación de respuesta a incidentes funcione de manera adecuada de acuerdo a las necesidades de la organización, es necesario establecer canales de comunicación adecuados para intercambiar información entre el proveedor del servicio y la organización sobre los aspectos importantes relacionados con la respuesta a incidentes. Tal información puede incluir: recursos críticos, integración de nuevos dispositivos, modificaciones en sistemas de información, dispositivos y configuración de red, etc. Esta comunicación y actualización es fundamental para evitar que haya incidentes que se manejen de forma inadecuada o incluso incidentes que no estén contemplados por el prestador del servicio. Es importante tener en cuenta que problemas como los que se mencionan pueden ocurrir aún si el centro de respuesta es operado por personal de la misma organización si no existe la comunicación adecuada.

2.7.7 Falta de correlación de información

Para la respuesta a incidentes por parte de una entidad externa, es fundamental la correlación de eventos de diferentes fuentes. Para ello, es importante establecer un esquema bajo el cual la entidad externa accederá a la información generada por los diversos dispositivos de la infraestructura tecnológica, particularmente de monitoreo y control de seguridad, de la organización. Es importante definir los canales de comunicación adecuados para acceder a tal información y definir responsabilidades sobre la información recolectada. Mucha de la información puede ser crítica para la organización y su revelación podría implicar un riesgo para la misma.

2.7.8 Manejo de incidentes en diversas ubicaciones geográficas

En un contrato de servicio de manejo de incidentes por parte de una entidad externa es importante definir los tiempos de respuesta, como parte del acuerdo de nivel de servicio (SLA, por sus siglas en inglés), de tal forma que se defina en qué situaciones el proveedor estará presente físicamente en las instalaciones de la organización, en cuáles instalaciones exactamente y en qué tiempos.

Tener un equipo de respuesta a incidentes alternativo dentro de la organización. Si se contrata de forma externa el servicio de respuesta a incidentes de forma completa, es importante mantener personal con las habilidades básicas para proporcionar esta respuesta o bien, procurar una

capacitación básica constante para contar con esas habilidades. Por diversas razones, el servicio de una entidad externa podría no estar disponible en el momento de que ocurra algún incidente crítico de manera repentina, que ponga en riesgo la información y/o la infraestructura tecnológica de la organización. En caso de que ocurra un incidente de esta naturaleza bajo tales circunstancias, es importante que el personal técnico de la organización esté capacitado sobre cómo responder al incidente cuando no esté presente el prestador contratado para tal servicio, de acuerdo a los procedimientos que deben definirse en conjunto con el proveedor.

2.8. Dependencias dentro de las Organizaciones

Dentro de las organizaciones existe generalmente personal muy experto en el manejo de algunos aspectos técnicos y que conoce sobre el ambiente mismo en que éstos se operan dentro de la organización. Es fundamental para el centro de respuesta a incidentes de seguridad identificar a estas personas dentro de la organización ya que en algún momento puede requerirse su participación.

Además del personal técnico experto, la buena operación del centro de respuesta depende también de la participación, colaboración, apoyo e interacción con otras unidades dentro de la propia organización

2.8.1 Administración

De muchas maneras, la operación del centro de respuesta a incidentes de seguridad informática depende de la administración de la organización. Es la administración quien se encarga de establecer la política de respuesta a incidentes, el presupuesto, el personal. Sin apoyo de la administración, un centro de respuesta a incidentes simplemente no puede operar de forma satisfactoria. Por esta misma razón es importante definir en qué lugar de la estructura organizacional se establece el centro de respuesta a incidentes. Generalmente es conveniente que se conserve una independencia de las áreas propiamente operativas.

2.8.2 Seguridad de la información

La interacción del personal del centro de respuesta a incidentes con el personal dentro de la organización que se encarga de la seguridad de la información es fundamental, entre otras cosas porque es muy común que sea a través de ellos como se reciba la notificación de incidentes

de seguridad ocurridos. Además, ellos son quienes operan y monitorean los controles de seguridad de la infraestructura, por lo que en muchos de los incidentes se trabaja de manera conjunta.

2.8.3 Telecomunicaciones

Una de las áreas con quienes es fundamental mantener un punto de contacto permanente es Telecomunicaciones. Muchos de los incidentes de seguridad informática tienen que ver con el tráfico de red de entrada y salida, ya sea de voz o datos. Esto implica, con frecuencia, estar en contacto con los proveedores del servicio de Internet (ISPs), monitorear y eventualmente contener el incidente en el perímetro de la red o en coordinación con otras entidades involucradas en el enlace a Internet, etc.

2.8.4 Soporte técnico

Cuando se responde a un incidente de seguridad, el personal involucrado en el manejo del incidente requiere de la colaboración o de la consulta a los expertos en la operación de la infraestructura relacionada con el incidente. Quienes administran sistemas, la red y desarrollan software son aliados muy útiles para entender el ambiente de operación en que ocurrió el incidente y, por tanto, vale la pena tomar en cuenta su opinión al momento de tomar decisiones importantes sobre la infraestructura.

2.8.5 Departamento jurídico

Un incidente de seguridad informática puede derivar en un proceso administrativo dentro de la organización por algún abuso o falta a una política de seguridad o incluso llegar hasta un proceso legal ante autoridades de procuración de justicia. Por ello es importante apoyarse en un departamento jurídico que, por una parte, revise las políticas y procedimientos de respuesta a incidentes de tal forma que se ajusten al marco regulatorio correspondiente y, por otra, proporcionen asesoría y eventualmente se trabaje en conjunto para dar curso a un seguimiento legal derivado de un incidente de seguridad.

2.8.6 Relaciones públicas e institucionales (comunicación social)

Es probable que, por el impacto de algunos incidentes, deba proporcionarse información a los medios y, por tanto, al público en general. En tal caso, es conveniente buscar el apoyo de la

entidad encargada de las relaciones públicas, institucionales o comunicación social de la organización. Con ellos se puede definir la forma precisa en que deben emitirse comunicados de acuerdo a las políticas de comunicación establecidas en la organización. No hacerlo de este modo podría ocasionar que se divulgara información innecesaria que eventualmente podría confundir al público y/o perjudicar a la organización si la comunicación no está adecuadamente estructurada.

2.8.7 Recursos Humanos

Junto con el departamento jurídico, el departamento de recursos humanos es una entidad a la que es muy útil recurrir ante incidentes que tienen que ver con abusos o faltas a estatutos y normas de la organización.

2.8.8 Planeación de la continuidad del negocio

Si un incidente afecta o puede afectar significativamente las operaciones normales de la organización, es necesario involucrar en el manejo del incidente al personal o comités encargados de ejecutar los planes de continuidad del negocio. Finalmente, quienes conocen los riesgos identificados en el plan de continuidad del negocio asociados con cada activo que pueda verse afectado por un incidente son quienes mejor pueden ayudar a determinar acciones de contención que minimicen el impacto sobre las operaciones de la organización.

2.8.9 Seguridad física y administración de instalaciones

Para el manejo de algunos incidentes es posible que se requiera la colaboración de las personas responsables de la seguridad física y de control de las instalaciones. En algunos casos es necesario incautar equipos que se encuentran en alguna oficina o instalación cerrada bajo llave. O bien, durante la respuesta a un incidente es probable requerir el acceso a instalaciones específicas para buscar información sobre el incidente, evidencia, realizar el monitoreo de algún área específica, etc.

2.9. Equipo de Respuesta

2.9.1 Descripción general

Este modelo se refiere en realidad a la ausencia de un centro de respuesta a incidentes constituido como tal. Es un modelo bajo el cual una organización responde a incidentes de seguridad

con los recursos humanos y materiales existentes sin que exista un equipo o centro dedicado para tal efecto. Operar de este modo en la organización significa que la respuesta a un incidente se realiza por parte de la persona que administra los dispositivos o recursos involucrados en él.

Es muy complicado establecer adecuadamente niveles de servicios y la respuesta a los incidentes de seguridad de la información es muy heterogénea ya que, aunque podría contarse con algún tipo de guías básicas, el éxito en la respuesta al incidente depende en gran medida de la capacidad y habilidades de administradores de sistemas, de red, desarrolladores, etc. Con este tipo de modelo es complicada la implementación de mejores prácticas en la respuesta a incidentes, investigación y seguimiento coordinados. Hay también muy poca retroalimentación sobre un incidente y, por tanto, el aprendizaje para robustecer la seguridad de la información es muy limitado.

Una desventaja importante de este esquema es que la responsabilidad de atención a incidentes recae en el mismo personal encargado de implementar los mecanismos de seguridad de la información, administrarlos y monitorearlos. No existe una independencia en la investigación de un incidente y en algunos casos la información de la investigación sobre el incidente podría no ser precisa debido a que probablemente se busquen cubrir omisiones de la propia operación.

2.9.2 Características particulares

Como no es propiamente un centro de respuesta a incidentes, no tiene una estructura definida para su operación, ya que ésta se basa en las circunstancias en las que se presente cada incidente que requiera ser atendido. El equipo de respuesta como tal incluso se conforma ad hoc a las circunstancias del incidente.

Los reportes de incidentes no llegan de forma centralizada y en realidad el personal responsable de cada activo implementa sus propios mecanismos para reportar y clasificar incidentes de seguridad.

No hay un sistema centralizado sobre información de reportes y seguimiento de incidentes. La retroalimentación sobre los incidentes ocurridos es generalmente muy limitada. Poca o complicada coordinación para el manejo de incidentes que involucren a varias áreas de la organización.

2.9.3 Servicios

Bajo este modelo, los servicios que se pueden proporcionar son limitados y regularmente se enfocan únicamente a la respuesta a incidentes e incluso eso se cubre de manera limitada. Ya que el personal involucrado en el equipo de seguridad tienen otras responsabilidades, generalmente lo que buscará al manejar un incidente es investigar o identificar superficialmente las causas y buscar la manera de mitigar el impacto del incidente. Es muy frecuente que el equipo de seguridad realice una investigación superficial del incidente, identifique probables causas y consecuencias y tome medidas en función de esos hallazgos superficiales. Una investigación superficial podría llevar incluso a conclusiones equivocadas y, por tanto, a no implementar las medidas preventivas adecuadas para evitar que el incidente se repita.

Además del servicio de manejo de incidentes, también el equipo de seguridad es el encargado de realizar medidas correctivas como configuración y mantenimiento de dispositivos de seguridad en diversos puntos de la infraestructura de cómputo y telecomunicaciones de la organización.

La detección de incidentes de seguridad es algo que se cubre con un equipo de seguridad ya que muchas veces es parte de las obligaciones de operación del personal que puede integrar el equipo de seguridad.

Con este modelo normalmente no se cubren servicios adicionales al manejo de incidentes como los de alertamiento y emisión de boletines. Al no haber una coordinación centralizada es difícil que se desarrollen programas de capacitación y difusión para la prevención de incidentes de seguridad.

Incluso dentro del manejo de los incidentes, generalmente no se realizan análisis exhaustivos que involucren el análisis de vulnerabilidades, análisis de software malicioso, análisis forense, etc. Cuando se llevan a cabo, se desarrollan porque existe una necesidad ineludible para realizarlos y la eficacia con que se realicen depende de las habilidades del personal del equipo de seguridad.

2.9.4 Recursos

Este modelo no requiere de recursos humanos adicionales ya que delega la responsabilidad del manejo de incidentes en el personal existente. Tampoco se requiere infraestructura adicional ya

que en realidad no se conforma un centro de respuesta y por tanto no hay nuevo equipo ni sistemas que soportar. Es probable, acaso, que se requiera equipo adicional que no se solicita de forma planeada sino como consecuencia de algún incidente ocurrido para el cual podría ser útil equipo adicional.

2.9.5 Ventajas y desventajas

Probablemente la única ventaja de este modelo es que no requiere recursos adicionales ni nueva estructura para la organización. Las desventajas, en cambio, son muchas ya que la respuesta a los incidentes se daría de forma heterogénea, sin la previsión suficiente para responder de manera adecuada ante circunstancias críticas.

Con este modelo no se cuenta con un punto único de contacto dentro de la organización para el manejo de incidentes y tampoco con los elementos necesarios para verificar la calidad del servicio ni el beneficio para la organización de la respuesta a incidentes.

2.10. Equipo de respuesta a incidentes Centralizado

2.10.1 Descripción General

En este modelo existe un único equipo de respuesta a incidentes que se encarga del manejo de todos los incidentes. El centro de respuesta cuenta normalmente con personal administrativo y operativo dedicado 100% a los servicios que presta el centro, particularmente la respuesta a incidentes de seguridad. Al tener personal dedicado, hay una variedad de servicios adicionales que el centro puede proporcionar para definir e impulsar estrategias de seguridad de la información en la organización.

Es un modelo adecuado para organizaciones pequeñas y para aquellas organizaciones grandes cuya infraestructura tecnológica no esté en sitios geográficamente distantes. El centro de respuesta centralizado es el único punto de contacto en toda la organización para la respuesta a incidentes y reportes de vulnerabilidades.

2.10.2 Características particulares

El centro de respuesta centralizado debe estar cerca de la gerencia/administración en la estructura jerárquica de la organización, en un nivel alto en la toma de decisiones respecto al control de la información.

La administración/coordinación del centro debe procurar allegarse de personal especializado en todas las áreas necesarias para contar con personal calificado para evaluar situaciones de emergencia adecuadamente y capaz de realizar análisis y emitir recomendaciones acertadas sobre las medidas que deben tomarse.

No todo el personal que participe en el centro de respuesta tiene que ser de tiempo completo. Puede buscarse un esquema de asesorías/consultorías bajo demanda para algunas cuestiones muy especializadas.

El centro de respuesta debe definir canales de comunicación a través de los cuales pueden realizarse los reportes de incidentes por parte de los usuarios, estableciendo claramente los medios, formas y horas de servicio del centro. Debe tomarse en cuenta que los usuarios del centro de servicios pueden ser miembros de la organización pero también entidades externas u otros centros de respuesta con los que se establezca contacto.

2.10.3 Servicios

Los servicios de un centro de respuesta centralizado son muy similares a los de un centro de respuesta distribuido. Al existir una administración/coordinación central, se puede implementar de manera eficiente el servicio de respuesta a incidentes y las actividades que ello conlleva: respuesta en sitio, análisis de vulnerabilidades, análisis de software malicioso, análisis forense, seguimiento legal, etc., de acuerdo a cómo lo requiera el incidente.

Al contar con personal dedicado para el centro de respuesta, deben implementarse servicios de prevención y de detección de incidentes. Entre otros, pueden desarrollarse programas de difusión y capacitación orientados a generar conciencia y difundir medidas preventivas entre el personal de la organización, en todos los niveles. Pueden diseñarse mecanismos y dispositivos de detección de incidentes que implementen un servicio proactivo de alertas tempranas sobre amenazas de seguridad de la información.

La cabeza del centro de respuesta debe proporcionar información a la administración/gerencia sobre el desempeño del centro de respuesta incluyendo información estadística precisa sobre las características de las solicitudes de servicio y el seguimiento de cada caso.

Algunos servicios adicionales como evaluación de tecnología de seguridad, evaluación de riesgos, participación en auditoría de seguridad, implementación de mejores prácticas, consultoría,

investigación de nuevas amenazas, son viables para un centro de respuesta a incidentes centralizado.

2.10.4 Recursos

Un centro de respuesta distribuido se conforma por una administración central y miembros en diversas unidades físicas o lógicas. Dentro de la estructura central, debe contarse con:

- Administrador/coordinador del centro de respuesta
- Administrador de la infraestructura tecnológica propia del centro de respuesta
- Personal administrativo
- Personal técnico para el manejo de incidentes
- Personal especializado para servicios adicionales
- Desarrolladores de sistemas web

Otros recursos humanos que pueden requerirse son:

- Editores (para todas las publicaciones)
- Personal de relaciones públicas
- Personal jurídico
- Expertos técnicos adicionales

Este personal puede no formar parte de la administración central ni estar necesariamente distribuidos en áreas de la organización, sino participar con el centro de respuesta bajo demanda.

La organización debe tener en cuenta que el centro de respuesta requiere recursos humanos especializados, lo cual regularmente implica tener que pagar salarios altos por el nivel de capacitación y también por la responsabilidad que implica el manejo de incidentes de seguridad de la información.

Dentro de los recursos materiales que deben contemplarse para la creación del centro de respuesta distribuido están:

- Instalaciones físicas
- Equipo de oficina

- Equipos de cómputo y telecomunicaciones
- Probablemente equipo de cómputo portátil
- Equipo para recolección de evidencia (equipo de red, recolectores de tráfico, discos duros grandes, etc.)
- Equipo para almacenamiento de grandes cantidades de información para la evidencia digital recolectada en los incidentes

Además de los requerimientos en equipo, se requiere software especializado para proporcionar el servicios de respuesta a incidentes:

- Sistema de seguimiento (tracking)
- Software para cómputo forense
- Software para pentest
- Software para análisis de software malicioso

2.10.5 Ventajas y desventajas

Este modelo es el más estable para un centro de respuesta a incidentes pero también el que más recursos requiere. Se puede contar con personal experto que se vaya especializando y adquiriendo experiencia específica en el manejo de incidentes. Al ser personal dedicado el que conforma el centro de respuesta, se pueden desarrollar con facilidad iniciativas de mejora continua en los procesos y servicios.

Requiere un cambio en la estructura de la organización y eso no siempre es sencillo. Una desventaja respecto del modelo distribuido es que el personal del centro de respuesta no está involucrado en el ambiente de operación de la infraestructura tecnológica de la organización y, por lo tanto, regularmente en el manejo de incidentes se requiere de la colaboración del personal operativo.

2.11. Equipo de respuesta a incidentes Distribuido

2.11.1 Descripción general

En este modelo, la organización cuenta con varios equipos de respuesta a incidentes. Todos los equipos conforman el centro de respuesta. Se crean o definen equipos de respuesta a incidentes

para responder incidentes específicos. Los equipos pueden crearse de acuerdo a segmentos lógicos o físicos. En este caso, los equipos de respuesta pueden crearse por cada división de la organización o bien por unidades geográficas. El personal de los equipos de respuesta a incidentes puede estar asignado a tareas operativas pero colabora con el centro de respuesta cuando ocurren incidentes en su circunscripción. La otra posibilidad es que el personal que está geográficamente distribuido pertenezca directamente al centro de respuesta y por lo tanto reporte únicamente a él.

Es importante que todos los equipos estén coordinados por una unidad central que permita garantizar que el servicio de respuesta a incidentes que proporciona cada uno de los equipos es consistente con el de todos los demás y con el que la organización ha definido. Establecer una entidad de coordinación centralizada también facilita el intercambio de información entre los distintos equipos de respuesta, lo cual es fundamental en este modelo ya que puede haber incidentes en que deban integrarse de manera coordinada más de uno de los equipos de respuesta. Además, al haber una administración centralizada del centro de respuesta, hay un control de las operaciones de todo el centro de respuesta y también hay un medio de comunicación claro hacia la dirección y administración de la organización, lo cual es muy útil para la toma de decisiones de manera efectiva en medio de una crisis generada por un incidente de seguridad.

Claramente, este modelo es más adecuado para grandes organizaciones o bien para aquellas que cuentan con varias unidades en diversos sitios geográficos.

2.11.2 Características particulares

Para que el centro tenga funcionalidad jerárquica debe estar ubicado, en la estructura de la organización, cerca de la dirección. El centro de respuesta debe contar con un administrador / director y puede contar con un equipo que dependa directamente de él. Como se mencionó, el personal que participa en el centro de respuesta puede estar formalmente asignados a otras áreas. Si es el caso, puede haber algunas personas que sí dependan directamente del administrador/directos del centro de respuesta.

Los miembros del centro de respuesta pueden ser administradores de red, de sistemas, personal de soporte técnico, y también personal del departamento jurídico o del departamento de relaciones públicas. La organización debe decidir cuántos miembros conformarán el centro de respuesta.

Si el personal del centro de respuesta estará asignado a otras funciones de manera cotidiana, es necesario dejar claro cuáles son las circunstancias bajo las cuales responderá al centro de respuesta y, por tanto, en qué circunstancias reportará a cada jefe. Además, deberán establecerse claramente los canales de comunicación que permitirán tomar acciones del centro de seguridad de manera inmediata cuando un incidente ocurre. Debe definirse también que cuando se alerta sobre un incidente y sobre la necesidad de participación de algún miembro del centro de respuesta, éste debe dejar sus labores cotidianas para integrarse al manejo del incidente.

Respecto de los mecanismos para reportar incidentes, es importante definir si éstos deben realizarse de manera directa a la coordinación del centro de respuesta, ya sea de manera directa o a través de una mesa de ayuda, o bien estos podrían realizarse de manera local a través de los equipos distribuidos. Dependiendo de la decisión, debe capacitarse adecuadamente al personal necesario en el proceso de reporte, clasificación y asignación de incidentes de seguridad.

2.11.3 Servicios

En este esquema organizado y estructurado de un centro de respuesta, al existir una coordinación central, se puede implementar de manera eficiente el servicio de respuesta a incidentes y las actividades que ello conlleva: respuesta en sitio, análisis de vulnerabilidades, análisis de software malicioso, análisis forense, seguimiento legal, etc., de acuerdo a cómo lo requiera el incidente.

La cabeza del centro de respuesta debe proporcionar información a la administración/gerencia sobre el desempeño del centro de respuesta incluyendo información estadística precisa sobre las características de las solicitudes de servicio y el seguimiento de cada caso.

Además de los servicios principales de respuesta a incidentes, la coordinación central puede implementar programas de prevención en el que participen todos los miembros del centro de respuesta. El servicio de alerta y avisos de seguridad sí es algo que debe implementarse en este modelo y la responsabilidad de ese servicio debe ser de la administración del centro de respuesta.

Algunos otros servicios pueden implementarse en ocasiones específicas y dependiendo de la disponibilidad el personal que participa en el centro de respuesta: evaluación de tecnología, implementación de mejores prácticas.

2.11.4 Recursos

Un centro de respuesta distribuido se conforma por una administración central y miembros en diversas unidades físicas o lógicas. Dentro de la estructura central, debe contarse con:

- Administrador/coordinador del centro de respuesta
- Administrador de la infraestructura tecnológica propia del centro de respuesta
- Personal administrativo (al menos una persona)
- Analistas para el manejo de incidentes
- Otros recursos humanos que pueden requerirse son:
    - Editores (para todas las publicaciones)
    - Personal de relaciones públicas
    - Personal jurídico
    - Expertos técnicos adicionales

Este personal puede no formar parte de la administración central ni estar necesariamente distribuidos en áreas de la organización, sino participar con el centro de respuesta bajo demanda.

La organización debe tener en cuenta que el centro de respuesta requiere recursos humanos especializados, lo cual regularmente implica tener que pagar salarios altos por el nivel de capacitación y también por la responsabilidad que implica el manejo de incidentes de seguridad de la información.

Dentro de los recursos materiales que deben contemplarse para la creación del centro de respuesta distribuido están:

- Instalaciones físicas
- Equipo de oficina
- Equipos de cómputo y telecomunicaciones
- Probablemente equipo de cómputo portátil
- Equipo para recolección de evidencia (equipo de red, recolectores de tráfico, discos duros grandes, etc.)

- Equipo para almacenamiento de grandes cantidades de información para la evidencia digital recolectada en los incidentes

Además de los requerimientos en equipo, se requiere software especializado para proporcionar el servicios de respuesta a incidentes:

- Sistema de seguimiento (tracking)
- Software para cómputo forense
- Software para pentest
- Software para análisis de software malicioso

2.11.5 Ventajas y desventajas

Al contar con una administración centralizada del centro de respuesta, los servicios se implementan de manera coordinada bajo definiciones estandarizadas y con la participación de personal especializado.

Una ventaja del centro de respuesta distribuido es que se conforma de gente experta de diversas áreas y que, si se opta por el esquema de trabajo parcial para el centro, el personal puede ser un apoyo para el centro de respuesta y para la organización en la implementación de medidas de prevención y detección en las diversas áreas, ya que deberá ser permanentemente capacitado y actualizado en materia de seguridad informática por el centro de respuesta.

La desventaja que puede tener este esquema es que no siempre es fácil ni lo más conveniente asignar nuevas responsabilidades al personal que ya tiene tareas operativas asignadas. Puede ser difícil coordinar al personal que participa en el centro de respuesta a incidentes ya que probablemente tenga que responder a dos jefes. La comunicación efectiva puede ser una de las debilidades de este esquema si no se definen los medias adecuadas para establecerla.

2.9. Centro Coordinador

2.9.1. Descripción general

Un centro de respuesta de este tipo tiene como funciones principales coordinar y facilitar la respuesta a incidentes de seguridad de la información y el manejo de vulnerabilidades en una circunscripción regularmente amplia, que abarca más allá de la organización a la que pertenece el

centro de respuesta. Esto es, se trata de un equipo que proporciona asesoría e información a otros equipos de otras entidades sobre las que no necesariamente ejerce autoridad directa.

Dentro de las actividades que realiza un centro coordinador está el intercambio de información, la definición de estrategias para mitigar el impacto de las amenazas de seguridad informática emergentes y recomendaciones para la recuperación en caso de incidentes. Con frecuencia, un centro coordinador realiza investigación sobre nuevas amenazas.

Una actividad importante de este tipo de centros es la generación de guías, boletines, mejores prácticas, avisos sobre soluciones para mitigar el impacto de incidentes y sobre recuperación luego de la ocurrencia de alguno.

La importancia de este tipo de centros radica en la influencia que deben ejercer en la toma de decisiones de seguridad de la información para las diversas organizaciones de su circunscripción. Hay varios centros de respuesta coordinadores reconocidos en todo el mundo, entre ellos CERT/CC, JPCERT/CC, DFN-CERT, CERT-NL, AP-CERT, TF-CSIRT (TERENEA Task Force).

2.9.2. Características particulares

La circunscripción de un centro de respuesta coordinador puede incluir, por ejemplo, divisiones de una corporación, diversas entidades de un gobierno, un estado un país entero.

Como en el caso de un centro de respuesta centralizado, un centro coordinador normalmente opera con personal dedicado, una ubicación física central y una administración/dirección única. Requiere personal especializado en manejo de incidentes y las áreas que ello involucra, aunque también se puede operar bajo un esquema de tener un equipo técnico base y contar con la referencia de especialistas en diversas tecnologías que pueden pertenecer a las mismas entidades dentro de la circunscripción del centro coordinador.

Las funciones principales del centro son actuar como un centro de coordinación eficiente en diversos niveles de las organizaciones dentro de la circunscripción para dirigir las acciones de respuesta ante incidentes y amenazas de seguridad de la información. En cuanto a la difusión de información sobre amenazas en curso o potenciales, el centro coordinador debe realizar una recolección y síntesis de información para emitir comunicaciones a las organizaciones en su circunscripción.

De igual forma que los centros de respuesta centralizados y distribuidos, el centro coordinador requiere de canales bien definidos para el proceso de reporte de incidentes y procedimientos claros para la clasificación y asignación de incidentes de seguridad.

2.9.3. Servicios

El servicios principal de un centro coordinador de respuesta a incidentes es el manejo de incidentes y puede proporcionar apoyo y asesoría técnica en tareas asociadas al mismo como respuesta en sitio, análisis de vulnerabilidades, análisis de software malicioso, análisis forense, apoyo técnico en el seguimiento de incidentes ante alguna autoridad de procuración de justicia, etc. No todas las tareas asociadas al manejo de incidentes son desarrolladas por un centro coordinador, a diferencia de un centro de respuesta centralizado. Es importante recalcar que la función básica de este tipo de centros es coordinar los trabajos de respuesta y actúa en conjunto con otros centros de respuesta en cada una de las organizaciones que conforman la circunscripción. Entonces, las tareas asociadas al manejo en sitio de incidentes normalmente son responsabilidad de los centros de respuesta de cada organización, con apoyo o coordinación de un centro coordinador de respuesta a incidentes.

Además, debe proporcionar el servicio de alerta y comunicación sobre amenazas a la seguridad de la información a las divisiones u organizaciones en su circunscripción. Es particularmente importante la síntesis de la información técnica disponible de modo que se proporcione un valor agregado a la recopilación de información sobre amenazas. En base a información sintetizada y concreta se pueden emitir comunicaciones y publicaciones valiosas para mitigar el impacto de las amenazas en la circunscripción.

Otros servicios que proporciona un centro coordinador es el análisis de amenazas, que involucra tareas como el análisis de software malicioso y la detección proactiva de amenazas. Además, es conveniente que de forma cotidiana o eventual realice evaluación de tecnología para la seguridad de la información, así como la evaluación de mejores prácticas y estándares de seguridad de la información.

Al ser una referencia en materia de seguridad de la información en su circunscripción, es muy frecuente que los centros coordinadores observen la necesidad u oportunidad de desarrollar programas de capacitación en sus áreas de especialidad: manejo de incidentes, análisis de amenazas, implementación de tecnología de seguridad informática, implementación de mejores prácticas, etc.

2.9.4. Recursos

Un centro coordinador de respuesta a incidentes requiere de una estructura operativa que le permita desarrollar los servicios para los que fue creado. Requiere de recursos humanos y materiales especializados. Los recursos humanos que se requieren, incluyen:

- Administrador/coordinador del centro de respuesta
- Administrador de la infraestructura tecnológica propia del centro de respuesta
- Personal administrativo (al menos una persona)
- Analistas para el manejo de incidentes
- Especialistas en evaluación de tecnologías
- Expertos en la implementación de mejores prácticas
- Editores (para todas las publicaciones)
- Personal de relaciones públicas

Además, como en los otros modelos, debe contarse en el mismo centro de respuesta o como consultores externos o en alguna de las organizaciones de la circunscripción a:

- Personal jurídico
- Expertos en tecnologías específicas.

Tener ubicados a estos expertos permite al centro coordinador consultar puntos específicos del análisis de incidentes y de los contenidos de comunicación que se generen.

Dentro de los recursos materiales que deben contemplarse para la creación del centro de respuesta distribuido están:

- Instalaciones físicas
- Equipo de oficina
- Instalaciones para laboratorios de pruebas, incluyendo equipo de cómputo, telecomunicaciones, etc.
- Equipos de cómputo y telecomunicaciones
- Equipo de cómputo portátil

- Equipo para recolección de evidencia (equipo de red, recolectores de tráfico, discos duros grandes, etc.)
- Equipo para almacenamiento de grandes cantidades de información para evidencia digital recolectada en los incidentes

Además de los requerimientos en equipo, se requiere software especializado para proporcionar el servicios de respuesta a incidentes:

- Sistema de seguimiento (tracking)
- Software para cómputo forense
- Software para pentest
- Software para análisis de software malicioso

2.9.5. Ventajas y desventajas

Una de las principales ventajas de este modelo de centro de respuesta es que permite contar con un grupo de especialistas en manejo de incidentes de seguridad de la información trabajando de forma coordinada en un mismo sitio de tiempo completo. Además, al operan de manera transversal entre organizaciones, el aprendizaje de casos específicos puede ser aprovechado por las demás organizaciones de la circunscripción.

Una desventaja es que los especialistas del centro coordinador no están involucrados en la operación cotidiana de las organizaciones que conforman la circunscripción por lo que, si no se establece la comunicación adecuada de consulta técnica, es probable que algunas de las comunicaciones y recomendaciones del centro coordinador parezcan operativamente inviables.

Puede ser complicada la planeación de un centro coordinador de respuesta ya que la cobertura podría ser muy amplia y crecer eventualmente. Por ello puede ser difícil establecer el tamaño del equipo y los recursos que se requieren, además de los medios de financiamiento.

Además, no siempre es sencillo establecer una independencia del centro de respuesta respecto de la organización que lo impulsa o lo financia.

CAPÍTULO 3

Propuesta de Especialización de Funciones en el interior de un Centro de Respuesta a Incidentes Informáticos

Resumen.

En el presente capítulo se documenta una propuesta de Especialización de Funciones a implementar en el interior de un Centro de Respuesta a Incidentes de Seguridad Informática.

Esta propuesta considera cuatro aspectos:

- Segregación de Funciones
- Descripción de dichas Funciones
- Desarrollo de Manuales y Procedimientos
- Diseño de un Flujograma del Proceso de Gestión de Incidentes, *end to end*.

En la sección “Segregación de Funciones” se mencionan aquellas que componen el core de un Centro de Respuesta a Incidentes de Seguridad Informática, para describir luego cada una de ellas en la sección siguiente; posteriormente se brindan pautas recomendables a seguir para el “Desarrollo de Manuales y Procedimientos” dentro del Centro, culminando con la presentación de un Flujograma *end to end* que describe las diferentes acciones, políticas, procedimientos, funciones y procesos involucrados en la gestión de incidentes de seguridad.

3. Funciones en el interior de un Centro de Respuesta a Incidentes Informáticos

3.1. Introducción

En el interior de un Centro de Respuesta a Incidentes de Seguridad Informática [CERT-hb] identificamos varias funciones a cumplir por sus integrantes.

Dichas funciones deberían ser independientes del modelo organizacional adoptado por el Centro. Sí es factible que las mismas posean diferente grado de importancia en la actividad del Centro, condicionado esto al modelo seleccionado (el cual puede cambiar a lo largo de la vida del Centro). Ahondaremos más adelante en ello, apoyándonos en algunos ejemplos para fijar el concepto que se desea transmitir. Por otro lado existe una dependencia más marcada y más fácilmente identificable con los servicios que le brinda el Centro a su Comunidad Objetivo (o "Constituency"). Este aspecto también será profundizado más adelante.

Siempre resulta conveniente realizar el ejercicio de identificar las funciones en cada Centro, ya sea en el momento que se está concibiendo la idea de su formación así como también durante su vida como tal. El análisis en el momento de la "tormenta de ideas" previo a su creación puede ayudar incluso a enriquecer la discusión sobre el modelo organizacional más conveniente. La realización de dicho ejercicio durante la vida del Centro siempre resultará provechosa para analizar tanto el funcionamiento del Centro como los servicios ofrecidos a la Comunidad Objetivo. Incluso la propia dinámica del Centro y hasta la consideración de cambio de modelo organizacional motivará el replanteo de si la actual segregación de funciones es la adecuada.

Una de las claves del éxito de un Centro de Respuesta es tener dichas funciones claramente identificadas y estar preparados para reaccionar en tiempo y forma para modificar su concepción e incluso para contemplar otras nuevas.

También resulta clave para el buen desempeño del Centro de Respuesta que la segregación de funciones se la considere como lo que es, una distribución de tareas y una identificación de responsables y referentes de cada una de ellas, como una forma de organizar el trabajo dentro del Centro.

Frecuentemente se denomina en la bibliografía y artículos de la temática al Centro de Respuesta como Equipo de Respuesta, lo que no hace más que resaltar el espíritu que debe subyacer en todo Centro de Respuesta para que lleve adelante su tarea: ser un equipo. De nada servirá crear un Centro de Respuesta donde se convoque a los mejores a los que se

pueda acceder en cada función identificada, si no se logra una cohesión entre las personas que llevan adelante dichas funciones (responsables o no de ellas) y logran trabajar como un verdadero equipo. No se debe perder de vista que el servicio fundamental que brinda un Centro de Respuesta es la gestión de incidentes y en muchos casos la gestión de incidentes podrá estar rodeada de estrés, nervios, presiones de diversa índole, y situaciones y estados de ánimo que ponen a prueba la vinculación entre las personas; en caso de no ser esta la mejor o por lo menos muy buena, el equipo sufrirá algún tipo de fisura y más tarde o más temprano lo afectará y por lo tanto también a la Comunidad Objetivo, por afectar los servicios que aquel debe brindar a ésta.

Por lo tanto, debemos segregar las funciones del Centro de Respuesta y no las personas que lo integran.

Para fijar el concepto pensemos en los numerosos ejemplos que han habido a lo largo de la historia del fútbol mundial en el que clubes invirtieron millones de dólares o euros para la contratación de grandes estrellas y conformar su plantel profesional, pero terminaron fracasando frente a otros que sin "grandes nombres" lograron un conformar un verdadero equipo. Esos clubes que fracasaron quizás identificaron clara y correctamente las principales funciones a llevar adelante en la cancha: golero, defensa, carrilero, armador, delantero de área, punta "por afuera" y para cada función, salieron a buscar al mejor y lo contrataron, pero nunca pudieron plasmar un verdadero equipo, porque en las actividades colectivas nunca la suma de los mejores esfuerzos redunda en el mejor resultado si no se complementa con una adecuada coordinación, vinculación y una clara definición de objetivos y estrategias para lograrlos.

Una práctica altamente recomendada en toda actividad colectiva (como es el caso de un Centro de Respuesta) es que la vinculación entre sus diferentes integrantes no sea únicamente técnica y siempre haciendo énfasis en la cadena de mando. Se deben fomentar así actividades sociales que fortalezcan la vinculación de los miembros del Centro, sus familias y amigos. Resulta así muy positivo que se compartan momentos de distensión como ser organizar comidas, reuniones, actividades deportivas, asistencia a eventos culturales y/o deportivos entre otras, donde se puedan fortalecer los vínculos entre ellos, lo que además de ser beneficioso para las personas, seguramente también lo será para el funcionamiento del Centro. En estos casos es conveniente la tarea (nada sencilla) que durante dichas actividades no se comenten aspectos vinculados al trabajo en el Centro de Respuesta. Es de destacar que hay un aspecto que juega a favor de que ello no ocurra y es que mucha de la información que se maneja en el Centro está clasificada como confidencial y por otro lado, es habitual

que sus integrantes firmen un NDA (Non-Disclosure Agreement), al que en la región también se le conoce como Compromiso de Confidencialidad, por lo que también por esa vía se verán impedidos de realizar comentarios, incluso a su familia. Finalmente, aunque no por ello menos importante, puede resultar muy positivo para todo el equipo que las personas que tienen a su cargo las funciones de dirección del Centro se desprendan por unas horas de dicho rol y asuman otro completamente distinto, buscando ser uno más en la actividad a realizar; por ejemplo que el Director del Centro tenga la iniciativa de: “yo me encargo de reservar la cancha para el partido de fútbol y mi señora de comprar lo que vamos a comer”.

Por otro lado, la propia esencia de los servicios que brinda un Centro de Respuesta implica que a veces la disponibilidad de sus integrantes se deba requerir fuera del horario “de oficina”. Esta modalidad de trabajo se debe contemplar de alguna forma, pudiendo ser mediante incentivos económicos, flexibilidad horaria u otros, e incluso con una combinación de ellos. Este tipo de prácticas ayudan a fidelizar a los integrantes del Centro ya que se sienten más cómodos en su trabajo cotidiano y les permite llevar adelante su vida privada de una manera adecuada.

3.2. Las Funciones

Las funciones identificadas en la presente propuesta son las siguientes:

- Directorio
- Director Ejecutivo
- Comité Ejecutivo
- Gerente Operacional
- Logística
- Investigación
- Legal
- Gestión de Incidentes
- Embajadores
- Formación Continua
- Comercial
- Financiero y Económico

Los nombres de cada una de las funciones, si bien son ampliamente difundidos, no significan ninguna regla a respetar y deben ser considerados como una posible referencia a seguir.

No es habitual encontrar un Centro de Respuesta que cuente con una persona física para cada una de las funciones mencionadas, y menos aún si se intenta realizar dicha asociación en el momento de la creación del mismo, por lo que la mayoría de los Centros nacen con un equipo de integrantes donde cada uno tiene la responsabilidad en más de una función, siendo posible que a medida que el Centro se afianza en su actividad pueda incorporar más integrantes y así tender a una relación más biunívoca entre funciones y personas.

3.2.1 Descripción de las Funciones

Para cada una de las funciones enumeradas en la sección 3.2. se ofrecerá a continuación una descripción, proporcionándose además un detalle de diferentes formas en que se pueden vincular entre sí.

3.2.1.1 Directorio

Un Centro de Respuesta podrá contar con un Directorio como componente más alto en el organigrama del mismo. En caso de existir, en general sus funciones estarán asociadas principalmente a aspectos políticos y de vinculación quizás con el gobierno, buscando brindar al centro el apoyo y el nexo político que pueda requerir.

Sus integrantes deberían ser miembros reconocidos en la comunidad donde actuará el Centro de Respuesta. Puede resultar conveniente que el Director Ejecutivo sea miembro del Directorio o que en su defecto, pueda ser convocado a las reuniones que se realicen. A priori no aparece como adecuado que un integrante del Comité Ejecutivo que no sea el Director Ejecutivo sea quien asista a las reuniones del Directorio, pues le agrega complejidad a la logística de las reuniones y no se trata de la persona que en ese momento está en contacto más directo con el resto de los integrantes del Centro.

La frecuencia de las reuniones del Directorio no debería ser muy alta (no menor a dos meses) pues los temas a tratar son en general de líneas estratégicas de ejecución a mediano o largo plazo.

3.2.1.2 Director Ejecutivo

Todo Centro de Respuesta deberá identificar quién (o quienes) tendrá a su cargo la función de Director Ejecutivo. Ésta función deberá recaer en una (o varias) persona con capacidad de mando, liderazgo y motivación claramente demostrable e identificable.

Quien lleve adelante dicha función debería estar capacitado y entrenado en el área de gestión de incidentes de seguridad así como en la gestión de proyectos y gestión empresarial. Ello no implica que cuente con las mejores certificaciones en las áreas mencionadas, pero sin duda que el tenerlas, redunda en un beneficio para el Centro en su operativa diaria, motiva a sus integrantes a capacitarse y entrenarse y presenta una mejor imagen del Centro frente a la Comunidad Objetivo.

Mencionamos en el párrafo anterior la posibilidad de que la función de Director Ejecutivo pudiera recaer en más de una persona. Con ello se quiere significar que la Dirección del Centro puede estar a cargo de un Comité Ejecutivo quien designa a uno de sus integrantes como Director Ejecutivo pro tempore (por un tiempo). En caso que el mando del Centro de Respuesta se organice de esta manera, resulta fundamental que el resto de los integrantes del Centro conozca de antemano y con una antelación razonable quién tendrá a su cargo la función de Director Ejecutivo y por cuánto tiempo. No es recomendable, salvo por causas debidamente justificadas, cambiar el Director Ejecutivo cada poco tiempo, por ejemplo cada un año, pues entre otros inconvenientes la logística no es sencilla y tanto para el resto de los integrantes del Centro como para la Comunidad Objetivo puede terminar siendo no la mejor imagen del mismo.

En caso de existir un Comité Ejecutivo, resulta fundamental que el mismo brinde una imagen homogénea y sin fisuras hacia el Centro y hacia la Comunidad Objetivo, siendo la situación ideal aquella en la que el Centro brinda todos sus servicios, en particular la gestión de incidentes de la misma forma, sin importar quién esté circunstancialmente ocupando el cargo de Director Ejecutivo. Podemos fijar este concepto con una situación no deseada, que sería por ejemplo el caso en que un integrante de la Comunidad Objetivo espera ansiosamente el cambio de Director Ejecutivo para contactar al Centro ante determinada inquietud o propuesta.

El Director Ejecutivo debe mantener reuniones periódicas con el resto de los integrantes del Centro de Respuesta o con algún representante de ellos (que debe ser miembro del Centro), con una frecuencia que no debería ser menor a una vez por semana. Sumado a ello, es recomendable que el Director tenga un contacto diario con ellos, pero no como una herramienta de presión y de “establecer presencia”, sino como una manera de estar al tanto de la

actividad del Centro y ofrecer el apoyo que el resto de los integrantes necesitan por el tenor de la actividad que realizan.

El Director Ejecutivo, en caso de existir el Comité Ejecutivo, debería elaborar un documento a presentar a cada uno de sus integrantes ("informe"), donde como mínimo se debería incluir:

- Reporte de actividades del Centro desde la última reunión
- Inquietudes surgidas en el Centro desde la última reunión
- Identificación de necesidades del Centro
- Planteos recibidos desde la Comunidad Objetivo
- Información relevante para el Centro, obtenida por vías formales e informales
- Propuesta de acciones futuras

Dicho documento se puede elaborar en conjunto con el resto de los integrantes del Centro o con un representante de ellos. Si el Comité Ejecutivo no existe dicho informe puede ser útil para presentar al Directorio (si existe).

El documento mencionado servirá como agenda para la reunión del Comité Ejecutivo y es recomendable que sea elaborado y distribuido, con las medidas de seguridad necesarias, con cierta antelación (por ejemplo dos días hábiles antes de la reunión) de forma que el resto de los integrantes del Comité dispongan de un tiempo prudencial para concurrir a la reunión con un conocimiento previo de los temas a tratar y que la misma resulte más provechosa.

Adicionalmente es altamente recomendable que se elabore un acta de la reunión del Comité Ejecutivo. La misma no tiene porqué ser distribuida al resto de los integrantes del Centro pero se debe asegurar que los mismos estén en conocimiento de aquellas decisiones relevantes para el funcionamiento del Centro y para el trabajo de cada uno de sus integrantes.

Podemos asociar, pero no con extrema rigurosidad, que el Director Ejecutivo estará más ligado a la "Misión" del Centro de Respuesta.

3.2.1.3 Comité Ejecutivo

La dirección ejecutiva de un Centro de Respuesta podrá recaer en un conjunto de Directores Ejecutivos actuando uno por vez con la función de Director Ejecutivo. Es recomendable que el número de integrantes del Comité Ejecutivo sea impar, para que la toma de algunas decisiones se pueda realizar por votación, aunque siempre es conveniente buscar el consenso y

fomentar el diálogo y no la imposición. En caso se tratarse de un número par de personas, puede adoptarse el criterio de que el voto del Director Ejecutivo actual valga doble.

En caso de existir el Comité, es recomendable que realice reuniones periódicas para que todos sus integrantes conozcan de primera mano la marcha del Centro y se analicen planteos e inquietudes que pudiesen llegar por diferentes vías, formales y no. Se entiende que un período razonable para las reuniones del Comité Ejecutivo es 15 o 30 días. Un tiempo menor podría llegar a ocasionar un desgaste excesivo para sus integrantes y una pérdida de eficiencia de cada reunión, por ejemplo por ausencia de algunos de sus integrantes ("está llloviendo, hoy no voy a la reunión del Comité, no importa tanto, igual nos reunimos dentro de dos días otra vez") y un tiempo mayor puede llegar a tener como consecuencia negativa el hecho que los tiempos de la actividad del Centro y los tiempos de respuesta requeridos por la Comunidad Objetivo no están acompasados con la frecuencia de reuniones el Comité Ejecutivo ("hace tres semanas que planteamos la necesidad de un plan de capacitación pero como el Comité Ejecutivo se reúne recién dentro de un mes y yo en quince días tengo que confirmar o no el gasto, tendré que buscar otra alternativa"), lo que puede terminar generando molestias, pérdida de integrantes de la Comunidad Objetivo, deterioro de la imagen del Centro y poniendo el riesgo su actividad de futuro.

También resulta importante que se contemple un mecanismo de convocatoria del Comité en carácter de grave y urgente ante hechos que así lo ameriten. Puede ocurrir que alguno de sus integrantes no pueda estar presente físicamente, por ejemplo, por encontrarse distante de las oficinas del mismo y sin la posibilidad de llegar a tiempo a la reunión citada o por encontrarse indispuesto en su hogar; en dicho caso resulta aconsejable un adecuado uso de las TICs, por ejemplo realizando una videoconferencia con las medidas de seguridad requeridas en estos casos, ya que si la reunión es convocada en carácter de grave y urgente es porque la temática de la misma es muy delicada y puede requerir de confidencialidad.

En caso de existir el Directorio, un representante del Comité Ejecutivo (preferentemente el Director Ejecutivo) debería elaborar un documento ("informe") a presentar a cada uno de sus integrantes, donde como mínimo se debería incluir:

- Un resumen de la información contenida en los documentos "agenda" y "acta" elaborados en el contexto del Comité Ejecutivo (si existe) o en su defecto un documento que reúna las cosas más importantes ocurridas en el seno del Centro desde la última reunión del Directorio
- Inquietudes o planteos que se vinculan a la función del Directorio

Dicho documento se puede elaborar en conjunto con el resto de los integrantes del Comité Ejecutivo.

El documento mencionado servirá como parte de la agenda para la reunión del Directorio y es recomendable que sea elaborado y distribuido, con las medidas de seguridad necesarias, con cierta antelación (por ejemplo dos días hábiles antes de la reunión) de forma que los integrantes del Directorio dispongan de un tiempo prudencial para concurrir a la reunión con conocimiento previo de los temas a tratar y que la misma resulte más provechosa.

Adicionalmente es altamente recomendable que se elabore un acta de la reunión del Directorio. La misma no tiene porqué ser distribuida al resto de los integrantes del Centro pero se debe asegurar que los mismos estén en conocimiento de aquellas decisiones relevantes para el funcionamiento del Centro y para el trabajo de cada uno de sus integrantes.

3.2.1.4 Gerente Operacional

Dentro de un Centro de Respuesta podemos identificar la función de Gerente Operacional. Se trata de una función en general siempre presente pero no siempre formalizada. Podemos asociar dicha función a aquella persona que tiene la visión más general y completa de la actividad del Centro, pero más cercana a la operación día a día del mismo. Adicionalmente suele ser la persona que tiene la tarea de representar al resto de los integrantes del Centro frente al Director Ejecutivo.

La función de Director Operacional puede ser desempeñada por una única persona o se puede rotar entre algunos o todos los integrantes del Centro. En caso de utilizar el mecanismo de rotación, es recomendable tener siempre el objetivo de que la función como tal se cumpla de la misma manera, siendo lo ideal que, para el Director Ejecutivo, resulte transparente quién la desempeña en determinado momento.

De haber rotación, y para no agregar demasiada complejidad a su gestión, la frecuencia de la misma no debería ser mayor a, digamos, una vez cada tres meses.

Como fortaleza de la función, podemos indicar que la presencia del Gerente Operacional sirve para organizar la vinculación entre el equipo técnico del Centro y el Director Ejecutivo. Su existencia permite que ambos tengan un punto de referencia para sus inquietudes facilitando el diálogo entre las partes.

Como debilidad podemos mencionar dos: una asociada a utilizar el mecanismo de rotación, por lo complejo que puede resultar su implementación, y otra asociada a no utilizar el mecanismo de rotación. En los Centro de Respuesta es relativamente frecuente que sus integrantes realicen diversas tareas y se roten en las mismas a lo largo del tiempo, este es un mecanismo utilizado para intentar que todos tengan un panorama general de cómo funciona el Centro, sirve para que “no siempre los mismos realicen las tareas más ingratas”, como estrategia de motivación y para conseguir más de una óptica sobre un mismo aspecto. La no realización de la rotación en la función del Gerente Operacional nos priva de los beneficios mencionados. Por otro lado, la elección del mismo es usual que surja del equipo técnico que compone el Centro, por lo que de ser así, debe ser una decisión fruto de un análisis profundo. Haciendo una analogía entre un Centro de Respuesta y una fábrica, el Gerente Operacional podría compararse con un Jefe de Producción, quien sabe todo lo que sucede, quien tiene un panorama general de cómo está funcionando el sistema, identifica y recibe los requerimientos de quienes trabajan allí, se vincula con la Alta Gerencia y traslada a los operarios las inquietudes de aquella y a aquella los de estos.

El Gerente Operacional debe fomentar siempre la noción de equipo dentro del Centro, aunque cada uno de sus integrantes esté realizando una actividad específica. Para ello es importante que todos los integrantes conozcan qué temas están llevando cada uno, siendo suficiente para ello una reunión informal, de pocos minutos de duración y la necesidad de documentos formales donde cada uno de los integrantes comente sus tareas actuales. Es usual que de éstas reuniones surjan iniciativas de colaboración de los integrantes entre para casos específicos y respuestas que se logran simplemente por comentar las inquietudes de cada uno.

3.2.1.5 Difusión

Todo Centro de Respuesta debe identificar la persona que tendrá a su cargo la responsabilidad de toda la actividad de difusión del mismo. Entendemos por ello todas las formas de comunicación posibles con diversos actores, como ser los integrantes de la Comunidad Objetivo, otros Centros de Respuesta, prensa, entre otros.

Ésta función no implica que toda comunicación con los actores mencionados debe ser validada previamente por quien asuma dicha responsabilidad, pero sí significa que dicha persona debe trabajar para que se definan y documenten pautas claras a seguir en cada uno de los casos.

Los objetivos fundamentales de la función de difusión de un Centro de Respuesta son:

- Hacer conocer la existencia del Centro
- Difundir a la Comunidad Objetivo información que puede resultar de su interés
- Fomentar la Capacitación y Entrenamiento de los integrantes de la Comunidad Objetivo

A continuación analizaremos cada uno de los objetivos mencionados

Al hacer conocer la existencia del Centro de Respuesta se busca la captación de potenciales nuevos integrantes de la Comunidad Objetivo así como también la identificación de necesidades no satisfechas de ella y la definición clara de los servicios brindados por el Centro y cómo acceder a los mismos. Las formas de hacer conocer la existencia del Centro son variadas. Una lista no exhaustiva es: organización de conferencias, seminarios, talleres de capacitación y entrenamiento, presencia en Internet en varias formas posibles (sitios web, RSS, listas de correo) donde se pueda tanto poner a disposición de todos información que puede resultar de interés como también, mediante el cual se pueda recibir las inquietudes de las personas, por ejemplo, completando un formulario o enviando un mensaje de correo electrónico a una dirección destinada a ello.

La difusión de información que puede resultar de interés para la Comunidad Objetivo puede ser una actividad tanto reactiva como proactiva. Puede ocurrir que la Comunidad Objetivo, o parte ella, le haya hecho saber previamente al Centro sobre los aspectos que les sería de interés estar informada (por ejemplo, vulnerabilidades de determinado producto) y el Centro de Respuesta implemente un procedimiento para cumplir con dichas expectativas (con costo o no para la Comunidad Objetivo); puede darse el caso que la misma información u otra, sea difundida al resto de los integrantes de la Comunidad Objetivo (con o sin costo para ella) si se cuenta con la autorización correspondiente. Por otro lado, puede ocurrir que el Centro de Respuesta, por iniciativa propia comience a difundir información que intuye o tiene la certeza que será de interés para la Comunidad Objetivo.

La actividad de Capacitación y Entrenamiento es útil, por un lado para generar un expertise en la Comunidad Objetivo que le será muy útil a la hora de enfrentar un incidente de seguridad, que los puede motivar a crear Centros similares y que le permitirá a los integrantes del Centro interactuar de mejor forma con los integrantes de la Comunidad Objetivo en el momento de gestionar un incidente de seguridad; por otro lado, puede serle útil al Centro como una forma de autofinanciarse y de posicionarse frente a la Comunidad Objetivo como un punto de referencia en la temática. La actividad de Capacitación y Entrenamiento no debe quedar circunscripta solamente a aspectos puramente técnicos, pudiendo ser muy enriquecedor para

ambas partes realizar talleres donde la Comunidad Objetivo encuentre un ámbito donde plantear sus inquietudes al Centro de Respuesta, por ejemplo, relacionadas a la forma de vincularse.

A continuación analizaremos las actividades de difusión en función de los actores mencionados:

- **Comunicación con la Comunidad Objetivo**

La misma siempre ser realizada en un tono respetuoso, intentando ponerse a la par de los conocimientos técnicos de la persona con la que se interactúa, con un alto espíritu de colaboración y con la libertad de tutear o no según se entienda oportuno. El Código de Ética es fundamental para establecer cómo vincularse.

En caso de estarse comunicando con varios integrantes de la Comunidad Objetivo, se debe evaluar y decidir si es conveniente que unos deduzcan quienes son los otros que están recibiendo la misma información. Salvo que se trate de personas que pertenezcan a la misma unidad de trabajo (e incluso tampoco en ese caso) es necesario ofrecer anonimato. Por ejemplo, ocultando las direcciones de correo electrónico de los destinatarios de un mensaje de correo electrónico.

- **Comunicación con otros Centros de Respuesta**

Fomentar la misma es de suma utilidad para todas las partes involucradas. Basta pensar en una realidad que cada vez nos golpea más fuerte, como es que los incidentes de seguridad traspasan fronteras de países y de redes empresariales, por lo que muchas veces un punto de contacto en el que confiamos puede resultar muy útil a la hora de gestionar un incidente de seguridad. Por otro lado la pertenencia a grupos de Centros de Respuesta propicia que se genere un ámbito donde entre pares se pueda intercambiar conocimiento para los servicios que brinda cada Centro. Conviene así analizar la posibilidad de ser miembros de foros como FIRST [FIRST] y asistir a conferencias de Centros de Respuesta como ser FIRST-TC [FIRST-TC] para fomentar y fortalecer estas redes de confianza entre Centros.

- **Comunicación con la prensa**

La esencia de la existencia de la misma puede resultar una cáscara de banana para el Centro de Respuesta. Es muy probable que la mejor noticia en materia de seguridad para la prensa esté vinculada al incidente más delicado que se esté gestionando en el Centro. Probablemente el responsable de Difusión no sea quien entable contacto con la prensa y quizás lo sea el Director Ejecutivo, pero sí es responsabilidad de aquel que tiene la posición frente a la prensa sea uniforme en todo el Centro, concientizando a todos sus integrantes de no ofrecer

flancos débiles por donde se pueda filtrar información, incluso antes técnicas elaboradas de Ingeniería Social.

El responsable de la Difusión deberá fomentar que la misma brinde una imagen única del Centro según el grupo de destinatarios (Comunidad Objetivo, Centros de Respuesta, prensa).

3.2.1.6 Infraestructura

En cualquier Centro de Respuesta encontraremos infraestructura que sirve como sustento para los servicios que se brindan. Habrá tanto infraestructura "de cara a la Comunidad Objetivo" como también "de uso exclusivo interno", y en ambos casos nos referimos a toda la tecnología de red, servidores, estaciones de trabajo, notebooks, equipamiento de laboratorio, de análisis forense, de análisis de artefactos, de preservación de evidencia, etc. La complejidad de la infraestructura podrá diferir mucho de un Centro a otro, pero ninguno podrá obviarla y por lo tanto, deberá administrarla.

Dicha responsabilidad deberá recaer en una persona con la debida capacitación e idoneidad para llevar la tarea adelante.

3.2.1.7 Triage

El servicio que determina la propia razón de la existencia de un Centro de Respuesta es la gestión de incidentes de seguridad. Dicha gestión involucra en sus etapas más tempranas la realización de la función de Triage. El concepto de triage no es exclusivo de la gestión de incidentes, aplicándose a otras áreas, como la medicina. Para comprender cabalmente qué implica y las posibles consecuencias de realizarlo correctamente o no puede resultar un buen ejercicio comentar su utilización en el área mencionada.

En la medicina de emergencias y desastres se efectúa triage para la selección y clasificación de los pacientes basándose en las prioridades de atención privilegiando la posibilidad de supervivencia, de acuerdo a las necesidades terapéuticas y los recursos disponibles. Este término se emplea para la selección de pacientes en distintas situaciones y ámbitos, en situación normal en las urgencias extra-hospitalarias y hospitalarias, y en situaciones de demanda masiva, atención de múltiples víctimas o de desastre. En situación normal se privilegia la atención del paciente más grave, el de mayor prioridad, por ejemplo: paro cardíaco. En situaciones de demanda masiva, atención de múltiples víctimas o desastre se privilegia a la víctima con mayores posibilidades de supervivencia según gravedad y la disponibilidad de recursos. Entendemos entonces por triage de urgencias el proceso de valoración clínica

preliminar que ordena los pacientes antes de la valoración diagnóstica y terapéutica completa en base a su grado de urgencia, de forma que en una situación de saturación del servicio o de disminución de recursos, los pacientes más urgentes son tratados primero, y el resto son controlados continuamente y reevaluados hasta que los pueda visitar el equipo médico.

El término triage (o triaje, aunque éste casi no se utiliza) no existe en la lengua española o portuguesa, y se lo podría asimilar al término “clasificación”. Se entiende que dicha traducción no es adecuada y por lo tanto se utilizará triage de aquí en adelante.

En el contexto de incidentes de seguridad, el triage implica la recepción por diversas vías de reportes de eventos o incidentes de seguridad y su clasificación mediante algún criterio. La clasificación que se le dé a lo reportado determinará la gestión a realizar, lo que no implica que no se pueda volver a clasificar si así se determina luego de analizarlo o en pleno proceso de gestión.

La persona encargada del triage podrá tener como tarea la asignación del integrante del Centro que deberá llevar adelante la gestión del incidente. Dicha decisión podrá ser tomada en conjunto con el Gerente Operacional e incluso contando con la opinión del Director Ejecutivo.

La persona idónea para esta actividad debe reunir algunas cualidades, como:

- Capacidad de correlacionar eventos e incidentes de seguridad
- Mantener la calma en momentos “complicados”
- Saber distinguir entre lo urgente y lo importante.

Diferentes aspectos deben considerarse en el momento de asignar un incidente a un integrante del Centro, un ejemplo de lista de dichos aspectos es:

- Expertise del potencial candidato
- Carga laboral actual del candidato
- Carga laboral futura del candidato
- Expectativa de duración de la gestión del incidente a gestionar
- Estado de ánimo del candidato
- Vinculación del candidato con quien reporta y otros posibles integrantes de la Comunidad Objetivo que podrían estar vinculados al incidente

3.2.1.8 Documentación

Todo Centro de Respuesta cuenta con una importante cantidad de Documentación y en diferentes medios y formatos, la que requiere de una gestión adecuada. Dicha gestión incluye la existencia de políticas y procedimientos que especifiquen cómo y cuándo:

- Generarla
- Clasificarla
- Almacenarla
- Respaldarla
- Destruirla
- Difundirla

Podemos identificar dos grandes tipos de información: información relevante para el funcionamiento mismo del Centro de Respuesta e información vinculada a los propios servicios que se brindan. En el primero están comprendidas todas las políticas y procedimientos del Centro. En el segundo encontramos toda la documentación generada durante la prestación de cada servicio; por ejemplo puede ser, toda la documentación que se genera como resultado de la gestión de un incidente de seguridad o toda la documentación generada como resultado de una auditoría de seguridad o toda la documentación generada para un plan de capacitación y/o entrenamiento.

La gestión de la documentación deberá contemplar la revisión periódica de ella, como instancia en la cual se puede modificar en base a la experiencia de haberla aplicado durante cierto tiempo. Ello puede resultar en la modificación de algunas de las políticas y procedimientos involucrados o la documentación de que luego de realizada la revisión, no se identificaron cambios necesarios.

3.2.1.9 Capacitación y Entrenamiento

La actividad de capacitación y entrenamiento es útil, por un lado para generar un expertise en la Comunidad Objetivo que le será muy útil a la hora de enfrentar un incidente de seguridad, que los puede motivar a crear Centros similares y que le permitirá a los integrantes del Centro interactuar de mejor forma con los integrantes de la Comunidad en el momento de gestionar un incidente de seguridad; por otro lado, puede serle útil al Centro como una forma

de autofinanciarse y de posicionarse frente a la Comunidad Objetivo como un punto de referencia en la temática. La actividad de capacitación y entrenamiento no debe quedar circunscripta solamente a aspectos puramente técnicos, pudiendo ser muy enriquecedor para ambas partes realizar talleres donde la Comunidad Objetivo encuentre un ámbito donde plantear sus inquietudes al Centro de Respuesta.

El responsable de dicha actividad tiene a su cargo la tarea de identificar temáticas que resultarían de interés para la Comunidad Objetivo. Para ello puede recurrir a diferentes fuentes de información como ser sitios en Internet específicos de seguridad, información de otros Centros de Respuesta, asistencia a seminarios, conferencias, capacitación y entrenamiento entre otros. Adicionalmente debe estar predispuesto para analizar propuestas que provengan o no de la Comunidad Objetivo y por cualquier vía respecto a una demanda insatisfecha, oculta o no, respecto a capacitación y/o entrenamiento.

3.2.1.10 Logística

En cualquier Centro de Respuesta, así como en cualquier empresa de cualquier tamaño, deben existir un conjunto de bienes fungibles y no fungibles a disposición de sus integrantes. Por ello, debe existir una persona responsable de asegurar la existencia de los mismos en las cantidades adecuadas para el correcto trabajo diario. Esta función puede recaer en un integrante del Centro sin formación técnica.

3.2.1.11 Investigación

Una función relevante para un Centro de Respuesta es la investigación. Las ventajas que ofrece dedicar parte del tiempo a esta función son variadas. Se pueden mencionar entre ellas: que es una herramienta que puede acercar al equipo información y conocimiento que puede ser de utilidad para el Centro y para la Comunidad Objetivo, le permite vincularse con Centros pares, mejora la reputación del Centro y sus integrantes y fomenta actividades similares en otros Centros y en la Comunidad Objetivo.

El realizar actividades de investigación y el compartir en diversos ámbitos sus avances, problemas y resultados es útil también para generar vínculos de confianza con quien se comparte. Las vías disponibles para compartir información vinculada a tareas de investigación (siempre y cuando no se esté limitado por la confidencialidad) son varias, desde informes publicados en Internet hasta la realización de reuniones, talleres o seminarios donde se puedan intercambiar ideas.

Los resultados de determinada investigación pueden ser la semilla para un nuevo servicio a ser brindado por el Centro o para la mejora de una ya existente. Cualquiera de los dos frutos son altamente valorados por la Comunidad Objetivo y ayudan a mejorar la imagen del Centro.

Como dijimos antes, las tareas de investigación se pueden llevar a cabo: exclusivamente en el Centro, en el Centro y en colaboración con otros Centros, en el Centro y con la participación de algunos integrantes de la Comunidad Objetivo o en el Centro y con la participación de personal de la organización que le sirve de hosting.

Los resultados de determinada investigación pueden ser la semilla para un nuevo servicio a ser brindado por el Centro o para la mejora de una ya existente. Cualquiera de los dos frutos son altamente valorados por la Comunidad Objetivo y ayudan a mejorar la imagen del Centro. Como dijimos antes, las tareas de investigación se pueden llevar a cabo: exclusivamente en el Centro, en el Centro y en colaboración con otros Centros, en el Centro y con la participación de algunos integrantes de la Comunidad Objetivo o en el Centro y con la participación de personal de la organización que le sirve de hosting.

Las actividades de investigación, más allá de cómo se lleven a cabo, fortalecen los lazos entre las partes involucradas y afianza la confianza entre ellos. Esta actividad puede tener un costo directo o no para las organizaciones a las que pertenecen los integrantes de la Comunidad Objetivo que participan de la misma.

3.2.1.12 Legal

Todo Centro de Respuesta debe contar con un asesor legal. La persona que cumpla dicha función puede ser o no integrante del Centro de Respuesta. En caso de no serlo, puede pertenecer a la organización que brinda el hosting al Centro o puede ser contratado por el Centro ante la necesidad de sus servicios.

Su presencia es fundamental en varias actividades del Centro. Por ejemplo, para la recolección y preservación de evidencia que puede llegar a ser utilizada más adelante en una instancia judicial o para asesorar a los integrantes del Centro en cómo deben ser redactados los informes asociados a un incidente de seguridad, informes en ciertas ocasiones solicitados por parte de un juez y hasta incluso como asesor legal en el momento de declarar en un juzgado.

Es recomendable que los integrantes del Centro de Respuesta realicen reuniones con su asesor legal de manera de estar al día con la legislación vigente en el país donde se encuentra brindando servicios el Centro. Los integrantes del Centro de Respuesta en general poseen

muy poca o nula formación en aspectos jurídicos y por la propia esencia de los servicios que brindan deben conocer las leyes, decretos y ordenanzas vinculadas a su tarea.

3.2.1.13 Gestión de Incidentes

La gestión de incidentes es el servicio fundamental de todo Centro de Respuesta, y la razón de su existencia. La función debe ser llevada adelante por todos los integrantes técnicos del Centro y apoyada también por los restantes integrantes.

Su función implica la gestión de incidentes de seguridad, pudiendo tener a su cargo también la función de triage, incluso al mismo tiempo.

La gestión de incidentes implica estar en contacto con quien lo reportó y quizás con otros integrantes de la Comunidad Objetivo así como con otros Centros de Respuesta e incluso representantes legales. Por vías formales o informales deberá informar al Gerente Operacional del estado de cada incidente que se encuentra gestionando y de la vida misma de él.

Más allá de la existencia de cursos de capacitación y entrenamiento en gestión de incidentes de seguridad, mucho se aprende gestionando incidentes de seguridad. Cuando un integrante del Centro comience a gestionar incidentes es conveniente que otro integrante ya avezado en dicha tarea asuma un rol de mentor o tutor, que lo pueda ir guiando, asesorando, formando y forjando la confianza de aquel en su nueva función.

3.2.1.14 Embajadores

En algunos Centros de Respuesta y dependiendo del modelo organizacional del mismo, puede ocurrir que personal de la organización que brinda el hosting al Centro trabaje en ciertos temas puntuales, como un integrante más del grupo.

Un caso en donde puede ocurrir ello es por ejemplo cuando se está gestionando un incidente de seguridad, que involucra a un activo de la organización perteneciente a una unidad distinta al Centro de Respuesta. Puede ocurrir entonces que se requiera la participación de algún administrador o “dueño” de dicho activo, por su conocimiento profundo del mismo. De ser así, puede ser útil para ambas partes que dicha persona, y mientras se realice la gestión del incidente, sea considerada un integrante temporal del Centro. Ello permitirá a dicha persona (y a la unidad que integra) conocer más de cerca la realidad del Centro y viceversa. Por otro lado puede ser útil también para identificar potenciales futuros integrantes del equipo.

Su participación en el Centro requerirá que previamente firme un NDA (Non-Disclosure Agreement) o Compromiso de Confidencialidad.

3.2.1.15 Formación Continua

No es posible concebir un Centro de Respuesta en el que sus integrantes no realicen actividades de capacitación y entrenamiento de manera frecuente. Resulta fundamental que continuamente se estén actualizando en las TICs así como en la evolución de los distintos vectores de ataque (conocidos y nuevos). Por ello es importante que los integrantes del Centro destinen parte de su tiempo de trabajo a estudiar, leer, ser curiosos en cuanto a cómo funciona determinado malware o un protocolo, una herramienta (Sniffer de paquetes, forense, etc.) qué servicios brinda un nuevo equipamiento o aplicación lanzada al mercado o cual es la realidad de las redes sociales, el spam, las botnets, los honeypots, entre otros ejemplos.

Pero tan importante como lo expresado en el párrafo anterior es que dicho conocimiento no quede cerrado en una sola persona. Resulta muy beneficioso para el Centro de Respuesta que mediante reuniones internas poco formales pero sí respetando cierta periodicidad se comenten acerca de lo estudiado o leído. Muy probablemente ello servirá para evacuar dudas, recibir preguntas que nunca se había plateado quien ha estudiado cierto tema, lo que puede ayudar a orientar y profundizar el estudio e incluso, para identificar nuevas líneas de investigación que se podrían explotar.

Por otro lado, la Comunidad Objetivo demanda, a veces explícitamente, que los integrantes del Centro de Respuesta (desde el Director Ejecutivo hasta quienes realizan gestión de incidentes, pasando por el gerente Operacional) estén aggiornatos en cuanto a su formación, lo que puede implicar la necesidad de que obtengan determinadas certificaciones con reconocimiento internacional, como por ejemplo las otorgadas por [ISC2], [ISACA] y [PMI]

3.2.1.16 Financiero y Económico

De alguna forma el Centro de Respuesta deberá disponer de los fondos para seguir existiendo. Se debe pagar salarios, leyes sociales, comprar hardware, software y libros, pagar el local donde opera y su equipamiento, la conectividad a Internet, asistencia a conferencias, viáticos entre otras cosas.

Podemos identificar dos grande modelos posibles de cómo un Centro de Respuesta puede obtener los rubros presupuestales necesarios.

El primero es que la organización que le brinda el hosting se encargue de destinar todos los fondos necesarios y el Centro de Respuesta “retorne” a través de los servicios que brinda, quizás de manera indirecta, sin la venta específica de ninguno de ellos. En la antípoda de

éste modelo se encuentra aquel en el que el Centro se autofinancia completamente, a través de la venta de diferentes servicios: capacitación, entrenamiento, auditorías, ethical hacking, consultorías entre otros.

Entre ambos modelos podemos encontrar diversas variantes posibles, según el contexto en el que se desempeña el Centro de Respuesta.

Ambos modelos mencionados requieren que alguien desempeñe la función de llevar adelante la gestión financiera y económica del Centro. Un análisis superficial podría determinar que en el primero de los modelos no es requerido este rol, pero debemos comprender que dicha gestión puede ser un insumo fundamental para, llegado el momento, justificar la existencia del Centro, más aún si consideramos que el retorno de la inversión (no gasto) que realiza la organización es difícil de medir. En el segundo modelo, sin duda que dicha gestión debe estar presente y quien la lleve adelante debe tener un contacto muy fluido con el Director Ejecutivo en particular y con el resto de los integrantes del Centro en general para buscar acompasar la gestión de incidentes y el resto de los servicios que se brindan y que podrían brindar con el objetivo de no tener números rojos.

3.2.1.17 Consideraciones finales

Es muy habitual en los Centros de Respuesta, desde los recién creados hasta los que ya han alcanzado un grado de madurez importante, que cada persona no tenga una única función asignada, salvo alguna función específica, como puede ser la vinculada a las actividades legales. Lo que a primera vista puede ser un síntoma de poco control, de falta de definiciones, en general se lo identifica con otra situación, que es aquella en la cual los diferentes integrantes pueden tener un panorama bastante completo de toda la "maquinaria" del Centro de Respuesta y por lo tanto, ver la realidad desde diferentes ópticas. El Centro de Respuesta es un mostrador y las funciones sus lados (sin duda un mostrador muy particular). Más de una vez hemos escuchado (hasta de nuestra propia boca) "sería bueno que te pusieras de mi lado del mostrador", y justamente ese es un modelo habitualmente encontrado en los Centros de Respuesta (casi sin excepciones en los Centros de Respuesta que recién nacen). Ello no debe confundirse con "todos hacemos de todo y al final nadie es responsable de nada" que termina traduciéndose en "nadie hace nada porque todos piensa que lo hace el otro", situación peligrosa y que puede llegar incluso a poner en riesgo la existencia misma del Centro. Es aquí donde resulta fundamental la capacidad organizativa del Centro y las especificación clara, por escrito y explícitamente reconocida por todos los integrantes de quienes son los

responsables de cada función, y eventualmente sus alternos ante la ausencia por alguna razón de aquellos.

3.3. Manuales y Procedimientos

En esta sección de la propuesta nos enfocaremos a prácticas recomendadas para el desarrollo de Manuales y Procedimientos en un Centro de Respuesta a Incidentes de Seguridad Informática.

Las prácticas no deben ser consideradas como un estándar a seguir pero sí reflejan los criterios que han venido siguiendo los integrantes de la Comunidad.

3.3.1 Motivación

En todo Centro de Respuesta la elaboración de Manuales y Procedimientos es una tarea fundamental tanto para su operación como para posicionarse adecuadamente frente a la Comunidad Objetivo.

Sabido es que la existencia de una Política de Seguridad es fundamental y fundacional en todo lo que respecta a la gestión de la seguridad de la información e informática en toda organización, más aún en aquella que sea o que contenga un Centro de Respuesta.

La creación de un Centro de Respuesta así como su reconocimiento en la comunidad de otros Centros de Respuesta requiere la elaboración de diferentes tipos de políticas. Las políticas brindan pautas primarias del “qué”, pero, salvo alguna situación especial y puntual, no abordan el “cómo”, y es aquí donde se comienza a identificar el rol fundamental de los procedimientos. Podríamos decir que los procedimientos son implantaciones específicas de una política en una realidad concreta.

3.3.2 Manuales

Los manuales (o tutoriales), que podemos definir como un documento donde se compendia lo sustancial sobre determinada materia, también debería ser un producto frecuente de elaboración/revisión por parte de los integrantes del Centro de Respuesta.

Podemos identificar motivos proactivos y reactivos para la elaboración/revisión de manuales. Entre los proactivos podemos mencionar la propia iniciativa de alguno o todos los integrantes del Centro de Respuesta de, cada cierto tiempo (por ejemplo tres meses) el Centro elabore un manual para poner a disposición de la Comunidad Objetivo y/o de toda la comunidad y/o de otros Centros de Respuesta.

Entre los reactivos, podemos mencionar la identificación de la necesidad, luego de haber gestionado un incidente de seguridad que vinculó a una materia, sobre la que se entiende que el integrante de la Comunidad Objetivo (y/o toda la Comunidad Objetivo y/o toda la comunidad y/u otros Centros de Respuesta) debería contar con un manual que arroje luz al respecto.

La elaboración periódica de manuales (proactivos o reactivos) sirve para posicionar al Centro de Respuesta como un punto de referencia en la comunidad en cuanto a seguridad.

En general los manuales elaborados son considerados un aporte a la comunidad, por lo que para su uso por parte de terceros sólo se solicita que se mencione la fuente y los autores.

3.3.3 Procedimientos

En todo Centro de Respuesta se deberán elaborar varios procedimientos que expliquen claramente cómo ejecutar las acciones relevantes sobre determinada tarea de forma que se realice eficaz y eficientemente.

La tarea de elaborar procedimientos (así como la tarea de elaborar políticas) no se acota a un momento de la vida del Centro de Respuesta. De una u otra manera y con picos y valles en cuanto a carga laboral aplicada a ella, varios integrantes del Centro estarán envueltos en crear nuevos procedimientos y analizar los ya existentes a los efectos de determinar si siguen siendo adecuados o requieren una actualización. La actualización de los procedimientos puede tener diferentes motivos, incluso combinados: nuevos requerimientos de la Comunidad Objetivo, nuevos desafíos del Centro de Respuesta, cambios tecnológicos, omisiones u errores en la versión actual, entre otros.

La necesidad de elaborar nuevos procedimientos también puede tener varios motivos, también incluso combinados: formalizar una actividad que se viene realizando siguiendo un procedimiento no escrito, una nueva política que fomenta la realización de uno o más procedimientos, entre otros.

La actividad cotidiana de los integrantes del Centro de Respuesta así como la interacción con miembros de la Comunidad Objetivo o de otros Centros de Respuesta serán disparadores de la creación o actualización de procedimientos.

3.3.4 Criterios de elaboración de Manuales

Los manuales no deben ser extremadamente largos. En general ello reduce su aprovechamiento, salvo excepciones.

Deben estar redactados en un lenguaje adecuado para el público objetivo. Pueden tener un contenido técnico muy alto o no, según para qué público estén pensados. Incluso en algunos casos puede ser oportuno generar diversos “sabores” de un mismo manual para llegar a diferentes sectores del público objetivo.

Desde el momento que se plantea la elaboración de un manual se debe identificar claramente el objetivo del mismo, el público objetivo, la extensión esperada del mismo (a veces también condicionada por el público objetivo), el plazo necesario para la elaboración, cuándo y cómo debería liberarse.

Es muy recomendable que los manuales respeten un template predefinido, pudiendo existir más de un template si existen varios públicos objetivos.

Resulta muy recomendable también que exista un procedimiento de elaboración de manuales, que comprenda, la forma (template/s), el o los estilos de redacción y las diferentes instancias de elaboración y aprobación a recorrer previo a su liberación.

El contemplar los estilos de redacción permite que, aun cuando los autores de los manuales sean distintos, ellos mantengan un estilo único, propio del Centro de Respuesta.

En las diferentes instancias de la elaboración de un manual pueden participar el Director Operacional, integrantes destinados a gestión de incidentes, el Responsable de Documentación, el Responsable de Capacitación y Entrenamiento, y el Responsable de Difusión, según establezca el Procedimiento de Generación de Manuales a elaborar.

Incluso los manuales y tutoriales elaborados podrán vincularse con actividades de capacitación y entrenamiento del Centro de Respuesta.

Es totalmente válido que la elaboración de un manual implique el uso de información disponible en algún medio, como ser libros, artículos, sitios de Internet. En todos los casos su uso deberá ser respetando las condiciones de uso explicitadas en ellos.

3.3.5 Criterios de elaboración de Procedimientos

La elaboración de procedimientos debería requerir la existencia de una política al respecto.

Toda aquella actividad que se realiza siguiendo determinada secuencia de acciones, utilizando determinadas herramientas (hardware o software) y alineada a una política implícita o explícita debería plasmarse en un procedimiento.

La tarea de elaborar un procedimiento, por sí misma, permitirá analizar con espíritu crítico que tan completo y adecuado era el procedimiento ad-hoc que se seguía hasta el momento, lo que sin duda permitirá documentar un procedimiento notoriamente mejor.

Para elaborar un procedimiento, en primer lugar se debe tener claramente identificada la necesidad del mismo. Luego se debe conocer si al respecto ya se sigue un procedimiento no escrito y de ser así, conocerlo en detalle. Luego se podrá comenzar, con una metodología top-down, a identificar las diferentes actividades y resultados que lo compondrán. La metodología permite, yendo de lo general a lo particular, identificar primero los aspectos medulares y luego, se podrá ir desglosando y detallando cada uno de ellos.

Para actualizar un procedimiento, los integrantes del Centro de Respuesta vinculados con lo que se procedimenta en él y quien detectó la posible necesidad de su actualización deben reunirse junto con una copia actual del mismo a los efectos de interactuar al respecto de la necesidad o no de su modificación. Si no se logra consenso, decidirá la opinión del Director Operacional y si persiste, la opinión del Director Ejecutivo.

Es necesario llevar un registro de versionado de toda la documentación en uso en el Centro de Respuesta, y en el caso que nos compete aquí, también de los procedimientos.

Un procedimiento terminado es correcto sí al ser leído por primera vez por una persona idónea en la materia a la cual refiere no tiene inconvenientes para comprenderlo y ponerlo en práctica.

El lenguaje utilizado en el mismo debe ser el adecuado para que se comprenda sin ambigüedades lo que se expresa. No deben existir huecos en un procedimiento, es decir, falta de pasos o incertidumbres en las acciones a tomar o a los resultados a obtener y cómo proseguir.

3.3.6 Difusión de Manuales

Respecto a los manuales, podemos encontrar dos grandes familias cuando hablamos de la difusión de los mismos. Por un lado aquellos que son de uso interno del Centro de Respuesta, por ejemplo por tratarse de una investigación cuyo tema y/o información asociada no es clasificada como pública y por otro, aquellos que sí pueden ser difundidos fuera del Centro de Respuesta, quizás con diferentes sabores según a quienes se les permite acceder y en qué condiciones.

El pasaje de un manual de uso interno (proceso de “desclasificación”) debería requerir un procedimiento asociado.

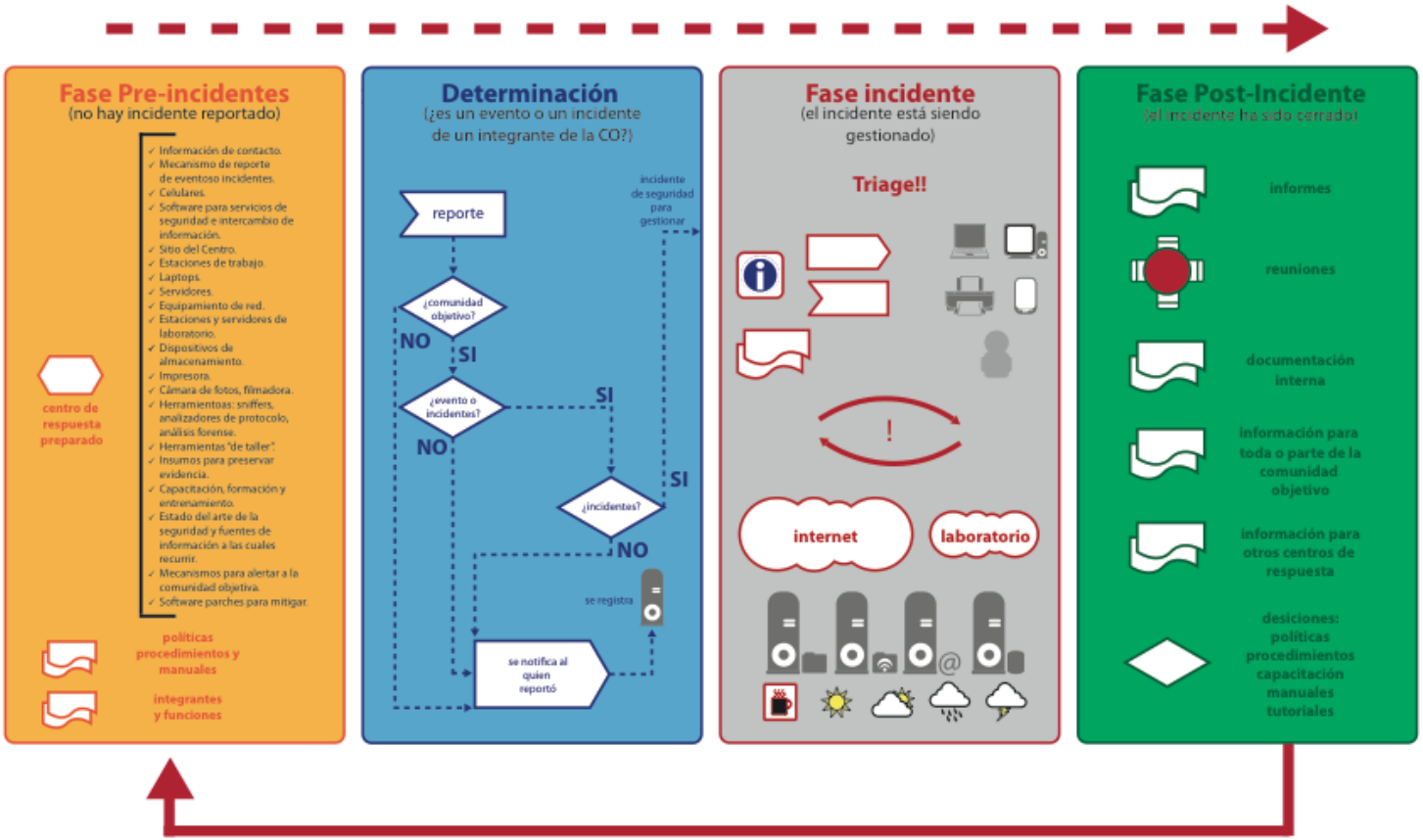
3.3.7 Difusión de Procedimientos

En general, los procedimientos elaborados en un Centro de Respuesta son de uso interno y no existe necesidad e incluso autorización para que salgan de ese ámbito. Un ejemplo típico de procedimiento que debería ser público es aquel asociado a cómo contactar al Centro de Respuesta para, por ejemplo, reportar un evento o incidente de seguridad.

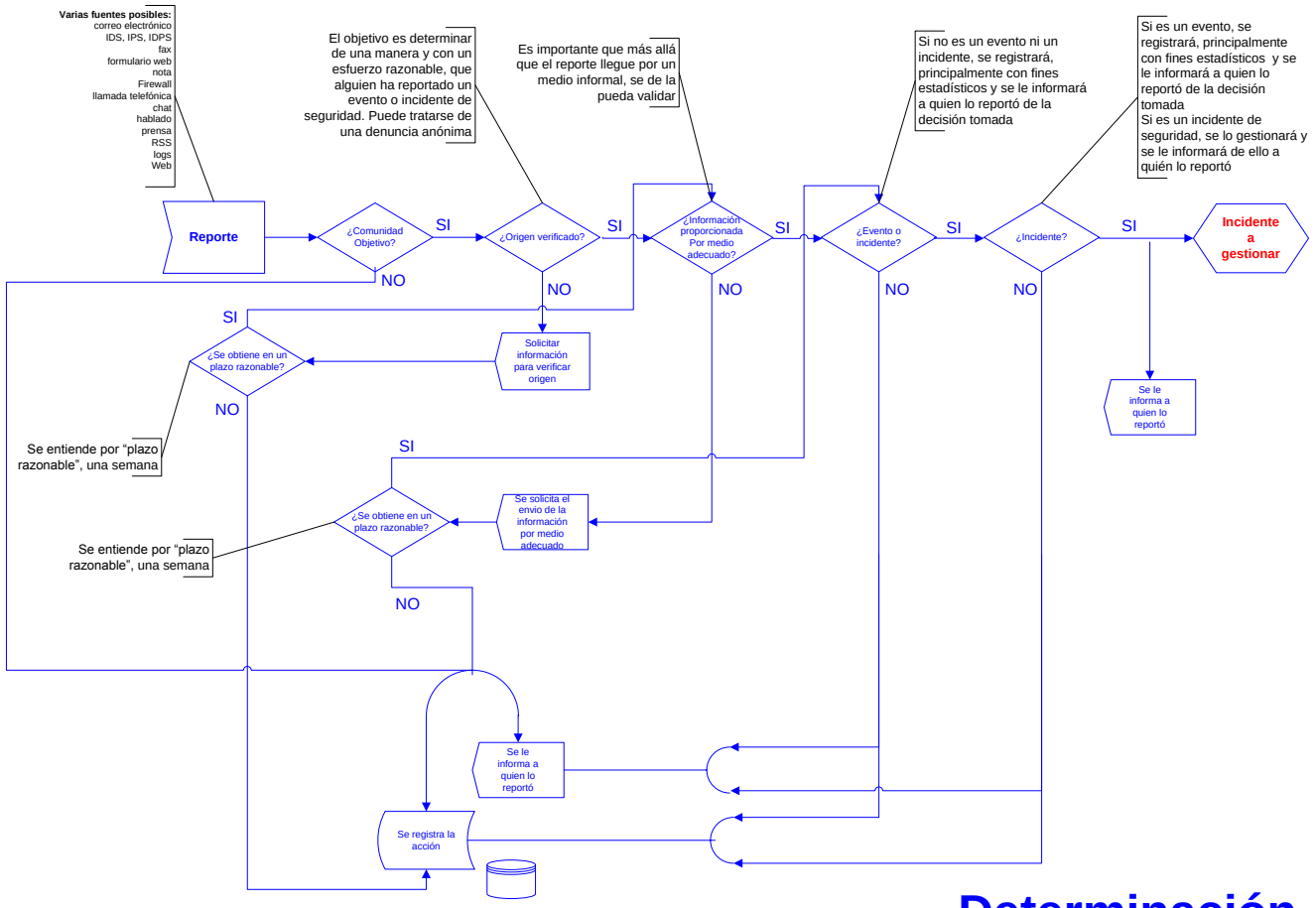
Debe estar claramente especificado dónde se encuentran disponibles y cuales son todos los existentes.

3.4. Diseño de un Flujograma del Proceso de Gestión de Incidentes, end to end

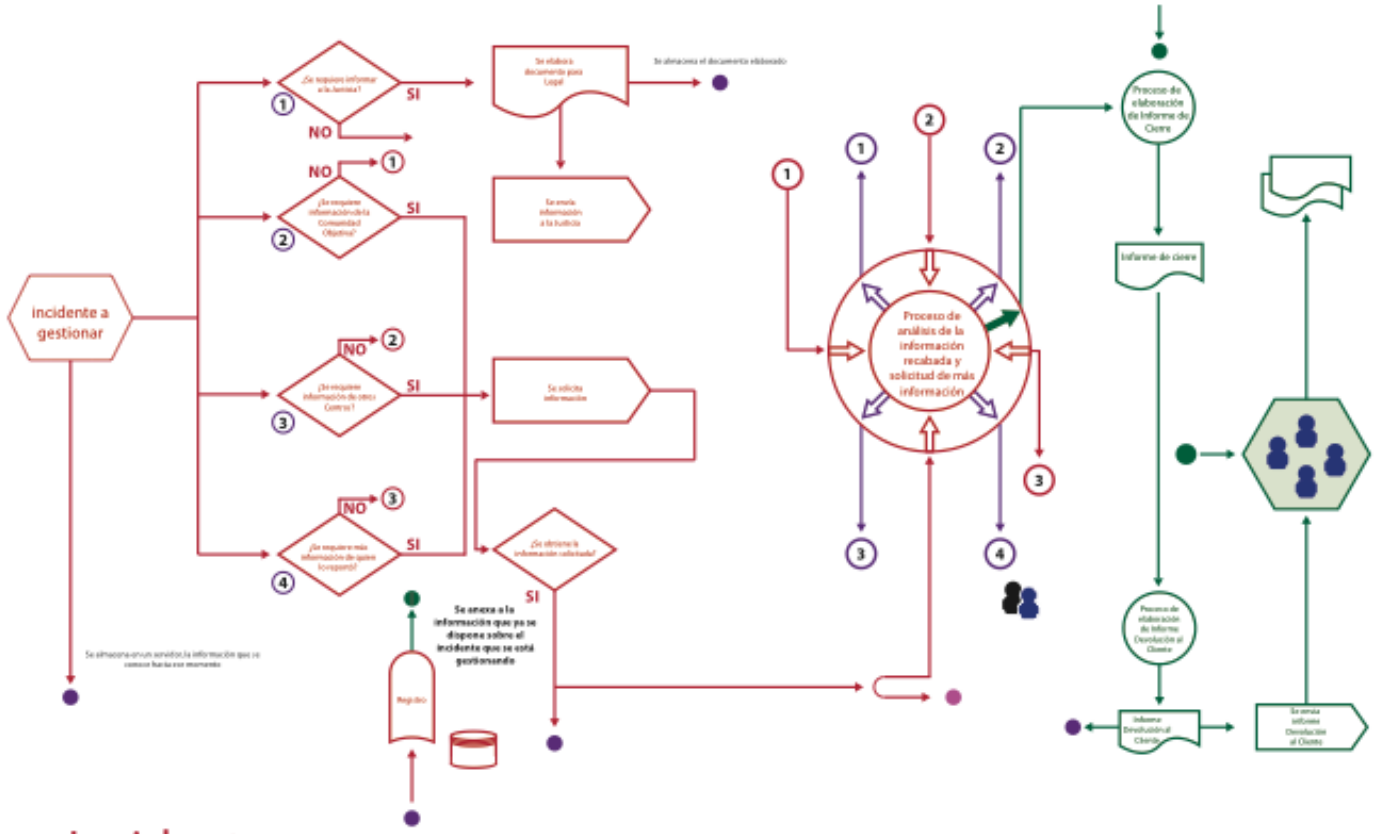
3.4.1 El Ciclo de Vida de un Incidente de Seguridad



3.4.2 El ciclo de vida de un incidente de seguridad



3.4.3 Gestión de Incidente de Seguridad



3.5. Propuesta de Políticas de Manejo de la Información.

3.5.1 Propuesta de Política de Acceso a la Información

Esta sección documenta una propuesta de Política de Acceso a la Información de un Centro de Respuesta a Incidentes de Seguridad Informática. No se pretende aquí establecer un estándar a seguir pero sí establecer aspectos fundacionales necesarios al momento de explicitar los lineamientos fundamentales para el acceso a la información en un Centro de Respuesta.

3.5.1.1 Texto de la Propuesta de Política de Acceso a la Información

3.5.1.1.1 Objetivo

Establecer qué tipo de información y cómo pueden acceder los integrantes del Centro de Respuesta, los integrantes de otros Centros de Respuesta, los integrantes de la Comunidad Objetivo y los actores legales que puedan estar involucrados en la gestión de un incidente de seguridad u otra actividad vinculada a algún servicio del Centro de Respuesta.

3.5.1.1.2 Alcance

Toda la información que disponga el Centro de Respuesta.

3.5.1.1.3 Contenido

Todo integrante del Centro de Respuesta tendrá acceso a toda la información vinculada a todos los eventos e incidentes de seguridad ya gestionados y en gestión.

El acceso a la información vinculada a un incidente ya cerrado será utilizada con el único fin de mejorar la capacitación, formación y entrenamiento de los integrantes del Centro de Respuesta. También podrá ser utilizada para la emisión de alertas, avisos o documentos de mejores prácticas, preservando siempre el anonimato de las personas e instituciones involucradas en el incidente así como toda la información particular del mismo, que seguirá siendo considerada como confidencial.

Toda la información suministrada por un integrante de la Comunidad Objetivo durante la gestión de un incidente de seguridad deberá ser considerada como confidencial y se le deberá informar de ello apropiadamente.

Todos los integrantes del Centro de Respuesta deberán tener firmada una copia impresa de un NDA (Non- Disclosure Agreement) o Compromiso de Confidencialidad y se deberá difundir apropiadamente en la Comunidad Objetivo tal situación.

Durante la gestión de un incidente de seguridad y cuando información vinculada al mismo deba ser facilitada a otro integrante de la Comunidad Objetivo o a algún integrante de otro Centro de Respuesta, se deberá hacer de acuerdo a lo expresado en la Política de Difusión de la Información. Las comunicaciones telefónicas, vía chat, o simplemente habladas sólo pueden ser utilizadas para coordinar actividades, pero siempre se debe dejar documentados, y con los niveles de seguridad adecuados (autenticación, integridad, confidencialidad, según corresponda), qué tipo de información se intercambió con quién, cuándo y por qué vía.

En la gestión de ningún incidente de seguridad se podrá obligar (sin acciones legales) a un integrante de la Comunidad Objetivo que facilite alguna información. Si el integrante del Centro de Respuesta que tiene a su cargo la gestión del incidente entiende que la información que no se logra obtener resulta importante para el éxito de la gestión del mismo, deberá hacérselo saber al miembro de la Comunidad Objetivo, teniendo siempre presente el Código de Ética del Centro.

El acceso a información en formato impreso o entregada en mano, así como aquella que esté contenida en algún medio de almacenamiento magnético o digital, deberá ser siempre posterior a la firma por ambas partes (quien la entrega y quien la recibe) de un documento (y su copia) que describa claramente y sin dejar lugar a ambigüedades o dudas, qué es lo que se está entregando/recibiendo, la fecha y hora de ocurrencia, con la presencia del Responsable Legal del Centro a los efectos de validar el acto y mediante el registro en imágenes y/o video de todo el proceso.

No podrán existir solicitudes de acceso a información en poder del Centro de Respuesta que no sean respondidas afirmativa o negativamente y el motivo de esto último.

3.5.2 Propuesta de Política de Protección de la Información

Esta sección documenta una propuesta de Política de Protección de la Información de un Centro de Respuesta a Incidentes de Seguridad Informática. No se pretende aquí establecer un estándar a seguir pero sí establecer aspectos fundacionales que se deben considerar al momento de establecer lineamientos fundamentales para la protección de la información en un Centro de Respuesta.

3.5.2.1.1 Objetivo

Establecer los lineamientos generales para la protección de toda la información utilizada por el Centro de Respuesta para su actividad cotidiana.

3.5.2.1.2 Alcance

Toda la información de que dispone el Centro de Respuesta.

3.5.2.1.3 Contenido

Discriminaremos en función de la clasificación documentada en la Política de Clasificación de la Información, que establece cuatro categorías: secreta, confidencial, uso interno y pública. Toda información, en cualquier medio, deberá explicitar de manera clara y sin lugar a dudas cómo está clasificada.

- **Información Secreta**

Cuando se trata de información en formato lógico, deberá almacenarse asegurando la confidencialidad con largo mínimo de clave de 2048 bits e integridad con función de hash SHA-2. Cuando se trata de información en formato físico, deberá almacenarse en sobre cerrado y en una caja fuerte ubicada dentro del sitio del Centro.

En la gestión de ningún incidente de seguridad se podrá obligar (sin acciones legales) a un integrante de la Comunidad Objetivo que facilite alguna información. Si el integrante del Centro de Respuesta que tiene a su cargo la gestión del incidente entiende que la información que no se logra obtener resulta importante para el éxito de la gestión del mismo, deberá hacérselo saber al miembro de la Comunidad Objetivo, teniendo siempre presente el Código de Ética del Centro.

El acceso a información en formato impreso o entregada en mano, así como aquella que esté contenida en algún medio de almacenamiento magnético o digital, deberá ser siempre posterior a la firma por ambas partes (quien la entrega y quien la recibe) de un documento (y su copia) que describa claramente y sin dejar lugar a ambigüedades o dudas, qué es lo que se está entregando/recibiendo, la fecha y hora de ocurrencia, con la presencia del Responsable Legal del Centro a los efectos de validar el acto y mediante el registro en imágenes y/o video de todo el proceso.

No podrán existir solicitudes de acceso a información en poder del Centro de Respuesta que

no sean respondidas afirmativa o negativamente y el motivo de esto último.

- **Deberá existir control de acceso a la misma.**

El acceso a la misma en forma remota deberá ser asegurando la confidencialidad y la integridad, utilizando algunos de los siguientes protocolos: https, sftp o ssh. De requerirse, la transmisión de información secreta será cifrada con clave pública de largo mínimo de 2048 bits.

No podrá almacenarse en estaciones de trabajo, servidores, notebooks o dispositivos de almacenamiento portátiles que no estén almacenados en una caja fuerte ubicada dentro del sitio del Centro. No debe ser comentada con ninguna persona ajena al Centro de Respuesta.

- **Información confidencial**

Cuando se trata de información en formato lógico, deberá almacenarse asegurando la confidencialidad con largo mínimo de clave de 2048 bits e integridad con función de hash SHA-2. Cuando se trata de información en formato físico, deberá almacenarse en sobre cerrado y en una caja fuerte ubicada dentro del sitio del Centro.

No debe existir ninguna fuente de información de la existencia de la misma, que tenga un nivel protección menor a la de la información que referencia. Deberá existir control de acceso a la misma.

El acceso a la misma en forma remota deberá ser asegurando la confidencialidad y la integridad utilizando algunos de los siguientes protocolos: https, sftp o ssh. De requerirse, la transmisión de información secreta será cifrada con clave pública de largo mínimo de 2048 bits.

Podrá almacenarse en estaciones de trabajo, servidores, notebooks o dispositivos de almacenamiento portátiles, asegurando confidencialidad con clave de largo mínimo de 2048 bits.

No podrá almacenarse en sistemas remotos propietarios de los integrantes del Centro. No debe ser comentada con ninguna persona ajena al Centro de Respuesta.

- **Información de Uso interno**

Cuando se trata de información en formato lógico, el nombre del mismo, el valor de la última versión, la fecha de creación, la fecha de hecho público y el valor del hash se deberá almacenar en un dispositivo de almacenamiento en una caja fuerte instalada dentro del sitio del Centro. Cuando se trata de información en formato físico, la misma no podrá salir del sitio

del Centro de Respuesta.

La información de uso interno no debe ser difundida fuera del ámbito del Centro de Respuesta. Deberá existir control de acceso a la misma. El acceso a la misma en forma remota deberá ser asegurando la confidencialidad y la integridad.

No debe existir ninguna fuente de información de la existencia de la misma, que tenga un nivel protección menor a la de la información que referencia.

En sistemas remotos propietarios de los integrantes del Centro sólo podrá ser almacenada cifrada con clave de largo mínimo de 2048 bits.

No debe ser comentada con ninguna persona ajena al Centro de Respuesta.

- **Información pública**

Cuando se trata de información en formato lógico, el nombre del mismo, el valor de la última versión, la fecha de creación, la fecha de hecho público y el valor del hash se deberá almacenar en un dispositivo de almacenamiento en una caja fuerte instalada dentro del sitio del Centro. Cuando se trata de información en formato físico, para que sea considerada válida y autentica, siempre debe existir la misma información en formato lógico según lo expresado en el párrafo anterior.

3.5.3 Propuesta de Política de Difusión de la Información

Esta sección documenta una propuesta de Política de Difusión de la Información de un Centro de Respuesta a Incidentes de Seguridad Informática. No se pretende aquí establecer un estándar a seguir pero sí establecer aspectos fundacionales que se deben considerar al momento de establecer lineamientos fundamentales para la difusión de la información en un Centro de Respuesta.

El Centro de Respuesta gestiona en su actividad diaria un importante volumen de información en diferentes formatos, que puede o no provenir de diversas fuentes, que puede o no ser remitida a diversos destinos y que puede ser o no sólo de uso interno, en todas las combinaciones posibles y utilizando métodos de difusión y mecanismos de protección variados.

3.5.3.1 Texto de la Propuesta de Política de Difusión de la Información

3.5.3.1.1 Objetivo

Determinar, para toda la información que gestiona el Centro de Respuesta, a quienes se puede difundir, utilizando qué métodos y con qué mecanismos de protección.

3.5.3.1.2 Alcance

Aplica a toda la información que gestione el Centro de Respuesta. En este contexto gestionar información implica alguna de las siguientes acciones con la información: recibir, procesar, almacenar, destruir, generar y enviar.

3.5.3.1.3 Contenido

- **Información recibida**

Toda la Información recibida en el Centro de Respuesta deberá preservar la clasificación otorgada por quién la generó. Una disminución del nivel de clasificación deberá requerir que previamente quien la haya generado otorgue por escrito el consentimiento correspon-diente. Toda la información asociada a la gestión de un incidente de seguridad o a un evento será clasificada como confidencial.

- **Información procesada**

Toda información procesada en el Centro de Respuesta deberá ser clasificada de acuerdo a lo expresado en la Política de Clasificación de la Información. Toda la información procesada en el Centro de Respuesta deberá preservar la clasificación otorgada por quién la generó y respetar las condiciones de difusión por él expresa-das. El cambio de algunas de estas condiciones deberá requerir que a priori se obtenga un consentimiento por escrito que lo autorice.

- **Información almacenada**

Ver Política de Almacenamiento de la Información.

- **Información destruida**

Ver Política de Destrucción de la Información.

- **Información generada**

Toda la información generada en el Centro deberá tener explicitada su clasificación en base a la Política de Clasificación de la Información.

- **Información enviada**

Si se trata de información generada en el Centro, se deberá difundir explicitando la clasificación de la misma. Quien envía la información, siempre debe verificar que el destinatario es quien se desea y que es correcto que sea recibida por él.

Si se trata de difusión de información generada por personas o sistemas externos al Centro de Respuesta y se requiere por parte del destinatario de la misma conocer su origen, previo a informarlo se debe contar con el visto bueno por escrito de tal autorización.

Si la difusión se hace en formato electrónico, a través de redes como ser Internet y es información clasificada como “confidencial” o “secreta”, se deberá hacer utilizando mecanismos que otorguen servicios de confidencialidad e integridad.

Si la difusión se hace en formato electrónico, mediante la entrega de algún dispositivo de almacenamiento (disco duro, pendrive, CD, DVD, u otro) y es información clasificada como “confidencial” o “secreta”, se deberá hacer utilizando mecanismos que otorguen servicios de integridad y de confidencialidad.

Si la difusión se hace en papel y es información clasificada como “confidencial” o “secreta”, se deberá hacer de forma tal que el contenedor de dicha información (por ejemplo: sobre, carpeta) ofrezca los mecanismos para detectar una eventual violación (lacrados, cierres de una uso solamente) y que por lo tanto la tanto la integridad como la confidencialidad podrían estar amenazadas.

Si la información que se difunde es para el uso en una investigación judicial (previa recepción de un Oficio Judicial), se le debe dar el tratamiento explicitado para la información clasificada como “confidencial” o “secreta” y además, se debe anunciar previamente al Responsable Legal del Centro y al Director Ejecutivo del Centro quienes deberán otorgar su consentimiento para realizarlo. En el caso de ser información en formato electrónico y mediante la entrega de algún dispositivo de almacenamiento el proceso de entrega se deberá realizar en presencia del Responsable Legal del Centro quién deberá labrar un acta que documente todo lo realizado. Se debe apoyar la actuación mediante el registro fotográfico y/o fílmico de todas las acciones involucradas a la entrega del dispositivo.

Si se trata de información ni “confidencial” ni “secreta”, se puede difundir por medios que no aseguren confidencialidad e integridad aunque, para una gestión ordenada, siempre se debe verificar que la misma ha llegado en tiempo y forma al destinatario deseado.

La entrega de información a la prensa deberá, previamente, requerir una solicitud por escrito donde se detalle claramente la información solicitada. Dicha solicitud así como el análisis de la información que se brindará (si corresponde) será analizada por el Director Ejecutivo del Centro, el Gerente Operacional, el Responsable de Difusión y el Responsable Legal. La información a brindar a la prensa podrá ser “generada”, “procesada” o “recibida”, debiendo cumplir los requisitos anteriormente expresados en cada caso, y se debe registrar toda la actividad.

3.5.4 Propuesta de Política de Guarda de la Información

Esta sección documenta una propuesta de Política de Guarda de la Información de un Centro de Respuesta a Incidentes de Seguridad Informática. No se pretende aquí establecer un estándar a seguir pero sí establecer aspectos fundacionales que se deben considerar al momento de establecer lineamientos fundamentales para el almacenamiento de la información en un Centro de Respuesta.

3.5.4.1 Texto de la Propuesta de Política de Guarda de la Información

3.5.4.1.1 Objetivo

Establecer, para toda la información que se almacena el Centro de Respuesta, qué tipos de protección y control se deben implementar.

3.5.4.1.2 Alcance

Comprende a toda la información almacenada en el Centro de Respuesta.

3.5.4.1.3 Contenido

Respaldos de la información

Se deben realizar respaldos (back-ups) de toda la información almacenada en formato electrónico de acuerdo a lo expresado en el Procedimiento de Respaldo de la Información. Los respaldos deben ser verificados periódicamente siguiendo el Procedimiento de verificación de Respaldos de la Información.

Los integrantes del Centro de Respuesta deberán identificar qué información y sistemas son críticos y determinar qué tipo de sitio de respaldo requiere el Centro. Todo ello deberá ser documentado. Se entiende por información crítica aquella que en caso de verse comprometida en cuanto a alguna de sus propiedades de seguridad, afectaría seriamente al dueño de la misma, pudiendo ser el Centro de Respuesta, alguna organización de la Comunidad Objetivo u Otros Centros de Respuesta.

Se entiende por sistema crítico aquel que en caso de verse comprometido en cuanto a alguna de sus propiedades de seguridad, afectaría seriamente la operación del Centro de Respuesta y por ende, a la Comunidad

Objetivo.

El respaldo de la información y sistemas críticos deberá realizarse de acuerdo a lo expresado en las secciones “Información Crítica” y “Sistemas Críticos” del Procedimiento de Respaldo de la Información y Sistemas Críticos. La información debe ser almacenada de forma tal que el medio de almacenamiento preserve o eleve la clasificación de la misma.

En el caso de información disponible en papel o en alguna unidad de almacenamiento (disco duro, pendrive, CD, DVD, u otro) clasificada como “confidencial” o “secreta”, es conveniente que la misma se almacene en una caja fuerte propiedad del Centro, ubicada en su sitio físico y cuya combinación de apertura no esté documentada próxima a la misma ni en un lugar fácilmente deducible.

La información “secreta” o “confidencial” almacenada en servidores y estaciones de trabajo del Centro de Respuesta debe estar almacenada cifrada utilizando algún algoritmo de razonable confianza.

Dos hashes (realizados con funciones distintas) de cada documento utilizado para la gestión del Centro de Respuesta deberán ser guardados en un dispositivo de almacenamiento de uso exclusivo colocado dentro de una caja fuerte propiedad del Centro y ubicada en su sitio físico.

Las notebooks del Centro de Respuesta deberán tener todos sus dispositivos de almacenamiento con todo su contenido cifrado con algún algoritmo de razonable confianza.

Los servidores del Centro de Respuesta deberán implementar un sistema de almacenamiento con redundancia e integridad de los datos almacenados.

Toda la información vinculada a cada incidente gestionado en el Centro de Respuesta deberá ser retenida, al menos tres años a partir de la apertura del mismo.

CAPÍTULO 4

Políticas de Gestión de Riesgos en un Centro de Respuesta

Resumen.

En estos últimos años, se ha evidenciado una tendencia en las mejores prácticas de seguridad de la información, a darle un mucho mayor énfasis a la importancia de la gestión de riesgos como pilar para facilitar, ordenar y mejorar la gestión de la seguridad.

Quizás el ejemplo más representativo de ello sea la evolución de las normas ISO 17799:1 e ISO 17799:2 a las normas ISO 27001 y 27002 entre los años 2005, 2007 y 2013. Si bien las normas ISO 17799 eran normas de seguridad de la información, no abordaban la temática de la gestión de riesgos. En cambio, la ISO 27001 remarca la necesidad de comenzar la gestión de la seguridad con una adecuada gestión de los riesgos de seguridad existentes en toda organización.

Este es el motivo por el cual resulta necesario que los CERTs, como toda organización, gestione sus riesgos en materia de seguridad de la información. Es por ello que el presente material se enfoca a presentar la problemática y proponer una metodología para la gestión de los riesgos en los CERTs.

4. Políticas de Gestión de Riesgos en un Centro de Respuesta

Objetivos

- Crear conciencia de los riesgos a los que se enfrentan los CERTs en materia de seguridad de la información.
- Transmitir la importancia de la gestión de riesgos para la gestión de la seguridad de la información.
- Introducir al proceso de gestión de riesgos de seguridad.

4.1. Introducción

Hoy en día se puede decir que la información conduce el mundo. Todas las organizaciones necesitan información para funcionar, para prestar sus servicios, para generar beneficios, para progresar, etc. Es por ello que se entiende que la información se ha convertido en un ACTIVO más de las organizaciones. Así como existen otros activos, como ser los inmuebles, las maquinarias, el mobiliario, etc., la información debe entenderse también como un activo. Y es más, la información es uno de los activos más valiosos de las organizaciones.

Debido a la importancia y el valor que tiene la información para las organizaciones, es que se ha convertido en uno de los blancos más elegidos a la hora de los ataques. Ya sea una organización o un individuo mal intencionado, puede querer hacerse de información útil de terceros que les pueda generar algún beneficio. Así es como hoy sufrimos ataques como el espionaje industrial, el robo de información, el robo de identidad, etc.

Pero la información no sólo es vulnerable a ser divulgada, sino que también puede sufrir modificaciones indebidas, ocasionando que ésta deje de ser confiable e íntegra. Y por último, también es posible que la información sufra ataques a su disponibilidad. Como se dijo, la información es un activo de mucho valor, pero si no se encuentra disponible en tiempo y forma para quienes la necesitan, es como si no se contara con ella. A veces, la falta de disponibilidad de la información puede causar grandes perjuicios a una organización (ej.: la caída de su sitio web). Esto es aprovechado en ocasiones por personas mal intencionadas que ocasionan denegaciones de servicio a la información de una organización con el objeto de causarle algún daño.

En definitiva lo que se ha mencionado hasta ahora no es ni más ni menos que las tres cualidades esenciales que deben ser preservadas de la información:

- **CONFIDENCIALIDAD**: garantizar que la información sea accedida sólo por personas autorizadas
- **INTEGRIDAD**: garantizar que la información sea modificada sólo por personas autorizadas y de la forma autorizada
- **DISPONIBILIDAD**: garantizar que la información se encuentre disponible en tiempo y forma para quienes la requieran (y se encuentren autorizados)

Cualquiera de estos principios puede ser vulnerado, ya sea por un ataque deliberado, como por un evento accidental. Ej.: la configuración insegura de una aplicación puede permitir la divulgación de información procesada por la misma, la corrupción accidental de una base de datos puede ocasionar la pérdida de la integridad de la información almacenada, la falla en un componente de hardware puede ocasionar la falta de disponibilidad de la información gestionada por dicho equipo.

4.1.1 Posibles pérdidas

Cuando se habla de incidentes de seguridad que pueden ocurrir, la primera pregunta que surge es ¿cuáles son las posibles pérdidas? Todo incidente de seguridad, ya sea intencional u ocasional trae aparejado una pérdida que puede variar en magnitud. Si bien los CERTs son equipos de respuesta a incidentes de seguridad que se producen en su área de cobertura, ellos mismos no están exentos de padecer incidentes de seguridad en su propia estructura.

Las pérdidas asociadas a un incidente de seguridad pueden estar asociadas a activos tangibles o intangibles, esto es:

- **Pérdida de imagen**: podría darse por ejemplo si un CERT es víctima de un Defacement, es decir, la modificación arbitraria del contenido de su sitio web.
- **Pérdida de confiabilidad**: podría darse si la base de datos de un CERT, donde se almacena información de las organizaciones a las que presta servicio se corrompe. Esto podría dificultar la gestión de incidentes que fuesen reportados posteriormente, lo cual afectaría la confiabilidad de las organizaciones hacia el CERT.

- **Pérdida de económica**: un caso de robo de equipamiento, en donde un tercero consigue hacerse de componentes del CERT implicaría una pérdida de dinero (además de la pérdida y divulgación de información del CERT, lo cual causaría también otro tipo de pérdidas).
- **Incumplimiento legal**: si un tercero mal intencionado lograra acceder a las bases de datos de un CERT, donde se almacenan datos de incidentes reportados por las organizaciones, y divulgara dicha información, se estaría violando la Ley de Protección de Datos Personales. Esto además estaría acarreando pérdidas económicas, debido a las multas severas previstas en la ley y pérdida de confiabilidad de las organizaciones.

4.1.2 Conceptos iniciales

Antes de ingresar en la temática de la gestión de riesgos, es preciso definir algunos conceptos que serán utilizados con frecuencia a lo largo de este curso, ya que representan la base de la gestión de riesgos.

4.1.2.1 Activo de información

Se conoce como Activo de una organización a todo bien tangible o intangible que ésta posee que puede producir un beneficio. Los Activos de Información son aquellos activos de una organización que representan, contienen, almacenan o transmiten información. Los activos de información se agrupan en diferentes tipos que se relacionan entre sí. Si bien no existe una clasificación taxativa de activos, es posible identificar los siguientes:

- Funciones de la organización
- Información
- Sistemas
- Equipamiento
- Instalaciones
- RRHH

4.1.2.2 Amenaza

Evento cuya ocurrencia podría impactar en forma negativa en la organización. Las amenazas explotan (toman ventaja de) las vulnerabilidades. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación. A continuación se presenta una posible clasificación:

- Eventos naturales: huracanes, terremotos, tormentas de nieve, erupciones volcánicas, inundaciones, etc.
- Eventos terroristas, sabotajes o actos de guerra: bombas, secuestros, ataques químicos, etc.
- Accidentes: explosiones, incendios, cortes de energía u otros suministros, rotura de tuberías, desastres nucleares, choques de vehículos, etc.
- Otros eventos: errores en dispositivos, pérdida de comunicación, errores en los sistemas, errores humanos, vandalismo, etc.

4.1.2.3 Vulnerabilidad

Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

Ej.: Un centro de cómputo que carece de un sistema de detección de incendios (ausencia de un control). Un procedimiento de backup de datos que se encuentra desactualizado (control débil).

4.1.2.4 Exposición

Instancia en la cual la información o un activo de información es susceptible a dañarse o perderse por el accionar de una amenaza. La exposición, no significa que el evento que produce la pérdida o daño del recurso “esté ocurriendo”, solo significa que podría ocurrir dado que existe una amenaza y una vulnerabilidad que ésta podría explotar.

Ej.: Los servidores de un centro de cómputos que no cuenta con UPS se encuentran expuestos a un corte de energía.

4.1.2.5 Probabilidad de ocurrencia

Frecuencia con la cual una amenaza puede ocurrir.

Ej.: Se determina que en cierta zona sísmica puede ocurrir un terremoto cada 2 años.

4.1.2.6 Impacto

Consecuencias que produce un incidente de seguridad sobre la organización.

Ej.: Un defacement en el sitio web de una organización podría ocasionar una pérdida de imagen a la misma.

4.1.2.7 Riesgo

Probabilidad de que una amenaza explote una vulnerabilidad, en combinación con el impacto que esto ocasiona. Se conoce por riesgo como la función que combina la probabilidad de ocurrencia y el impacto de un incidente de seguridad.

4.1.2.8 Incidente de seguridad

Un incidente de seguridad es un evento adverso (evento con consecuencias negativas), que puede comprometer o compromete la confidencialidad, integridad o disponibilidad de la información.

Un incidente de seguridad se produce cuando una amenaza explota una vulnerabilidad.

Ej.: Un intruso irrumpe en un sistema de información, una inundación daña los expedientes almacenados en el archivo, un usuario ingresa a un sistema con la identidad de otro y efectúa una transacción que él no tiene permiso para realizar.

4.1.2.9 Control – Contramedida - Salvaguarda

Cualquier tipo de medida, que permita detectar, prevenir o minimizar el riesgo asociado con la ocurrencia de una amenaza específica. Para disminuir el nivel de un riesgo es necesario disminuir uno o los dos valores que intervienen en su fórmula, esto es, impacto o probabilidad de ocurrencia

Ej.: sistema biométrico de control de acceso al centro de cómputos, Hardening de un servidor, procedimiento de ABM de usuarios.

4.1.2.10 Relación entre conceptos

Los **activos** pueden presentar **vulnerabilidades** y encontrarse **expuestos a amenazas**.

Las **amenazas explotan vulnerabilidades**, ocasionando **incidentes de seguridad**.

Probabilidad de ocurrencia y el impacto de un incidente de seguridad determinan un **riesgo.**

Los **riesgos pueden ser mitigados** mediante la **implementación de controles**.

4.1.3 Proceso de gestión de riesgos

4.1.3.1 Política de gestión de riesgos

Al comenzar un proceso de gestión de riesgos es altamente recomendable definir una política. Una política es uno de los documentos que forman parte del esquema normativo de toda organización. Se trata de un documento global, que debe establecer pautas generales para definir la actividad en cuestión, en este caso, la gestión de riesgos.

A continuación se detallan algunas características clave que debe cumplir una política de gestión de riesgos:

- Alinearse a cualquier política existente en el CERT. No debe contradecirse con ninguna otra política existente.
- Ser aprobada por la autoridad, debido a su alcance estratégico.
- Contemplar como mínimo el siguiente contenido:
    - Objetivos de la gestión de riesgos
    - Definición de niveles aceptables de riesgo
    - Metodologías a adoptar
    - Definición de roles y responsabilidades

4.1.3.2 La gestión de riesgos

La gestión de riesgos es un proceso continuo y cíclico. No sirve de mucho realizar un análisis de riegos una vez y luego no revisarlo nunca más, ya que todo en las organizaciones es dinámico. Cualquier cambio organizacional, ya sea de tecnología, de recursos humanos, de estructura, etc.,

ocasiona modificaciones en el mapa de riesgos de la misma. Es por ello que se apunta a la gestión de riesgos como proceso continuo. La gestión de riesgos incluye el análisis de riesgos, pero éste es sólo una etapa del ciclo mayor

La gestión de riesgos se compone de dos fases:

A. Evaluación de riesgos

A su vez, la evaluación de riesgos comprende las siguientes tareas:

1. Identificación de riesgos
2. Análisis de riesgos

B. Tratamiento de riesgos

A su vez, el tratamiento de riesgos comprende las siguientes tareas:

1. Selección e implantación de técnica de tratamiento
2. Seguimiento y medición de resultados

La gestión de riesgos es un proceso cíclico que comienza en algún momento pero nunca finaliza, sino que sigue iterando y repitiendo paso a paso, con el objeto de mejorarse progresivamente. Por ello es necesario controlar la eficacia de todos los pasos del proceso de gestión de riesgos para lograr la mejora continua.

Una organización se encuentra siempre sometida a cambios. Los cambios pueden ser de diferentes tipos, por ejemplo:

- Cambios externos: como ser variaciones en las amenazas a los activos de información.
- Cambios internos: como ser cambios en su estructura, sus funciones, cambios tecnológicos, etc.

Todo cambio debe ser analizado para evaluar cómo afecta al mapa de riesgos existente. Esto se debe a que un cambio puede modificar los niveles de riesgo existentes, generar nuevos riesgos o eliminar otros existentes. Esto se debe a la posible variación de cualquier componente de riesgo: amenaza, vulnerabilidad, probabilidad de ocurrencia e impacto.

En esto consiste la retroalimentación del ciclo, ya que cualquier cambio organizacional ocasionará una nueva evaluación de los riesgos y una revisión de las medidas de tratamiento. Asimismo, deben programarse revisiones periódicas, independientemente a los cambios que se produzcan.

4.1.3.3 Evaluación de riesgos

La evaluación de riesgos es la primera de las dos fases que componen el proceso de gestión de riesgos de seguridad. Su objetivo es tomar conocimiento de los riesgos a los que se expone la organización, en materia de seguridad de la información.

La evaluación de riesgos se compone de dos tareas claramente diferenciadas, las cuales se detallan a continuación.

4.1.3.4 Identificación de riesgos

Para poder analizar los riesgos, primero éstos deben ser identificados. Esto consiste en conocer todos los componentes que combinados generan los riesgos.

- **Identificación de Activos**

El primer componente que debe identificarse son los activos de información de la organización. Los activos pueden agruparse en dos grandes conjuntos: tangibles e intangibles. A continuación vemos los ejemplos más comunes de activos:

- **Tangibles**
  - Funciones de la organización: procesos que se llevan a cabo en la organización para cumplir con sus objetivos. Ej.: compras, liquidación de haberes, gestión contable, etc.
  - Información: toda la información de la organización, en cualquier medio de almacenamiento como papel, CDs., bases de datos, archivos, etc. Ej.: información contable, información estratégica, información operativa, etc.
  - Sistemas: todo el software existente en la organización para soportar el desarrollo de sus funciones. Ej.: sistemas de gestión, aplicativos, motores de base de datos, sistemas operativos, etc.
  - Equipamiento: todos los componentes tecnológicos que dan soporte al desarrollo de las funciones de la organización. Ej.: servidores, PCs, routers, switches, etc.
    - Instalaciones: Edificaciones donde se ubica la organización, incluyendo el equipamiento no tecnológico que permite el funcionamiento de la organización. Ej.: instalación de refrigeración, sistemas contra incendios, muebles, etc.
  - RRHH: miembros de la organización.

- **Intangibles**
  - Privacidad
  - Seguridad y Salud de los empleados
  - Imagen y Reputación
  - Continuidad de las actividades
  - Moral del empleado

- **Identificación de dependencias entre activos**

Los activos identificados en el inventario no son componentes aislados, sino que deben verse como parte de una red en la cual existen dependencias entre dichos activos. Por ello aparece como importante el concepto de “dependencias entre activos” o la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

Se dice que un “activo superior” depende de otro “activo inferior” cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

- **Valoración de activos**

Luego de confeccionar el inventario de activos, es preciso evaluar el valor que cada uno de ellos representa para la organización. Esto se debe a que no todos los activos representan el mismo valor, y esto debe ser conocido para el momento de realizar el análisis costo-beneficio de implementar controles sobre dichos activos.

El valor de un activo depende de muchos factores que deben tenerse en cuenta. Algunos de ellos pueden expresarse en forma cuantitativa, y otros en forma cualitativa. A continuación se lista una especie de check list de aspectos a considerar para determinar el valor de un activo, también denominados elementos de valoración. Debe tenerse en cuenta que estos puntos no aplicarán a todos los activos, ya que depende del tipo de activo que se trate:

- Costo de reposición: adquisición e instalación
- Costo de mano de obra (especializada) invertida en recuperar (el valor) del activo
- Lucro cesante: pérdida de ingresos

- Daño a la organización por pérdida de confidencialidad
- Daño a la organización por pérdida de integridad
- Daño a la organización por pérdida de disponibilidad
- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- Sanciones por incumplimiento de la ley u obligaciones contractuales
- Daño a otros activos, propios o ajenos
- Daño a personas
- Daños medioambientales

El valor puede ser propio del activo, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos. Muchas veces se decide valorar sólo el nivel de Información (datos), y obtener el valor de los activos de los niveles restantes mediante acumulación.

- **Identificación de Amenazas y vulnerabilidades**

Los activos identificados pueden presentar vulnerabilidades y estar expuestos a amenazas. Ambas situaciones deben ser identificadas en esta parte del proceso ya que son la base para la evaluación de riesgos.

Como primera medida deben evaluarse las amenazas que pueden afectar a cada uno de los activos identificados. No todas las amenazas afectan a todos los activos, es más, en general para cada tipo de activo existe un conjunto de amenazas relacionadas. Existen catálogos de amenazas por tipo de activo que resultan de gran utilidad a la hora de identificar las amenazas. A continuación se citan algunos ejemplos de amenazas por tipo de activo.

Activo	Amenaza
Entorno	Desastres naturales Incendio
Equipamiento	Desastres naturales Incendio

	Fallas de hardware Fallas de administración Robo
Sistemas	Código malicioso Fallas de administración Intrusión
Información	Robo Alteración Divulgación Destrucción
Funciones de la organización	Interrupción
RRHH	Desastres naturales Incendio Enfermedades Huelgas Ingeniería social

- **Identificación de controles**

Se debe tener en cuenta que, para que las amenazas se materialicen sobre los activos, éstos deben presentar alguna vulnerabilidad que las amenazas puedan explotar. Si no existen vulnerabilidades, entonces el activo no se encuentra expuesto, y por ende, no existirá riesgo. Por lo dicho, resulta necesario analizar las vulnerabilidades que presenta un activo, para así poder efectuar una relación: ACTIVO – VULNERABILIDAD – AMENAZA

Dado que una vulnerabilidad es la inexistencia o la debilidad de un control, resulta necesario en esta etapa analizar los controles existentes en los activos. Además, los controles existentes influirán en la probabilidad de ocurrencia y el impacto de las amenazas, lo cual será evaluado más adelante en el proceso:

- Probabilidad de ocurrencia: existen controles cuyo objetivo es tratar de evitar que ocurran incidentes. Se denominan controles preventivos

- Impacto: existen controles que buscan detectar la ocurrencia de incidentes, denominados controles detectivos, y controles cuyo objetivo es minimizar los efectos de un incidente y recuperarse de los mismos, denominados controles correctivos.

4.1.3.5 Análisis de riesgos

Los riesgos son determinados por una combinación de la probabilidad de ocurrencia y el impacto de una amenaza sobre un activo vulnerable. Para poder calcular el nivel de riesgo, es necesario conocer las dos variables que lo determinarán: probabilidad de ocurrencia e impacto.

- **Determinación de la probabilidad de ocurrencia de las amenazas**

Se trata de la frecuencia con la cual una amenaza puede materializarse en un período determinado. El período más comúnmente empleado para esta evaluación es un año, por lo que debe estimarse la cantidad de veces que puede ocurrir una amenaza en un año. Continuando con el proceso descrito, deben analizarse para cada activo, y para cada amenaza cuántas veces en un año podría esta materializarse.

Determinar la probabilidad de ocurrencia no es una tarea simple, ya que como su nombre lo indica no es algo exacto, sino una estimación. Existen datos que pueden colaborar en la determinación de la probabilidad de ocurrencia:

- Información histórica de la organización: si la organización guarda un registro de los incidentes ocurridos, podrá conocer cuántas veces se ha materializado una determinada amenaza en un plazo determinado
- Información estadística del mercado: existen fuentes de información que brindan datos sobre el índice de ocurrencia de amenazas. Es el caso por ejemplo de los desastres naturales.

- **En el caso de ataques deliberados**
  - Motivación de la fuente de amenaza: la fuente de amenaza es aquello que la ocasiona, por ejemplo, un intruso es la fuente de amenaza de una intrusión a un sistema. Se estima que si la motivación de la fuente de amenaza es alta, entonces es más probable de que la misma ocurra.
  - Capacidades de la fuente de amenaza: se estima que si las capacidades que debe tener la fuente de amenaza para concretarla son bajas, entonces es más probable que la misma ocurra. Por ejemplo, existen actualmente numerosas herramientas de

libre acceso en internet para la intrusión en sistemas, con lo cual las capacidades que debe tener un intruso son bajas ya que con la ayuda de dichas herramientas puede lograr su cometido. Esto hace que la probabilidad de ocurrencia de las intrusiones aumente.

- **Inversión requerida**

Se estima que si se requiere de una inversión importante para efectuar un ataque, entonces es la probabilidad de ocurrencia de dicho ataque disminuye.

- **Determinación del impacto de las amenazas**

Se denomina impacto al nivel de daño sobre un activo derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación que causan las amenazas, es posible calcular el impacto que estas tendrían para la organización.

Existen dos tipos de impacto a calcular: acumulado y repercutido.

- El ***impacto acumulado*** se calcula teniendo en cuenta:
  - El valor acumulado de un activo: dado por su valor propio y el acumulado de los activos que dependen de él
  - La degradación causada por las amenazas a las que se expone el activo

  El impacto acumulado es:
  - Tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.
  - Tanto mayor cuanto mayor sea la degradación del activo afectado.

  Por el contrario, el ***impacto repercutido*** se calcula teniendo en cuenta:
  - El valor propio del activo
  - La degradación causada por las amenazas a las que se exponen los activos de los que dependen

  El impacto repercutido también se calcula para cada activo y por cada amenaza.

  El impacto repercutido es:
  - tanto mayor cuanto mayor es el valor propio de un activo.
  - tanto mayor cuanto mayor sea la degradación del activo atacado.

- tanto mayor cuanto mayor sea la dependencia del activo atacado.

- **Cálculo del riesgo**

El riesgo es una función de la probabilidad de ocurrencia y del impacto de una amenaza. El nivel de riesgo es directamente proporcional a la probabilidad de ocurrencia y al impacto, es decir que si cualquiera de las dos variables aumenta, entonces también aumentará el nivel de riesgo.

- El ***riesgo acumulado*** de un activo se calcula teniendo en cuenta:
  - el impacto acumulado sobre un activo debido a una amenaza
  - la probabilidad de ocurrencia de la amenaza

El riesgo acumulado se calcula para cada activo y por cada amenaza.

El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

- El ***riesgo repercutido*** de un activo se calcula teniendo en cuenta:
  - el impacto repercutido sobre un activo debido a una amenaza
  - la probabilidad de ocurrencia de la amenaza

El riesgo repercutido se calcula para cada activo y por cada amenaza

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

4.1.3.6 Tratamiento de riesgos

Una vez evaluados y conocidos los riesgos, es necesario definir qué se hará con cada uno de ellos. La etapa de conocimiento y evaluación de los riesgos es tan importante como la de su tratamiento. Existe un conjunto de alternativas sobre las formas de tratar los riesgos. La organización deberá evaluar qué alternativa le conviene para tratar cada uno de sus riesgos y formalizar las decisiones tomadas en un Plan de Tratamiento de Riesgos, estableciendo en el mismo prioridades de implementación y plazos de cumplimiento.

4.1.3.6.1 Selección e implantación de técnicas de tratamiento

Las formas de tratamiento de riesgos son:

- **Mitigar el riesgo**

Mitigar el riesgo implica implementar controles que reduzcan una de las dos variables, o ambas a la vez, que determinan el nivel de riesgo, esto es:

- La probabilidad de ocurrencia: por ejemplo, eliminar el material inflamable del centro de cómputos reduciría la probabilidad de que se produzca un incendio.
- El impacto: por ejemplo, contar con un sitio alternativo de procesamiento reduciría el impacto en caso de ocurrir un desastre natural que afecte al sitio primario.

La decisión de qué control implementar debe responder a un análisis correcto del costo-beneficio de la implementación del control.

Análisis costo-beneficio

En líneas generales, una organización no debería invertir en un control que resulte más costoso que la pérdida que pudiera sufrir por no tener dicho control implementado (en el peor de los escenarios).

- **Aceptar el riesgo**

Los riesgos no pueden ser mitigados totalmente, por lo que en cierta instancia se debe terminar asumiendo o aceptando ciertos riesgos. Por otra parte, existen ocasiones donde no vale la pena tomar ninguna otra acción dado que la relación costo-beneficio de tratar el riesgo no lo justifica.

Es por ello que la organización debe definir un Nivel de Riesgo Aceptable, de manera que todos los riesgos que se encuentren por debajo de este nivel puedan ser aceptados por la organización. El Nivel de Riesgo Aceptable se define en los mismos términos que se definen los niveles de riesgo. La definición de este nivel es sumamente crítica, ya que el establecimiento de un nivel inadecuado puede ocasionar pérdidas importantes a la organización.

- **Transferir el riesgo**

Esta medida de tratamiento involucra a terceras partes, quienes sostienen o comparten una parte del riesgo. Generalmente hay algún costo financiero asociado a la transferencia de parte del

riesgo a otra organización, tal como las cuotas abonadas a los seguros. La transferencia de un riesgo a otras partes reduce el riesgo original para la organización que transfiere.

- **Evitar el riesgo**

Quizás esta sea la opción menos común, ya que consiste en no seguir adelante con la actividad que probablemente crea el riesgo (cuando esto sea practicable), de manera que el mismo ya no exista. Una de las formas más simples de evitar un riesgo es eliminar el activo que lo presenta.

Ocurre en ocasiones que se combinan más de una estrategia de tratamiento para un mismo riesgo. Por ejemplo, para el tratamiento del riesgo incendio, se contrata un seguro (transferencia de parte del riesgo) y se implementan sistemas de detección y extinción (mitigación del riesgo).

Por otra parte, ciertas técnicas de tratamiento de riesgo pueden servir para tratar más de un riesgo a la vez. Por ejemplo, la contratación de un seguro edilicio puede servir para tratar varios riesgos causados por diferentes amenazas (incendio, robo, inundación, etc.).

Luego de definir el Plan de Tratamiento de Riesgos debe calcularse el riesgo residual, es decir, aquel riesgo remanente luego de haber implementado las técnicas de tratamiento.

4.1.3.6.2 Seguimiento y monitoreo

Una vez tratados los riesgos, es preciso garantizar que se cumple con los objetivos previstos. Es decir, que cada medida de tratamiento implementada presenta los resultados esperados. Para ello es necesario efectuar un seguimiento y monitoreo de los riesgos mitigados y transferidos.

Esto se logra estableciendo métricas que evalúen el desempeño de los controles implementados y muestren si se logra reducir los riesgos para los cuales se seleccionaron.

Por ejemplo:

Riesgo identificado: incendio del centro de cómputos
Nivel de riesgo inicial: 3 (en una escala del 1 al 5)
Estrategia de mitigación: Transferencia (mediante seguro contra incendio) y mitigación (mediante un sistema de detección y extinción de fuego)
Nivel de riesgo residual esperado: 1

En este ejemplo, las métricas deberían evaluar si el nivel de riesgo residual esperado se está

cumpliendo, por ejemplo, evaluando si se efectúa un mantenimiento al sistema de detección y extinción, o si la póliza contra incendio se encuentra actualizada con las recientes adquisiciones de equipamiento.

El progreso real respecto de los planes de tratamiento de los riesgos provén una medida importante de desempeño y deberían ser incorporados en el sistema de información, medición y administración de desempeño de la organización.

En caso de que se detecte alguna insuficiencia en el desempeño de las medidas de tratamiento, se deberán efectuar las correcciones necesarias, esto es, ajustar el tratamiento o cambiar de estrategia.

4.1.4 Documentación y comunicación

Debe registrarse en forma adecuada cada etapa del proceso de gestión de riesgos. Deberían documentarse las hipótesis, métodos, fuentes de datos, análisis, resultados y razones para las decisiones.

Los registros de tales procesos son útiles para:

- Demostrar que el proceso es conducido apropiadamente.
- Proveer evidencia de un enfoque sistemático de identificación y análisis de riesgos.
- Proveer un registro de los riesgos y desarrollar la base de datos de conocimientos de la organización.
- Proveer información a los tomadores de decisiones.
- Alinearse a lo recomendado por las auditorías.

Los resultados de la gestión de riesgos deben ser comunicados en principio a los tomadores de decisiones y a las autoridades de la organización.

4.1.5 Mejora continua

El proceso de gestión del riesgo de seguridad de la información debe tender a un enfoque de mejora continua. En cada iteración del ciclo deben evaluarse un conjunto de factores con el objeto de verificar que el proceso:

- Se encuentra alineado con la estrategia de la organización
- Resulta de utilidad para la toma de decisiones
- Responde a los requisitos legales y normativos

- Presenta criterios adecuados para el cálculo de riesgos
- Cuenta con los recursos necesarios
- Presenta una definición adecuada de nivel de riesgo aceptable

Asimismo, deberán considerarse cualquier oportunidad de mejora detectada en el proceso, con el objetivo de planificar las modificaciones necesarias al circuito para colaborar en la mejora continua del mismo.

4.2. Gestión de Recursos Humanos en un CSIRT

Resumen.

El pilar fundamental de una Organización, Institución o Equipo, son las personas que lo constituyen. Para lograr el éxito en las tareas desarrolladas, es indispensable establecer pautas y procedimientos para el Personal, que se enmarquen dentro de un Programa de Gestión de los Recursos Humanos. Y si éste, se alinea con el Proceso de Administración de Riesgos, se obtienen aún mejores resultados.

El vínculo laboral comienza a gestarse en el proceso de selección de las personas, se establece en su contratación, se profundiza con los mecanismos de integración, capacitación, motivación y protección, y finaliza al momento de la desvinculación. Establecer los procedimientos adecuados para cada una de las instancias, potencia los beneficios del vínculo y minimiza los riesgos que pueden surgir.

En el presente documento se analiza la importancia del Factor Humano en las Instituciones y en particular en los CSIRT's, se establecen los perfiles requeridos, diferenciando el Rol Gerencial del Técnico, y se remarca el valor de la Capacitación, de la Motivación y de la Protección del personal. Se establecen las Pautas de una Política de Gestión de Riesgos y del Plan de Contingencia relativos los Recursos Humanos. Finalmente se presentan cuatro Procedimientos considerados fundamentales para la gestión del Personal del CSIRT: de Selección, Vinculación, Protección de Identidad y Desvinculación.

Los anexos contienen puntos esenciales para la elaboración de un Plan de Capacitación, de Compromisos de Confidencialidad, de Evaluaciones del Personal, de Actas de Desvinculación y de Registro de los Riesgos.

Toda la información comprendida en este documento constituye una guía para Gestionar el staff de un CSIRT y sus Riesgos asociados, sobre la cual cada uno deberá realizar la adaptación correspondiente a sus necesidades particulares.

Objetivos

- **Inmediato**

Establecer las principales recomendaciones sobre la gestión de los Recursos Humanos que componen un CSIRT, basadas en las mejores prácticas, para optimizar la prestación de sus servicios, disminuyendo los riesgos inherentes al personal que lo integra.

- **De desarrollo**

Implementar un sistema de Gestión del Capital Humano de los CSIRT's, que permita medir su efectividad y mitigar oportunamente los riesgos asociados.

4.2.1 Introducción

Es indudable que el componente humano dentro de cualquier Equipo u Organización, es esencial para lograr el cumplimiento de los objetivos que procuran alcanzar. Por ello es necesario adoptar las medidas adecuadas para su administración.

Dada la naturaleza sensible del servicio que brindan los Centros de Respuesta a Incidentes de Seguridad Informática, la buena gestión del personal que lo integra y el desarrollo de vínculos que promuevan la solidez del Equipo, son fundamentales para su éxito.

A través de un Programa Integral de Gestión del Personal de un CSIRT se pretende superar la complejidad que traen consigo la libertad de información y todos los avances tecnológicos que la fomentan, a través del fortalecimiento de sus miembros.

Todos los aspectos que inciden en el vínculo profesional serán detenidamente analizados, abarcándose desde el establecimiento de criterios de selección del personal, mecanismos de integración progresiva y de retención, de protección y de desvinculación; de modo que en todas las instancias del proceso laboral, los riesgos asociados a las personas sean controlados.

4.2.2 Importancia del Capital Humano y la Gestión de sus riesgos

Así como los riesgos, el personal siempre forma parte de la Organización. Cada decisión que se toma en la Empresa tiene un componente humano; cuál opción es elegida y cómo se lleva a cabo depende de las personas que participan en ella. Por lo tanto, la gestión de los RRHH

debe estar integrada al proceso de toma de decisiones, así como también al de Administración de Riesgos.

Existen tres dimensiones a través de las cuales el factor humano interviene en el Proceso de Administración de los Riesgos. La primera, como una fuente de Riesgos, capaces de materializarlos a través de sus propias acciones. Éstas pueden ser intencionales, por falta de capacitación o debido a otro tipo de errores que no tengan un propósito malicioso. Una segunda dimensión es la del Recurso Humano como víctima de la materialización de ciertos riesgos, como por ejemplo la pérdida de una vida humana o el daño en su salud. Finalmente, como ejecutores de los procedimientos de gestión de Riesgos establecidos, influyen directamente en las decisiones que se tomen basadas en los Análisis de Riesgos que realizan.

Es necesario alinear las actividades de gestión del personal y la metodología de Administración del Riesgo a los objetivos de la Institución, a su misión y valores. Garantizando que la persona correcta esté en el puesto apropiado, que sea entrenada, protegida y recompensada adecuadamente, incrementa la posibilidad de que tome decisiones más eficaces; lo que contribuye con la prevención de riesgos.

Las siguientes preguntas pueden servir de referencia para iniciar el análisis de la situación respecto al personal:

- ¿Ha sido contratada la persona correcta para el puesto?
- ¿Está la persona apropiadamente calificada, preparada y capaz para realizar la tarea que se le requiere?
- ¿Está la performance de los miembros alineada con la misión, valores y objetivos de la Institución?
- ¿Está la comunidad satisfecha con el nivel de servicio brindado?
- ¿Ha sido provista la correcta dirección y guía al personal para asegurar que ellos entienden las tareas asignadas?
- ¿Son los recursos adecuados o apropiados para cubrir las necesidades del rol, incluyendo el entrenamiento?
- ¿Es la remuneración acorde con los niveles adecuados?

- ¿Está el personal adecuadamente motivado para hacer las tareas requeridas de la mejor manera?

4.2.3 Medidas preventivas de los riesgos asociados a las personas

A continuación se plantean diversos aspectos sobre los cuales se puede profundizar, utilizándolos como mecanismos de prevención de los riesgos asociados al personal:

- Análisis del puesto y descripciones documentadas. Permite determinar claramente las obligaciones y las habilidades tanto personales como técnicas requeridas para el puesto.
- Contratación, cuyo objetivo es cubrir cada puesto vacante con la persona adecuada. Es una de las actividades más difíciles, por ello lo más adecuado es establecer los requerimientos de la forma más detallada posible y procedimientos de selección del personal.
- Integración y Capacitación. El proceso de integración es a través del cual se introduce al personal en la misión, valores y cultura de la Institución y su Comunidad. La capacitación es fundamental para brindar los servicios de forma adecuada.
- Disciplina, implica darle a cada empleado las Normas, Políticas y Procedimientos utilizados en la Organización y luego trabajar con él para que los incorpore.
- Seguridad, tanto física, ambiental y emocional que permitan el desempeño de las tareas asignadas con el menor nivel de riesgo posible.
- Compensación, incluye la recompensa monetaria como la no monetaria. Deben ser viables para la organización así como también cumplir con las necesidades del empleado.
- Evaluación del personal, es necesario que sea continua, en conjunto con el personal, sobre cómo está desempeñando sus tareas en relación a lo requerido; permitiendo una instancia de retroalimentación, en la que se identifiquen aspectos a mejorar y en la que se intercambien las distintas necesidades y visiones.

4.2.4 Gestión del Personal de un CSIRT

4.2.4.1 Consideraciones generales

El equipo de un CSIRT debe:

- Proveer un canal seguro para recibir reportes de incidentes.

- Proveer de asistencia a los miembros de su comunidad para el manejo de los incidentes a la vez de capacitarlos.
- Brindar la información adecuada y de la manera correcta a las partes involucradas, en relación a los incidentes.

El trabajo de un CSIRT es básicamente la provisión de servicios, siendo imprescindible que exista confianza en un staff competente y fidedigno. De los mayores retos para un equipo de Respuesta a incidentes de seguridad informáticos es la selección del staff. Se podría pensar que uno de los atributos más importantes es la experiencia en seguridad de los sistemas y sus conocimientos técnicos. Sin embargo, el éxito del equipo puede verse comprometido si uno de sus integrantes se comporta inadecuadamente, degradando la confianza en el equipo. Por ello, los atributos personales resultan extremadamente importantes para la elección de un nuevo miembro.

Es recomendable contratar personas con menos experiencia técnica pero con buenas habilidades en el trato interpersonal y en la comunicación, ya que la experiencia la puede adquirir en el trabajo diario y en base a un sistema de entrenamiento que se haya establecido en el CSIRT.

Se debe considerar también el presupuesto que se dispone para el reclutamiento y mantenimiento de los integrantes de un CSIRT. Los recursos económicos disponibles, afectan la calidad del equipo ya que de éstos dependen los salarios, la capacitación, la infraestructura, y otros factores que contribuyen a desarrollo de las actividades del CSIRT. Determinar el número apropiado a trabajar en él, es un balance entre la expectativa de trabajo que existe y las restricciones presupuestales.

Según expertos en el tema, casi el único atributo en común de los CSIRT existentes es que no cuentan con fondos apropiados, no tienen suficiente personal mientras que sí experimentan una gran demanda de sus servicios

La composición de un CSIRT varía de equipo en equipo, en función de elementos tales como su misión y objetivos, la naturaleza y el rango de los servicios que ofrece, la disponibilidad de personal experto, de las tecnologías utilizadas, del tipo de incidentes que se manejan, etc.

La conformación del Equipo se puede realizar de diversas formas:

- Contratar personal dedicado exclusivamente al CSIRT.
- Utilizar personal de sistemas y de redes ya existente.
- A través de tercerizaciones del servicio.

- Extensión del grupo por un lapso determinado cuando el flujo de trabajo así lo requiera.

Esta última posibilidad contempla las necesidades de contratar personal extra en ocasiones donde la complejidad amerite la participación de un experto en un tema puntual, o en momentos en que el número de integrantes del CSIRT no pueda cumplir con las demandas que se experimenten. En este caso hay que realizar consideraciones especiales y tener previsto la implantación de procedimientos de seguridad adecuados, que reduzcan los riesgos que esto implica, a niveles que sean aceptables.

Visto que la tasa de incidentes no es constante, el éxito de un CSIRT usualmente se mide en referencia a su actuación durante los tiempos de mayor demanda. Debe haber entonces, capacidad suficiente de personas para manejar efectivamente los incidentes complejos. Un fallo en esto resultará en perjuicio de la reputación de todo el grupo.

Cuando el nivel de incidentes a resolver disminuye, existen otras tareas muy importantes y motivadoras para realizar, tales como el desarrollo de herramientas, preparación de seminarios, investigaciones sobre ciertos temas de interés, etc.

Dentro del CSIRT, debe de existir un referente, que cumpla el rol Gerencial, con gran capacidad de liderazgo que, además de dirigir el trabajo diario del Equipo, gobierne las decisiones estratégicas, de políticas y procedimientos, de infraestructura y las acciones operativas que así lo requieran. Nos referiremos a esta figura como el Gerente del CSIRT y lo distinguiremos del Personal Técnico.

La habilidad del CSIRT para brindar los servicios necesarios a su comunidad depende de la calidad, motivación y gestión de sus integrantes. El CSIRT debe asegurar que:

- El staff se selecciona basado en sus méritos, que es administrado y motivado adecuadamente, que entiende sus responsabilidades y recibe el entrenamiento preciso.
- Se evita la discriminación tanto de género como de raza, tanto en la selección de los candidatos como en las oportunidades de crecimiento profesional y/o académico dentro del Equipo.
- Se promueve un clima positivo y constructivo dentro del Equipo y en el relacionamiento de éste con los demás involucrados (la comunidad, otros CSIRT's, proveedores, medios de comunicación, etc.).

- Que se recompensa adecuadamente, tanto en plazos como en montos, y se utilizan otros mecanismos de retribución no monetarios.

Una nota aparte aquí es la consideración de otro tipo de personal que está vinculado al CSIRT, como por ejemplo de limpieza, instalaciones, de seguridad, y otros; para quienes se deben establecer las condiciones de acceso. Su entrada puede ocurrir durante las horas de trabajo del Equipo o luego de éstas. Aquí resultan esenciales llevar a cabo las buenas prácticas de los miembros del Equipo, tales como no dejar información sensible en los escritorios durante su ausencia, no dejar los equipos abiertos, etc. Un mecanismo adicional de seguridad podría ser el impedimento del ingreso del personal ajeno al Equipo fuera del horario de trabajo del mismo, así se garantiza que hay un miembro presente siempre que un externo acceda a las instalaciones del CSIRT.

4.2.4.2 Capacitación

Un eslabón fundamental para el desarrollo de un Equipo de Respuesta a Incidentes Informáticos es el entrenamiento de sus miembros. Es necesario desde tres perspectivas:

- Al personal nuevo, es importante brindarle las herramientas de conocimiento necesarias para realizar su trabajo.
- Al personal que ya está trabajando, para expandir su sapiencia y así generar un círculo virtuoso de conocimiento que se expanda al resto de los integrantes.
- Para estar al día con las últimas tecnologías y los mecanismos de ataque contra ellas.

La existencia de Plan o Programa de Capacitación para los miembros del CSIRT contribuye a la reducción de los riesgos que se pueden materializar por falta de información y entrenamiento del personal.

En primera instancia, cuando un nuevo miembro ingresa al CSIRT, se lo debe instruir en la Misión, los Objetivos, las Políticas, los Procedimientos y en el ambiente operacional del equipo.

Iniciación en:

- Temas de confidencialidad y no revelación de la información.
- Políticas y Procedimientos de Seguridad Informática y gestión de Riesgos.
- Código del Conducta.

- Políticas de uso aceptable.
- Cuestiones legales.
- Visión general de los procedimientos de respuesta a incidentes.

Temas respectivos a la Organización:

- Líneas generales de la Comunidad para la cual trabajan.
- Historia y Organización del CSIRT, así como la misión, los objetivos y valores que se manejan internamente.
- Aspectos legales pertinentes.

Cuestiones Técnicas:

- Herramientas y procedimientos de clasificación, correo electrónico y manejo de incidentes.
- Comunicaciones seguras.
- Incidentes de baja prioridad.
- Incidentes con alta prioridad.

Cuestiones de comunicación y trato con los medios:

- Políticas de relacionamiento con los medios.
- Comunicación con la Comunidad y con otros terceros, tanto por vía oral como escrita.

Ante el estrés que produce el manejo de información sensible, el nuevo integrante puede sentirse abrumado con todo el material recibido en el CSIRT. Es necesario darle el tiempo adecuado para que incorpore todo ello y no exponerlo al principio a tareas delicadas.

Es deseable tratar de asegurar que la persona nueva pueda aprender la profesión sin generar errores de gran costo. Además de lo ya mencionado, una contribución a ello sería designar a un miembro con experiencia del CSIRT como su instructor, para que le proporcione toda la información necesaria, e incluso lo monitoree durante los primeros días, apoyándolo en las tareas que se le asignen.

Otro mecanismo de integración a las actividades del Equipo es que dedique un tiempo a la observación del manejo de los incidentes por parte de miembros expertos.

Lo referido anteriormente se basa en la idea que cada nuevo integrante realice una adaptación progresiva, tanto a nivel personal como técnico, al Equipo y a sus tareas. Se establece así la forma en que actuará el nuevo personal, desde un nivel básico a su llegada para convertirse en un gestor de incidentes completo, dedicándose a tareas más complejas.

Es importante que el conocimiento ya adquirido por el Equipo, se organice en Procedimientos y materiales de estudio, lo que permite resaltar las áreas en las que el CSIRT ya ha adquirido experticia y que los mismos miembros del CSIRT se vuelvan mejores entrenadores.

La Capacitación es continua, no tiene final ya que debe acompasar los cambios que se van produciendo a nivel tecnológico. Debe extenderse el conocimiento adquirido a todo el Equipo, generando un proceso beneficioso de retroalimentación y de respaldo en el momento de instruir a la Comunidad y/o a otros Equipos de Respuesta. Y como una de las formas de prevención es el conocimiento, el establecer un Plan adecuado de capacitación contribuye a disminuir el riesgo de la materialización de incidentes informáticos.

4.2.4.3 Motivación y Retención del Staff

La baja oferta de personal experto para los CSIRT's, y la alta inversión que se realiza en sus capacitaciones llevan a considerar seriamente los mecanismos para evitar la posibilidad que abandonen el Equipo. Una vez que se invirtió tiempo y recursos para identificarlo, contratarlo y entrenarlo, lo más importante luego es retenerlo.

Las dos razones principales por las que el personal de un CSIRT puede tomar la decisión de dejar el Equipo son el agotamiento y el bajo salario, si bien también influye el ambiente laboral, la noción de grupo y pertenencia, las posibilidades de crecimiento personal y profesional. Es en estas áreas donde hay que concentrar esfuerzos para evitar las posibles pérdidas.

El Riesgo de trabajo es entendido como la posibilidad de que, al realizar una tarea, ésta genere incidentes y/o accidentes, concepto bien importante.

Es parte de la responsabilidad de cualquier Institución cuidar a sus empleados, protegerlos de accidentes y asegurándoles un ambiente de trabajo saludable. Las condiciones de trabajo no deben perjudicar ni física, ni moralmente. A través de Procedimientos de protección física, ambiental y de identidad se puede respaldar a los miembros del Equipo. Su seguridad debe ser meticulosamente planificada.

Durante la gestión de los incidentes, los integrantes del CSIRT, en su comunicación con la Comunidad o con otros involucrados, deben realizar indicaciones. A partir de éstas, pueden surgir malos entendidos y errores, con resultados adversos; por lo que se hace necesario establecer mecanismos de protección de identidad para los miembros del CSIRT.

En todo el Equipo, e Institución a la que responde, se debe fomentar una "cultura de seguridad y prevención de riesgos", que conduzca a alcanzar altos niveles de productividad y una consecuente eficiencia en su gestión. Partiendo de la idea de prevenir, se hace necesario promover conciencia en los miembros del Equipo sobre la prevención de actos inseguros y de errores humanos.

Se puede establecer un marco a través del cual los miembros reporten y resuelvan sus errores, haciendo énfasis en la solución y no en el problema. Tales políticas pueden plantear que todos los eventos complejos requieran una revisión de las acciones por las figuras gerenciales y por el resto del staff, para determinar qué se puede hacer en el futuro para prevenir su reiteración. Esto puede implicar cambios en el corto plazo en los procedimientos, o de largo plazo en el entrenamiento. Lo importante es que todos sientan que pueden reportar los problemas sin miedo a sufrir represalia.

Los controles de seguridad a través de los cuales se procura evitar fugas de información, errores en el manejo de los datos y sistemas, y proteger la confidencialidad de las actividades del CSIRT, no están asociados a restricciones en las libertades de los trabajadores sino que son importantes para el amparo de los mismos.

- **Principales factores de error humano:**
    - La falta de capacitación
    - Condiciones inadecuadas de trabajo tanto ambientales, de tiempo y sociales.
    - Mal ingreso o mal manejo de la información por distracción y/o agotamiento.
    - Realizar asunciones incorrectas por insuficiente información.
    - Inadecuada interpretación de las conclusiones

Ver Procedimiento de Protección de Identidad de los miembros del CSIRT.

4.2.5 Política Gestión de Riesgos RRHH del CSIRT

Política ajustada a la “Política de Gestión de Riesgos” planteada en la sección 4.1.

4.2.5.1 Objetivo

Evitar y/o minimizar los riesgos a los que se expone el personal del CSIRT, contribuyendo a mejorar la eficiencia del Equipo.

4.2.5.2 Alcance

Esta política es aplicable a todos los miembros del CSIRT y debe estar alineada con otras directivas particulares de la Comunidad a la cual brinda sus servicios.

4.2.5.3 Proceso Gestión de Riesgos

El Proceso de Gestión de Riesgos de los RRHH del CSIRT se divide en dos grandes instancias: la Evaluación de Riesgos y el Tratamiento de los mismos.

- **Evaluación de riesgos**
  - **Identificación de Riesgos**
    - Identificación de Activos, en este caso nos vamos a referir al Recurso Humano como activo, en sus tres dimensiones, víctima de un Riesgo, generador del mismo y como tomador de decisiones dentro del Proceso de Gestión de Riesgos.
    - Identificación de dependencias entre activos, se establecerá la red de vinculaciones entre otros activos y el personal.
    - Valoración de activos, dado que se trata de personas, y por lo tanto los activos más críticos, es de gran significancia cualquier riesgo que puedan experimentar o generar. Por ello es muy importante realizar una correcta valuación.
    - Identificación de Amenazas y vulnerabilidades, a continuación se plantea una guía (no exhaustiva) de factores a analizar para identificar en ellos posibles amenazas y vulnerabilidades:
      - Exigencias de las actividades que se realizan en el puesto de trabajo. Las exigencias de las tareas recogen los requerimientos, normas, procedimientos que rigen al personal en el desempeño seguro de su trabajo (Código de Ética,

Políticas de Seguridad, Procedimientos y/o Política de Comunicación, Procedimiento de Protección de identidad, etc.). Además también abarca los requerimientos y exigencias técnicas para el uso de los medios de trabajo, herramientas y lugar físico, que garanticen la seguridad de las personas en primer lugar y la de los distintos procesos que se llevan a cabo por el Equipo.

- Análisis del factor humano. Una vez que éste se encuentre desempeñándose en determinado puesto de trabajo dentro del CSIRT (luego de haber sido elegido en un correcto proceso de selección de personal), es importante monitorear las actividades que realiza y apoyarlo en las dificultades que se le presenten. Es importante aquí considerar las Evaluaciones periódicas del personal.
- Análisis de los medios y las condiciones de trabajo. Los medios de trabajo constituyen la tecnología e infraestructura con las que cuenta la persona para la realización de sus actividades y son vulnerables de sufrir siniestros que afecten la integridad del personal, además de ser un posible blanco de acción maliciosa por parte del personal.
- Legislación. Considerar el marco legal en el que se desenvuelve el CSIRT es vital para su correcto desempeño, y es un gran factor de riesgo el no cumplirlo. Todas las actividades que estén regidas por éste, deben ser monitoreadas para garantizar su cumplimiento.
- Recursos económicos. La forma de planificar los recursos, debe seguir al previo análisis de la necesidad de los mismos. Es importante saber con qué recursos se cuentan para distribuir el capital de la manera más eficiente.
- Estimulación y recompensa del personal. Son factores que permiten disminuir los riesgos de fraude y abandono por parte del personal, riesgos muy costosos en caso que se materialicen.

- Identificación de controles, son todas las acciones que permiten reducir la probabilidad y/o el impacto de la materialización de los riesgos identificados. Estos pueden ser desde Políticas y/o Procedimientos establecidos para el desarrollo de las actividades del CSIRT, como instancias de Evaluación, Diálogo, etc.; que puedan

generar instancias de intercambios entre los miembros del CSIRT para la toma de decisiones adecuada.

- **Análisis de riesgos (Ver mecanismos establecidos en la sección 4.1)**

  - **Determinación de la probabilidad de ocurrencia de las amenaza.** Se trata de la frecuencia con la cual una amenaza puede materializarse en un período determinado. El período más comúnmente empleado para esta evaluación es un año, por lo que debe estimarse la cantidad de veces que puede ocurrir una amenaza en un año. Continuando con el proceso descrito, deben analizarse para cada activo, y para cada amenaza cuántas veces en un año podría esta materializarse

  - **Determinación del impacto de las amenazas**. Se denomina impacto al nivel de daño sobre un activo derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación que causan las amenazas, es posible calcular el impacto que estas tendrían para la organización.

  - **Cálculo del riesgo.** El riesgo es una función de la probabilidad de ocurrencia y del impacto de una amenaza. El nivel de riesgo es directamente proporcional a la probabilidad de ocurrencia y al impacto, es decir que si cualquiera de las dos variables aumenta, entonces también aumentará el nivel de riesgo.

- **Tratamiento de riesgos**

Selección e implantación de técnica de tratamiento

- **Mitigar el riesgo**. En este caso se busca reducir la probabilidad y/o el impacto del riesgo asociado de manera que el nivel de riesgo residual sea aceptable.

- ***Aceptar el riesgo.*** El riesgo se considera tolerable en su forma y exposición actual, y no se toma ninguna acción particular al respecto (o se mantienen los controles existentes). Esto sucede porque dada las características de los riesgos, que la mayoría no se puede eliminar, es necesario establecer un nivel de tolerancia de ciertos riesgos.

- ***Transferir el riesgo***. Esta respuesta implica compartir cierta parte del riesgo con un tercero, lo cual usualmente toma la forma de un seguro, un contrato de cobertura o la tercerización de un determinado proceso o función.

- ***Evitar el riesgo.*** Esta respuesta es cuando no se vislumbran acciones o controles que puedan conducir el riesgo dentro de los parámetros aceptables, y se cesan las operaciones que generan esta clase de riesgo.

- **Seguimiento y medición de resultados**

Una vez definida la respuesta ante los distintos riesgos, es necesario implementar actividades de control para garantizar que dichas respuestas están operando adecuadamente en la práctica y de acuerdo a lo establecido. Es decir, que cada medida de tratamiento implementada presenta los resultados esperados.

- **Documentación y Comunicación**

A efectos de garantizar una adecuada práctica de Administración de Riesgo a todo nivel, será necesario que la información relevante sea identificada, registrada y comunicada.

El contenido de la información debe ser adecuado (estar a un nivel correcto de detalle), oportuno (estar disponible cuando se requiere), actualizado (ser la última información disponible), exacto (datos correctos) y accesible (que quien necesite, pueda obtenerla fácilmente). Además de la información adecuada, será necesario contar con mecanismos efectivos de comunicación dentro del Equipo y desde el Equipo para los terceros involucrados. Los canales de comunicación se deben ajustar a las necesidades de cada Equipo.

- **Mejora continua**

El proceso de gestión de Riesgos no es una foto de un momento determinado, sino que es un proceso sistemático que requiere una evaluación continua para su mejora. En cada ciclo de Análisis de Riesgo se deben analizar los factores que inciden en el proceso, verificando su alineación con los objetivos del Equipo, su adecuación y los cambios que requieran realizarse. También deben considerarse los cambios dentro del mismo proceso, con el objetivo de mejorarlos. Ver Anexo 8.5, Ejemplo de Registro de Riesgos.

4.2.5.4 Roles y Responsabilidades

Si bien los Roles y Responsabilidades de los miembros del CSIRT dependen de cada Centro en particular (de los lineamientos de la Organización a la que pertenecen, de la composición del Equipo, etc.), se plantearán a nivel general las correspondientes funciones.

La imagen del CSIRT la representa cada uno de sus miembros, por lo que hay que considerar que se trabaja en representación de un Equipo y los riesgos también así se han de evaluar.

La figura del rol Gerencial del CSIRT debe dirigir y monitorear todo el proceso de Gestión de Riesgos y, cuando le corresponda, establecer los criterios de evaluación y tratamiento. Lo que debe procurar el Gerente del CSIRT es que la relación puesto-trabajador sea eficaz, disminuyendo así una gran fuente de riesgos. Debe plantearse si existen los puestos de trabajo necesarios para llevar a cabo los procesos establecidos, si los fines son adecuados para cumplir con los objetivos del proceso, si los puestos están pensados para alanzar un rendimiento eficaz, si existen mecanismos de medición del rendimiento y si se realizan diagnósticos, tomándose las medidas preventivas y correctivas necesarias para evitar la materialización de riesgos.

El resto de los miembros del CSIRT, como responsables de los propios riesgos que ellos puedan generar, deben ser conscientes de su trabajo y de lo que éste implica, de realizar correctamente todos los Procedimientos establecidos, cumpliendo con las Políticas y las Normas vigentes. Frente a cualquier duda, deben preguntar y asesorarse.

4.2.5.5 Plan de Contingencia frente a Errores Humanos

4.2.5.5.1 Objetivo

Ejecutar acciones oportunas ante cualquier contingencia que se pudiera presentar como consecuencia de Errores Humanos de los miembros del Equipo, para salvaguardar a las personas involucradas, la Comunidad, los bienes y la reputación del CSIRT.

4.2.5.5.2 Alcance

Todos los integrantes del Equipo y los terceros involucrados.

4.2.5.5.3 Plan de contingencia

El Plan de Contingencias define las responsabilidades del personal clave y los procedimientos de respuesta, a partir de la identificación de los riesgos específicos del personal, con el fin de minimizar el impacto de su materialización.

4.2.5.5.4 Actividades de un Plan de Contingencia

- Una vez documentados los riesgos del CSIRT, se deben seleccionar aquellos relacionados al factor humanos que afectarían la continuidad del negocio.
- Se deben establecer responsables sobre los mismos, quienes responderán en caso de que ocurra.
- Se establecerán también Procedimientos asociados a la Protección física, ambiental y de identidad del Personal (Procedimientos de Trabajo Seguro).
- Se realizarán Inspecciones de seguridad
- Se harán Reportes de incidentes.
- Se efectuarán charlas de inducción al trabajador nuevo
- Se investigará en caso de ocurrir accidentes.
- Se realizarán simulacros de emergencias

4.2.6 Procedimientos asociados al Personal del CSIRT

4.2.6.1 Procedimiento de Selección del Personal del CSIRT

La contratación de personal para un CSIRT es solo el comienzo del proceso del establecimiento del vínculo laboral; pero por ello no deja de ser un paso fundamental cuyo objetivo es identificar al candidato más adecuado.
Al momento de contratar personal para un CSIRT, es importante haber establecido un procedimiento apropiado para hacerlo, que permita identificar las fortalezas y debilidades de cada uno de los postulantes, reuniendo la mayor información posible para una toma de decisión fundamentada. Resulta muy beneficioso el aporte del resto del Equipo en la selección del nuevo miembro, en la medida de lo posible, que existan instancias de relacionamiento con los aspirantes.

4.2.6.1.1 Objetivo

Establecer un procedimiento para la selección de personal, procurando que este se ajuste a los conocimientos, habilidades y condiciones específicas exigidas para el puesto de trabajo de acuerdo a las necesidades del CSIRT.

4.2.6.1.2 Alcance

Este procedimiento se aplica a todas las actividades relacionadas con la selección del personal para el CSIRT.

4.2.6.1.3 Responsabilidades

Es responsabilidad del Gerente del CSIRT proporcionar al Área de RRHH (en caso de que así esté establecido en la Organización) una descripción del cargo que se necesita ocupar y los requerimientos que debe cumplir el candidato.

Es responsabilidad del Área RRHH (cuando esté así determinado) realizar la convocatoria para los postulantes y evaluar de cada uno la integridad de la documentación entregada y el chequeo de los antecedentes de conducta y laborales. Si la contratación se realiza a través de un tercero, éste será el responsable de realizar lo establecido para el Área RRHH.

Es responsabilidad del Gerente del CSIRT realizar las instancias correspondientes para seleccionar el candidato adecuado.

4.2.6.1.4 Descripción

Cuando surge la necesidad de contratar personal para desempeñar tareas en el CSIRT, su Gerente debe enviar al Área de RRHH (siempre que así se estipule) un documento de solicitud de vacante en el que se indique los motivos de necesidad, la descripción del cargo a ocupar y los requerimientos técnicos que debe presentar el candidato; teniendo la viabilidad presupuestaria para ello.

El Área de RRHH debe encargarse de realizar el llamado correspondiente y de verificar que cada candidato ha presentado documentación fidedigna que acredita el cumplimiento de los requisitos.

Una vez que están los candidatos que cumplen con lo solicitado, el Gerente del CSIRT junto con quien estime adecuado comenzará con el Proceso de entrevistas:

- Llamada telefónica, a través de la cual se pueden testear las habilidades de comunicación del candidato.
- Planificación de la entrevista personal, que abarque tanto aspectos técnicos como personales.
- Entrevista inicial
    - Presentación del candidato

- Entrevista individual con Gerente del CSIRT
- Entrevista grupal con el resto del equipo, o quienes se considere necesario

- Discusión interna sobre el candidato
- Chequeo de referencias en caso de ser necesario nuevamente.
- Si se estima conveniente, se puede citar otra instancia de reunión, en donde el candidato realice una presentación de un tema técnico, y así se podrá evaluar su capacidad en esta área.

Una vez cumplidos todos los pasos y, si identifica el candidato adecuado, se procede con el Procedimiento de Vinculación.

Si, a través de este procedimiento, no se hallara el postulante conveniente, se pueden realizar modificaciones en algunas de las instancias, en particular en los requerimientos iniciales, que permita redireccionar la búsqueda hacia las personas correctas.

4.2.6.2 Procedimiento de Vinculación del Personal al CSIRT

Mencionado el carácter sensible de la información que maneja un CSIRT, establecer procedimientos adecuados para administrar tanto el ingreso de nuevo personal al Equipo como su desvinculación, es de gran significación.
De quienes ingresan, se espera que firmen documentos específicos en relación al CSIRT (además de los requeridos por la Comunidad a la que brindan sus servicios), como ser de no divulgación de información específica al CSIRT (Compromiso Confidencialidad[1]), de la conectividad de la red y las interacciones con los medios.

4.2.6.2.1 Objetivo

El objetivo del presente procedimiento es establecer el mecanismo que se debe utilizar en todos los casos de contratación de empleados que brinden su servicio al Centro de Respuesta a Incidentes de Seguridad Informáticos (CSIRT).

[1] Ver Anexo 8.2

4.2.6.2.2 Alcance

Este procedimiento tiene como alcance a todos los empleados que se vinculen al CSIRT.

4.2.6.2.3 Responsabilidades

Es responsabilidad del Gerente del CSIRT facilitar al personal que ingresa al Equipo, las Políticas de Seguridad, el Código de Ética, las Políticas de Gestión de incidentes, de Acceso a la Información, y todos aquellos documentos necesarios en donde se establezcan sus derechos y obligaciones; haciéndole firmar que comprende lo que en ellos se establece.

Es responsabilidad de los empleados que ingresan al CSIRT, aceptar y acatar por escrito los estándares establecidos en los documentos recibidos, de acuerdo a lo que cada uno indique. Es responsabilidad de quien ha elaborado cada documento, responder ante cualquier consulta de duda al respecto.

Es responsabilidad del Gerente del CSIRT hacer firmar a quien ingresa al Equipo, un Compromiso de confidencialidad antes de que acceda a las instalaciones o a información específica, en el que se establece su obligación de no divulgación de la información sensible mientras que desempeña sus funciones y también luego una vez finalizado el vínculo laboral. Es responsabilidad del nuevo empleado velar por el cumplimiento de las Políticas establecidas. En caso de violar o ignorar las responsabilidades y estándares definidos en los documentos que recibe, habilitará a que se ejerzan contra él todas las acciones y recursos legales pertinentes.

Es responsabilidad del Gerente del CSIRT, hacer cumplir el presente procedimiento así como realizar seguimiento del mismo.

4.2.6.2.4 Descripción

El Gerente del CSIRT, entregará al nuevo empleado los documentos de Política, Reglamentación y el Código de Ética, haciéndolo firmar una copia de su recibo; a la vez que también es responsable de que firme el Compromiso de Confidencialidad respectivo.

El Gerente del CSIRT será responsable de la adecuada Capacitación de los nuevos ingresos, en temas de funcionamiento del CSIRT, sus procedimientos asociados, seguridad y conocimientos técnicos.

4.2.6.3 Procedimiento de Protección de Identidad de los miembros del CSIRT

4.2.6.3.1 Objetivo

El objetivo de este procedimiento es establecer mecanismos de protección de la identidad a los integrantes de Equipo para el desarrollo de su trabajo en forma segura.

4.2.6.3.2 Alcance

El mismo se aplica a todos los miembros del CSIRT en la ejecución de sus tareas.

4.2.6.3.3 Responsabilidades

Es responsabilidad de la Organización a la cual pertenece el CSIRT brindar condiciones de seguridad a todos sus empleados.

Es responsabilidad del Gerente del CSIRT establecer mecanismos de protección a todos los que trabajan en este Centro, acordes con las necesidades.

Es responsabilidad de todos los integrantes del CSIRT cumplir con el procedimiento establecido que procura proteger la identidad en la actuación a nombre del Centro, cuando las necesidades del caso y su complejidad lo requieran.

4.2.6.3.4 Descripción

El Gerente del CSIRT analizará los requerimientos de seguridad que tienen sus empleados, determinando en qué ocasión se amerita el uso del procedimiento de protección a la identidad.
Cada empleado del CSIRT velará por la adecuada difusión de la información, considerando que lo que él dice tanto a la Comunidad, a otros CSIRT's y terceros involucrados, puede conducir a la resolución del problema pero también puede no hacerlo, generando graves consecuencias. Al momento de emitir su juicio, debe procurar que el mismo quede registrado, de forma de respaldar su actuación; y ser cuidadoso en lo que aconseja, pues los resultados pueden ser muy importantes.
Cuando es necesario, porque el Gerente junto con los técnicos así lo consideren, se debe actuar con el amparo sobre su identidad, gestionando el incidente de tal modo que no quede expuesto quién es la persona que implicada en su resolución.
En caso de que se produzca un inconveniente, es el Gerente del CSIRT que lo deberá solucionar.

4.2.6.4 Procedimiento de Desvinculación del Personal al CSIRT

La importancia de este procedimiento radica en los riesgos que conlleva este tipo de instancias, donde alguien con información sensible perteneciente al CSIRT, se desvincula de él.

Los motivos para que eso acontezca, básicamente son los siguientes:

- Renuncia
- Despido
- Jubilación
- Fatalidad

Si una persona abandona el equipo por su propia voluntad, es de gran valor entender las razones que llevaron a esa decisión. Por ello, es recomendable realizar una instancia de diálogo, en la que puedan exponerse los motivos de la partida, los cuales se deben tomar con gran seriedad. Si una persona es despedida, deben tenerse en cuenta otros criterios de finalización del vínculo laboral para asegurar que no ocurra inconveniente alguno. Ante la fatalidad de la muerte, o una instancia en la que un miembro del Equipo se vea impedido de concurrir a trabajar por un tiempo significativo, debe tenerse en cuenta la necesidad de contar con mecanismos que permitan acceder a las tareas que realizaba. En este punto vale destacar que nadie debe ser imprescindible ni para la Organización ni para un Centro de este tipo.

4.2.6.4.1 Objetivo

El objetivo de este procedimiento es establecer los pasos a seguir en los casos de empleados que, por determinado motivo, se desvinculan al CSIRT.

4.2.6.4.2 Alcance

El mismo se aplica a todos los empleados que finalicen su vínculo laboral con el CSIRT, ya sea por decisión propia, por requerimientos legales o por decisión del Gerente del Equipo y o de la Organización.

4.2.6.4.3 Responsabilidades

El Gerente del CSIRT debe llevar el registro y mantenimiento referente a los permisos que se le han otorgado así como también los permisos de acceso a salas restringidas, de manera de garantizar que una vez finalizadas todas las tareas de inhabilitación, la persona no tendrá ninguna posibilidad de acceso.

El Gerente del CSIRT debe realizar la solicitud a quien corresponda, de la baja de todos los permisos a los distintos activos de información, aplicaciones, autorizaciones de acceso a salas restringidas, que el empleado usufructúe antes de la desvinculación.

El Gerente del CSIRT debe solicitarle a la persona que se desvincula, toda documentación, tarjetas de acceso, y otros dispositivos que pertenezcan a la Empresa; siendo responsable también de elaborar un Acta donde se registren los elementos devueltos.

Es responsabilidad del Gerente del CSIRT, modificar las contraseñas de los sistemas a los que accedía el involucrado una vez que éste se retire. Es responsabilidad de quien se desvincula del Equipo, reintegrar todas aquellas credenciales y dispositivos que se le otorgaron para desempeñar su trabajo.

4.2.6.4.4 Descripción

El Gerente del CSIRT le requerirá al empleado que cesa en sus funciones, que haga entrega de toda acreditación que identifique con el Equipo del CSIRT y de la Organización para la que sirve, así como también todas las tarjetas de acceso, llaves y dispositivos que poseía. Se elaborará un Acta que registre los elementos que han sido devueltos por la persona que se retira del Equipo[2], la cual deberá estar firmada por las dos partes. En caso de que no puedan recolectarse elementos específicos tales como llaves o tokens, se deberá implementar un Plan de Contingencia adecuado.

Procederá a su vez a gestionar la solicitud de baja de los permisos y derechos de acceso que el empleado tenga a todas las aplicaciones y accesos a salas en los edificios de la Empresa así

[2] Ver Anexo 8.4

como también a modificar las contraseñas de los sistemas. En caso de que se trate de un despido, se designará un miembro del Equipo para que escolte a la persona involucrada en su retirada de las instalaciones del CSIRT.

El Gerente del CSIRT le recordará los documentos con los cuales se comprometió desde el momento de su vinculación y que esas responsabilidades no cesan frente a su partida.

4.2.7 Anexos

4.2.7.1 Perfiles requeridos

Si bien existen diferentes requerimientos, de acuerdo al cargo que se vaya a desempeñar dentro del CSIRT, a continuación se expondrán las características que deben estar presentes, dividiéndolas de acuerdo al perfil Gerencial y al Técnico.

A su vez, distinguiremos los requisitos en tres grupos: capacidades personales, capacidades técnicas y otros requerimientos. El orden en que están planteadas las mismas no hacen referencia al nivel jerárquico de las mismas.

4.2.7.1.1 Nivel Gerencial

- **Capacidades personales:**
  - Integridad. Es un valor especialmente importante para el Gerente del CSIRT, quien debe tratar información extremadamente sensible y que, en caso de ser utilizada de forma incorrecta, puede derivar en graves consecuencias.
  - Capacidad de tomar decisiones. La calidad del servicio que brinde el Equipo, depende directamente de las decisiones más críticas que se tomen, las cuales muchas veces deben realizarse en momentos de estrés.
  - Capacidad de Liderazgo. Estar al frente de un Centro de Respuesta a Incidentes Informáticos requiere una personalidad que pueda persuadir a los miembros restantes del Equipo para realizar las acciones que considera apropiadas.
  - Capacidad de comunicación y de relacionamiento con las personas. El CSIRT es un grupo y debe actuar como tal, por lo que la comunicación es vital y así también los vínculos interpersonales que en él se generen. El rol promotor del Gerente en este

aspecto es fundamental. También es quien establece los mecanismos de Comunicación en el resto del equipo, para con la Comunidad, en el relacionamiento con los medios y otros terceros.

- Gran resistencia al estrés. Las tareas que se desarrollan en el CSIRT generalmente están acompañadas de un alto nivel de estrés, ya sea por lo que involucra el incidente que se pretende resolver o por los tiempos necesarios para resolverlo. Como es el Gerente el que respalda todas las decisiones (especialmente las más delicadas), debe tener la capacidad de abstraerse del estrés y tomar las medidas adecuadas.
- Capacidad de dirigir y potenciar al resto del Personal. Además del liderazgo, el Gerente de un CSIRT debe tener la capacidad de identificar las áreas en las que cada uno de los miembros es mejor y potenciarlos en ello, sabiendo dirigirlos apropiadamente.
- Capacidad de coordinación. Los tiempos que maneja un CSIRT para la resolución de incidentes, muchas veces son muy acotados, y la diversidad de las tareas que se deben cumplir agregan complejidad al tema. Por lo tanto, la figura gerencial debe tener la capacidad de distribuir en el tiempo las actividades que se deben realizar, de la forma más eficiente posible.
- Capacidad de delegar. Si bien es importante que el Gerente esté involucrado en los temas más complejos, debe tener la capacidad de delegar tareas y saber discernir cuáles son las que requieren esencialmente su participación y cuáles no. Para ello debe confiar en su staff.
- Capacidad de mantener el control. Durante la dirección de un CSIRT, se viven situaciones de gran tensión y que pueden involucrar diversos riesgos, incluso el de vida. Por ello, es fundamental que el Gerente del CSIRT sea capaz de mantener el control en momentos tan difíciles, para poder brindar el servicio de forma adecuada.

- **Competencias técnicas:**
  - Conocimiento experto que permita dirigir todas las operaciones del CSIRT.
  - Estar actualizado de forma permanente con los avances tecnológicos y profundizar en el manejo de los mismos, explorando sus vulnerabilidades.
  - Amplio conocimiento y experiencia en técnicas de intrusión.

- Saber las distintas técnicas de comunicación.

- **Otros requerimientos:**
  - Amplia experiencia laboral en seguridad de las TI.
  - Disposición a trabajar 24 horas al día, 7 días a la semana o de guardia.
  - Conocimiento de la gestión de riesgos y sus aplicaciones prácticas.

4.2.7.1.2 Nivel Técnico

- **Capacidades personales:**
  - Integridad. El personal del equipo debe ser confiable, discreto y capaz de manejar la información sensible de manera confidencial; cumpliendo con las normas, las políticas organizacionales y con los procedimientos establecidos.
  - Capacidad de tomar decisiones. Los servicios que brinda el CSIRT requieren mayormente respuestas y soluciones rápidas, para ello es indispensable ser capaz de decidir el modo de actuación de forma expeditiva.
  - Flexibilidad, creatividad y espíritu de equipo. Los servicios que brinda un CSIRT se basan principalmente en trabajos de equipo, por ello es muy importante el espíritu de trabajo colectivo que tengan sus miembros, en el cual cada uno aporte sus experiencias y conocimientos para el beneficio de todos. El ambiente tecnológico en el que trabaja un CSIRT, requiere que sus miembros sean flexibles a los cambios, pudiéndose adaptar fácilmente.
  - Capacidad de comunicación. Ya que los integrantes del CSIRT en la mayor parte de su trabajo deben comunicarse con su comunidad, con su propio equipo, otros equipos de respuesta, con una variedad de expertos técnicos, y otros individuos con distintos niveles de conocimiento técnico; es imprescindible que sepan hacerse entender. A través de una buena comunicación se asegura que se obtiene y se transmite la información necesaria; para saber qué está pasando, qué factores son importantes, qué acciones se deben realizar y para transmitir en lo que se ha trabajado y la contribución que pueden realizar los involucrados. Capacidad de decir las palabras correctas a las personas correctas.
    - Comunicación oral

- Comunicación escrita

- Capacidad de realizar trabajo sistemático, siguiendo políticas y procedimientos, tanto de la Organización como del Equipo de Respuesta. En esto es muy importante que cada uno comprenda la utilidad y el motivo de cada procedimiento, y que tenga la posibilidad de aportar su visión en las actualizaciones de los mismos.
- Resistencia al estrés. Deben ser capaces de darse cuenta cuando se ven envueltos en tales situaciones y comunicarlo al resto del equipo, y tomar las decisiones adecuadas para recobrar la tranquilidad. Deben mantener la calma en situaciones de tensión.
- Mente abierta y ganas de aprender y de capacitarse. Los avances tecnológicos constantes traen consigo el requerimiento de actualización continua. Por ello es que resulta relevante esta característica, la que permite acompasar los cambios que suceden y estar preparados para enfrentarlos.
- Capacidad de reconocer errores propios y/o limitaciones. Es importante saber los propios límites de cada uno y especialmente en equipos como estos, donde es imprescindible el buen manejo de los incidentes.
- Diplomacia. La comunidad con la cual un CSIRT interactúa tiene una gran variedad de objetivos y necesidades, así como también diversos niveles de conocimiento y formas de reaccionar frente a incidentes. Por lo tanto, el staff de un CSIRT debe ser capaz de anticipar potenciales puntos de confrontación y responder apropiadamente, manteniendo buenas relaciones.
- Capacidad de solucionar problemas. Debido al tipo y al volumen de información al que está expuesto un CSIRT, si no hay capacidad de discernimiento y de resolución de problemas por parte del staff, éste se puede ver desbordado por la situación. Para resolver un problema, debe saber delegar, y solicitar la contribución de otros; saber requerir más información de otras fuentes, verificándola y sintetizándola.
- Detallista y analítico. El manejo de incidentes de carácter sensible requiere suma atención a los detalles que lo componen y una mente que analice los acontecimientos paso a paso; aunque sin perder la simplicidad en la visión.
- Capacidad de administrar los tiempos de manera efectiva. Esto permite priorizar entre la gran diversidad de tareas a las que están sometidos los miembros de un CSIRT

(tales como analizar, coordinar, responder a los incidentes; preparar presentaciones, capacitarse, coordinar y realizar reuniones).

- Capacidad de realizar presentaciones. El alto nivel de intercambio con otras instituciones o personas fuera del CSIRT requiere la capacidad por parte de sus miembros de realizar presentaciones técnicas, informar a la Alta Gerencia, presentarse en paneles de discusión, en conferencias, u otro tipo de exposiciones al público.

- **Competencias técnicas:**
  - Conocimiento y entendimiento de los principios básicos de la seguridad.
  - Conocer vulnerabilidades de los sistemas.
  - Conocer Internet, su historia, filosofía, estructura y la infraestructura que la sostiene.
  - Protocolos de Red. Los miembros del CSIRT necesitan tener un básico entendimiento sobre los protocolos, sus especificaciones y cómo se utilizan. También deben entender los típicos ataques que éstos pueden sufrir, así como también saber las estrategias para mitigar o eliminarlos.
  - Conocimiento sobre los servicios y las aplicaciones de redes.
  - Entendimiento de los conceptos de seguridad de las redes así como también capacidad de reconocer puntos vulnerables en las configuraciones de las mismas.
  - Temas de seguridad de los servidores y sus sistemas operativos. Deben tener experiencia en utilizar los distintos sistemas operativos y familiaridad en el manejo y mantenimiento del sistema operativo, como administrador.
  - Entender los diferentes tipos de ataques mediante códigos maliciosos.
  - Para algunos de los miembros se requiere experiencia en programación de redes y sistemas.
  - Habilidades en el manejo de incidentes, habilidades asociadas a las actividades subyacentes del día a día.
  - Deben reconocer las técnicas de intrusión.
  - Dada la importancia de la Comunicación, ya mencionada, los miembros del staff deben saber las distintas técnicas de comunicación.

- Ser capaces de realizar Análisis de Incidentes y de realizar el mantenimiento de los incidentes registrados.

- **<u>Otros requerimientos:</u>**
  - Disposición a cumplir regímenes de horario extensos cuando así se necesite, incluso trabajar con turnos de guardia.
  - Estabilidad económica.
  - Trabajar como testigo experto en caso de que se requiera, si su trabajo implica recolección de evidencia forense.

No hay un solo grupo de habilidades que sea adecuada al equipo de un CSIRT, éstas varían en función de la clase de equipo, de los incidentes que atienden, el tipo de tecnologías que utilizan. A modo general se establecieron anteriormente las características fundamentales.

Una nota muy importante en este tema, es que ningún integrante debe ser indispensable. Para evitar ello, los integrantes deben cumplir con los mayores requisitos posibles. Lo que es importante es que el Gerente tenga un suplente, con capacidades similares, que pueda tomar su lugar en caso de que éste no se encuentre disponible.

4.2.7.2 Plan de capacitación para los miembros del CSIRT

Como se ha mencionado previamente, contar con un Plan o Programa de Capacitación para los miembros del CSIRT es un fundamental para constituir un equipo con sólidos conocimientos que pueda atender los requerimientos de su Comunidad de forma adecuada.
Este Programa debe abarcar aspectos de iniciación, tanto respecto a Normas, Políticas y Procedimientos del Equipo de la Organización de la que depende, así como en aspectos técnicos primarios.

4.2.7.2.1 Introducción

- Líneas generales de la Comunidad para la cual trabajan.
- Historia y Organización del CSIRT, así como la misión, los objetivos y valores que se manejan internamente.
- Temas de confidencialidad y no revelación de la información.
- Código de Conducta.

- Políticas de uso aceptable.
- Visión general de los procedimientos de respuesta a incidentes y la gestión de Riesgos.
- Comunicación con la Comunidad y con otros terceros, tanto por vía oral como escrita.
- Políticas de relacionamiento con los medios.

4.2.7.2.2 Aspectos Técnicos

- Herramientas y procedimientos de clasificación, correo electrónico y manejo de incidentes.
- Comunicaciones seguras.
- Incidentes de baja prioridad.
- Incidentes con alta prioridad.

4.2.7.2.3 Respecto al Manejo de incidentes

- Creación de un CSIRT
- Gestión del CSIRT
- Fundamentos del Manejo de Incidentes
- Manejo de Incidentes Avanzados

4.2.7.2.4 Referente a la Seguridad en las Redes

- Visión General de la creación y la gestión del CSIRT
- Seguridad de la Información para el Staff Técnico
- Seguridad de la Información Avanzada para el Staff Técnico

4.2.7.2.5 Certificaciones:

- CISSP: Dominio de conocimiento en tecnología y gerencia en Seguridad de la Información (www.isc2.org)
- CISM: Conocimiento en gerencia de Seguridad de la Información. (www.isaca.org)
- ABCP o CBCP: Conocimiento en planes y gestión de la continuidad de la operación. (www.drii.org)
- CISA: Experiencia en auditoría de sistemas. (www.isaca.org)

- ISO 27001 Lead Auditor: Conocimiento en auditoría de sistemas de gestión en seguridad de la información SGSI.

4.2.7.3 Modelo Compromiso de Confidencialidad

En la ciudad de _____, a los _____ días del mes de_____ de dos mil_____ el Sr./Sra. _____, titular del documento N°_____, en su carácter de miembro del _____ o de persona vinculada al mismo cualquiera sea la naturaleza de su relación, constituyendo domicilio para todos sus efectos en esta ciudad en la calle _____, declara:

PRIMERO: Objeto del presente Acuerdo.-

En virtud de la prestación de servicios de carácter laboral mencionada, el trabajador puede tener acceso a instalaciones, dependencias, recursos, sistemas, documentos en soporte papel, documentos electrónicos, soportes informáticos, electrónicos y telemáticos susceptibles de contener información considerada confidencial; frente a los que está obligado a mantener su sigilo, no divulgándola. Ésta comprenderá toda la información que, por su naturaleza o contenido, en caso ser expuesta pueda causar cualquier tipo de daño, perjuicio o desventaja para el CSIRT o la Comunidad a la que pertenece o brinda sus servicios.

SEGUNDO: Obligaciones asumidas por la vinculación con _____

1- Se prohíbe divulgar y se exige mantener estricta confidencialidad respecto de toda la información, documentos, contratos, propuestas y material del CSIRT que se confieran por escrito o se reciban verbalmente durante las tareas ejecutadas en el cumplimiento de su labor.

2.- Adoptar medidas de seguridad razonables y prudentes para proteger la información reservada, incluyendo sin limitarse a ello, las disposiciones de seguridad que se le instruyan al firmante, en concordancia con las Políticas y Procedimientos de la Seguridad de la Información.

TERCERO: En caso de desvinculación laboral.-

Tras la terminación de la relación laboral, cualquiera sea su causa, mantendrá su deber de sigilo y secreto profesional respecto de la información confidencial a que haya tenido acceso durante el desempeño de sus funciones.

CUARTO: Sanción por Incumplimiento.-

En caso de incumplimiento del presente compromiso, el CSIRT queda plenamente facultado para disponer las medidas legales y reglamentarias que por derecho correspondan.

QUINTO: Definiciones:

a) Información Secreta: Datos que tienen asignados el máximo nivel de seguridad limitándose su acceso dentro de la organización, y que requieren por su esencia un alto grado de integridad. Su divulgación a terceros no autorizados puede provocar severos impactos a la operativa e imagen del Equipo y/o Instituciones involucradas.
b) Información Confidencial: Datos que tienen asignados un nivel de seguridad menos restrictivo que los anteriores dentro de la organización en razón de ser menos sensibles.
c) Información de Uso Interno: Datos de carácter privativo al funcionamiento de la Institución, que en el caso de ser revelados a terceros pueden acarrear daños o ser utilizados por personas ajenas a la misma, para fines particulares. El tratamiento de estos datos, sólo pueden ser accesibles a los miembros del Equipo o personas vinculadas al mismo que necesitan conocer o utilizar la información de un área o sector en particular, inherentes a sus funciones.
d) Información Pública: Esta categoría incluye cualquier otra información que no se encuentre comprendida en las anteriores, no requiriendo protección contra accesos no autorizados.

En señal de conformidad se suscriben dos ejemplares del mismo tenor, en lugar y fecha arriba indicados.

Firma……

Contra firma……

C.I. N°. ……

4.2.7.4 Evaluaciones del Personal

La **evaluación de desempeño** es el proceso por el cual se estima el rendimiento global del empleado, es un procedimiento **sistemático** y **periódico** de comparación entre el desempeño de una persona en su trabajo y una pauta de eficiencia (generalmente la descripción y especificación del cargo). Es un sistema de apreciación del **desempeño del individuo** en el cargo y de su **potencial de desarrollo**. Por lo general, el evaluador suele ser un supervisor o superior que conozca bien el puesto, generalmente el jefe directo.

Además de mejorar el desempeño, muchas Instituciones utilizan esta información para determinar las compensaciones. Un buen sistema de evaluación puede también identificar problemas. Las personas que se desempeñan de manera insuficiente pueden poner en evidencia procesos equivocados de selección, orientación y capacitación, o puede indicar que el diseño del puesto o los desafíos externos no han sido considerados en todas sus facetas.

Factores que generalmente se evalúan:

- Conocimiento del trabajo
- Calidad del trabajo
- Relaciones con las personas
- Capacidad de iniciativa
- Capacidad de Cooperación
- Capacidad analítica

Objetivos de la evaluación de desempeño

- Para detectar necesidades de instrucción y perfeccionamiento.
- Para detectar el potencial de desarrollo del trabajador.
- Para aplicar incentivos salariales por buen desempeño.
- Para mejorar la comunicación entre los distintos niveles de mando.
- Para auto-perfeccionamiento de los empleados.

Etapas de una Evaluación.

- Definir objetivos
- Establecer a quien está dirigido.
- Determinar quién es el evaluador y quién revisará la evaluación.
- Definir la Periodicidad.

- Elegir el método.
- Capacitar al evaluador.
- Realizar la Evaluación.
- Analizarla.
- Comunicar los resultados.
- Utilizar los resultados.

4.2.7.5 Modelo de Acta de Desvinculación Laboral

ACTA DE DESVINCULACIÓN LABORAL.-

En la Ciudad de _____, a los_____días del mes de _____del año dos mil_____, comparece_____, titular del Documento _____, domiciliado/a en_____de esta Ciudad, con motivo de la finalización de su vínculo laboral con_____; para hacer entrega de los siguientes dispositivos que le habían sido entregados por motivos laborales:

-

-

Conforme con el Acto precedido, y recordando mi obligación de mantener la confidencialidad de la información manejada durante dos años más,

FIRMA_____ CONTRAFIRMA_____

4.2.7.6 Modelo de Registro de riesgos

DESCRIPCIÓN DEL RIESGO
- Nombre o título del Riesgo
- Descripción del Riesgo, incluyendo su alcance.
- Naturaleza del Riesgo, incluyendo detalles de la clasificación del mismo y su impacto en el tiempo.
- Agentes involucrados en el Riesgo.
- Responsable de Riesgo.
- Probabilidad e impacto.
- Nivel de exposición al Riesgo.
- Mecanismos de control existentes.
- Potenciales mejoras a realizar en los mecanismos de control.
- Recomendaciones de Mejora para la gestión del Riesgo.
- Responsabilidades para implementar las mejoras.
- Responsabilidades para auditar el cumplimiento del proceso

Tabla Comparativa de los Riesgos identificados

Descripción del Riesgo	Probabilidad	Impacto	Nivel de Exposición	Controles existentes

5. Terminología

Caja Fuerte	Una Caja Fuerte es un compartimiento de seguridad que ha sido inventado para que su apertura sea muy difícil para personas no autorizadas y así poder guardar elementos de valor. Por lo general son fabricadas en un metal extremadamente duro, por lo que son muy pesadas y constan de un sistema de cierre que solo se puede abrir mediante claves secretas, y que estas claves pueden cambiarse para preservar más aún la seguridad.
Canales de Comunicación Seguros	Se refiere a la transmisión protegida de la información compartida entre los diferentes equipos, y no a la utilización adecuada de la información por los equipos.
CIAC	Computer Incident Advisory Capability (CIAC). Es un equipo asesor en capacidades de incidentes computacionales del Departamento de Energía de los Estados Unidos.
Criptografía	Es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.
CSIRT	Según CERT/CC, un Computer Security Incident Response Team (CSIRT). Es una organización responsable de recibir reportes de incidentes de seguridad, analizarlos y responderlos.
DCS	Distributed Control System, Sistema de Control Distribuido más conocido por sus siglas en inglés DCS. Es un sistema de control por lo general un sistema de fabricación, proceso o cualquier tipo de sistema dinámico, en el que los elementos del tratamiento no son centrales en la localización (como el cerebro), sino que se distribuyen en todo el sistema con cada componente subsistema controlado por uno o más controladores. Todo el sistema de los controladores está conectada por redes de comunicación y de monitoreo.
DES	Data Encryption Standard (DES). Es un algoritmo de cifrado, es decir, un método para cifrar información, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta, y las continuas sospechas sobre la existencia de alguna puerta trasera para la National Security Agency (NSA). Posteriormente DES fue sometido a un intenso análisis académico y motivó el concepto moderno del cifrado por bloques y su criptoanálisis.
DFN-CERT	Es una comunidad alemana de equipos de respuesta a emergencias que se dedica a la investigación y educación.

DNS	Domain Name System (DNS), Sistema de Nombre de Dominio. Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado al internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.
FAQ	Frequently Asked Questions (FAQ), es el término Preguntas Frecuentes o preguntas más frecuentes. Se refiere a una lista de preguntas y respuestas que surgen frecuentemente dentro de un determinado contexto y para un tema en particular.
FINGER	El servicio Finger (puerto 79, TCP) es un protocolo que proporciona información de los usuarios de una máquina, estén o no conectados en el momento de acceder al servicio.
Firewall	Un Firewall o Cortafuego es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.
Firma Digital	La Firma Digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.
FTP	File Transfer Protocol (FTP), Protocolo de Transferencia de Archivos. En informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo. El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21.
Hardware	Es el conjunto de materiales que componen una computadora.
Hosting	El alojamiento web (en inglés web hosting) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía Web. Los Web Host son compañías que proporcionan espacio de un servidor a sus clientes.

Hub	Un Hub o concentrador es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Se han dejado de utilizar debido al gran nivel de colisiones y tráfico de red que propician.
ICMP	Internet Control Message Protocol (ICMP), Protocolo de Mensajes de Control de Internet. Es el sub-protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.
IDS	Intrusion Detection System (IDS), Sistema de Detección de Intrusos. Es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas. El IDS suele tener sensores virtuales con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.
IPS	Intrusion Prevention System (IPS), Sistema de Prevención de Intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.
NetBIOS	NetBIOS, "Network Basic Input / Output System". Es en sentido estricto, una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico. Desde su creación, NetBIOS se ha convertido en el fundamento de muchas otras aplicaciones de red.
NNTP	Network News Transport Protocol (NNTP), Protocolo para la Transferencia de Noticias en Red. Es un protocolo inicialmente creado para la lectura y publicación de artículos de noticias en Usenet.
NTP	Network Time Protocol (NTP). Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.
Outsourcing	La Subcontratación es el proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato. Esto se da especialmente en el caso de la subcontratación de empresas especializadas. Para ello, pueden contratar sólo al personal, en cuyo caso los

	recursos los aportará el cliente (instalaciones, hardware y software), o contratar tanto el personal como los recursos.
PCS	Personal Comunication System (PCS), Servicio de Comunicación Personal. Es el nombre dado para los servicios de telefonía móvil digital en varios países y que operan en las bandas de radio de 1800 o 1900 MHz.
PEM	Formato de archivo empleado para almacenar certificados digitales.
Pendrive	Una memoria USB (de Universal Serial Bus; en inglés Pendrive, USB Flash Drive) es un pequeño dispositivo de almacenamiento que utiliza memoria flash para guardar la información que puede requerir y no necesita baterías (pilas). La batería era necesaria en los primeros modelos, pero los más actuales ya no la necesitan. Estas memorias son resistentes a los rasguños (externos), al polvo, y algunos al agua –que han afectado a las formas previas de almacenamiento portátil-, como los disquetes, discos compactos y los DVD. En España son conocidas popularmente como pendrives o lápices USB.
PGP	Pretty Good Privacy (PGP), Privacidad Bastante Buena. Es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.
POP	Post Office Protocol, (POP), Protocolo de la Oficina de Correo. En informática se utiliza el POP3 en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto.
Proxy	En el contexto de las redes informáticas, el término Proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.
Red de Confianza	Es un ambiente de trabajo donde los usuarios registran las claves de otros usuarios para poder establecer comunicaciones seguras entre sus pares.
Router	Router. Enrutador, Direccionador, Ruteador o Encaminador. Es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.
SCADA	Supervisory Control and Data Acquisition (SCADA), Registro de Datos y Control de Supervisión. Es una aplicación de software especialmente diseñada para funcionar sobre ordenadores (computadores) en

	el control de producción, proporcionando comunicación con los dispositivos de campo (controladores autónomos) y controlando el proceso de forma automática desde la pantalla del ordenador. También provee de toda la información que se genera en el proceso productivo a diversos usuarios, tanto del mismo nivel como de otros usuarios supervisores dentro de la empresa (supervisión, control calidad, control de producción, almacenamiento de datos, etc.).
Segmento de Red	Un segmento de red suele ser definido mediante la configuración del hardware (comúnmente por Router o Switch) o una dirección de red específica. Una gran red en una organización puede estar compuesta por muchos segmentos de red conectados a la LAN principal llamada backbone, que existe para comunicar los segmentos entre sí.
Servidor Web	Es un programa que implementa el protocolo HTTP (HyperText Transfer Protocol). Este protocolo pertenece a la capa de aplicación del modelo OSI y está diseñado para transferir lo que llamamos hipertextos, páginas Web o páginas HTML (HyperText Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música.
SMTP	Simple Mail Transfer Protocol (SMTP), Protocolo Simple de Transferencia de Correo. Es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.
Software	Es el conjunto de programas que puede ejecutar el hardware para la realización de las tareas de computación a las que se destina.
Switch	Switch o Conmutador. Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.
Telnet	Telnet (TELecommunication NETwork) es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla remotamente como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.
TFTP	Trivial File Transfer Protocol (TFTP), Protocolo de Transferencia de Archivos Trivial. Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para

	transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arranca desde un servidor de red.
Usuario	Es la persona que utiliza o trabaja con algún objeto o que es destinataria de algún servicio público, privado, empresarial o profesional.
VPN ó RPV	Virtual Private Network (VPN), Red Privada Virtual (RPV). Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada.
Web	World Wide Web, Red Global Mundial. Es la forma abreviada de referirse al conjunto de todas las páginas que pueden consultarse en Internet.
Workflow	Workflow, Flujo de Trabajo. Es el estudio de los aspectos operacionales de una actividad de trabajo: cómo se estructuran las tareas, cómo se realizan, cuál es su orden correlativo, cómo se sincronizan, cómo fluye la información que soporta las tareas y cómo se le hace seguimiento al cumplimiento de las tareas.

6. Bibliografía

CAPITULO 1

- West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. **Handbook for Computer Security Incident Response Teams (CSIRTs)** (CMU/SEI-98-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1998.
- Kossakowski, Klaus-Peter. **Information Technology Incident Response Capabilities**. Hamburg: Books on Demand, 2001 (ISBN: 3-8311-0059-4).
- G. Killcrece et al, Organizational Models for Computer Security Incident Teams
- (CSIRTs), Handbook CMU/SEI-2003-HB-001, diciembre 2003.
- N. Brownlee; E. Guttman. **Expectations for Computer Security Incident Response**. Junio 1998.
- Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. **CSIRT Services List**. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2002.
- G. Killcrece et al, **Organizational Models for Computer Security Incident Teams (CSIRTs), Handbook** CMU/SEI-2003-HB-001, diciembre 2003.
- Kossakowski; Klaus-Peter & Stikvoort, Don. **A Trusted CSIRT Introducer in Europe.** Amersfoort, Netherlands: M&I/Stelvio, February, 2000. (see "Appendix E, Basic Set of Information").
- 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.

CAPITULO 2

- [1] Grance, Tim; Kent Karen; Kim, Brian; Computer Security Incident Handling Guide. Recommendations of the National Institute for Standards and Technology; NIST; January 2004
- [2] Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; Zajicek, Mark; Organizational Models for Computer Security Incident Response Teams (CSIRTs); CMU/CEI-2003-HB-001
- [3] UNAM-CERT. Taller de creación de equipos de respuesta a incidentes.

- [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

- [CERT-hb] M. West-Brown, D. Stikvoort, K. Kossakowski, G. Killcrece, R. Ruefle y M. Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)*, abril 2003. En línea: http://www.cert.org/archive/pdf/csirt-handbook.pdf. Última visita: noviembre 2009.
- [FIRST] *Forum of Incident Response and Security Teams*, http://www.first.org. Última visita: noviembre 2009
- [FIRST-TC] *FIRST Technical Colloquia*, http://www.first.org/events/colloquia. Última visita: noviembre 2009
- [ISACA] ISACA, http://www.isaca.org. Última visita: noviembre 2009
- [ISC2] *International Information Systems Security Certification Consortium, Inc.*, http://www.isc2.org. Última visita: noviembre 2009
- [PMI] *Project Management Institute*, http://www.pmi.org. Última visita: noviembre 2009

- [CERT03tr] G. Killcrece, K. Kossakowski, R. Ruefle y M. Zajicek, *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*, octubre 2003. En línea: http://www.cert.org/archive/pdf/03tr001.pdf. Última visita: noviembre 2009.
- [ISS-CSIRP] *Internet Security Systems, Computer Security Incident Response Planning - Preparing for the Inevitable*. En línea: http:// documents.iss.net/whitepapers/csirplanning.pdf. Última visita: noviembre 2009.
- [RFC2350] N. Brownlee y E. Guttman, *Expectations for Computer Security Incident Response*, junio 1998. En línea: http://www.rfc-editor.org/rfc/rfc2350.txt. Última visita: noviembre 2009.
- [RFC4949] R. Shirey, *Internet Security Glossary*, Version 2, agosto de 2007. En línea: http://www.rfc-editor.org/rfc/rfc4949.txt. Última visita: noviembre 2009.
- [SP800-61] K. Scarfone, T. Grance y K. Masone, *Computer Security Incident Handling Guide – Revision 1*, marzo de 2007. En línea: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf. Última visita: noviembre 2009.
- [TWri01] T. Wright, *How to Design a Useful Incident Response Policy*, octubre 2001. En línea: http://www.securityfocus.com/infocus/1467. Última visita: noviembre 2009.

- [18044] ISO/IEC TR 18044:2004. Gestión de incidentes de la seguridad de la información.
- [27001] ISO/IEC 27001:2005. Sistemas de Gestión de la Seguridad de la Información – Requisitos.
- [27002] ISO/IEC 27002:2005(17799). Código de buenas prácticas para la gestión de la seguridad de la información.

CAPITULO 4

- ISO/IEC 27005 - Tecnología de la información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información
- NORMA IRAM - ISO/IEC 27001 - Tecnología de la información - Sistemas de gestión de seguridad de la información (SGSI) - Requisitos
- NORMA IRAM - ISO/IEC 27002 - Tecnología de la información - Técnicas de Seguridad Código de práctica para la gestión de la seguridad de la información
- MAGERIT – versión 2
- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
- NIST SP 800-30 - Risk Management Guide for Information Technology Systems

CAPITULO 4.2

- [Ministerio08] *Informe Final para la constitución de un CSIRT Colombiano- Modelo de Seguridad- Estrategia de Gobierno en Línea, 2008.*
- [RM] Risk Management and the HR Executive-Written by Valerie Frederickson, MS, CMP.
- [RFC235098] RFC2350 - Expectations for Computer Security Incident Response, N. Brownlee, The University of Auckland, 1998.
- [Smi95] Forming an Incident Response Team. Danny Smith. Australian Computer Emergency Response Team, 1995.
- [Castillo] Procedimiento para la gestión de los Riesgos Laborales de forma integrada y con un enfoque de procesos y su implicación en los resultados económicos, en la calidad de vida laboral y la productividad del trabajo Ing. Luís Alberto Castillo Ros

Lacnic
Rambla República de México 6125
Montevideo C.P. 11400 Uruguay

Phone: + 598 2604 2222
ISBN: 978 - 9974 - 98 - 741 - 8
Edición 2012