CAPÍTULO III

ORGANISMOS COMPETENTES Y REGLAS DE DERECHO PROCESAL

1. COMITÉ DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA *(COMPUTER SECURITY INCIDENT RESPONSE TEAM –CSIRT-)*

1.1 Consideraciones generales

La seguridad de la información es una tarea a cargo de todos los Organismos del Estado que tienen una infoestructura que, al ser comprometida, puede poner en riesgo la Seguridad Nacional. Pero esta preocupación también es extensiva a las instituciones financieras privadas y todos los entes vinculados al sistema financiero; puesto que, como la experiencia reciente lo ha demostrado, la falla en el sistema de distribución monetaria puede causar caos en toda la nación.

Es por ello necesario que el Estado cuente con un organismo autónomo, que brinde soporte a incidentes de seguridad informática a las diferentes instituciones públicas y privadas que lo requieran, para que, de esta forma se garantice, en buena medida, si bien no un sistema invulnerable, si un sistema más seguro y confiable.

Un Equipo de Respuesta, a Incidentes de Seguridad Informática, es una herramienta valiosa para la preservación de la infoestructura crítica de los Estados. Ejemplo de esto son los múltiples Centros alrededor del mundo donde, a partir de la implementación de los mismos, se han reducido los incidentes de seguridad y los que han ocurrido son rápidamente controlados, generando una respuesta de carácter nacional. Ello ha evitado la propagación de los daños, ahorrando pérdidas y costos por la destrucción de *hardware*, *software*, información estratégica nacional y, lo más importante, protegiendo la seguridad informática nacional.

La implementación de un CSIRT en cada país, es de trascendental importancia, toda vez que pueden monitorear la red para detectar actividades ilícitas. En el caso de México, según lo expuso su Coordinador General de CSIRT, en el taller de delitos cibernéticos realizado del 9 al 14 de julio del 2012, en Montevideo, utilizan el CSIRT para monitorear las actividades de los cárteles del narcotráfico, lo cual les ha sido de mucha utilidad para combatir ese flagelo. De manera que, la función de un CSIRT es muy amplia y necesaria para combatir prácticas ilícitas, a todo nivel, mediante el uso de la red.

1.2 Resolución AG/RES 1939 (XXXIII-0/03)

Para poder explicar el origen o nacimiento del CSIRT, a nivel internacional, citamos la resolución AG/RES 1939, proferida por la Asamblea General de la Organización de Estados Americanos (OEA), aprobada en la cuarta sesión plenaria celebrada el 10 de junio del año 2003. A través de este instrumento se consideró que los Estados Miembros de la OEA debían desarrollar una estrategia para hacer frente a las **amenazas de seguridad cibernética**. También se fundamenta esta resolución en la continuidad derivada de la

aprobación de la resolución de la Asamblea General de las Naciones Unidas, aprobada en diciembre del 2002; resolución número 27/239 sobre los elementos para la creación de una **Cultura Mundial de Seguridad Cibernética para Sistemas y Redes de Información**.

Al considerarse la necesidad de la resolución AG/RES 1939 de la OEA, se tuvo a la vista el informe de la XII Reunión del Comité Directivo Permanente de la Comisión Interamericana de Telecomunicaciones (COM/CITEL), por medio del cual se señala que la "*creación de una cultura de ciberseguridad, para proteger la infraestructura de las telecomunicaciones, aumentando la conciencia entre todos los participantes de las Américas en las redes y sistemas de información, relacionados con el riesgo de dichos sistemas y desarrollando las medidas necesarias para hacer frente a los riesgos de seguridad, respondiendo rápidamente a los ciber-incidentes*" es parte de los mandatos de la CITEL.

En la parte resolutiva de la resolución AG/RES 1939, se dispone:

1.2.1 Encomendar al Comité Interamericano contra el Terrorismo (CICTE). La Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Expertos Gubernamentales sobre Delito Cibernético de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA), que se aseguren de que la Conferencia de la Organización de los Estados Americanos (OEA) sobre Seguridad Cibernética, propuesta por la Argentina, empiece a trabajar en el desarrollo de un proyecto de estrategia integral de la OEA sobre seguridad cibernética, que aborde los aspectos multidimensional

y multidisciplinario de la seguridad cibernética, y que informen sobre los resultados de la reunión y sobre el trabajo de seguimiento que se considere apropiado, a la Comisión de Seguridad Hemisférica para su consideración.

1.2.2 Encomendar al Consejo Permanente que, a través de la Comisión de Seguridad Hemisférica, desarrolle un proyecto de estrategia de seguridad cibernética para los Estados Miembros, en coordinación y colaboración con la CITEL, el CICTE, el Grupo de Expertos Gubernamentales sobre Delito Cibernético de la REMJA y cualquier otro órgano de la OEA que se considere apropiado, sin perjuicio de sus respectivos mandatos, misiones y requerimientos existentes sobre presentación de informes, teniendo en consideración cualquier actividad pertinente en los Estados Miembros relativa a la protección de infraestructura crítica, y que presente este proyecto de estrategia sobre seguridad cibernética al Consejo Permanente para su consideración.

1.2.3 Solicitar al Consejo Permanente que informe a la Asamblea General, en su trigésimo cuarto período ordinario de sesiones, sobre la implementación de esta resolución.

1.3 Necesidad del CSIRT

La Internet ha generado diversidad de amenazas que ponen en peligro a las personas y sus bienes. Tal como lo han considerado diversos organismos internacionales como la Organización de Estados Americanos (OEA), ente que indicó que lamentablemente "*la Internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial de usuarios de Internet.*

La información que transita por Internet puede ser malversada y manipulada para invadir la privacidad de los usuarios y estafar a los negocios. La destrucción de los datos que residen en las computadoras conectadas por Internet puede obstaculizar las funciones del gobierno e interrumpir el servicio público de telecomunicaciones y otras infraestructuras críticas"[70].

Debido a esas amenazas existentes en Internet, en la Conferencia Especial sobre Seguridad[71] los Estados Miembros de la OEA consideraron el tema de la seguridad cibernética y acordaron lo siguiente: "*Desarrollaremos una cultura de seguridad cibernética en las Américas adoptando medidas de prevención eficaces para prever, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, luchando contra las amenazas cibernéticas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas...*"

Fue así como los Estados del Hemisferio, reunidos en el cuarto período ordinario de sesiones del Comité Interamericano contra el Terrorismo (CICTE), una vez más declararon su compromiso por combatir el terrorismo, incluidas las amenazas a la seguridad cibernética, la cual identificaron como una de las amenazas terroristas emergentes. En esa ocasión, el CICTE también consideró el documento "***Marco para establecer una red Interamericana CSIRT de Vigilancia y Alerta***".

70 Organización de Estados Americanos, *UNA ESTRATEGIA INTERAMERICANA INTEGRAL DE SEGURIDAD CIBERNÉTICA: UN ENFOQUE MULTIDIMENSIONAL Y MULTIDISCIPLINARIO PARA LA CREACIÓN DE UNA CULTURA DE SEGURIDAD CIBERNÉTICA*, Anexo A.

71 Conferencia Especial sobre Seguridad que se llevó a cabo en México, del 28 al 30 de octubre del año 2003.

Es así como vemos la obligación del Estado de Guatemala, como miembro de la OEA, de dar cumplimiento a los acuerdos y compromisos celebrados a través de ese organismo internacional, especialmente lo relativo a la formación de una Red Interamericana de Vigilancia y Alerta, para la rápida divulgación de información sobre seguridad cibernética y la respuesta a crisis, incidentes y amenazas de seguridad informática.

Las siglas "**CSIRT**", significan en idioma español: "***Equipo de Respuesta a Incidentes de Seguridad Informática***". Su significado original deriva del idioma inglés: "***Computer Security Incident Response Team***".

A nivel internacional, se sabe que un CSIRT constituye un equipo de personas expertas en seguridad informática, cuya misión principal se refiere a la prevención, tratamiento y respuesta a un incidente de seguridad informática.

1.4 Funciones del CSIRT

En la iniciativa de Ley de Delitos Informáticos, número 4055, se incluyó la normativa relativa al CSIRT. En el artículo 21 de dicha iniciativa de ley, se establece:

> "Se crea el Comité de Respuesta a Incidentes de Seguridad Informática para Guatemala, que, por sus siglas en inglés, podrá denominarse "CSIRT-gt", como un ente adscrito al Ministerio de la Defensa Nacional.
>
> El CSIRT-gt tendrá a su cargo la promoción de la seguridad informática a nivel nacional, lo que incluye las funciones siguientes:

a. **Proactivas**: Consistentes en educación, asesoramiento técnico, alertas y promoción de estándares de seguridad;

b. **Reactivas**: Consistentes en la asistencia a incidentes de seguridad informática, tanto a instituciones públicas como privadas y la realización de todos aquellos actos de mitigación de daño en materia informática. Asimismo, el CSIRT-gt deberá formular las recomendaciones necesarias para el cumplimiento de la presente ley, su reglamento y las normas relativas a la prevención de incidentes de seguridad informática contenidas en manuales, reglamentos o circulares emitidos por dicho Comité;

c. **Investigación y desarrollo**: Consistentes en actividades que generen proyectos de investigación y desarrollo de tecnologías convergentes a la iniciativa de seguridad informática.

Con la regulación del CSIRT dentro de la ley de Delitos Informáticos, consideramos que el Estado de Guatemala está dando un paso trascendental en la lucha contra el terrorismo y la inseguridad cibernética.

1.5 Ejemplos de Centros de respuesta a incidentes de seguridad informática en América Latina

1.5.1 Brasil

En la república federativa de Brasil organizacionalmente existe el Gabinete de Seguridad Institucional – **GSIPR**-, el cual, según el capítulo 6 de la ley No. 10,683 del 29 de mayo de

2003, tiene como áreas de competencia: "... ***es la responsable de coordinar las actividades de inteligencia federal y de seguridad de la información***..."

Estas áreas están representadas por dos instituciones: (1) Departamento de Seguridad de la Información y Comunicaciones – DSIC y, (2) La Agencia Brasileña de Inteligencia – ABIN.

En el Decreto Nº 5.772, del 08 de mayo del 2006, se crea dentro del GSIPR el Departamento de Seguridad de la Información y comunicaciones – DSIC-.

Según la ley en cita, los campos que abarca la Seguridad de la información y comunicaciones son:

a) Seguridad de Recursos Humanos.
b) Seguridad de los Sistemas de Información y Comunicaciones.
c) Seguridad de áreas e Instalaciones.
d) Seguridad de Materiales.
e) Detección y preservación de amenazas.
f) Valoración de las amenazas por quiebra de la seguridad.

Así mismo, los productos y servicios del Departamento de Seguridad de la Información y Comunicaciones DSIC son:

a) Sistema de Seguridad y acreditación (SISC).
b) Portal de difusión de información sobre SIS.
c) Publicaciones y medios sobre SIC.
d) Normas, requisitos y metodología para la gestión de SIC.
e) Cursos, Simposios, Seminarios y Workshop en SIC.

f) Tratamiento de incidentes en redes y sistemas computacionales.

Las competencias establecidas en la Ley de Brasil para el)SIC, son:

- Estudiar legislaciones correlacionadas e implementar las propuestas sobre materias relacionadas a seguridad de la información y comunicaciones.

- Avalar tratados, acuerdos suscritos en actos internacionales, relacionados a la seguridad de la información y comunicaciones.

- Adoptar las medidas necesarias y coordinar el funcionamiento del Sistema de Seguridad y Acreditamiento – SISC, de personas y empresas, trato de asuntos, documentos y tecnología sigilosa.

- Planificar y coordinar la ejecución de actividades de seguridad de la información en la administración del manejo de documentos, información y tecnología reservada.

- Definir requisitos metodológicos para la implementación de seguridad de la información y comunicaciones, por los órganos de administración pública federal.

- Operacionalizar y mantener el Centro de Tratamiento y Respuesta a incidentes ocurridos en la redes de computadoras de la Administración pública federal.

El DSIC realiza las actividades siguientes:

a) Revisión de la legislación aplicable.
b) Propuesta de Decreto Presidencial que norma la acreditación de la seguridad.
c) Acuerdos Internacionales sobre materias clasificadas.
d) Concepción del modelo Brasileño de gestión de materiales sensibles.
e) Proyecto de desarrollo de sistemas de información.
f) Propuesta de Normas Generales de Acreditación.
g) Cursos de formación de Gestores y multiplicadores de la Seguridad de la Información.
h) Entrenamiento en Fundamentos de Seguridad de la Información.

Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil CERT.br.

Dentro del Departamento de Seguridad de la Información y Comunicaciones - DSIC-, funciona el CERT.br, que es el equivalente al Centro de Respuesta a Incidentes de Seguridad Informática CSIRT.

El CERT.br, anteriormente denominado NBSO/Brazilian CERT, o grupo de respuesta a incidentes de seguridad para la Internet brasileña, mantenido por el NIC Brasil del Comité Gestor de Internet de Brasil, ahora es el responsable de recibir, analizar y responder a incidentes de seguridad, que relacionan a redes conectadas a Internet en Brasil.

A través del proceso de respuesta a incidentes en sí, el CERT.br también actúa a través de trabajo de concientización sobre los problemas de seguridad; correlaciona los eventos en la Internet brasileña y da auxilio al establecimiento de nuevos CSIRTS en Brasil.

Los servicios que presta el CERT.br, son:

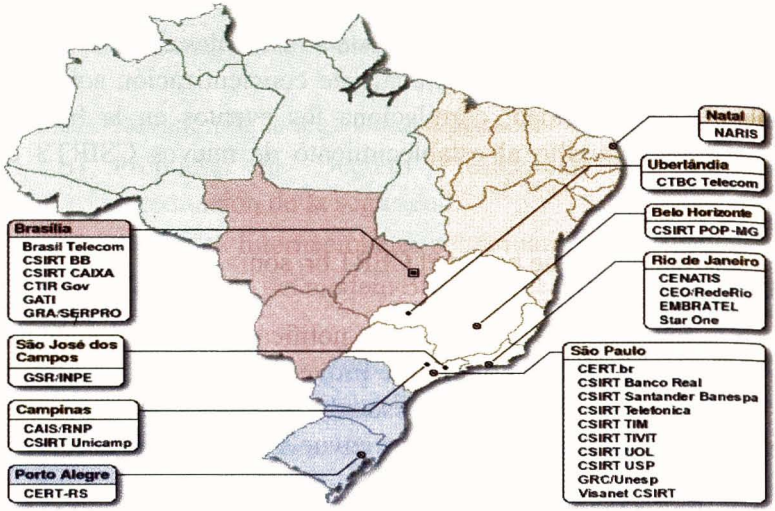
- Ser un punto único para notificaciones de incidentes de seguridad, a modo de proveer coordinación y apoyo necesario en el proceso de respuesta a incidentes, colaborando con las partes envueltas cuando sea necesario.

- Establecer un trabajo colaborativo con otras entidades, como la policía y proveedores de acceso a servicios de Internet.

- Dar soporte en el proceso de recuperación y análisis de sistemas comprometidos.

- Ofrecer entrenamiento en el área de respuesta a incidentes de seguridad, especialmente para miembros de CSIRTS para instituciones que están creando su propio grupo.

  En el siguiente mapa se pueden apreciar otros Centros de Respuesta en Brasil:



1.5.2 Uruguay

El CSIRT de ANTEL es un Centro de Respuesta a Incidentes orientado a la Comunidad Objetivo, que está integrado por ANTEL (la corporación y unidades de negocios) y los clientes más importantes de ANTELDATA y de ANCEL. Cuando ocurren incidentes de seguridad es necesario que las comunidades tengan un modo efectivo y coordinado de responder.

La velocidad con la cual la organización pueda reconocer, analizar y responder a un incidente de seguridad, limitará los daños y disminuirá los costos de recuperación.

El CSIRT de ANTEL tiene como servicio central realizar una gestión de incidentes de seguridad eficaz y eficiente. Para ello

72 CERT.br

sus integrantes buscan, en el contexto de su Código de Conducta, relacionarse con equipos pares y con su comunidad, capacitarse permanentemente, estar al día tecnológicamente y así mejorar de manera continua todos los servicios brindados.

Los servicios que presta el CSIRT de ANTEL son:

a) Reactivos:

1. Alertas,
2. Manejo de incidentes

b) Proactivos:

1. Anuncios.
2. Detección de incidentes.

También se dedica a:

- Desarrollo de técnicas y herramientas.
- Elaboración de políticas y mejores prácticas (*best practices*).

Como valor agregado del CSIRT de ANTEL tiene: (a) Capacitación y entrenamiento; (b) Análisis de riesgo; (c) Consultoría de seguridad; y, (d) Concientización de la comunidad en temas de seguridad.

1.6 Objetivos de un CSIRT

Los objetivos de un CSIRT son los siguientes:

1) Mejorar el nivel de Seguridad Informática en el país.

2) Contar con una unidad, que dé soporte y respuesta a los incidentes de seguridad informática.

3) Tomar acciones proactivas en este aspecto de la seguridad nacional.

1.7 Desarrollo de CSIRT

1.7.1 Localización Organizacional

Por el nivel de las instituciones que soportará su nivel es estratégico, por lo que podrá funcionar como una secretaría de la PRESIDENCIA o como un ente autónomo, dentro de una institución de Seguridad.

En la Iniciativa de Ley 4055, Ley de Delitos Informáticos, se propone la creación del Comité de Respuesta a Incidentes de Seguridad Informática para Guatemala, como un ente adscrito al Ministerio de la Defensa Nacional. La idea de que el CSIRT sea parte del Ministerio de la Defensa, radica en la función de dicho Ministerio en cuanto a brindar seguridad o protección del territorio guatemalteco. En este caso, se estaría protegiendo el Ciberespacio que tenga infraestructuras físicas dentro del territorio guatemalteco.

1.7.2 Ambiente físico

El Equipo de Respuesta a Incidentes de Seguridad Informática, puede poseer sus propias instalaciones o ser albergado por una institución afín.

Ésta debe contar con:

1.7.2.1 Áreas administrativas

Donde se pueda atender a los diferentes usuarios, si fuera el caso, tales como salas de apoyo, salas de reuniones que podrán ser compartidas con el resto de la organización.

1.7.2.2 Áreas de soporte administrativo del Centro

Como su nombre lo indica, se encarga de satisfacer las necesidades administrativas del Centro.

1.7.2.3 Áreas operacionales

Tales como salas de trabajo de los equipos técnicos, sala de servidores y sala de laboratorio; son consideradas ambientes críticos y deberán tener implementaciones de aspectos de seguridad física específicos.

Para los ambientes críticos deberán ser contempladas las siguientes características de seguridad:

- Ambiente aislado de otros departamentos.
- Acceso restringido al ambiente de trabajo.
- Puertas con mecanismos de seguridad (contraseñas, botones magnéticos, por factores biométricos).
- Formas de identificar y mantener almacenados los datos de acceso.

1.7.3 Características de Seguridad

Se recomienda que el acceso y permanencia en el lugar por terceros (proveedores, visitantes, personal de limpieza y otros) sea acompañado por un miembro del Centro.

1.7.4 Infraestructura de red

La infraestructura de red del Centro debe ser separada de la infraestructura de la organización donde esté conectada. El Centro debe poseer una estructura propia de sub-redes y dominios.

Se recomienda que el Centro tenga estructura aislada, permitiendo implementar compartimientos de redes con funciones diferenciadas. Por lo menos dos compartimientos deben existir con:

a. Redes de computadoras del Centro.

b. Red de laboratorio de tests y estudios.

c. Redes conectadas al ambiente externo.

d. Protegidas por recursos de seguridad (Firewall, proxy, IDS, IPS, entre otros).

Para que el Centro pueda operar con todas sus atribuciones se hacen necesarios, como mínimo, los siguientes equipos y recursos de uso general:

1.7.4.1 Equipo y recursos de conectividad

1) Ruteadores.
2) Switches.
3) Hubs.
4) Cableado.
5) Internet.
6) Servidores para ejecución de las siguientes funciones:

    a) Sistema de firewall.
    b) Sistema de detección de intrusos.
    c) Servicios de Email, Web, NTP, DNS.
    d) Registro de actividades (logs);
    e) Sistema de archivos.
    f) Intranet.
    g) Sistema de acceso remoto.
    h) Sistema de backup.
    i) Máquinas de laboratorio.

1.7.5 Infraestructura de Hardware

Cada miembro del Centro debe contar con estación de trabajo, computadora portátil y un escritorio. Adicionalmente deberán existir computadoras portátiles para el desarrollo del Servicio remoto.

1.7.5.1 Equipamiento para seguridad de ambiente físico

1) Caja fuerte a prueba de fuego.

2) Infraestructura de protección contra interrupciones de energía eléctrica:

a) Estabilizadores.
b) Nobreaks.
c) Generadores Alternos

1.7.5.2 Infraestructura de protección contra incendios (prevención, detección y alarma).

1.7.5.3 Sistema de refrigeración y aire acondicionado compatible con las especificaciones de los servidores y equipos.

1.7.5.4 Otros equipos

1) Proyector multimedia.
2) Impresora.
3) Fax.
4) Escáner.
5) Dispositivos para realización de copias de seguridad como: grabadoras de CD, DVD y cinta magnética.
6) Triturador de papel.
7) Línea telefónica independiente.
8) Material de oficina.

1.7.6 Infraestructura de Software

Se recomienda que los servidores y escritorios del Centro utilicen *software* libre.

Se debe asegurar que todos los sistemas operacionales, *software* y configuraciones de los equipos utilizados en

las redes operacionales del Centro, sigan un estándar, de forma que cumplan los siguientes requisitos:

- Estar configurados de modo seguro.
- Tener instaladas las últimas actualizaciones y correcciones de seguridad.
- Poseer habilitados sistemas de registros de actividades (logs).
- Poseer el siguiente *software, p*ara que el Centro pueda operar con todas sus atribuciones:
  - Sistemas operativos para servidores, estaciones de trabajo y portátiles.
  - Sistemas de información en la WEB, para recolectar información de incidentes y divulgación (alertas, recomendaciones, estadísticas).
  - *Firewall* corporativo, para las estaciones de trabajo y portátiles.
  - Para detección de intrusiones.
  - *Software* de criptografía y firma digital.
  - Sistemas para gestión de llaves y certificados digitales.
  - *Software* de laboratorio:
    Las máquinas del laboratorio para tests y estudios, deben tener instalados y configurados los sistemas operativos y software utilizado por las diferentes dependencias del Estado y organizaciones públicas y privadas a las que se les dé soporte; para ello deben ser adquiridas licencias de estos productos.

1.7.7 Infraestructura de comunicación

Para proveer un mínimo de servicio se necesitan los siguientes recursos de comunicación:

a. Conexión de alta velocidad a Internet.

b. PBX, ramales y correo de voz.

c. FAX.

d. Teléfonos móviles, localizador personal, con la intención de viabilizar la operación 24 / 7.

e. Unidad de respuesta automática.

1.7.8 Público objetivo

Dirigido a todos los órganos y entidades públicas y privadas que presenten incidentes y requieran soporte.

1.7.9 Misión

Actuar en el tratamiento y prevención de incidentes de seguridad, envolviendo computadores y redes de los Órganos y entidades.

1.7.10 Autoridad

El objetivo de esta entidad es la coordinación y el análisis de las acciones relativas al tratamiento de incidentes de seguridad en redes de computadores, por lo tanto no le corresponderá imponer Normas o Procedimientos.

1.7.11 Servicios Prestados

1.7.11.1 Servicios Reactivos: Servicios que ocurren en respuesta a una actividad o a una requisición efectuada al Centro.

1.7.11.1.1 Tratamiento de Incidentes. Compuesto por notificación del incidente, análisis del incidente y Respuesta al incidente.

Recibir notificaciones de incidentes habilita el CSIRT a servir como un punto central de contacto para notificación de problemas locales.

Análisis de Incidentes. Examinar todas las informaciones disponibles sobre un incidente, incluyendo artefactos y otras evidencias relacionadas con la actividad.

El propósito del análisis es identificar el objetivo del incidente, su extensión, su naturaleza y cuáles son los perjuicios causados. Proponer estrategias de contención y recuperación.

1.7.11.1.2 Soporte a la Respuesta a Incidentes. Auxilia los administradores en el proceso de recuperación. Este auxilio puede ser prestado vía teléfono, e-mail, fax o a través de la indicación de documentos que puedan auxiliar en el proceso de recuperación.

El Centro coordina las acciones entre las redes envueltas en un incidente, lo que puede envolver redes y otros centros externos a su ámbito de actuación. El proceso de coordinación puede envolver la colecta de informaciones de contacto, la notificación de redes que puedan estar envueltas y la generación de estadísticas relativas a los incidentes.

El Centro, en este caso, actúa como un facilitador del proceso de incidentes y en el intercambio de informaciones entre las partes envueltas.

Distribución de alertas, recomendaciones y estadísticas, diseminar informaciones relativas a nuevos ataques y a tendencias de ataques, siendo observadas por el propio Centro, por otros centros y empresas proveedoras de software utilizados por el público objetivo del Centro.

Distribución de alertas para los órganos y entidades. Estas alertas, en general serán redistribuciones de alertas emitidas por proveedores, por el *Computer Emergency Response Team* (CERT/CC) y otros Centros. El Centro, al redistribuir, puede acrecentar recomendaciones específicas para su público y atribuir diferentes grados de severidad.

1.7.11.2 **Servicios Proactivos.** Servicios que tienen como objetivo aumentar el grado de seguridad

de las instituciones atendidas, de modo que sea evitado que ocurran incidentes de seguridad o, en caso ocurran, que el impacto sea el menor posible.

1.7.11.2.1 Acompañamiento y Colecta de Información.

Este proceso envuelve el acompañamiento de listas de discusión, periódicos, revistas, congresos del área, relaciones de cooperación con otros grupos, a modo de tener acceso a informaciones sobre nuevas tendencias observadas en otros puntos de la Internet.

1.7.11.2.2 Capacitación en el Área de Tratamiento de Incidentes.

El Centro puede proveer entrenamiento para Equipos de Respuesta a incidentes de los órganos y entidades, abordar respuesta a incidentes de seguridad, utilización de herramientas, formación y estructuración de grupos de respuesta a incidentes, entre otros.

1.7.11.2.3 Actividades Notificadas.

Tentativas de ataques, proporcionando datos consolidados de las fuentes disponibles con detectores de intrusiones y demás. Incidentes como negación de servicio, *spam*, invasiones, proporcionando toda la información disponible. Situaciones en que las redes fueron causantes de incidentes, proporcionando igualmente toda la información disponible.

1.7.11.2.4 Distribución del Centro

El modelo de coordinación seleccionado debe ser centralizado. Este modelo incorpora ventajas para la gerencia que se apropia de información de fuentes dispersas y distintas, ordenando las posibles soluciones para las causas más probables de incidentes de seguridad.

1.7.11.2.5 La Estrategia centralizada tiene como objetivo:

a) Servir como punto de convergencia de las informaciones relativas a Incidentes de seguridad en redes de computadores.
b) Analizar e identificar tendencias y estándares.
c) Prever posibles impactos de los incidentes de seguridad y definir acciones estratégicas.
d) Asesorar el proceso decisorio con relación a la seguridad de la información.
e) Perfeccionar los mecanismos de difusión de información relativas a incidentes de seguridad en redes de computadores.
f) Promover mecanismos para viabilizar la conexión informacional.

1.7.12 Horario de Funcionamiento del Centro

El Centro proveerá, continuamente, atención a incidentes, es decir todos los días y horarios de la semana, incluyendo sábados, domingos y días festivos.

Para ello, deberá contar con equipo de trabajo en horario comercial, proveyendo soporte en los períodos nocturnos, fines de semana y festivos en régimen de sobre aviso.

1.7.13 Organización del Trabajo y Requisitos de Recursos Humanos

Un cuadro de personal adecuado es, ciertamente, un factor crítico para el éxito. Todo el equipo técnico deberá trabajar en un régimen de dedicación íntegra y exclusiva.

Es importante que los miembros del Equipo sean personas dedicadas, innovadoras, detallistas, flexibles, analíticas e íntegras.

1.7.14 Estructura organizacional del Centro

1.7.14.1 Grupo Coordinador:

Este grupo será el encargado de establecer las políticas del Centro; se reunirá en casos de emergencia informática, recibirá informes mensuales del Director del Centro y participará en el proceso de selección de los integrantes fundadores, por única vez.

Conformado por representantes de las siguientes instituciones:

a) Un representante del Ministerio de Relaciones Exteriores.
b) Un representante del Ministerio de la Defensa.

c) Un representante de la Superintendencia de Telecomunicaciones.
d) Un representante de la Superintendencia de Bancos.
e) Un representante del Cluster de Tecnología.

1.7.14.2 Dirección del Centro:

a) Director
b) Analista

1.7.14.3 Coordinación General de Soporte a Incidentes:

a) Director
b) Coordinador
c) Analista
d) Programador

1.7.14.4 Coordinación de Tratamiento a Incidentes:

a) Director
b) Coordinador
c) Analista
d) Programador

1.7.14.5 Coordinación de Diseminación de Información:

a) Director
b) Analista

1.7.15 Características generales necesarias para todos los miembros del Centro:

- Disponibilidad de dedicación integral y exclusiva.
- Realización de investigación social.
- Habilidad para hablar otros idiomas.
- Buena técnica de redacción.
- Curso superior en Análisis de Sistemas, Ingeniería de Informática o áreas afines.
- Sólidos conocimientos técnicos en seguridad de sistemas y redes.
- Experiencia en el área de seguridad de la información.
- Facilidad de comunicación verbal y escrita.
- Estar actualizado en asuntos relativos a la seguridad.
- Disponibilidad para viajar.

1.7.16. Características específicas y atribuciones para los miembros del Centro

1.7.16.1. Director:

- Gerenciar y coordinar las actividades de los Grupos
- Proveer direccionamiento estratégico al Grupo.
- Proveer las condiciones de trabajo para Funcionamiento del Grupo.
- Representar al Grupo ante los Órganos superiores de la administración.
- Realizar los contactos con los Órganos de comunicación.

- Comprobada capacidad de liderazgo, Coordinación y trabajo en equipo.
- Experiencia en el trato con los medios de comunicación.

1.7.16.2 Coordinador General:

- Dar apoyo a la dirección estratégica.
- Atribuir tareas y deberes a las coordinaciones y supervisar sus actividades.
- Participar del proceso de selección de nuevas contrataciones.
- Elaborar plan de metas y previsiones presupuestarias para el Centro.
- Elaborar informes periódicos de las actividades desarrolladas.
- Representar al Centro ante Órganos técnicos nacionales e internacionales.
- Poseer conocimiento en arquitecturas de redes y protocolos internet.
- Tener experiencia en la supervisión de ejecución de actividades.
- Comprobada capacidad del trabajo en equipo.

1.7.16.3 Analista

- Desempeñar las actividades operacionales de las coordinaciones de tratamiento de incidentes y diseminación de informaciones.
- Conocimiento en Arquitecturas de redes y protocolos Internet.

- Conocimiento especializado en sistemas operacionales, técnicas y herramientas de seguridad.
- Experiencia amplia en administración de redes y sistemas operacionales.
- Experiencia en programación.
- Experiencia en ministrar entrenamientos (deseable).
- Habilidad en relacionamiento interpersonal (deseable).

1.7.17. Recursos

1.7.17.1 Humanos

El Grupo coordinador debe estar conformado por personal de las diferentes instituciones que, por su importancia, deben participar activamente en este Centro. Dicho personal debe poseer conocimiento y experiencia laboral reconocida en el área informática.

Para el resto de cargos se hace necesaria la contratación de personal, con las características indicadas supra. Para contratar a este personal se deberá de llevar un proceso de selección cuidadoso y completo. La primera selección la efectuará el Grupo coordinador, posteriormente lo hará el Director y los diferentes coordinadores de área, según sea la especialidad que se requiera.

1.7.17.2. Institucionales

Se necesita la participación de:

- Ministerio de la Defensa Nacional.
- Ministerio de Relaciones Exteriores.
- Superintendencia de Telecomunicaciones.
- Superintendencia de Bancos.

Debido a que el proyecto es de carácter nacional, y que las instituciones citadas forman parte de la infoestructura crítica del Estado, su participación es indispensable y le otorga legitimidad a la entidad.

1.7.17.3. Económicos

Debido que el costo de la implementación de un Centro de Respuesta a Incidentes de Seguridad Informática es oneroso, por la variedad y complejidad del equipo necesario, los recursos económicos deben ser coordinados con instituciones nacionales o internacionales donantes.

1.7.17.4. Materiales

Estos deben ser contemplados en el presupuesto de funcionamiento del centro e incluidos en la solicitud de fondos a entidades externas.

2. FISCALÍA ESPECIAL DEL MINISTERIO PÚBLICO

Debido a la especialidad que implica la investigación y persecución penal en materia de delitos informáticos, consideramos pertinente la creación de una Fiscalía Especial del Ministerio Público, para poder realizar dichas funciones. Actualmente, en nuestro país no existe una Fiscalía especializada en esta materia.

Las funciones de la Fiscalía Especial del Ministerio Público deben llevarse a cabo con las demás instituciones vinculadas con la investigación penal en materia informática, para llevar a cabo una mejor investigación en la materia.

En la mayoría de países, que actualmente cuentan con legislación especial sobre cibercrimen, se han creado instituciones, dependencias o fiscalías especializadas para contrarrestar este tipo de conductas ilícitas.

En la Iniciativa de Ley de Delitos Informáticos, número 4055, se regula sobre la creación de una Fiscalía especializada del Ministerio Público para Delitos Informáticos, según consta en el artículo 25 de dicho proyecto de ley, el cual dice así: "*El Ministerio Público deberá contar con una Fiscalía Especial en la investigación y persecución de los delitos contenidos en la presente ley. La que debe ser creada y organizada en el plazo de tres meses a partir de la entrada en vigencia de la presente ley. Para la operatividad de esta fiscalía, se conformará una fuerza de tarea conjunta.*"

Debe tenerse presente que la Fiscalía especializada de Cibercrimen tendrá la función de investigación y persecución de

los delitos informáticos. Por ello, también es necesario que exista una organización en las instituciones dedicadas a la investigación criminal relativa a delitos informáticos, para lograr la eficiencia en los análisis y expertajes referentes a delitos informáticos. Con esta organización se evitaría que cada institución como Ministerio Público, Policía Nacional Civil, entre otras, tenga su propia unidad o departamento de análisis de prueba. Todas esas dependencias quedarían bajo el control y administración del Ministerio Público, como ente encargado de la investigación y persecución de los delitos. Esta finalidad se lograría mediante la vigencia de la Iniciativa de Ley de Delitos Informáticos, toda vez que en su artículo 26 se regula la organización de la fuerza de tarea conjunta, de la manera siguiente: "***Artículo 26. Garantía de funcionamiento de la persecución penal***. *Para la garantía del funcionamiento armónico y adecuado de la persecución penal, las dependencias centralizadas, descentralizadas, autónomas y semiautónomas, que hasta la entrada en vigencia de la presente ley realizan actividades concernientes a la investigación de delitos informáticos, deberán poner a disposición directa del Ministerio Público las unidades o dependencias que estén creadas y en funcionamiento, a efecto de que esta coordine la actividad de investigación relacionada a los delitos contenidos en la presente ley y otros que, por su naturaleza, se necesite de la aplicación de conocimientos técnicos especializados. Dichas dependencias conformarán una fuerza de tarea conjunta. El CSIRT-gt deberá proporcionar la asesoría técnica que sea necesaria para la investigación de delitos informáticos.*"