UNIVERSIDAD APEC

Escuela de Graduados

Tesis para optar por el título de Maestría en el Programa de:

Maestría en Gerencia y Productividad

Título:

"Propuesta para la Implementación de un Centro de Respuestas a Incidentes de Seguridad Informática Nacional – CSIRT- RD, Año 2014".

Sustentante:

Nombre:	***Matrícula***
Engel Rivas	***2011-1188***

Asesora:

Edda Freites, MBA

Santo Domingo, D. N.

Agosto, 2014

RESUMEN

Un Centro de Respuestas a Incidentes de Seguridad Informática - CSIRT, es un ente referencia mundial, desde el surgimiento de los controles y medidas de seguridad para la protección de la información sensible y confidencial de las empresas y entidades gubernamentales. La Republica Dominicana desde inicios de la década del 2000, había estado formando las bases necesaria de unidades y departamentos encargados de dar respuestas a los incidentes informáticos de la nación, ya a partir de 2003, se crearon los departamentos de respuestas a incidentes de seguridad informática, esto por requerimiento y exigencias ante los incidentes recurrentes. No obstante, ante el aumento sofisticado de los incidentes de seguridad informática, dichos departamento han tenido que ir actualizándose e innovando las respuestas y medidas preventivas. De esta manera, los países desarrollados han adoptado la medida de implementar Centros de Respuestas a Incidentes de Seguridad Informática – CSIRT, siendo el mismo un solo punto de recepción de incidentes, donde el mismo posee las últimas tecnologías y medidas de control y prevención, para contrarrestar los incidentes y ataques informáticos. En esta investigación serán utilizados las entrevistas, cuestionarios, estudios exploratorios y estadísticos para diseñar un Centro de Respuestas a Incidentes de Seguridad Informática Nacional– CSIRT-RD, acorde con los estándares internaciones y otros CSIRT internacionales de referencia. Luego de concluida la investigación, serán recomendadas las acciones y bases iniciales para el inicio de la implementación de un centro de respuestas a incidentes de seguridad informática nacional – CSIRT-RD, el cual será capaz de responder antes las demandas de incidentes actualmente registrados en los organismos actuales de la Policía Nacional Dominicana, los cuales son el Departamento de Investigación y Crímenes de Alta Tecnología – DICAT y el Departamento Nacional de Investigaciones – DNI. El CSIRT-RD consolidara en una sola unidad estos departamentos en materia criminal cibernética.

INTRODUCCION

La información, activo valioso de hoy en día, la cual en el transcurso de los siglos y las décadas ha ido evolucionando su potencial e importancia, a tal grado, que en la actualidad es un recurso muy apreciado y protegido por personas, empresas, instituciones y gobiernos.

La lucha y el poder de la información ha provocado delitos, crímenes de guerra, amenazas, desfalcos y una serie de atrocidades históricas, lo cual ha tenido como consecuencia, la creación y el surgimiento de controles y medidas de seguridad, tanto física, como lógica. De esa manera, nace el concepto de seguridad informática, al punto de convertirse en un pilar y/o soporte importante en las empresas, tanto privadas, como gubernamentales, para la protección y cuidado de su información sensible o confidencial.

Este trabajo de investigación tendrá como objetivo general el diseñar e implementar un centro de respuestas a incidentes de seguridad informática nacional para la republica dominicana, con el propósito de eventualmente responder ante delitos informáticos relacionados a la nación y su población.

La estructura del proyecto consta de la manera siguiente: Capitulo I, se exponen los antecedentes históricos de la seguridad informática y los CSRIT, así como las bases iniciales para las implementaciones de CSIRTs. El Capitulo II, expone las estructuras organizacionales de referencia de un CSIRT. El Capítulo III, detalla la propuesta para la implementación inicial de un CSIRT.

INDICE GENERAL

ÍNDICE DE TABLAS

INDICE DE GRAFICOS

CAPITULO I

ANTECEDENTES DE LA SEGURIDAD DE LA INFORMACION

INFORMACION BASICA - CENTROS DE RESPUESTAS DE INCIDENTES DE SEGURIDAD INFORMATICA – CSIRT

Es obvio que los sistemas de negocios y de información están muy dependientes de los procesos productivos, industriales, de servicios, gubernamentales y casi cualquier sector activo de la sociedad. Esta dependencia de los sistemas de información en general, requiere dotar de seguridad a los mismos para preservar la calidad de los servicios y velar por la eficacia y eficiencia de los procesos de negocio y el valor de sus activos.

1.1 ANTECEDENTES SEGURIDAD DE LA INFORMACION

Desde el surgimiento del Internet en la década de los 80s y la evolución de los sistemas de información y computacionales en las empresas como fuente vital para su desarrollo y estabilidad, las amenazas, las vulnerabilidades y los ataques informáticos se han desarrollado increíblemente, afectando a millones de usuarios y ocasionando perdidas tangibles e intangibles a las empresas, como pérdidas millonarias de dinero y reputación.

En la actualidad, es un hecho incuestionable que la gran mayoría de los procesos de negocios e industriales son soportados, automatizados y gestionados por sistemas de información y computacionales, los mismos también apoyan las actividades gerenciales y las tomas de decisiones;

Requiere un accionar proactivo y su incorporación como elemento estratégico. A modo de ejemplo, una empresa que gestione adecuadamente la seguridad de la información, por un lado da cumplimiento a sus obligaciones y regulaciones, y a su vez genera confianza en sus clientes y potenciales inversores.

La seguridad de la información, no es un activo a comprar, ni un fin en sí mismo, tampoco un estado a alcanzar haciendo una determinada inversión; debe gestionarse, debe existir una meta concreta, criterios generales de evaluación y de decisión, y debe poder medirse. Es un sistema dinámico en constante evolución que debe ser evaluado y monitoreado, con métricas establecidas que permitan comparar conscientemente y lo más objetivamente posible, escenarios diferentes y tomar decisiones con respecto a los riesgos que se afrontan y los recursos disponibles.

En tal sentido, muchas empresas e instituciones organizadas hoy en día poseen gerencias, departamentos y unidades de seguridad de la información, con el fin de contrarrestar los ataques, fraudes y amenazas de las que son objeto. Este tipo de estrategias se ha expandido a tales magnitudes, que hoy en día la información es el activo principal, con el mismo se pueden cometer fraudes millonarios y hasta hacer manipulaciones y cambios de paradigmas a nivel mundial. Los involucrados en el uso de

Los involucrados en el uso de sistemas de información y computacionales (proveedores, usuarios, empresas, fabricantes, administradores, otros) deben estar en constante aprendizaje de las amenazas y vulnerabilidades existentes, así como de las técnicas disponibles para poder contrarrestarlas.

Esto obliga a las organizaciones a contar con personal especializado en seguridad y manejo de incidentes informáticos, involucrados en los procesos de monitoreo, análisis de nuevas amenazas y vulnerabilidades en equipos y

sistemas informáticos y diseño de metodologías para la resolución de incidentes de seguridad informáticos.

La definición de un grupo dedicado a manejar los ataques informáticos tanto externos como internos que puedan afectar a los sistemas e información de una organización tiene sus orígenes en la década de los 80, cuando el virus Moris infecto a miles de computadoras en poco tiempo, produciendo pérdidas cercanas a los 196 millones de dólares. Este ataque llevo a la creación del Equipo de Respuesta a Emergencia Computacionales (CERT) localizado en la Universidad de Carnegie Mello en Pittsburg Pensilvania con la finalidad de brindar soporte ante eventos similares.

[1]El nombre que se ha definido al equipo encargado del manejo de incidentes tiene algunas variantes a nivel mundial (Rajnovic, 2011):

- *CERT – Computer Emergency Response Team*
- *CIRT – Computer Incident Response Team*
- *IRT – Incident Response Team*
- *ERT – Emergency Response Team*

Se pueden encontrar variaciones a estos nombres, incluida la letra S de seguridad:

- *CSIRT – Computer Security Incident Response Team*
- *SIRT – Security Incident Response Team*
- *SERT – Security Emergency Response Team*

Dependiendo de la población a la cual el grupo ofrece sus servicios, los CSIRT se categorizan en: *académico, comercial, nacional o interno.*

[1] Proyecto AMPARO - CSIRT

Los CSIRT Nacionales tienen como principal enfoque ser el punto de contacto principal que brinde soporte a todo un país sobre aspectos de prevención, identificación, tratamiento y resolución de ataques e incidentes de seguridad sobre sistemas informáticos.

Los CSIRT Internos brindan soporte a organizaciones privadas y generalmente no publican las amenazas informáticas de las que fueron objeto de ataque, no de los procesos que efectúan para prevenirlas o tratarlas.

Los CSIRT Académicos prestan servicio a la institución educativa a la que pertenecen, así como a su comunidad de usuarios (estudiantes, profesores e investigadores), pero adicionalmente tiene como responsabilidad la investigación, elaboración, promoción y diseminación de prácticas de seguridad para el bienestar de la sociedad.

[2]Este monográfico está orientado a cubrir la necesidad de un CSIRT Nacional para la Republica Dominicana. En la actualidad existen organismos de seguridad del estado, orientados a la seguridad informática, los mismos son:

- *Departamento de Investigación de Crímenes y Delitos Informáticos de Alta Tecnología de la Policía Nacional – DICAT*

- *División de Investigación de Delitos Informáticos de la Dirección Nacional de Investigación – DIDI*

Estos departamentos dependientes de la Policía Nacional, actualmente están encargados de canalizar y responder ante los incidentes de seguridad. La finalidad de esta propuesta es crear y unificar estas dependencias en un solo organismo de seguridad tecnológica, un Centro de Respuestas a Incidentes de Seguridad Informática – CSIRT Nacional.

(Yunes, 2014)

[2] Entrevista Lic. Coronel Licurgo Yunes, Enc. DICAT

1.2 ¿QUÉ SE PROTEGE CON UN CSIRT?

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

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.**

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.**

1.3 ALCANCE DEL CSIRT

Las interacciones entre un equipo de respuesta a incidentes y los integrantes del equipo de respuesta de la comunidad requieren:

- Que la comunidad entienda las políticas y los procedimientos del equipo de respuesta

- Que muchos equipos de respuesta colaboran para manejar incidentes, la comunidad también debe entender la relación entre su equipo de respuesta y otros equipos.

- Y por último, muchas interacciones se aprovecharán de las infraestructuras públicas existentes, de modo que la comunidad necesita saber cómo las comunicaciones serán protegidas.

1.3.1 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.

¿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 de su equipo.

1.3.2 Relaciones entre diferentes CSIRT y Entidades

En algunos casos, un CSIRT puede ser capaz de operar eficazmente por sí mismo y en estrecha colaboración con sus integrantes. Pero con las redes internacionales de hoy en día es mucho más probable que la mayoría de los incidentes a cargo de un CSIRT participarán partes externas a él. Por lo tanto, el equipo tendrá que interactuar con otros CSIRTs y sitios fuera de su comunidad.

La comunidad debe comprender la naturaleza y el alcance de esta colaboración, como información muy sensible acerca de los componentes individuales pueden ser divulgados en el proceso. La colaboración entre los CSIRTs podría incluir las interacciones al preguntarle a los otros equipos de asesoramiento, la difusión de conocimiento de los problemas y trabajar en cooperación para resolver un incidente de seguridad que afectan a uno o más comunidades de los CSIRTs.

Tenga en cuenta que hay una diferencia entre un acuerdo de interconexión, donde los CSIRTs implicados estén de acuerdo para trabajar juntos y compartir la información y la cooperación simple, donde 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. Sin embargo, el mismo conjunto de intercambio de información que se utiliza para fijar las expectativas de una comunidad de usuarios ayudará a las demás partes para comprender los objetivos y los servicios de un CSIRT específico para ser un punto de apoyo ante un eventual incidente.

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 CSIRTs. 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 de CSIRTs nacionales en otros países para hacer frente a todos los sitios implicados en un ataque a gran escala. La colaboración entre CSIRTs 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).

- 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, CSIRTs, 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 de prensa.

(Msc. Ing. Eduardo Carozo Blusmztein, CIS, 2010)

1.4 PERSONAL QUE INTEGRA UN CSIRT

A continuación se listan una serie de características que son valiosas de tomar en cuenta para el proceso de reclutamiento de personal para la formación de un CSIRT, siendo las siguientes:

- Diversidad de conocimientos tecnológicos.
- Personalidad: habilidad de comunicación y relación personal.
- Personas dedicadas, innovadoras, detallistas, flexibles y metódicas.
- Experiencia en el área de seguridad de la información.
- Se maneje coherentemente con los valores personales y de la organización.

Pueden asumir las funciones de: gerente, líder del equipo y/o supervisores. Para puestos tales como:

Encargados de tratamiento de incidentes: personal técnico que está capacitado para el tratamiento de un incidente informático.

Encargados de tratamiento de vulnerabilidades: personal técnico que está especializado en el tratamiento de deficiencias o fallos en la programación o configuración de un sistema informático.

Personal de análisis y seguimiento de casos: son los responsables de llevar los registros y brindar el seguimiento adecuado de los casos y su análisis respectivo.

Especialistas en plataformas operacionales: técnicos experimentados y especializados en el manejo de plataformas informáticas que tienen dominio del equipo y sus respectivos sistemas informáticos.

Instructores: son los encargados de brindar enseñanza en los diferentes temas dónde tengan su respectiva especialización.

Técnicos de Soporte: personal especializado en el manejo de hardware y/o software para la realización de tareas específicas.

Otras funciones:

- Personal de Apoyo.
- Redactores Técnicos.
- Administración de Redes y/o Sistemas.
- Desarrolladores Web.
- Asesoría de Prensa o Contactos Medios.
- Abogados en oficinas que lo respaldan.

1.5 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 políticas de seguridad para un CSIRT a implementar es imprescindible para que sus lineamientos y directrices ante la comunidad que soportara dicho CSIRT.

1.5.1 Definición y Propósito

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 por qué 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 y limitaciones de los recursos y servicios informáticos. Esta es la tabla del contenido que debe tener una política de seguridad de la información:

[3]Cuadro No. 1 – Contenido 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.

A continuación se brinda un listado de las políticas recomendadas que tiene que tener como mínimo una organización:

[4]Cuadro No. 2 – Políticas Recomendadas

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 elementos claves en la seguridad: disponibilidad, utilidad, integridad, autenticidad, confidencialidad y posesión.	• Alcances. (facilidades, sistemas y personas.) • Objetivos. • Descripción de los elementos involucrados. • Responsabilidades. • 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.

[3] Cuadro No. 1 - SANs Institute – www.sans.org/policies

[4] Cuadro No. 2 - SANs Institute – www.sans.org/policies

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).

[5]Cont. **Cuadro No. 2 – Políticas Recomendadas**

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.

[5] Cont. Cuadro No. 2 - SANs Institute – www.sans.org/policies

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.

1.6 GESTIÓN DE INCIDENTES

1.6.1 Definición y Propósito

La Gestión de Incidentes tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible.

La Gestión de Incidentes no debe confundirse con la Gestión de Problemas, pues a diferencia de esta última, no se preocupa de encontrar y analizar las causas subyacentes a un determinado incidente sino exclusivamente a restaurar el servicio. Sin embargo, es obvio, que existe una fuerte interrelación entre ambas.

Los objetivos principales de la Gestión de Incidentes son:

- Detectar cualquiera alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio según se define en el SLA correspondiente.

El siguiente diagrama resume el proceso de gestión de incidentes:

[6]Grafica No. 1 – Gestión de Incidentes

Fuente: Proyecto AMPARO – CSIRT

Aunque el concepto de incidencia se asocia naturalmente con cualquier malfuncionamiento de los sistemas de hardware y software según el libro de Soporte del Servicio de ITIL un incidente es:

"***Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo***".

[6] Grafica No. 1 – Proyecto AMPARO - CSIRT

Por lo que casi cualquier llamada al Centro de Servicios puede clasificarse como un incidente, lo que incluye a las Peticiones de Servicio tales como concesión de nuevas licencias, cambio de información de acceso, etc. siempre que estos servicios se consideren estándar.

Cualquier cambio que requiera una modificación de la infraestructura no se considera un servicio estándar y requiere el inicio de una Petición de Cambio que debe ser tratada según los principios de la Gestión de Cambios.

Los principales beneficios de una correcta Gestión de Incidentes incluyen:

- Mejorar la productividad de los usuarios.
- Cumplimiento de los niveles de servicio.
- Mayor control de los procesos y monitorización del servicio.
- Optimización de los recursos disponibles.
- Una base de datos de gestión de configuraciones más precisa pues se registran los incidentes en relación con los elementos de configuración.
- Y principalmente: mejora la satisfacción general de clientes y usuarios.

1.6.2 Nivel de Prioridad y Escalonamiento

Nivel de Prioridad

Es frecuente que existan múltiples incidencias concurrentes por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas.

El nivel de prioridad se basa esencialmente en dos parámetros:

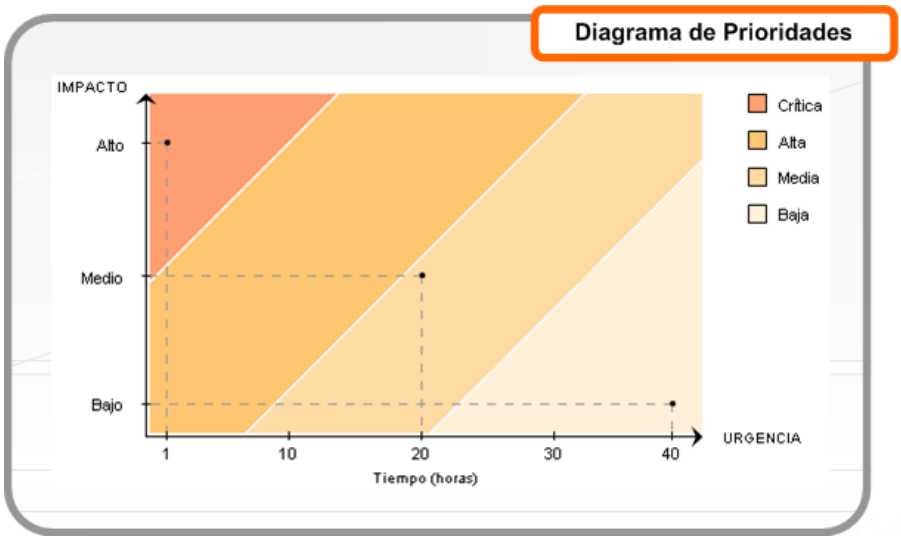
- **Impacto:** determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.

- **Urgencia:** depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente y/o el nivel de servicio.

Dependiendo de la prioridad se asignarán los recursos necesarios para la resolución del incidente. La prioridad del incidente puede cambiar durante su ciclo de vida.

Por ejemplo, *se pueden encontrar soluciones temporales que restauren aceptablemente los niveles de servicio y que permitan retrasar el cierre del incidente sin graves repercusiones. Es conveniente establecer un protocolo para determinar, en primera instancia, la prioridad del incidente.* El siguiente diagrama nos muestra un posible "diagrama de prioridades" en función de la urgencia e impacto del incidente:

[7]Grafica No. 2- Diagrama de Prioridades



Fuente: Proyecto AMPARO - CSIRT

[7] Grafica No. 2 – Proyecto AMPARO - CSIRT

Escalonamiento

Es frecuente que el Centro de Servicios no se vea capaz de resolver en primera instancia un incidente y para ello deba recurrir a un especialista o a algún superior que pueda tomar decisiones que se escapan de su responsabilidad. A este proceso se le denomina escalado.

Básicamente hay dos tipos diferentes de escalado:

- **Escalado funcional:** Se requiere el apoyo de un especialista de más alto nivel para resolver el problema.

- **Escalado jerárquico:** Debemos acudir a un responsable de mayor autoridad para tomar decisiones que se escapen de las atribuciones asignadas a ese nivel, como, por ejemplo, asignar más recursos para la resolución de un incidente específico.

El proceso de escalado puede resumirse gráficamente como sigue:

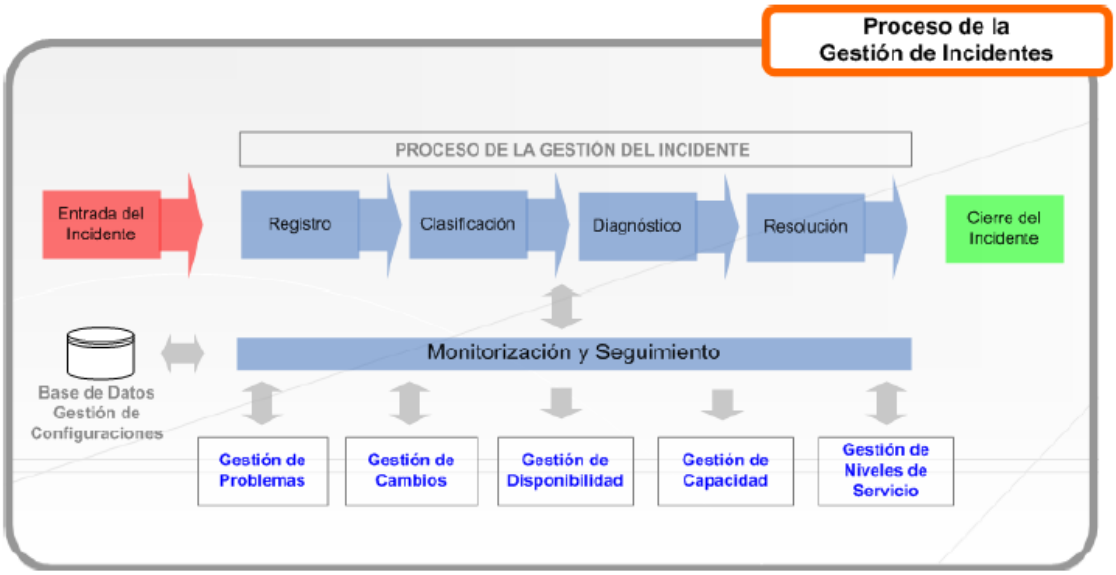
[8]Grafica No. 3 – Proceso de Escalonamiento

Fuente: Proyecto AMPARO – Incident Response

[8] Grafica No. 3 – Proyecto AMPARO – Incident Response

1.6.3 Proceso y Flujo

El siguiente diagrama muestra los procesos implicados en la correcta Gestión de Incidentes.



[9]Grafica No. 4 - Proceso de la Gestión de Incidentes

Fuente: Proyecto AMPARO – Gestión de Incidentes

- **Gestión de Configuraciones:** la base de datos de Gestión de Configuraciones juego un papel clave en la resolución de incidentes pues, por ejemplo, nos muestra información sobre los responsables de los componentes de configuración implicados. La base de datos de Gestión de Configuraciones también nos permite conocer todas las implicaciones que pueden tener en otros servicios el malfuncionamiento de un determinado elemento de configuración.

- **Gestión de Problemas:** ofrece ayuda a la Gestión de Incidentes informando sobre errores conocidos y posibles soluciones temporales. Por otro lado, establece controles sobre la calidad de la información registrada por la Gestión de Incidentes para que ésta sea de utilidad en la detección de problemas y su posible solución.

[9] Grafica No. 4 - Proyecto AMPARO – Gestión de Incidentes

- **Gestión de Cambios:** la resolución de un incidente puede general una petición de cambio que se envía a la Gestión de Cambios. Por otro lado, un determinado cambio erróneamente implementado puede ser el origen de múltiples incidencias y la Gestión de Cambios debe mantener cumplidamente informada a la Gestión de Incidencias sobre posibles incidencias que los cambios realizados puedan causar en el servicio.

- **Gestión de Disponibilidad:** utilizará la información registrada sobre la duración, el impacto y el desarrollo temporal de los incidentes para elaborar informes sobre la disponibilidad real del sistema.

- **Gestión de la Capacidad**: se ocupará de incidentes causados por una insuficiente infraestructura IT. (Insuficiencia del ancho de banda, capacidad de procesamiento, etc.).

- **Gestión de Niveles de Servicio:** La Gestión de Incidentes debe tener acceso a los niveles de servicio acordados con el cliente para poder determinar el curso de las acciones a adoptar. Por otro lado, la Gestión de Incidentes debe proporcionar periódicamente informes sobre el cumplimiento de los niveles de servicio contratados.

1.6.4 Clasificación

La clasificación de un incidente tiene como objetivo principal el recopilar toda la información que pueda ser de utilizada para la resolución del mismo.

Categorización: se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente o del grupo de trabajo responsable de su resolución. Se identifican los servicios afectados por el incidente.

Establecimiento del nivel de prioridad: dependiendo del impacto y la urgencia se determina, según criterios preestablecidos, un nivel de prioridad.

Asignación de recursos: si el Centro de Servicios no puede resolver el incidente en primera instancia designará al personal de soporte técnico responsable de su resolución (segundo nivel).

Monitorización del estado y tiempo de respuesta esperado: se asocia un estado al incidente (por ejemplo: registrado, activo, suspendido, resuelto, cerrado) y se estima el tiempo de resolución del incidente en base al nivel de servicio correspondiente y la prioridad.

1.6.5 Soporte a Incidentes

Todo CSIRT debe poseer un soporte de incidentes a través de pasos y flujo ya organizado.

A continuación se brinda una tabla que contiene los pasos recomendados para el soporte de incidentes:

[10]Cuadro No. 3 – Pasos de Soporte de Incidentes

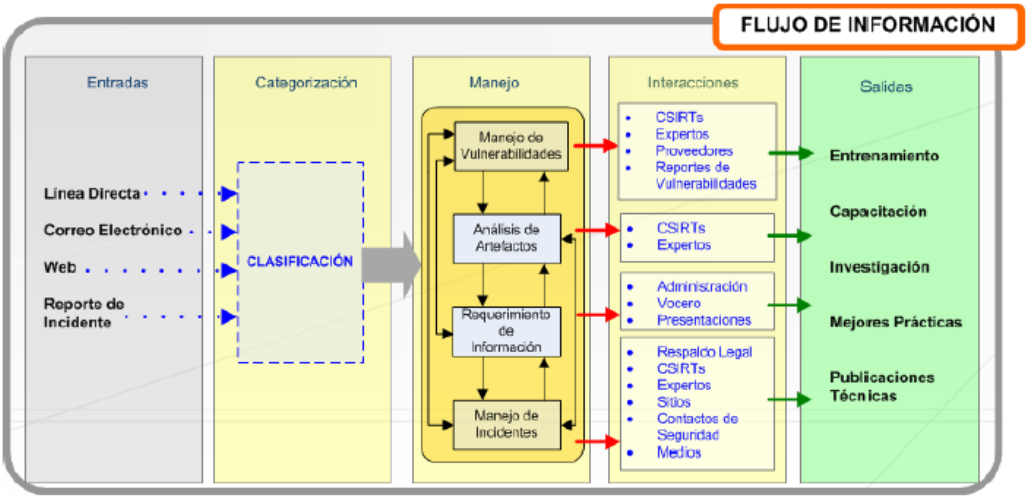
PASOS RECOMENDADOS PARA EL SOPORTE DE INCIDENTES		
No. PASO	**NOMBRE**	**DESCRIPCIÓN**
1	Reporte de un incidente a ser atendido	Las personas autorizadas por parte de las Unidades de Negocio reportan situaciones o funcionamientos anormales en la infraestructura IT (equipos, redes, servidores, servicios, etc.) Los incidentes son reportados por diferentes medios: Email, personalmente, por Web utilizando el Portal de Autoservicio y por Teléfono.
2	Registro y documentación del incidente reportado	El agente de soporte o usuario identifica el tipo de incidente (alertas, errores, caídas del sistema, actualizaciones, etc.) que se reporta y la prioridad (alta, media, baja) que se debe asignar. Registra la persona que reporta el incidente y el elemento involucrado en el incidente, obtiene instantáneamente una visión de toda la información de la persona, ¿quién es?, ¿cómo debe ser atendida?, incidentes pendientes, etc. Realiza un diagnostico inicial de lo que sucede.
3	Preparación de la solución del incidente	Cuando el agente de soporte o usuario registra la información básica del incidente, se asigna el tiempo máximo de solución que depende de los acuerdos de nivel de servicio pactados. Se despliegan soluciones sugeridas tomadas de la historia de incidentes similares y de la Ba-

[10] Cuadro No. 3 – Pasos de Soporte de Incidentes

		se de Conocimiento. Se sugieren tareas para planear la solución del servicio con tareas internas. Y se despliegan plantillas con ayudas para diagnosticar el problema y para comunicarse con el Cliente: plantillas para envío de email y para llamadas entrantes y salientes.
4	Proceso de solución utilizando herramientas de software como apoyo.	Se envían alertas por email para listas de notificación previamente creadas. Se remite el incidente a otros usuarios (responsables de la solución) si es necesario. Se realizan tareas internas para completar actividades necesarias en la solución. Se le comunica a la unidad de negocio por diferentes medios los avances realizados en la solución del incidente. Todo el proceso se realiza teniendo en cuenta el tiempo máximo de solución asignado al incidente, para lo cual se envían alertas por email a los responsables.
5	Identificación y solución de problemas	Como parte del proceso de solución se analiza toda la información de incidentes similares sobre los mismos elementos de la infraestructura IT, los diagnósticos realizados y las tareas o actividades internas realizadas para dar una solución. Si se identifican situaciones recurrentes, se registra la causa común como un problema, que al ser solucionada, soluciona todos los incidentes que tienen esa causa en común. De esa manera se evita que se presenten incidentes similares y se mejora el nivel de satisfacción de las unidades de negocio con el soporte técnico que se presta.
6	Cierre exitoso del incidente	Se comunica a la unidad de negocio el cierre del incidente reportado cumpliendo las políticas de servicio prometidas y respetando los tiempos máximos de solución pactadas según el tipo de incidente que se reportó y la prioridad asignada. Se documenta detalladamente el cierre del servicio para que enriquezca la Base de Conocimiento de la organización y pueda ser utilizada como una solución sugerida para un próximo servicio.

Y finalmente un esquema de cómo fluiría la información podría ser de la siguiente manera.

[11]Grafica No. 5 – Flujo de Información



[11] Grafica No. 5 – Proyecto AMPARO – Information Process

CAPITULO II

MODELOS ORGANIZACIONALES Y ESTRUCTURAS DE REFERENCIAS ACTUALES – CSIRT

Las naciones y países desarrollados han hecho esfuerzos considerables en contra de los crímenes cibernéticos y delitos informáticos. La información, el recurso más valioso de nuestra era, es considerado de valor incalculable para los países desarrollados, por lo que, dicha información es protegida y custodiada por organismos de seguridad estatales, ejemplo: NSA, FBI, Interpol, etc.

Ese combate a los crímenes cibernéticos y delitos informáticos se ha reflejado en los países en vía de desarrollo o subdesarrollados, tomando medidas semejantes. Ejemplo de ello, son los avances en Latinoamérica en la implementación de Agencias, Departamentos, CSIRT u otros. En este capítulo vamos detallar los modelos organizacionales y estructuras de referencias existentes de CSIRTs en Latinoamérica, así como, las agencias y departamentos existentes en Republica Dominicana.

2.1 MODELOS ORGANIZACIONES DE LOS CENTROS DE RESPUESTAS A INCIDENTES DE SEGURIDAD INFORMÁTICA – CSIRT NACIONAL

En la creación e implementación de un CSIRT, hay que estudiar y seleccionar el modelo organizacional de CSIRT a desarrollar.

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, no obstante, dependiendo de

la experiencia y madurez del equipo, estos se podrán ir incrementando según sea la estrategia adoptada.

A continuación detallamos los diferentes tipos de modelos organizaciones de CSIRTs que pueden implementarse, según las necesidades de lugar:

[12]Cuadro No. 4 - de Modelos Organizaciones CSIRT

Modelo	Descripción	Servicios
Equipo de Seguridad	Es la organización que se da de hecho cuando no existe un CSIRT constituido. No hay una asignación formal de responsabilidades respecto a los incidentes de seguridad. El personal existente, usualmente de TI, maneja los eventos de seguridad como parte de su actividad habitual.	**Básicos:** • Análisis de Incidentes. • Respuesta al incidente en el lugar. • Coordinación de respuesta a incidentes. • Respuesta a Vulnerabilidades. • Respuesta a Artefactos. • Configuración y mantenimiento de herramientas. • Servicios de detección de intrusiones. **Adicionales:** • Alertas y Advertencias. • Análisis de Vulnerabilidades.

[12] Cuadro No. 4 – Guide CSIRT - Models

		• Coordinación de respuesta a vulnerabilidades. • Análisis de Artefactos. • Coordinación de la respuesta a Artefactos.
Modelo Distribuido	Es una estructura central pequeña (al menos un gerente de seguridad) supervisa y coordina al personal del equipo distribuido en la organización. El personal del equipo distribuido es personal previamente existente en la organización. Se le asignan explícitamente responsabilidades relativas a seguridad, a las que se dedica parcial o totalmente. Este modelo se adecúa bien a organizaciones grandes en las que un equipo centralizado puede ser insuficiente.	**Básicos:** • Alertas y Advertencias. • Análisis de Incidentes. • Soporte telefónico / correo electrónico. • Coordinación de respuesta a incidentes. • Coordinación de respuesta a vulnerabilidades. • Anuncios. **Adicionales:** • Respuesta al incidente en el lugar. • Análisis de Vulnerabilidades. • Respuesta a Vulnerabilidades. • Análisis de Artefactos. • Respuesta a Artefactos. • Coordinación de la respuesta a Artefactos. • Observatorio tecnológico. • Auditorías o evaluaciones de seguridad.

Cont. **Modelo Distribuido**		• Configuración y mantenimiento de herramientas. • Desarrollo de herramientas. • Servicios de detección de intrusiones. • Difusión de información relacionada con seguridad. • Análisis de Riesgo. • Planificación de la continuidad del negocio y recuperación de desastres. • Consultoría de seguridad. • Concientización. • Educación / Capacitación. • Evaluación y/o certificación de productos.
Modelo Centralizado	Consta de un equipo centralizado de personal a tiempo completo que toma la responsabilidad sobre la seguridad en toda la organización.	**Básicos:** • Alertas y Advertencias. • Análisis de Incidentes. • Soporte telefónico / correo electrónico. • Coordinación de respuesta a incidentes. • Coordinación de respuesta a vulnerabilidades. • Coordinación de la respuesta a Artefactos. • Anuncios.

Cont. **Modelo Centralizado**		• Observatorio tecnológico. • Difusión de información relacionada con seguridad. **Adicionales:** • Respuesta al incidente en el lugar. • Análisis de Vulnerabilidades. • Análisis de Artefactos. • Auditorías o evaluaciones de seguridad. • Configuración y mantenimiento de herramientas. • Desarrollo de herramientas. • Servicios de detección de intrusiones. • Análisis de Riesgo. • Planificación de la continuidad del negocio y recuperación de desastres. • Consultoría de seguridad. • Concientización. • Educación / Capacitación. • Evaluación y/o certificación de productos.

Modelo Coordinador	Es un equipo centralizado que coordina y facilita el manejo de incidentes de seguridad. Por lo general atiende a una comunidad objetivo formada por organizaciones externas múltiples y diversas.	**Básicos:** • Alertas y Advertencias. • Análisis de Incidentes. • Soporte telefónico / correo electrónico. • Coordinación de respuesta a incidentes. • Coordinación de respuesta a vulnerabilidades. • Coordinación de la respuesta a Artefactos. • Anuncios • Observatorio tecnológico. • Difusión de información relacionada con seguridad. • Concientización. • Educación / Capacitación. **Adicionales:** • Análisis de Vulnerabilidades. • Respuesta a Vulnerabilidades. • Respuesta a Artefactos. • Desarrollo de herramientas. • Análisis de Riesgo. • Planificación de la continuidad del negocio y recuperación de desastres. • Evaluación y/o certificación de productos.

Según hemos visto y analizado los diferentes modelos organizacionales de CSIRTs existentes, un CSIRT Nacional debe adoptar el **Modelo Coordinador**, el cual centraliza en un solo punto las respuestas a los incidentes de seguridad y se relaciona con demás entidades externas, como:

- CSIRTs Internacionales.
- Agencias de Seguridad Internacionales (FBI, CIA, NSA, Interpol, etc.).
- Entidades Gubernamentales Locales.
- Organismos de Seguridad Ciudadana Locales (Policía Nacional, DNCD, DNI, etc.).

Esta relación va desde intercambios de información valiosa, hasta apoyo mutuo relacionado a la solución en equipo de un incidente de seguridad.

2.2 SELECCIÓN DEL MODELO DE CENTRO DE RESPUESTAS CSIRT

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 y/o entidades relacionadas.

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. En el caso de un CSIRT Nacional, se debe proporcionar un servicio 24x7, por razones de seguridad nacional a los ciudadanos y disponibilidad de los servicios críticos (luz, agua, medicina, etc.) en caso de ser atacados o afectados.

El servicio 24x7 de 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 o naciones 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 y aceleradas a dar respuestas de forma inmediata u oportuna. 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 de centro de respuestas a incidentes, 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:

2.2.1 Costos

El personal del centro 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 como: redes, seguridad, infraestructura, telefónica, electrónica y demás; adicional a esto, el personal de respuesta a incidentes también debe conocer y operar las herramientas propias de la actividades de investigación, recolección de evidencias y forense sobre los incidentes.

Otros costos importantes a tener en cuenta son los que se refieren a la seguridad física del área de trabajo del centro de respuesta, los medios y dispositivos de comunicación, entre ellos: celulares, laptops, equipos para hacer pruebas, laboratorios y equipamiento forense.

2.2.2 Experiencia en el 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.

Al respecto, es posible que personal externo (Outsourcing) especializado en respuesta a incidentes cuente con mayor experiencia que el personal interno de un CSIRT, en áreas como: 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 los falsos positivos.

2.2.4 División de la Responsabilidades

Es frecuente y normal que en la implementación de un CSRIT de cualquier tipo: Nacional, Educativo, Organizaciones, etc.; existan entidades externas que manejan servicios de monitoreo, operaciones y asesoría que se relacione con los incidentes de seguridad.

En el caso de contratar 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.

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.

2.2.5 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.

Con ellos se puede definir la forma precisa en que deben emitirse comunicados de acuerdo a las políticas de comunicación establecidas en el CSIRT. No hacerlo de este modo, podría ocasionar que se divulgara información innecesaria que eventualmente podría confundir al público o a la entidad o persona afecta por el incidente.

2.3 ESTRUCTURAS DE REFERENCIA – CSIRTs GLOBALES

A nivel internacional, tanto en países desarrollados como en países en vía de desarrollo, existen centros de respuestas a incidentes de seguridad o en su defecto Centro de Respuestas a Emergencias de Informática, lo cual es lo mismo. Estos CSIRT no solo están orientados a nivel Nacional, también existen CSIRTs a nivel educativo, organizaciones y de empresas ya establecidas que representan alguna marca o producto, como: **Apple, Adobe, Microsoft, IBM, Intel**, en otros.

[13]A nivel global existe una entidad que registra y relaciona casi la mayoría de los CSIRT o CERT, es la asociación global de los CSIRTs: **Forum de Equipos de Seguridad y Respuesta de Incidentes (Forum of Incident Response and Security Teams, FIRST)**.

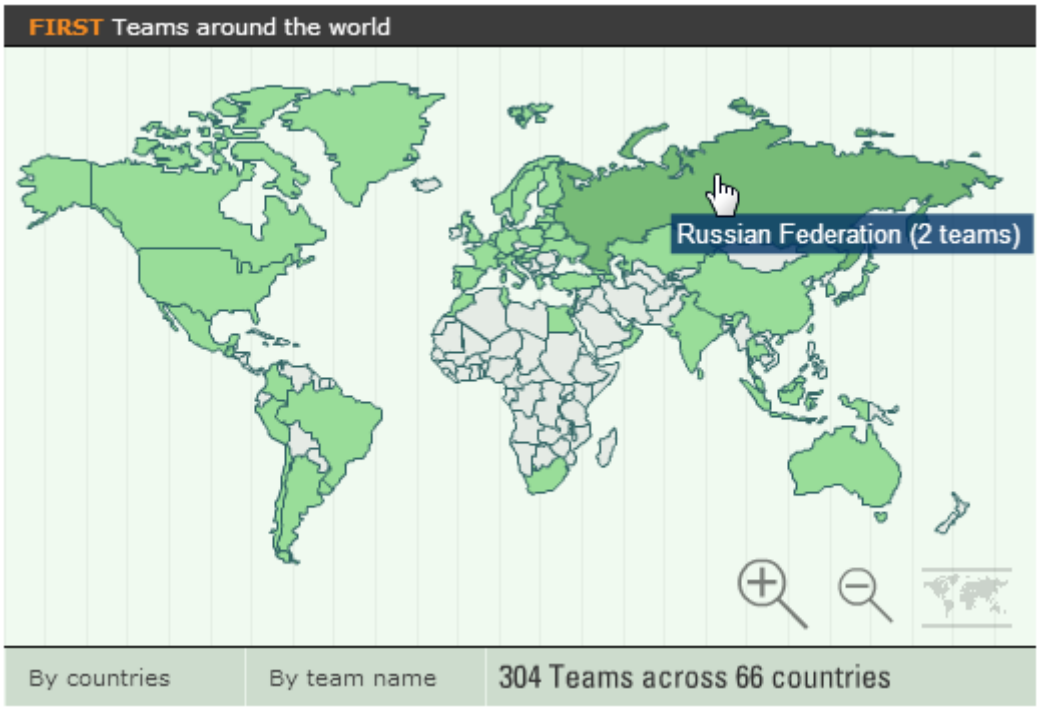
[13] FIRST – Forum of Incident Response and Security Teams - Documents

El **FIRST** engloba CIRSTs diversos:

[14]Grafica No. 6 – Listado de algunos CSIRTs Globales

Team name	Official Team name	Country
AAB GCIRT	ABN AMRO Global CIRT	NL
AboveSecCERT	Above Security Computer Emergency Response Team	CA
ACOnet-CERT	ACOnet-CERT	AT
Adobe PSIRT	Adobe Product Security Incident Response Team	US
ADP CIRC	ADP CIRC	US
ADPCERT	Abu Dhabi Police CERT	AE
aeCERT	The United Arab Emirates - Computer Emergency Response Team	AE
Amazon SIRT	Amazon Security Incident Response Team	US
Apple	Apple Computer	US
ASEC	AhnLab Security E-response Center	KR
ASTAR CERT	A*STAR CERT TEAM	SG
AT&T	AT&T	US
AusCERT	Australian Computer Emergency Response Team	AU
B-CIRT	Boeing - Computing Incident Response Team	US
BAC-SIRT	Bank of America Computer Incident Response Team	US
BASF gCERT	Global BASF CERT	DE
Bell IPCR	Bell Canada Information Protection Centre (IPC) Response	CA
BELNET CERT	BELNET CERT	BE
BF-SIRT	Basefarm SIRT	NO
BFK	BFK edv consulting	DE
BIRT	BrandProtect IRT	CA

[15]Grafica No. 7 – Mapa Geográfico de Países con CSIRTs (en verde)



Fuente de Graficas: FIRTS

[14] Grafica No. 6 - Listado de algunos CSIRTs Globales

[15] Grafica No. 7 - Mapa Geográfico de Países con CSIRTs (en verde)

2.4 ESTRUCTURAS LOCALES – REPUBLICA DOMINICANA

La Republica Dominicana actualmente cuenta con el **Departamento de Investigación de Crímenes y Delitos de Alta Tecnología – DICAT**, encargado de dar recibir, analizar y dar respuestas a los incidentes tecnológicos del país, el mismo está bajo la dirección y mando de la **Policía Nacional**, a continuación su creación, evolución y funciones:

[16]HISTORIA

• JULIO 2003

• Soporte del DSTI a la Dirección de Investigaciones Criminales.

• JULIO 2003

• Creación DIDI Departamento Nacional de Investigaciones.

• NOVIEMBRE 2005

• Creación del DICAT Departamento de Investigación de Crímenes de Alta Tecnología.

CREACION Y MOTIVACION

- Incremento (Delitos Electrónicos).
- Nuevas Formas y Métodos.
- Integración a los esquemas internacionales.

MISION

Impulsar, coordinar y realizar investigaciones relacionadas con la criminalidad de las nuevas tecnologías y las comunicaciones.

[16] Documentación - Departamento de Investigación de Crímenes de Alta Tecnología - DICAT

FUNCIONES

- Investigar todas las denuncias de crímenes o delitos considerados de alta tecnología.
- Responder con capacidad investigativa a todas las amenazas y ataques a la infraestructura critica nacional.
- Desarrollar análisis estratégicos de amenazas informáticas.
- Desarrollar inteligencia en internet.
- Dar soporte a la dirección de investigaciones criminales en la investigación de crímenes y delitos tradicionales en los que hayan componentes tecnológicos.

El **DICAT** hoy en día está activo y es uno de los departamentos más solicitados por la ciudadanía por su eficiencia en la respuesta y solución de incidentes y crímenes tecnológicos, a continuación varias estadísticas de incidentes registrados:

[17]**Cuadro Estadístico No. 1:** Total de casos relacionados con Redes Sociales

DELITOS	DIFAMACION				ROBO DE IDENTIDAD				ACOSO				HACKING				TOTAL GENERAL
	facebook	HI5	Twitter	TOTAL	facebook	HI5	Twitter	TOTAL	facebook	HI5	Twitter	TOTAL	facebook	HI5	Twitter	TOTAL	
2007	0	6	0	6	0	0	0	0	0	0	0	0	0	0	0	0	6
2008	2	35	0	37	0	5	0	5	0	0	0	0	3	0	0	3	45
2009	17	20	1	38	1	4	0	5	0	0	0	0	2	1	0	3	46
2010	79	7	1	87	3	0	0	3	2	0	0	2	4	0	0	4	96
2011	69	0	5	74	1	0	0	1	0	0	0	0	7	0	0	7	82
2012	47	0	2	49	3	0	0	3	0	0	0	0	11	0	0	11	63
TOTAL	214	68	9	291	8	9	0	17	2	0	0	2	27	1	0	28	338

Fuente: Sección DICRIM

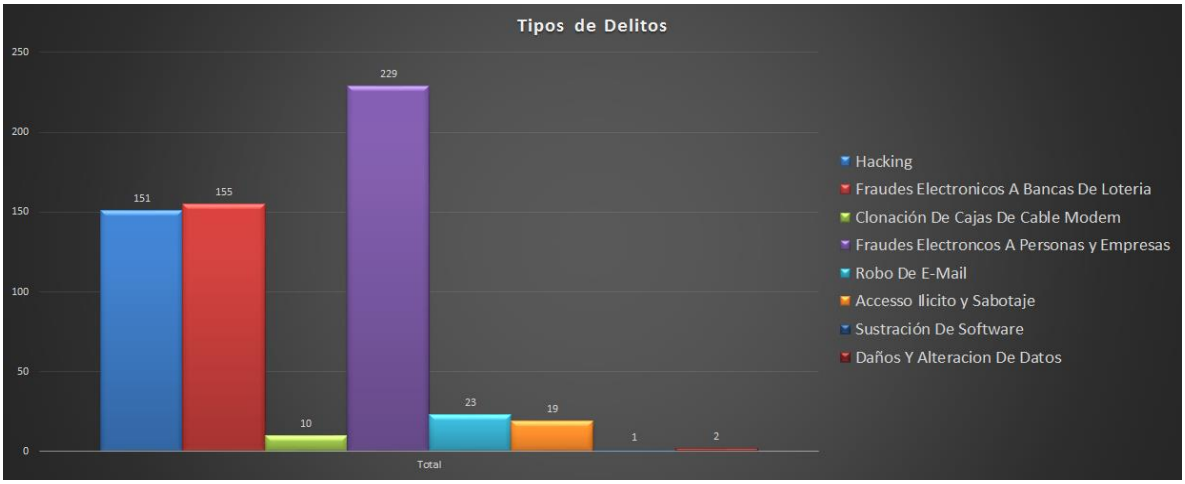
[17] Estadística Lineal No. 1 - Departamento DICAT, Policía Nacional Dominicana – Sección DICRIM

[18]**Cuadro Estadístico No. 2:** Casos resueltos de Phishing en el país del 2007-2013

ENTIDADES BANCARIAS	CASOS RESUELTOS	MONTOS EN PESOS	MONTOS EN DOLARES	MONTOS EN EUROS
ENTIDAD BANCARIA 01	139	8,780,704.00	/	/
ENTIDAD BANCARIA 02	66	22,552,944.00	12,000.00	/
ENTIDAD BANCARIA 03	168	14,843,745.00	74,429.89	1,000.00
ENTIDAD BANCARIA 04	7	2,697,192.00	/	/
ENTIDAD BANCARIA 05	11	1,129,242.00	24,784.19	/
ENTIDAD BANCARIA 06	1	1,666,000.00	/	/
ENTIDAD BANCARIA 07	1	/	/	378.00
ENTIDAD BANCARIA 08	8	120,649.14	/	/
ENTIDAD BANCARIA 09	1	/	/	5,777.00
ENTIDAD BANCARIA 10	28	1,805,725.00	1,654,185.00	/
ENTIDAD BANCARIA 11	2	/	/	35,952.00
TOTAL MONTOS	432	53,596,201.14	1,765,399	43,107.00

Fuente: Sección Inteligencia

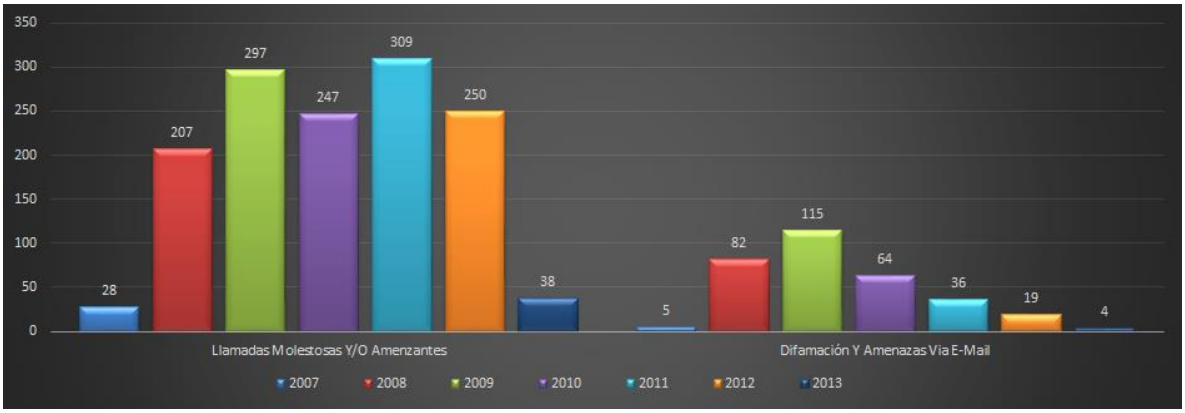
[19]**Estadística Grafica No. 1:** Casos resueltos de lo diferentes tipos de crímenes hacking 2007-2013



Fuente: Sección Inteligencia, DICAT

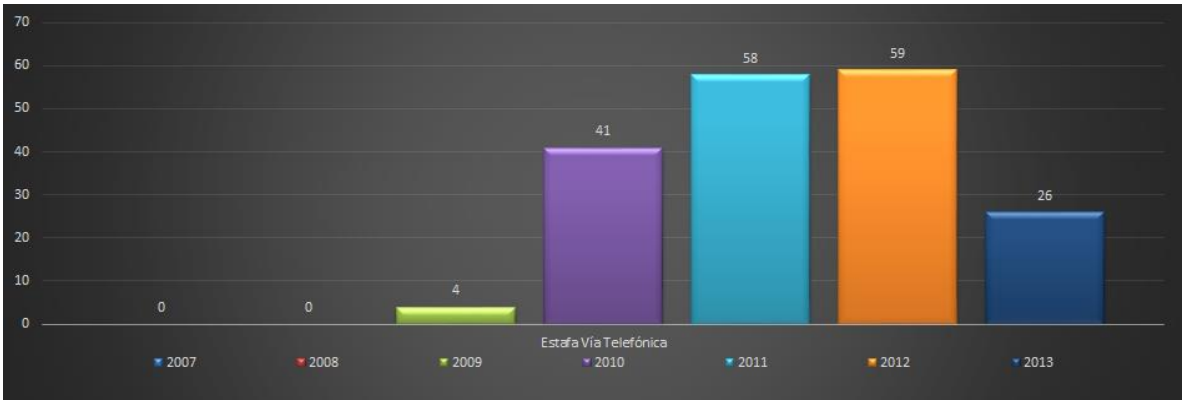
[18] Estadística Lineal No. 2 - Departamento DICAT, Policía Nacional Dominicana – Sección Inteligencia
[19] Estadística Grafica No. 1 - Departamento DICAT, Policía Nacional Dominicana - Sección Inteligencia

[20]**Estadística Grafica No. 2:** Llamadas y Correos electrónicos amenazantes y molestosos



Fuente: Sección Inteligencia, DICAT

[21]**Estadística Grafica No. 3:** Estafas vía telefónica y/o Llamadas inteligentes



Fuente: Sección Investigación, DICAT

Limitaciones del DICAT

El DICAT a diferencia de un CSIRT Nacional posee las siguientes limitaciones y desventajas:

- No tiene relaciones con entidades y agencias internaciones de seguridad informática (FBI, NSA, CIA, Interpol, etc.).
- No comparte conocimiento e información de crímenes cibernéticos y tecnológicos con los demás CSRIT globales.
- No posee una estructura centralizada de crímenes tecnológicos.

[20] Estadística Grafica No. 2 - Departamento DICAT, Policía Nacional Dominicana - Sección Inteligencia
[21] Estadística Grafica No. 3 - Departamento DICAT, Policía Nacional Dominicana - Sección Investigación

- Es dependiente de otras instituciones, carencia de autoridad.

Estas limitaciones y otras hacen que la implementación de un CSIRT Nacional se lleve a cabo. La estructura actual del DICAT es un avance para que un CSIRT Nacional sea conformado.

2.5 SERVICIOS Y APLICACIONES QUE APOYAN LA IMPLEMENTACIÓN DE UN CSIRT NACIONAL

Sistemas de Seguimiento de Incidentes

En el idioma 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, la cual 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. Un ejemplo real de estos sistemas, es el empleado actualmente en el **Sistema Nacional de Emergencia 9-1-1 de la Republica Dominicana**, el cual consta un sistema centralizado de recepción de llamadas (incidentes) y son canalizados a un especialista. En el caso de un CSIRT Nacional, sería un sistema similar, el cual registrará y dará seguimiento al incidente reportado, por diferentes canales alternos (vía telefónica, email, físicamente, solicitud vía web, otros.).

Correo Electrónico Seguro

La implementación de un correo electrónico para la recepción de incidentes e intercambio de información confidencial sobre incidentes con otras entidades, agencias y CSIRT globales es de suma importancia. La implementación de certificados personales ayudara a una comunicación más segura, 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.

[22]Red Perimetral Segura

Todo CSIRT debe poseer una infraestructura (red, servidores y PCs) y un perímetro de red y comunicación seguras. Esto conlleva tener equipos de seguridad como Firewalls, IPS, IDS, otros.

Un CSIRT Nacional debe poseer un sistema o una red diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Los dispositivos de seguridad de red perimetral son configurados para *permitir, limitar, cifrar y descifrar* el tráfico entre los diferentes ámbitos sobre

[22] CSIRT Guide – Network Security

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.

Laboratorios de Pruebas (Honeypots)

Los laboratorios de pruebas en los CSRIT y agencias de seguridad son muy esenciales a la hora de capturar, analizar y estudiar casos de incidentes e investigaciones forenses. En los laboratorios de pruebas debe haber un equipo para realizar capturas y de esa manera poder analizar los incidentes y ataques de los atacantes o hackers. Es como dice un refrán: "*Debes conocer a tu enemigo como a ti mismo*". Esos equipos, red o software son llamados Honeypot y Honeynet (señuelos).

Los *Honeypot y Honeynet* son software o conjuntos 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.

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 una debilidad, ya sea en su implementación o en su uso.

Toda infraestructura tecnológica avanzada, como los CSIRT, necesitan 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, NNTP, NTP, TFTP, FTP, TELNET, SMTP, Servidores Web.

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 sofisticados, 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.

Una red tecnológica CSIRT debe poseer una solución de anti-virus empresarial, capaz de cubrir todas las conexiones internas y puntos externos donde la misma intercambia información hacia el Internet o con terceros.

Herramientas de Análisis Forense

La Informática Forense es una ciencia relativamente nueva y no existen estándares aceptados, aunque algunos proyectos están en desarrollo. En la actualidad existen varias herramientas que nos sirven para realizar análisis forenses informáticos 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.

En un CSIRT deben existir herramientas de análisis forense para la investigación, análisis y recolección de datos. Estas herramientas son esenciales para las investigaciones de recolección de evidencias y datos, donde se debe encontrar hipótesis y soluciones.

2.6 BENEFICIOS DE LA IMPLEMENTACIÓN DE UN CSIRT NACIONAL

Un Centro de Respuesta a Incidentes de Seguridad Informática tiene como beneficio principal la capacidad que le brindará a su comunidad en poderles 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 los beneficios que se obtiene al tener un CSIRT:

- Un punto de contacto focal y confiable dentro de la comunidad para el manejo de incidentes de seguridad informática.
- Promueve un desarrollo en la utilización de infraestructura tecnológica basado en las 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 eficaces 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.

2.7 ANÁLISIS FODA GENERAL DE UN CSIRT NACIONAL

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 nos apoye en el proceso de tomas de decisiones acordes con los objetivos y políticas de nuestro CSIRT.

[23]Cuadro No. 5 – Análisis FODA CSIRT

ANALISIS FODA GENERAL PARA UN CSIRT	
ELEMENTO	**DESCRIPCION**
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.

[23] Cuadro No. 5 – CSIRT Guide – CSIRT FODA

OPORTUNIDADES	• Desarrollo de relaciones comerciales de largo plazo con los clientes. • Búsquedas 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.

Cuadro No. 5 – CSIRT Guide – CSIRT FODA

CAPITULO III

PROPUESTA PARA LA IMPLEMENTACION DE UN CENTRO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMATICA NACIONAL – CSIRT- RD

En las últimas décadas la Republica Dominicana ha invertido gran parte de su presupuesto y PIB en la seguridad ciudadana, en equipamiento, proyectos de reestructuración de las entidades castrenses y en sistemas de respuestas a emergencias, ejemplo de esto es el reciente **Sistema Nacional de Emergencias e Incidentes 9-1-1**, el cual es un avance en materia de seguridad ciudadana.

La implementación de este Sistema 9-1-1 en la Republica Dominicana abre las puertas a nuevos proyectos de seguridad, que a nivel global son referenciados como buenos y validos por la veracidad y rapidez a la hora de incidentes y emergencias. Uno de esos sistemas globales es el Centro de Respuestas a Incidentes de Seguridad – CSIRT, este sistema esta implementado de forma global en una gran variedad de países de todos los continentes. En el caso de la Republica Dominicana, se tiene el interés y el apoyo de las autoridades para la implementación de un CSIRT-RD Nacional; actualmente existen las bases para iniciarlo, esas bases son las entidades de seguridad criminales existentes, como: DICAT, DIDI y el DNI, las cuales formaran o se integraran de forma efectiva en la implementación del CSIRT-RD Nacional.

3.1 BASES INICIALES PARA LA FORMACIÓN DE UN CSIRT NACIONAL

Las bases iniciales para la formación e implementación de un CSIRT Nacional conllevan la siguiente planeación de presupuestos:

- **PRESUPUESTO DE INVERSION**: Comprende todo el cuadro de adquisición de máquina y equipo 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:** Tienen 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 probables 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.

3.2 DESCRIPCIÓN DE LAS FUNCIONES DE UN CSIRT

La implementación de un CSIRT Nacional conlleva una descripción de funciones dentro del mismo, las cuales van a desempeñar una serie de responsabilidades.

- **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 capacitada y entrenada 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.

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.

- **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.

- **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.

- **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.

Infraestructura

En cualquier Centro de Respuesta encontraremos infraestructura que sirve como sustento para los servicios que se brindan. Habrá tanto infraestructura “de cada a la Comunidad Objetivo” como también “de uso exclusivo interno”, y en ambos casos nos referiremos 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.

Considerando la dinámica con la que se cuente para la adquisición del equipamiento necesario deberá proveer las necesidades a mediano y largo plazo de forma de trasladarlas en tiempo y forma al Director Ejecutivo, vía el Director Operacional en caso de existir. Una de sus tareas será identificar la disponibilidad requerida en cada sistema y por lo tanto, las alternativas para lograrla.

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 comprendidos 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.

Capacitación y Entrenamiento

La actividad de capacitación y entrenamiento es útil, por un lado para generar un expertis 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 resultaría 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.

- **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.

- **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.

3.3 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:

- **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.

- **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.

- **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.

- **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.

- **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.).

- **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.

- **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.

- **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.

- **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.

3.4 RECOMENDACIONES DE LA ARQUITECTURA DE REDES

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.

- **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.

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.

- **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.).

- **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.

Cuadro No. 6 - Detalle de Infraestructura

Equipo	Elemento
Equipos y medios de conectividad	• Routers. • Switches. • Hubs. • 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).
Servidores	• Firewall. • Detección de Intrusos. • Correo electrónico, WEB, NTP, DNS. • Registro de bitácoras de sistemas. • Archivos. • Intranet. • Acceso Remoto (RPV). • Backup. • De Pruebas.
Estaciones de Trabajo y	• Estaciones de trabajo.

Equipos Portátiles	• 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, nobreaks, 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.

- **Software**

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

- Que los sistemas operacionales de los servidores, estaciones de trabajo y equipos portátiles utilicen software libre, siempre que esto sea posible.

- Procesos de aseguramiento de sistemas.
- Sistemas operacionales.
- 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.

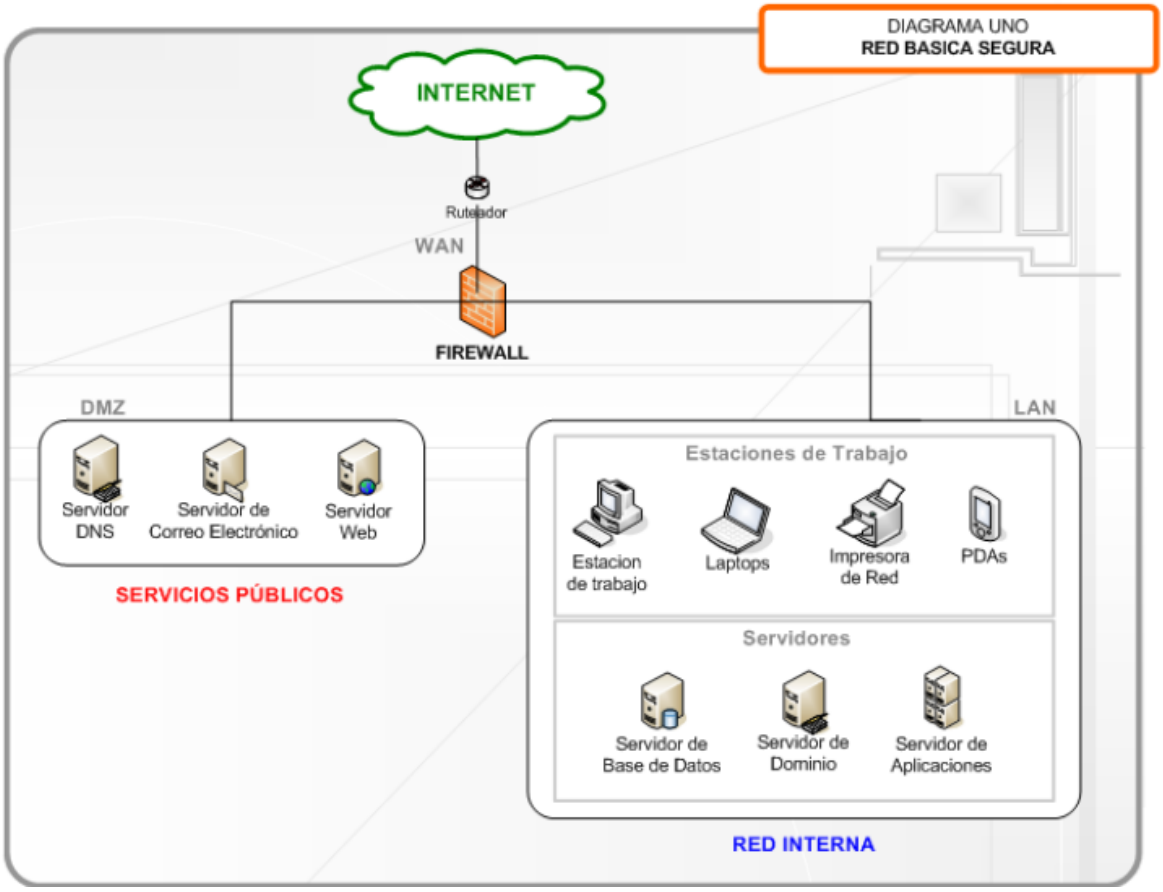
- **Infraestructura de Telecomunicaciones**

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.
- Telefonía Móvil para hacer viable la operación 7x24.

- **Diagramas Sugeridos**

[24]Esquema No. 1: Red Básica Segura



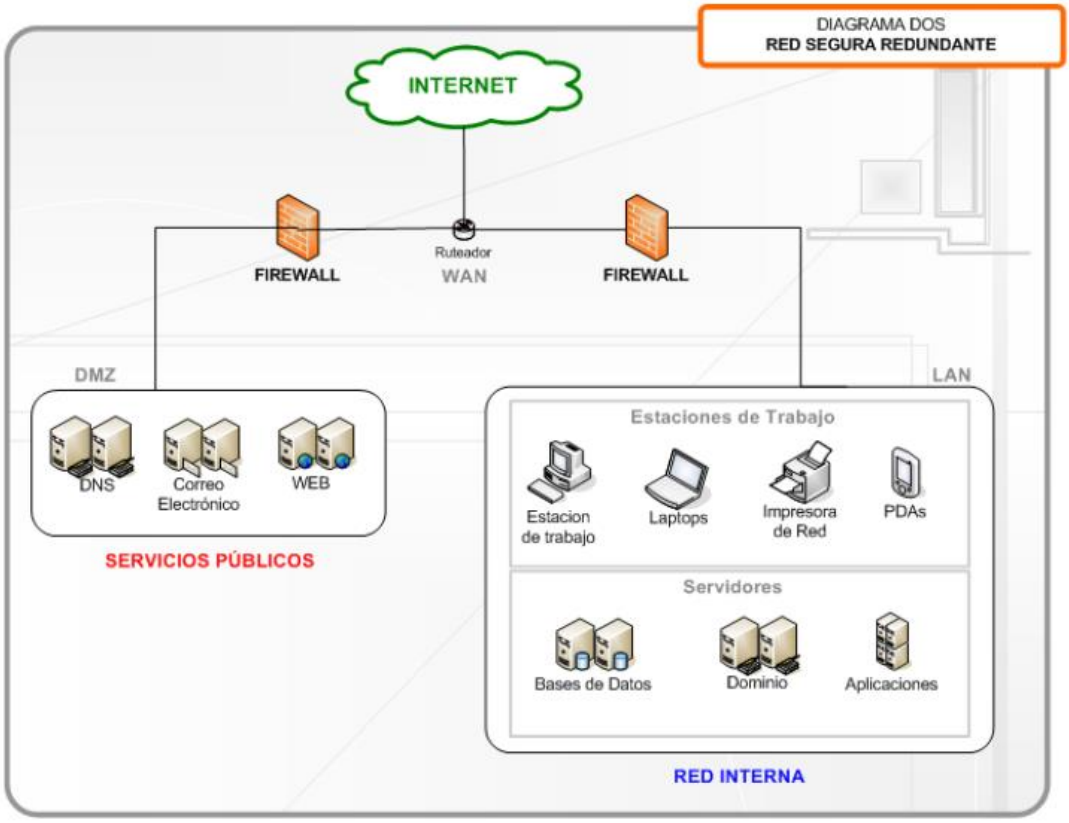
[25]Detalle No. 1: Red Básica Segura

Detalles	Descripción
	• Esquema para brindar servicios reactivos. • No posee redundancia de servidores.

[24] Fuente Esquema No. 1: CSIRT Guide, Networking Best Practices.
[25] Fuente Detalle No. 1: CSIRT Guide, Networking Best Practices.

Características	• Dos segmentos básicos de red administrados por un Firewall. • Acceso a Internet mínimo de 2 Mbps.
Software	• Se puede utilizar software libre.

[26]Esquema No. 2: Red Segura Redundante



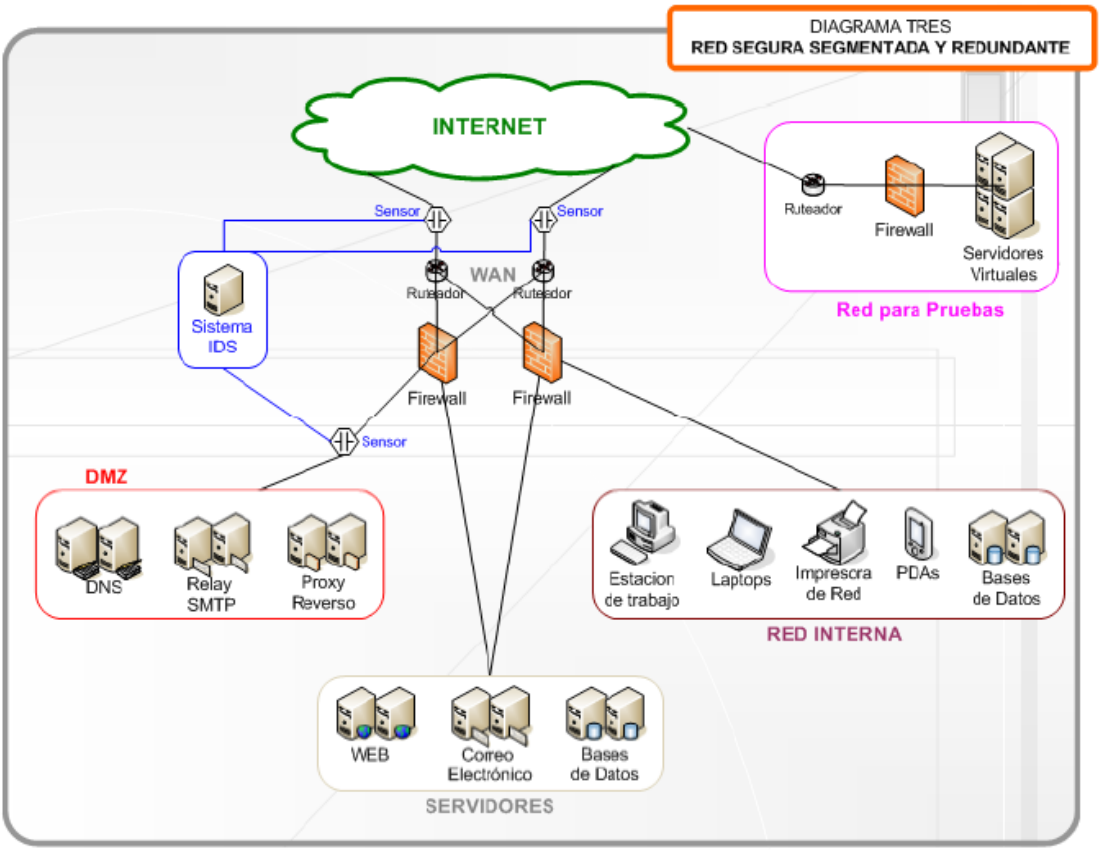
[27]Detalle No. 2: Red Segura Redundante

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.

[26] Fuente Esquema No. 2: CSIRT Guide, Networking Best Practices.
[27] Fuente Detalle No. 2: CSIRT Guide, Networking Best Practices.

Software	• Se puede utilizar software libre.

[28]Esquema No. 3: Red Segura Segmentada y Redundante



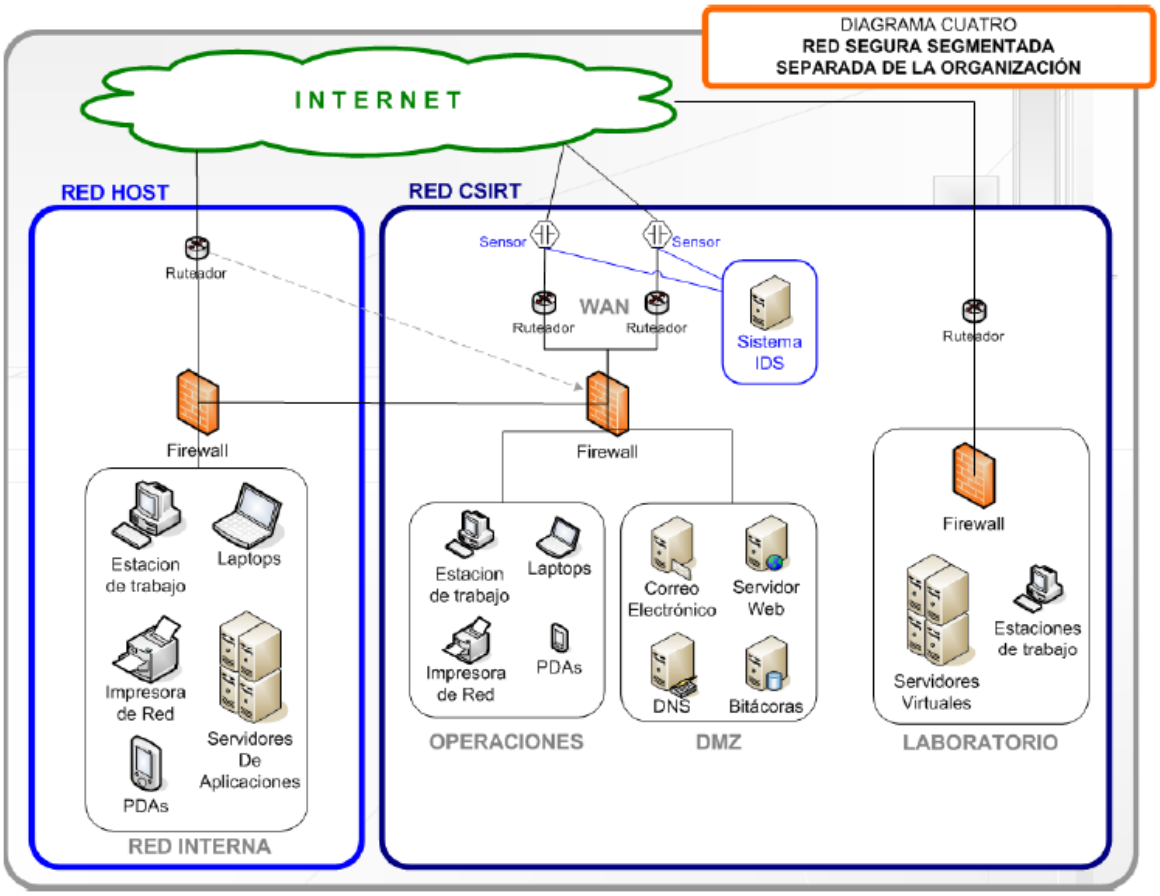
[29]Detalle No. 3: Red Segura Segmentada y Redundante

Detalles	Descripción
	• Esquema para brindar servicios reactivos y proactivos.

[28] **Fuente Esquema No. 3**: CSIRT Guide, Networking Best Practices.
[29] **Fuente Detalle No. 3**: CSIRT Guide, Networking Best Practices.

Características **Cont. Características**	• 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.

[30]**Esquema No. 4: Red Segura Segmentada Separada de la Organización**



[31]**Detalle No. 4: Red Segura 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).

[30] Fuente Esquema No. 4: CSIRT Guide, Networking Best Practices.
[31] Fuente Detalle No. 4: CSIRT Guide, Networking Best Practices.

Cont. Características	• 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.

3.5 SERVICIOS INFORMÁTICOS INICIALES DE UN CSIRT

Los servicios informáticos que brinde un CSIRT deben de ir de la mano del tipo de servicios que otorgue el CSIRT a su comunidad. Para ello es relevante tener claro que tipos de servicio brindará el CSIRT y sus respectivas necesidades de servicios informáticos que tiene que implementar.

3.5.1 Servicios 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:

[32]Cuadro No. 7 - Servicios CSIRT

Detalles	Descripción
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 Reactivos	• 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.

[32] Fuente Cuadro No. 7: www.SANS.org/ITServices

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.

Fuente Cuadro No. 7: www.SANS.org/ITServices

3.5.2 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, suelen llamarse los triple AAA:

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.

Cuadro No. 8 – Métodos de Protección CSIRT

Detalles	Descripción
Sistemas de Detección y Protección de Intrusos – IDS, IPS	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 y preventivos antes los ataques externos a la red interna de la organización que se protege. En el caso de un CSIRT, el mismo debe contar con ambos sistemas, tanto de detección de intrusos y de prevención de intrusos, para de esta manera asegurar el perímetro interno de la red.
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.

3.6 SERVICIOS PRINCIPALES DE UN CSIRT

Un centro de respuesta a incidentes puede proporcionar diversos servicios de seguridad de la información, pero es conveniente que cuando está recién formado, se enfoque de manera principal 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 un servicio que puede incluir diversos aspectos: gestión de incidentes, atención en sitio, coordinación de equipos, cómputo forense, análisis de software malicioso, etc.

Entre las muchas actividades adicionales que puede proporcionar un centro de respuesta a incidentes de seguridad de la información están:

3.6.1 Emisión de boletines y alertas de seguridad

Las actividades de prevención son importantes ya que contribuyen a evitar incidentes de seguridad informática derivado s 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.

3.6.2 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 incidente.

3.6.3 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.

3.6.4 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. En realidad, 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.

3.6.5 Implementación de Mejores Practicas

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.

CONCLUSIONES

La implementación de un Centro de Respuestas a Incidentes de Seguridad Informática Nacional – CSIRT en la Republica Dominicana va a significar un avance en materia de criminología, ya que estaremos a la altura de muchos países desarrollados, con unidades semejantes para hacerle frente al auge de crímenes cibernéticos de hoy en día.

En este estudio de investigación, hemos analizado y estudiados las unidades y departamentos actuales de respuestas a incidentes informáticos de la Republica Dominicana, haciendo comparación con los actuales CSIRT a nivel internacional.

La Republica Dominicana actualmente cuenta con las bases iniciales y visión para la implementación de un CSIRT-RD, esto sería posible con el apoyo incondicional del gobierno y entidades privadas. Como referencia del Sistema Nacional de Incidentes y Emergencias – 9-1-1, el mismo ha representado un avance para la nación, alineándonos a los estándares internacionales. De esa misma manera, con la implementación del CSIRT-RD, estaremos a la vanguardia de la seguridad y tecnología.

BIBLIOGRAFIA

Libros y Manuales

- CSIRT Guide – Creating and Managing Computer Security Team – Software Engineering Institute – año 2008.

- Proyecto Amparo – Manual: Gestión de Incidentes de Seguridad Informática – año 2010.

- Estadísticas y Documentación – Departamento de Investigaciones y Crímenes de Alta Tecnología – DICAT.

- 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 Universi-ty, 2002.

, ,

- 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; Ru-efle, Robin; & Zajicek, Mark. Handbook for Computer Security Incident Response Teams (CSIRTs) (CMU/SEI-2003-HB-002), 2003.

Enlaces de Internet

- [CERT-hb] M. West-Brown, D. Stikvoort, K. Kossakowski, G. Killcrece, R. Ruefle y M. Zaji-cek, Handbook for Computer Security Incident Response Teams (CSIRTs), abril 2003. En línea: http://www.cert.org/archive/pdf/csirt-handbook.pdf.

- [FIRST] Forum of Incident Response and Security Teams, http://www.first.org.

- [FIRST-TC] FIRST Technical Colloquia, http://www.first.org/events/colloquia

- [ISACA] ISACA, http://www.isaca.org.

- [ISC2] International Information Systems Security Certification Consortium, Inc., http://www.isc2.org.

- [PMI] Project Management Institute, http://www.pmi.org.

ANEXOS

1. La selección y definición del tema de investigación

Titulo

Propuesta para la implementación de un Centro de Respuestas a Incidentes de Seguridad Informática Nacional – CSIRT, año 2014.

El objeto de estudio de esta investigación es la Protección de las Infraestructuras Criticas de la Información, en base al segmento de servicio al que esté destinado así deberá de ser su alcance para cubrir requerimientos de protección sobre los servicios que brinda.

El CSIRT debe de brindar servicios de seguridad a las infraestructuras críticas de su segmento básicamente. 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.

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.

2. Planteamiento del problema de investigación

´las empresa y organizaciones hoy en día gastan millones implementando medidas de seguridad (equipos, dispositivos, etc.) para protegerse, pero dicho dinero lo desperdician, porque ninguna de estas medidas cubre el eslabón mas débil, la educación y concientización de la "gente" que usa los equipos". (Kevin Mitnick)

Antes de continuar, es importante comprender claramente lo que se entiende por el término "**Centro de Respuesta a Incidentes de Seguridad Informática - CSIRT**".

Para los objetivos de esta propuesta, un 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.

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 y definir los servicios que el equipo ofrece. Además, cada CSIRT debe publicar sus políticas y procedimientos de operación. Esto requiere que el equipo también publique cómo y dónde reportar los incidentes.

Hoy en día, la accesibilidad, las comunicaciones y los enlaces a través de la red global, la Internet, hacen de la información sensitiva y confidencial un activo sumamente valioso, que puede ser utilizada para fines personales, daños a terceros y perjuicios. Dada estas situación de inseguridad han surgidos grupos y comunidades de entes maliciosos (*hackers, crackers*) que

amenazan contra la seguridad individual, grupal y hasta nacional de los países a nivel mundial. Debido a esta amenaza las naciones organizadas que velan por la seguridad de sus ciudadanos y entidades, están poniendo énfasis en asegurar sus activos (recursos, informaciones), a través de la formación, educación y creación de alternativas que ayuden a salvaguardar y asegurar dichos recursos. Una de las medidas tomadas actualmente son la creación e implementación de *"Centros de Respuestas a Incidentes de Seguridad Informática – CSIRT",* dicho equipo es el arma de protección ante los grupos y comunidades maliciosas (hackers, crackers). Este CSIRT deberá responder de forma efectiva y oportuna ante los ataques, fraudes e intentos de esos grupos y comunidades maliciosas, deberá rendir informes y educar a su comunidad para evitar futuras perdidas.

3. Objetivos de la investigación

Objetivo General

- Diseñar e implementar un CSIRT con el propósito de proteger las infraestructuras críticas de la información, en base al segmento de servicio al que esté destinado, así deberá de ser su alcance para cubrir requerimientos de protección sobre los servicios que brinda.

Objetivos Específicos

- Analizar y diseñar los lineamientos y acciones para la formación y creación de un CSIRT.

- Identificar y hacer el modelo, la estructura y los recursos del CSIRT.

- Realizar la segregación de funciones, procesos y procedimientos que sustentaran el flujo del CSIRT.

4. Justificación de la investigación

a. Justificacion Teorica.

Un CSIRT a nivel nacional representa para el país un avance a nivel tecnológico y un punto de avance en el intercambio a nivel de tecnológico y de conocimientos entre las naciones regionales donde estén implementados CSIRTs.

b. Justificación Metodológica

Específicamente se quiere diseñar un esquema para la implementación inicial de un CSIRT, en el ámbito de cubrir las necesidades de los ciudadanos en lo que respecta de poseer un CSIRT y que el mismo pueda salvaguardar y asegurar los activos (informaciones, datos, equipos) de los ciudadanos. Para lograr esto, debemos identificar cuáles son las principales necesidades a nivel de seguridad de la información que ameritan los ciudadanos y analizar las consecuencias que puedan tener si alguno de los ciudadanos es objeto de algún ataque o “hacking”.

A partir de este punto, podemos establecer estrategias para la implementación del CSIRT que se adapten a las diferentes situaciones y casos que hayan vivido los ciudadanos, para de esta manera satisfacer las necesidades de los ciudadanos en este ámbito.

c. Justificación Práctica

La implementación de un CSIRT Nacional contemplará un foco tecnológico a nuevos horizontes a nivel internacional, esto traerá como consecuencia la búsqueda de talento, la inversión en TICs y la innovación del gobierno central. La ciudadanía debe culturizarse para el buen uso de esta nueva iniciativa tecnológica nacional, el mimo va a representar un avance a nivel organizacional y de contacto entre los ciudadanos.

A nivel internacional, el país será visualizado como un ente de ejemplo ante la innovación y los avances, esto traerá consigo el aumento de confianza de los inversionistas internacionales a nivel de materia tecnológica y áreas afines.

5. Marco de referencia

a. Marco Teórico

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 ser-vicios basados en las necesidades de su área de cobertura de servicio. (Proyecto AMPARO, 2011)

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. (Proyecto AMPARO, 2010)

Un CSRIT es un concreto equipo dentro de una organización, el mismo realiza planes y estrategias para una efectiva respuesta de un incidente. Un CSRIT es muy parecido a un Equipo de Respuestas de Emergencias. (Software Engineering Institute, CSIRT Guide, 2008)

b. Marco Conceptual

Comunidad. Por ejemplo, podrían ser empleados de una empresa o de sus suscripto-res de pago, o podría ser definido en términos de un enfoque tecnológico, como los usuarios de un sistema operativo determinado. Una comunidad CSIRT puede ser de-terminado de varias maneras. La definición de la comunidad debe crear un perímetro alrededor del grupo al que el equipo proporcionará el servicio. Es importante que exista una sección de política del documento, la cual debe de explicar cómo serán tratadas las solicitudes fuera del perímetro definido. (Proyecto AMPARO, 2011)

Seguridad organizacional. Aspectos relativos a la gestión de la seguridad dentro de la organización (cooperación con elementos externos, outsourcing, estructura del área de seguridad, etc.).

Gestión de Problemas. Ofrece ayuda a la Gestión de Incidentes informando sobre erro-res conocidos y posibles soluciones temporales. Por otro lado, establece controles sobre la calidad de la información registrada por la Gestión de Incidentes para que ésta sea de utilidad en la detección de problemas y su posible solución. (Software Engineering Institute, CSIRT Guide, 2008)

Gestión de Cambios. La resolución de un incidente puede general una petición de cambio que se envía a la Gestión de Cambios. Por otro lado, un

determinado cambio erróneamente implementado puede ser el origen de múltiples incidencias y la Gestión de Cambios debe mantener cumplidamente informada a la Gestión de Incidencias sobre posibles incidencias que los cambios realizados puedan causar en el servicio. (Software Engineering Institute, CSIRT Guide, 2008)

La infraestructura de la red. El CSIRT debe estar separado de la infraestructura de la organización en que esté hospedada. El CSIRT debe tener una estructura propia de sub-redes 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 me-dio de dispositivos de seguridad según su necesidad. (Firewall, Proxy, IDS, IPS, etc.)

(Software Engineering Institute, CSIRT Guide, 2008)

6. Aspectos Metodológicos.

6.1 Tipos de estudio

En la presente investigación se utilizaran los siguientes tipos de estudio:

Exploratorio, este es la base de la investigación, se utiliza cuando un tema no ha sido abordado o ha sido poco estudiado. A través del estudio exploratorio se ha planteado el problema de la investigación y las hipótesis.

Descriptivo, este será utilizado para dar detalles de las variables que intervienen en la problemática. Esta investigación detallará las posibles razones por las cuales el sistema de entregas de materiales a la linea de Keypads no permite enviar los componentes a las áreas especificas donde serán manufacturados los productos, también cuales serian las posibles alternativas para mejorar dicho proceso.

6.1 Métodos de Investigación

Observación, a través de la observación de dichos modelos podemos sintetizar las ideas más convenientes para formar un nuevo CSIRT Nacional. Con el análisis de las muestras de observación podemos destacar los aspectos más destacados y más críticos para la iniciación y planeación del CSRIT.

Inductivo, a través de la observación de muestras similares y particulares, con el propósito de llegar a una conclusión y premisas que puedan ser aplicadas.

Análisis, con la identificación de cada una de las partes que caracterizan una realidad actual o ejemplo, para de esa manera establecer una relación Causa-Efecto entre los elementos que compone el objeto de investigación.

7. Tabla de contenido.

- Próximos pasos
- Aseguramiento Contra Situaciones Hostiles
- Control de Accesos
- Conclusiones

1.3 Recomendaciones sobre la arquitectura de redes de un CSIRT

- Ambiente Físico
- Infraestructura de Red
- Hardware
- Software
- Infraestructura de Telecomunicaciones
- Diagramas Sugeridos
- Esquema Uno: Red Básica Segura
- Esquema Dos: Red Segura Redundante
- Esquema Tres: Red Segura Segmentada y Redundante
- Esquema Cuatro: Red Segura Segmentada Separada de la Organización
- Servicios informáticos iniciales de un CSIRT
- Servicios CSIRT

1.3 Servicios informáticos de un CSIRT

1.4 Aplicaciones que apoyan la implementación de los servicios informáticos CSIRT

1.5 Beneficios en la implementación de un CSIRT

1.6 Análisis FODA General para un CSIRT

CAPITULO II.

- MODELOS ORGANIZACIONALES DE CENTROS DE RESPUESTA A INCIDENTES.

- MODELOS ORGANIZACIONALES DE CENTROS DE RESPUESTA A INCIDENTES.

- MODELOS DE REFERENCIA.

- Equipo de seguridad

- Equipo de respuesta a incidentes centralizado.

- Equipos de respuesta a incidentes distribuidos.

2.1 Equipo coordinador.

- CENTROS DE RESPUESTA EXISTENTES
- NOMBRE DEL CENTRO DE RESPUESTA
- LA CIRCUNSCRIPCIÓN DEL CENTRO DE RESPUESTA
- MISIÓN DEL CENTRO DE RESPUESTA.

2.2 SERVICIOS PRINCIPALES

- Emisión de boletines y alertas de seguridad
- Análisis de vulnerabilidades
- Detección de incidentes
- Difusión y capacitación
- Implementación de mejores prácticas
- REPORTE, CLASIFICACIÓN, ASIGNACIÓN
- AUTORIDAD
- PERSONAL DEL CENTRO DE RESPUESTA
- Empleados

- Parcialmente empleados

2.3 Outsourcing

- SELECCIÓN DEL MODELO DE CENTRO DE RESPUESTA
- Costos
- Experiencia del personal
- Estructura organizacional
- División de responsabilidades
- Protección de información confidencial
- Falta de conocimiento específico sobre la organización
- Falta de correlación de información
- Manejo de incidentes en diversas ubicaciones geográficas

2.4 DEPENDENCIAS DENTRO DE LAS ORGANIZACIONES

- Administración
- Seguridad de la información
- Telecomunicaciones
- Soporte técnico
- Departamento jurídico
- Relaciones públicas e institucionales (comunicación social)
- Recursos humanos

CAPITULO III.

PROPUESTA DE ESPECIALIZACIÓN DE FUNCIONES EN EL INTERIOR DE UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS

3.1 SEGREGACIÓN DE FUNCIONES

- Introducción
- Las funciones

3.2 Descripción de las Funciones

- Directorio
- Director Ejecutivo
- Comité Ejecutivo
- Gerente Operacional
- Difusión
- Infraestructura
- Triage
- Documentación
- Capacitación y Entrenamiento
- Logística
- Investigación

Conclusiones

Bibliografía

Anexos

9. Cronograma de trabajo

Tareas	Meses															
	1				2				3				4			
	Semanas															
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Fase 1																
Ajuste del Anteproyecto	■	■														
Levantamiento de Información de Casos y Modelos existentes.		■	■	■												
Fase 2																
Ajuste de instrumentos para la recolección de información			■	■	■											
Recolección de Datos				■	■	■										
Tabulación de la información							■	■								
Análisis e Interpretación de la información								■	■	■						
Fase 3																
Elaboración del informe final									■	■	■					
Revisión del informe por parte del asesor												■	■			
Reajuste luego de revisión final														■	■	
Entrega del informe final																■

10. Presupuesto

	Monto Estimado	
	Ingresos	**Egresos**
Recursos Propios	RD$64,600.00	
Total Ingresos	**RD$64,600.00**	
Gastos:		
Honorarios de los investigadores		RD$30,000.00
Pago De Asesores		RD$20,000.00
Pago digitación, encuadernación e impresión de informaciones		RD$ 2,500.00
Compra de papel para impresión		RD$ 600.00
Empastado		RD$ 600.00
Fotocopias		RD$ 400.00
Transporte		RD$ 5,500.00
Pago De Internet		RD$ 1,500.00
otros gastos		RD$ 3,500.00
Total Egresos		**RD$64,600.00**