1. CAPÍTULO UNO - ACTIVIDADES REALIZADAS POR SSI/UNAM-CERT DE LA DGTIC DE LA UNAM.

En este capítulo se describe la misión, visión e historia de la Subdirección de Seguridad de la Información UNAM-CERT de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC), así como sus actividades principales y los servicios que proporciona

1.1.Historia de la SSI/UNAM-CERT

En esta sección se indica en forma cronológica la evolución que ha tenido la Subdirección de Seguridad de la Información (UNAM-CERT) a lo largo de los años. Las fuentes de referencia de los eventos indicados son la tesis de licenciatura del Doctor Diego Zamboni y el testimonio del Ing. Rubén Aquino Luna, actual Subdirector de Seguridad de la Información, quien ha formado parte de la organización desde hace diez años.

1975 – En una entrevista realizada por Diego Zamboni en 1995 al Sr. Rafael Durán, el entonces jefe del Departamento de Operación de la DGSCA, se mencionó la existencia de los primeros problemas de seguridad en cómputo en RED-UNAM.

> *"Desde 1975 se tenían problemas de seguridad en cómputo. Estos eran con los sistemas Burroughs. Ya había en ese entonces en la Universidad gente con la capacidad y el interés de romper las barreras de seguridad impuestas por el sistema, por "el simple gusto de hacerlo". Contra estas violaciones de seguridad nunca fue posible tomar alguna acción formal debido a la falta de legislación al respecto, así como las fricciones y conveniencias políticas que, desgraciadamente, siempre han invadido los ámbitos académico y científicos en nuestra Universidad". [1]*

1993 – Ocurre una intrusión no autorizada en la supercomputadora Cray Y-MP4/46, propiedad de la Dirección General de Servicios de Cómputo Académico. A raíz del incidente, el personal directivo de la DGSCA se percató de la importancia de la seguridad en cómputo, por lo que tomó la decisión de crear el equipo de respuesta a incidentes que con el tiempo evolucionaría en lo que hoy es la Subdirección de Seguridad de la Información (UNAM-CERT).

La tesis de licenciatura del Doctor Zamboni es el único documento en el que se tiene una descripción detallada del incidente, del cual se menciona lo siguiente:

"El 10 de Julio de 1993, la Lic. Martha A. Sánchez Cerezo, jefe del Departamento de supercómputo, descubrió en la supercomputadora una cuenta llamada god, asignada a un usuario no existente. La falsedad de esta cuenta era evidente desde su nombre (god es "Dios" en inglés).

Al hacer una revisión detallada de la cuenta, se vio que pertenecía a todos los grupos y tenía activados todos los permisos, situación en la que ningún usuario de la Cray (ni siquiera root) se encuentra." [1]

1993 – A raíz del incidente con la supercomputadora Cray, personal de la UNAM tiene el primer contacto con el Coordination Center de Carnellie Mellon de Estados Unidos (CERT/CC). El CERT/CC es el primer equipo de respuesta a incidentes de todo el mundo y ha realizado varias contribuciones al área de seguridad de la información.

> *"Se notificó al CERT [CER90] de lo sucedido, informando solamente de lo ocurrido en las estaciones de trabajo (no en la Cray), a petición de Cray Research, Inc. El CERT solicita que se le notifique de cualquier incidente de seguridad con los siguientes objetivos:*
>
> *(a) Establecer, cuando sea posible, patrones de acción que puedan indicar un incidente ocasionado por el mismo atacante en otros sitios.*
> *(b) Proporcionar asesoría en el manejo del incidente.*
>
> *(c) Alertar a otros sitios sobre ataques del mismo tipo que puedan realizarse". [1]*

El entonces Ingeniero Diego Zamboni crea el equipo de respuesta a incidentes de seguridad en cómputo, el cual pertenecía a la Dirección de Supercómputo de la DGSCA, nombre de la DGTIC hasta el 2010.

El Ingeniero Diego Zamboni publica su tesis de licenciatura "Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix", en la cual se hace un análisis del estado de la seguridad en cómputo de RED-UNAM en aquel momento.

1994 – El Área de Seguridad en Cómputo organiza la primera edición del Día Internacional en Cómputo (DISC) en México. [2]

El Día Internacional de la Seguridad en Cómputo, conocido internacionalmente como *Computer Security Day [3]*, pretende concientizar a todos los usuarios de sistemas computacionales sobre cómo tomar las medidas pertinentes para proteger apropiadamente la información en cualquiera de sus formas.

El DISC fue fundado en 1988 como una iniciativa del Grupo de Interés Especial en Seguridad, Auditoría y Control (SIGSAC)[4] de la Association for Computing Machinery (ACM), y actualmente se realiza en más de 40 países de manera simultánea, ofreciendo la posibilidad de llegar a mucha más gente que una conferencia tradicional. [5]

1995 – El plan de becarios de supercómputo ofrece el módulo de especialización "seguridad en cómputo".

1998 – El área de seguridad en cómputo ofrece pláticas de concientización de seguridad en el marco del Día Internacional de la Seguridad en Cómputo (DISC). En este evento también se observa la participación de ponentes de organizaciones especializadas en seguridad, tanto de México como del extranjero, del ámbito académico y del ámbito empresarial. El programa del DISC de 1998, es testimonio de la participación de grandes personalidades del área de seguridad de la

información en este evento, entre los cuales se destacan Miguel de Icaza, creador de GNOME; Theo de Raadt, creador de Open BSD y fundador de Core Technologies; José Neif Jury de Open Source México, Nicholas P. Cado de la Nasa, así como miembros Purdue University, de la Universidad de la Coruña y de la Universidad de Waterloo.

Actualmente UNAM-CERT considera el DISC de 1998 como el primer congreso de seguridad en cómputo, debido a la participación de miembros de organizaciones nacionales e internacionales, tanto de empresas como de universidades.
Actualmente es difícil determinar quiénes fueron todos los que formaron parte del Área de Seguridad en Cómputo, pero gracias a un programa del DISC 1998 se sabe que parte de sus integrantes fueron:

- *Juan C. Guel López*
- *Fidencio A. Basilio Cruz*
- *Israel Quiroz Plata*
- *Manuel Moreno*
- *Olga Lidia Torres Rivera*
- *César Vega*
- *Iliana Meneses*

1999 – El licenciado Juan Carlos Guel se integra como Jefe del Área de Seguridad en Cómputo y bajo su liderazgo se convierte en Departamento de Seguridad en Cómputo, se aumentan los recursos asignados a la organización, tanto humanos como materiales. En ese entonces los servicios ofrecidos eran asesorías de seguridad (revisión y configuración de equipos). Se amplía el ámbito de acción del DSC a otras dependencias de la UNAM. [6]

El ingeniero Rubén Aquino se integra como becario en supercómputo con especialidad en seguridad en cómputo.

1999 **-** *2001* – Trámite de acreditación ante FIRST (Forum of Incident Response Security Teams). No existía ningún equipo de respuesta a incidentes en México que fuera reconocido internacionalmente, por lo que se vio la necesidad de ubicarse como punto de contacto internacional para atender incidentes no sólo en RED-UNAM, sino en México. Al mismo tiempo, la acreditación le permitió a UNAM-CERT obtener visibilidad internacional para lograr acuerdos con grupos nacionales e internacionales.

2003 – Durante la dirección de Juan Carlos Guel, se lanza la iniciativa de extender la educación de seguridad de la información a nivel nacional; mediante la colaboración de la ANUIES (Asociación Nacional de Universidades e Instituciones de Educación Superior). Se crea la Red Nacional de Seguridad en Cómputo (RENASEC), con el objetivo de albergar y compartir las iniciativas, acuerdos y noticias en materia de seguridad informática, a más de 145 Instituciones de Educación Superior del país.

2005 – Se crea Honeynet UNAM-CHAPTER. El Proyecto Honeynet fue fundado en 1999 y es una organización internacional de investigación sin fines de lucro, dedicada a mejorar la seguridad de Internet sin ningún costo para el público. Se forma por varios grupos alrededor del mundo, conocidos como capítulos y formados por voluntarios. [7]

La participación de UNAM-CERT en el Proyecto Honeynet le permitió establecer nuevos vínculos y visibilidad con organizaciones internacionales, así como estar a la vanguardia de nuevas tecnologías de detección de intrusos, análisis de malware, respuesta a incidentes, cómputo forense y demás temas de interés para la seguridad de la información.[8]

2010 – Durante la dirección del Ing. Rubén Aquino, el Departamento de Seguridad en Cómputo se convierte en la Subdirección de Seguridad de la Información, con lo que se actualiza el alcance y el ámbito de acción de la organización.

Se obtiene la certificación ISO 27001:2005, con el objetivo de certificar el proceso de respuesta y atención a incidentes de seguridad en cómputo.

2011 – Se obtiene la recertificación del estándar ISO 27001:2005.

1.2.Misión

La Subdirección de Seguridad de la Información (SSI) nace como la entidad responsable de atender, investigar y operar la seguridad en cómputo de la UNAM, en base a estos objetivos la SSI establece las siguientes misiones estratégicas:

Para con nuestra Universidad:

- Proporcionar servicios de asesoría y atención a incidentes en materia de seguridad informática a cada una de sus entidades que la conforman, satisfaciendo sus necesidades en base a la capacidad tecnológica que se disponga.

Para con nuestra comunidad:

- Proporcionar información clara, precisa y objetiva de los problemas de seguridad informática a los cuales se afrontan cotidianamente, así como auxiliar en la solución de estos problemas.

Para con nuestros Académicos:

- Proporcionar las herramientas tecnológicas y el entorno adecuado para que desarrollen sus potenciales personales y profesionales.

1.3.Visión

La SSI de la UNAM se consolidará como el órgano rector en la operación y dirección de las políticas de seguridad que la Universidad requiera. Así como el principal generador de recursos humanos capacitados de alto nivel en materia de seguridad que la Universidad y el país requieren.

1.4.Servicios proporcionados por UNAM-CERT

Cuando se creó el área de seguridad en cómputo en la DGSCA en 1994, los únicos servicios proporcionados eran atención respuesta a incidentes de seguridad en cómputo, revisión de configuraciones y difusión de buenas prácticas de seguridad en sistemas de cómputo.

A medida que la organización creció, se tuvo la necesidad de ofrecer otros servicios y fue necesario establecer varios departamentos especializados en áreas de seguridad informática. Cada uno de ellos ofrece varios servicios tanto a la comunidad universitaria como al público en general, mismos que están descritos en la tabla 1.1

Departamento	*Servicios Proporcionados*
Respuesta a incidentes y detección de intrusos.	Análisis de tráfico de red. Respuesta a incidentes de seguridad de la información. Análisis forense. Servicios administrados de seguridad. Revisión de configuraciones.
Auditoría y nuevas tecnologías	Análisis de vulnerabilidades. Pruebas de penetración en sistemas. Implementación de mejores prácticas.
Operación Interna y PKI	Cursos de capacitación. Asistencia en problemas de seguridad específicos de plataformas Windows.
Seguridad en Sistemas	Desarrollo de los sistemas utilizados internamente por UNAM-CERT. Desarrollo y mantenimiento de los portales web de seguridad de UNAM-CERT. Responsables de la divulgación de noticias de seguridad a la comunidad.

Tabla 1.1 Descripción de servicios ofrecidos por los departamentos de UNAM-CERT

1.5. Servicios proporcionados por el Departamento de Respuesta a Incidentes y Detección de Intrusos

El Departamento de respuesta a incidentes y Detección de Intrusos realiza acciones preventivas y reactivas de incidentes de seguridad en cómputo ocurridos dentro y fuera de RED-UNAM. Este departamento está dividido en respuesta a incidentes, análisis de malware, análisis de tráfico y detección de intrusos.

1.5.1. Análisis de tráfico de red

A través de este servicio se caracterizan los flujos de información existentes en la red del cliente. Permite identificar el tráfico malicioso que no es visible por el usuario final o el administrador, también se pueden identificar ataques internos o robo de información. Derivado de las actividades realizadas, al final se emiten recomendaciones que permitirán limpiar el tráfico de la red, aumentando la eficiencia de la operación interna a nivel de infraestructura tecnológica de comunicaciones.

1.5.2. Respuesta a incidentes de seguridad de la información

Este servicio permite identificar, contener, erradicar y recuperar la estabilidad de la infraestructura tecnológica ante un incidente de seguridad de la información.

1.5.3. Análisis forense

El UNAM-CERT proporciona el servicio de análisis forense informático para la investigación de incidentes de seguridad informática y de posibles delitos o faltas en los que está involucrado un sistema informático o de infraestructura.

Este servicio permite identificar huellas específicas de actividad en un sistema informático y determinar los eventos relevantes para una investigación. Los resultados obtenidos pueden ser útiles como elemento para deslindar responsabilidades y para mejorar la seguridad de la infraestructura informática de la organización.

1.5.4. Revisión de configuraciones

En este servicio se lleva a cabo la revisión de configuraciones con el propósito de determinar si se cuenta con el nivel de seguridad mínimo para el servidor analizado. Se elabora un reporte en el que se indican qué aspectos fueron analizados, qué hallazgos se obtuvieron y de qué manera. Por último se indican recomendaciones para llevar el equipo a un nivel de seguridad aceptable. Estas recomendaciones deben ser implementadas por el cliente.

Se identifican errores en la implantación de mecanismos de seguridad como firewalls, IPSs, IDSs, antispam, antivirus entre otros.

1.5.5. Programas de capacitación

Uno de los servicios de mayor valor que proporciona la SSI/UNAM-CERT es la transferencia de conocimiento. Este servicio se proporciona a través de sus programas de capacitación, ya sea por medio de cursos a la medida o sus líneas de especialización impartidas durante los Congresos de

Seguridad. El Departamento de Respuesta a Incidentes y Detección de Intrusos es responsable de las siguientes líneas de especialización:

- Cómputo forense y legislación relacionada.
- Cómputo forense en red.
- Detección de intrusos.

1.6. Servicios proporcionados por el resto de los departamentos de UNAM-CERT

1.6.1. Análisis de vulnerabilidades y pruebas de penetración

Este servicio busca identificar defectos de configuración presentes en la infraestructura tecnológica del cliente, también revisa errores de diseño y la efectividad de los mecanismos de seguridad existentes ante un ataque. Las pruebas de penetración (pentest) son realizadas por un equipo SWAT del UNAM-CERT de alta efectividad que permite encontrar puntos de entrada en la red del cliente, tal y como serían vistos por un usuario malintencionado dentro y fuera de la red. Las pruebas se llevan a cabo de acuerdo a las buenas prácticas de OSSTMM y pueden ser de caja negra, caja blanca o caja gris. El equipo a cargo de este servicio cuenta con capacitación avalada por el Instituto SANS en áreas de hacking ético y análisis de redes.

1.6.2. Análisis de riesgos

A través de la metodología OCTAVE este servicio permite identificar el inventario de activos de información valiosos para la organización. Tras esta identificación se calculan los riesgos de acuerdo a las amenazas y vulnerabilidades presentes.

1.6.3. Creación de políticas de seguridad de la información

A través de este servicio se identifican las necesidades de seguridad de la información del cliente y se generan recomendaciones que podrán ser traducidas en políticas conjuntamente con los responsables dentro de la organización. Dichas políticas proveen el marco necesario para la instauración de un esquema integral de seguridad de la información.

1.6.4. Implantación de ISMS de acuerdo al estándar ISO 27001

Este servicio contempla el ciclo de implantación del proceso de seguridad de la información a través del ISMS (Information Security Management System) de acuerdo al estándar ISO 27001. Se basa en el ciclo PDCA (plan, do, check, act) de mejora continua. En este servicio se acompaña al cliente en la implantación de los controles del estándar de acuerdo al alcance definido y del análisis de riesgos en búsqueda de la certificación por parte de una autoridad avalada por ISO.

El grupo de profesionales involucrados en este servicio cuenta con experiencia en la implantación del estándar en diversas organizaciones. Los auditores se encuentran certificados para realizar la auditoría interna.

1.6.5. Programas de capacitación

Uno de los servicios de mayor valor que proporciona la SSI/UNAM-CERT es la transferencia de conocimiento. Este servicio se proporciona a través de sus programas de capacitación, ya sea por medio de cursos a la medida o sus líneas de especialización:

- Administración y seguridad en Windows
- Administración y seguridad en UNIX
- Cómputo forense y legislación relacionada
- Seguridad perimetral y de red
- Técnicas de intrusión, análisis de vulnerabilidades y pentest
- Detección de intrusos
- Mejores prácticas en seguridad de la información

REFERENCIAS DEL CAPÍTULO

[1] ZAMBONI, Diego. *Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix* [en línea], Facultad de Ingeniería UNAM 1995,. Formato PDF, Disponible en Internet: http://homes.cerias.purdue.edu/~zamboni/pubs/thesis-bs.pdf.

[2] http://www.disc.unam.mx/1998/, Área de Seguridad en Cómputo, 7 de mayo de 2011.

[3] http://www.computersecurityday.org, Día de la Seguridad en Cómputo, 7 de mayo de 2011.

[4] http://www.sigsac.org/, Grupo de Interés Especial en Seguridad, Auditoría y Control (SIGSAC) de la Association for Computing Machinery (ACM), 7 de mayo de 2011.

[5] http://www.disc.unam.mx/2003/espanol/indexea3d.html?liga=que, diciembre de 2010, Lista de eventos del día de la seguridad en cómputo, 7 de mayo de 2011.

[6] http://www.riuady.uady.mx/seguridad/articulos.php?id=208, Semblanza de Juan Carlos Guel, escrito por la Universidad Autónoma de Yucatán, 7 de diciembre de 2010.

[7] http://project.honeynet.org, Sitio oficial del Proyecto Honeynet, 7 de mayo de 2011.

[8] http://www.honeynet.unam.mx/, Sitio del capítulo Honeynet UNAM, 7 de mayo de 2011.