Capítulo 2.
Proyectos Alternos

Capítulo 2.
Proyectos Alternos

2.1 Sede Laboral

La Subdirección de Seguridad de la Información SSI/UNAM-CERT pertenece a la Dirección General de Cómputo y Tecnologías de la Información y Comunicación de la UNAM, se ubica físicamente en el Circuito Exterior S/N Frente a la Facultad de Contaduría y Administración, Delegación Coyoacán, C.P. 04510, México D.F.

El Departamento de Seguridad en Cómputo (DSC) nació en el año 1999, y sus antecedentes fueron el Equipo de Seguridad en Cómputo (ESC) y el Área de Seguridad en Cómputo (ASC), los cuales datan desde 1994. Surge bajo la necesidad de contar con un equipo de expertos en seguridad informática que pudiera satisfacer el requerimiento en esta materia que la DGTIC y la misma Universidad tenían. En el año de 2001 obtiene el reconocimiento ante FIRST (Forum of Incident Response and Security Teams) de CERT (Computing Emmergency Response Team, o bien Equipo de Respuesta a Incidentes en Seguridad en Cómputo).

Comencé a trabajar en la SSI/UNAM-CERT el mes de junio del 2009 para el proyecto de seguridad en Unix, dentro de mis principales actividades estaban la investigación y pruebas de herramientas de seguridad informática enfocadas a sistemas Unix, así como apoyar en las labores de administración de los servidores Unix del Departamento.

Mis actividades dentro de este proyecto consistieron en preparar el ambiente de pruebas para las herramientas antispam, configurar los equipos y verificar el correcto funcionamiento de los scripts utilizados para dicho propósito.

2.2 Implantación de controles para el estándar ISO 27001:2005

Uno de los proyectos más importantes fue el de “Implantación de controles para el estándar ISO 27001:2005”. Como se sabe, el ISO/IEC 27001 Fue desarrollado como un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de un *SGSI (Sistema de Gestión de Seguridad de la Información)* para cualquier tipo de organización.

El objetivo principal del SGSI en este caso, fue que la SSI UNAM/CERT era capaz de demostrar que la información dentro del proceso de manejo de incidentes era segura, es decir, que la información se manejaba bajo características de confidencialidad, integridad y disponibilidad, que garantice la continuidad en sus operaciones. Para ello se consideró como base el estándar ISO/IEC 27001:2005.

Entre sus principales acciones de un SGSI están:

- Identificar activos de la organización y su impacto dentro de la misma.
- Efectuar un análisis y evaluación del *riesgo*.
- Determinar opciones de tratamiento del riesgo.
- Implementación de controles para minimizar las posibilidades de que las amenazas puedan causar daño en la organización.

El proceso para el cual se buscaba obtener la certificación ISO/IEC 27001 era el relacionado al Manejo de Incidentes dejando pendientes las áreas restantes como candidatas de certificación para proyectos posteriores.

Como conclusiones de este proyecto, se buscó:

- Lograr la concientización del personal de la SSI UNAM/CERT sobre la importancia de obtener la certificación ISO/IEC 27001 para el proceso de Manejo de incidentes.
- El personal de la SSI UNAM/CERT debía contribuir en las tareas que permitan la obtención de toda aquella información utilizada para la creación, la implementación y la conservación del SGSI.

Durante la realización del proyecto se implementaron varias políticas de seguridad, diseñadas por la persona encargada de dicha área, enfocadas hacia los usuarios internos, uso correcto de los equipos, problemas en caso de fallas de seguridad, contraseñas, etc.

Como líder del proyecto “Seguridad en UNIX” e integrante del área de Operación Interna de la SSI UNAM/CERT me correspondió realizar los siguientes procedimientos para el proyecto antes mencionado:

- Procedimiento para el funcionamiento de los servidores de correo y almacenamiento.
- Procedimiento para el monitoreo del servidor de correo y almacenamiento.
- Procedimiento de hardening en los equipos de cómputo.
- Procedimiento para agregar información al servidor de almacenamiento.
- Procedimiento para pruebas de compatibilidad de software y hardware

2.3 Difusión de noticias sobre seguridad informática.

Como parte de las actividades de la SSI UNAM/CERT está difundir noticias actualizadas sobre seguridad informática. Es por eso que cada integrante tiene asignado un día en específico para realizar el alta de la noticia asignada realizando las siguientes actividades:

- Recepción de la noticia asignada mediante correo electrónico.
- Traducción de la misma.
- Una vez traducida y revisada se sube al sitio web de la SSI UNAM/CERT en la parte de noticias.

Es una actividad que se sigue realizando hasta el día de hoy y se ve reflejada día a día en el sitio web correspondiente.