CUDI-CDR
Draft 2
Categoría: Informativo
Grupo de Seguridad

Mayo-2004
M. Farias-Elinos (ULSA)
C. A. Altamirano (UNAM)
L. Gómez (CICESE)
M. Mendoza (CICESE)
G. Castillo (CELANESE)

Perfil del Oficial de Seguridad Informática

Resumen:

En este documento se definen los requisitos mínimos y deseables, así como las responsabilidades, objetivo, misión y habilidades de la figura del Oficial de Seguridad Informática (OSI) que deberá de existir en cada institución miembro de RedCUDI.

Palabras claves: *Seguridad, Oficial de Seguridad, perfil del oficial de seguridad informática*.

Derechos de Copia
Copyright (C) CUDI-CDR-Grupo de Seguridad (2004). Todos los derechos Reservados
La distribución de este memo no esta limitada.

Tabla de contenido

1 Introducción 1
2 Definición 2
3 Misión 2
4 Objetivos 2
5 Formación 3
6 Habilidades personales 3
7 Deberes y responsabilidades 4
8 Sugerencias adicionales 5
9 Datos autores 6

1 Introducción

La falta de una figura encargada de coordinar, planear y promover las actividades que tengan que ver con la parte de seguridad informática genera una situación que se ve reflejada en el crecimiento de problemas de seguridad que se presentan dentro de las instituciones, tales como intrusiones, robo de información, problemas de virus, entre otros, mejor conocidos como incidentes [1]; agregando la falta de una legislación informática donde se tipifique los delitos informáticos [2]. Esto aunado a la ignorancia de saber cuales son las capacidades necesarias y suficiente en conocimientos, formación y habilidades, así como las responsabilidades y deberes de la figura encargada de la seguridad en la institución hacen que sea difícil el poder seleccionar a la persona indicada que se encargue de ver lo referente a la seguridad informática dentro de las instituciones.

El propósito de tener una figura denominada Oficial de Seguridad Informática (OSI) es tener a alguien al cual se pueda recurrir en caso de algún problema de seguridad, un encargado de difundir las alertas, así como el proponer y definir esquemas que reduzcan los incidentes de seguridad que se presenten.

2 Definición

El Oficial de seguridad informática (OSI), es la persona responsable de planear, coordinar y administrar los procesos de seguridad informática en una organización

3 Misión

El Oficial de seguridad informática tiene la función de brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la organización.

4 Objetivos

- Definir la misión de seguridad informática de la organización en conjunto con las autoridades de la misma.
- Aplicar una metodología de análisis de riesgo para evaluar la seguridad informática en la organización.
- Definir la Política de seguridad informática de la organización.
- Definir los procedimientos para aplicar la Política de seguridad informática.
- Seleccionar los mecanismos y herramientas adecuados que permitan aplicar las políticas dentro de la misión establecida.
- Crear un grupo de respuesta a incidentes de seguridad, para atender los problemas relacionados a la seguridad informática dentro de la organización.
- Promover la aplicación de auditorias enfocadas a la seguridad, para evaluar las prácticas de seguridad informática dentro de la organización.
- Crear y vigilar los lineamientos necesarios que coadyuven a tener los servicios de seguridad en la organización.
- Crear un grupo de seguridad informática en la organización.

5 Formación

- Licenciatura en el área de cómputo.
- Conocimientos en:

Conocimientos y experiencia mínima	***Conocimientos y experiencia deseable***
❑ Sistemas Operativos (Windows, Linux, UNIX) a nivel de usuario avanzado ❑ Pila de protocolos TCP/IP ❑ Protocolos de comunicación (RPC, TCP, UDP) ❑ Lenguajes de programación (C, C++) ❑ Legislación informática	❑ Sistemas Operativos (Windows, Linux, UNIX) a nivel de administrador ❑ Protocolos de seguridad (IPSec) ❑ Herramientas de Seguridad (scanners, firewalls, IDS) ❑ Programación de sockets (RAW, TCP, UDP) ❑ Criptografías ❑ Mecanismos de Seguridad (firmas digitales, certificados) ❑ Conocimientos de estándares ❑ Programación del Shell ❑ Computo Forense

- Tener iniciativa y habilidades de Planeación, organización y comunicación.

Habilidades Técnicas:

- Capacidad para detectar, aislar y resolver problemas

6 Habilidades personales

Proceso psicológico	***Características deseables***
Atención	Focalizada, que se mantenga por largos periodos de tiempo. Concentración de la atención.
Pensamiento	Capacidad de reflexión, de análisis y de síntesis. Habilidad para pensar creativamente. Habilidad para la toma de decisiones. Pensamiento flexible.
Memoria	Habilidad para organizar información en la memoria de corto y de largo plazo

Proceso psicológico	*Características deseables*
Comunicación y Lenguaje	Habilidad para expresar claramente sus ideas Habilidad para comunicarse con personas no expertas y expertas en el área.
Trabajo independiente	Habilidad para el trabajo independiente y autónomo.
Habilidades sociales	Habilidad para relacionarse con otros y para pedir ayuda cuando sea necesario. Habilidad para trabajar en equipos reales y virtuales.
Previsión	Habilidad para prever y solucionar conflictos
Conocimientos	Persona con conocimientos de experto en el área de cómputo
Establecimiento de prioridades y toma de decisiones	Habilidad para organizar el trabajo y las decisiones

7 Deberes y responsabilidades

Los deberes y responsabilidades del OSI deben establecerse claramente y requieren ser aprobados por la administración y/o directivos.

A continuación un listado de deberes y responsabilidades recomendados:

- El OSI tiene como principal responsabilidad la administración y coordinación diaria del proceso de Seguridad Informática de la institución donde labora.
- Tiene como responsabilidad asegurar el buen funcionamiento del proceso de Seguridad Informática de la institución. Debe ser el punto de referencia para todos los procesos de seguridad y ser capaz de guiar y aconsejar a los usuarios de la institución sobre cómo desarrollar procedimientos para la protección de los recursos de software y hardware.
- Una tarea clave para el OSI es guiar al cuerpo directivo y a la administración de la organización ante incidentes de seguridad mediante un Plan de Respuesta a Incidentes, con el fin de atender rápidamente este tipo de eventualidades.
- El OSI es responsable de proponer y coordinar la realización de un análisis de riesgos formal en seguridad de la información que abarque toda la organización.
- Es deber del OSI el desarrollo de procedimientos de seguridad detallados que fortalezcan la política de seguridad informática institucional.
- El OSI debe ser miembro activo del grupo de seguridad de CUDI, y mantener contacto con los OSI de otras organizaciones, estar suscrito a listas de discusión y de avisos de seguridad.
- Es responsabilidad del OSI promover la creación y actualización de las políticas de seguridad informática, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.

- Es responsabilidad del OSI el desarrollo de un Plan de Seguridad de la Información.
- El OSI debe atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.
- Es responsabilidad del OSI la elaboración de un Plan de Respuesta a Incidentes de Seguridad, con la finalidad de dar una respuesta rápida, que sirva para la investigación del evento y para la corrección del proceso mismo.
- El OSI debe crear una base de datos para el registro de incidentes en su red, la cual debe poder ser accedida por los miembros del grupo de seguridad de CUDI.
- Es responsabilidad del OSI coordinar la realización periódica de auditorias a las prácticas de seguridad informática, así como, dar seguimiento al corto plazo de las recomendaciones que hayan resultado de cada auditoria.
- El OSI debe ser el punto central dentro de la organización para la revisión de problemas de seguridad de la información existentes y de aquellos que se consideran potenciales.
- El OSI debe establecer la misión y metas internas en cuanto a la seguridad de la información, de acuerdo a la misión y metas organizacionales.

8 Sugerencias adicionales

Dado que el OSI debe contar con el respaldo de los directivos de la organización, se recomienda que tenga un puesto donde reporte directamente al director de Sistemas, Telemática o la entidad responsable de los servicios de redes e informáticos de la organización.

Es altamente recomendable que no sea una sola persona quien se encargue de la Seguridad, si es posible, apoyarlo con al menos 2 técnicos que faciliten las labores del OSI, si no lo es, se recomienda que se asignen colaboradores técnicos en otros departamentos que tengan la responsabilidad de colaborar con el OSI cuando éste lo requiera.

Se recomienda que las auditorias informáticas se lleven a cabo por un grupo ajeno al OSI, de preferencia el departamento de Contraloría interna, Auditorias o algo similar, de existir en la organización; en su defecto se contraten como servicio externo.

9 Datos autores

Mario Farias-Elinos
Universidad La Salle (ULSA)
Escuela de Ingeniería / Dirección de Posgrado e Investigación
Benjamín Franklin 47
Col. Hipódromo Condesa
México, DF, 06140
e-mail: elinos@ci.ulsa.mx

María Concepción Mendoza Díaz
Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE)
Dirección de Innovación y Desarrollo
Km. 107, Carretera Tijuana-Ensenada
Ensenada, BCN, 22860
e-mail: comedi@cicese.mx

Juan Gabriel Castillo Martínez
Complejo Cangrejera
Grupo Celanese
Depto. EHS
Tel.-921-21-1-50-36
(Dirección y ciudad)
Email:jcastillo@celanese.com.mx

Carlos A. Vicente Altamirano
Universidad Nacional Autónoma de México (UNAM)
Dirección General de Servicios de Cómputo Académico (DGSCA)
Centro de Operación de la Red
Circuito Exterior S/N, C.U.
México, DF, 04510
e-mail: carlos@antares.noc.unam.mx

Lidia Gómez Velazco
Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE)
Dirección de Telemática
Km. 107, Carretera Tijuana-Ensenada
Ensenada, BCN, 22860
e-mail: lgomez@cicese.mx

Referencias

[1] CERT/CC Statistics 1998-2003, http://www.cert.org/stats/cert_stats.html, 2004

[2] M. Farias-Elinos, Ma. C, Mendoza-Diaz & L. Gómez-Velazco. **"Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática"**, Techno-Legal Aspects of Information Society and New Economy: an Overview, Marzo 2003