FACULTAD DE INGENIERIA, ARQUITECTURA Y URBANISMO

ESCUELA DE INGENIERIA DE SISTEMAS

PERFILES PROFESIONALES PARA SEGURIDAD INFORMÁTICA

Un enfoque práctico

Autor:

Salazar Lluén Daniel

Chiclayo, Octubre del 2009

PERFILES PROFESIONALES PARA SEGURIDAD INFORMÁTICA

Un enfoque práctico

Autor:

Salazar Lluén Daniel

CONTENIDO

INDICE DE GRAFICOS

INDICE DE CUADROS

INDICE DE ANEXOS

1. INTRODUCCIÓN

La seguridad informática, que contempla en la actualidad un importante número de disciplinas y especialidades distintas y complementarias, se ha convertido en una pieza fundamental en el entramado empresarial, industrial y administrativo de los países.

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 problema de seguridad que se presentan dentro de las instituciones, tales como intrusiones, robo de información, problemas de virus, entre otros más, mejor conocidos como incidentes; agregando la falta de una legislación informática donde se tipifique los delitos informáticos. 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.

Es por ello que poco a poco las organizaciones han tomado conciencia del problema de la seguridad informática y paulatinamente incorporan la figura del Oficial de Seguridad Informática (OSI).

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 presentes.

2. LA FUNCION DE SEGURIDAD INFORMÁTICA EN LA EMPRESA

Este siempre ha sido un tema complicado porque cada organización es distinta y no hay un acuerdo sobre la mejor manera de organizar un área de seguridad informática en una empresa.

2.1 Componentes principales de un Área de Seguridad Informática

Existen diversas funciones que debe desempeñar un área de seguridad informática y éstas se pueden agrupar de la siguiente manera:

a. Normatividad
b. Operaciones (O Producción)
c. Supervisión (O Soporte)
d. Desarrollo

Hay un par de áreas que no son tan comunes: normatividad y desarrollo. Al revisar las responsabilidades y funciones de cada área quedará más claro el por qué. Por lo pronto les comento que es menos probable encontrar estas 2 áreas en empresas medianas o pequeñas, mientras que en empresas grandes es más común que existan las 4 áreas junto con la figura del líder de área.

Líder de área: Esta figura, a la cual se le suele conocer como CISO (*Chief Information Security Officer* - Oficial de Seguridad informática). Entre sus responsabilidades se encuentran:

- Administración del presupuesto de seguridad informática
- Administración del personal
- Definición de la estrategia de seguridad informática (hacia dónde hay que ir y qué hay que hacer) y objetivos
- Administración de proyectos
- Detección de necesidades y vulnerabilidades de seguridad desde el punto de vista del negocio y su solución

El líder es quien define, de forma general, la forma de resolver y prevenir problemas de seguridad con el mejor costo beneficio para la empresa.

A. Normatividad -

Es el área responsable de la documentación de políticas, procedimientos y estándares de seguridad así como del cumplimiento con estándares internacionales y regulaciones que apliquen a la organización. Dado que debe interactuar de forma directa con otras áreas de seguridad y garantizar cumplimiento, es conveniente que no quede al mismo nivel que el resto de las áreas pero todas reportan al CISO. Por esta razón se le suele ver como un área que asiste al CISO en las labores de cumplimiento.

B. Operaciones -

Es el área a cargo de llevar a cabo las acciones congruentes con la estrategia definida por el CISO lograr los objetivos del área (en otras palabras, la "gente que está en la trinchera").

Entre sus responsabilidades se encuentran:

- Implementación, configuración y operación de los controles de seguridad informática (Firewalls, IPS/IDS, antimalware, etc.)
- Monitoreo de indicadores de controles de seguridad
- Primer nivel de respuesta ante incidentes (típicamente a través de acciones en los controles de seguridad que operan)
- Soporte a usuarios
- Alta, baja y modificación de accesos a sistemas y aplicaciones
- Gestión de parches de seguridad informática (pruebas e instalación)

C. Supervisión -

Es el área responsable de verificar el correcto funcionamiento de las medidas de seguridad así como del cumplimiento de las normas y leyes correspondientes (en otras palabras, brazo derecho del área de normatividad).

Entre sus responsabilidades se encuentran:

- Evaluaciones de efectividad de controles
- Evaluaciones de cumplimiento con normas de seguridad
- Investigación de incidentes de seguridad y cómputo forense (2° nivel de respuesta ante incidentes)
- Atención de auditores y consultores de seguridad

Noten que las actividades de monitoreo las realiza el área de operaciones y no el área de supervisión. Esto es porque el monitoreo se refiere a la vigilancia del estado de la seguridad de la empresa a través de los controles, pero las actividades del área de supervisión se limitan a la vigilancia de las actividades de seguridad que realizan otras áreas. La única excepción es la investigación de incidentes. Operaciones no investiga porque en algunos casos podrían se juez y parte. Por ejemplo, en el caso de una intrusión no es válido que el mismo personal que operaba los controles que protegían el servidor investiguen el suceso porque no puede haber objetividad (aunque no sea el propósito de la investigación, de cierta manera los resultados de la misma podrían calificar indirectamente la efectividad del personal del área de operaciones).

D. Desarrollo -

Es el área responsable del diseño, desarrollo y adecuación de controles de seguridad informática (típicamente controles de software).

Entre sus responsabilidades se encuentran:

- Diseño y programación de controles de seguridad (control de acceso, funciones criptográficas, filtros, bitácoras de seguridad de aplicativos, etc.)
- Preparación de librerías con funciones de seguridad para su uso por parte del área de Desarrollo de Sistemas
- Soporte de seguridad para el área de Desarrollo de Sistemas
- Consultoría de desarrollos seguros (integración de seguridad en aplicaciones desarrolladas por Sistemas).

Básicamente se trata de un área de desarrollo enfocada a cuestiones de seguridad. La razón de requerir un área dedicada para esto es que la integración de controles efectivos en software es una tarea muy compleja; el perfil de un programador promedio no incluye experiencia ni conocimientos en seguridad (y particularmente en criptografía). Esta es la razón por la cual sólo las grandes empresas cuentan con un área de desarrollo de seguridad que está formada por especialistas en vez de programadores ordinarios.

2.2 ¿Dónde debe estar la función de Seguridad Informática?

Este es otro problema para el cual no hay una respuesta única. Podemos empezar por listar las áreas o direcciones de las cuales no debe de depender el área de Seguridad Informática:

- **Sistemas -**
  Mucho de lo que vigila el área de operaciones de seguridad son precisamente los sistemas y las redes de telecomunicación. El área de sistemas tiene como prioridad la operación, y los controles tienden a impactar de cierta forma el desempeño y flujo operativo (pero no por esto dejan de ser necesarios). El hecho de que Seguridad Informática dependa del Área o Dirección de Sistemas genera conflictos de interés.

- **Auditoría Interna -**
  La función de auditoría es verificar la efectividad y existencia de controles en todas las áreas de la organización (incluyendo Seguridad). Auditoría no opera, pero el área de Operaciones de Seguridad sí, por lo que habría conflictos de interés (Auditoría revisaría en parte algo que ella misma hace, lo que la convertiría en juez y parte)

- **Unidades operativas del negocio -**
  Por la misma razón que para el área de Sistemas

Por supuesto hay algunas áreas que no hace mucho sentido que incluyan la función de Seguridad Informática (Recursos Materiales y Recursos Humanos, por ejemplo), pero hay áreas donde sí puede colocarse esta función, como por ejemplo:

- **Cumplimiento -**
  Cumplimiento no es Auditoría. El área de Cumplimiento define establece las normas internas y supervisa su aplicación de la misma manera que las áreas de Normatividad y Supervisión lo hacen dentro de la función de Seguridad Informática.

- **Jurídico -**
  Esta área atiende todos los asuntos legales de la empresa. Como tal el tener al área de Seguridad dentro de la misma constituye un excelente apoyo para implementar controles que garanticen el cumplimiento de la ley.

- **Finanzas -**
  Esta área se asegura del buen uso del dinero de la empresa. Contar con un área de Seguridad Informática le permite asegurar la implementación adecuada de controles para minimizar riesgos que tengan impacto económico (fraudes, fugas de información, etc.). Dada la

dependencia de los sistemas informáticos para el manejo de las finanzas en la actualidad este esquema es una buena opción para algunas empresas.

- **Riesgos -**

  El área de Seguridad Informática dependiendo del área de riesgos permite controlar y evaluar la mitigación de aquellos riesgos que afectan a los sistemas informáticos y la información que se almacena, procesa, genera o transmite a través de los mismos. Dada la dependencia que tienen muchos procesos productivos de los sistemas de información en la actualidad, ésta es una buena opción también para muchas empresas.

- **Dirección General** –

  Permite tener un estricto control de los recursos informáticos de la Empresa. Desafortunadamente este esquema es difícil por la diferencia de lenguajes y niveles entre ambas áreas así como las prioridades y el poco tiempo que suele tener la Dirección General, pero algunas organizaciones así lo tienen (por ejemplo, algunos Bancos).

Podría parecer que la existencia de las áreas de Operaciones y Desarrollo de Seguridad generan un conflicto de interés en los casos anteriores, pero no es así, ya que el conflicto está controlado por la separación interna de funciones dentro de la misma Área de Seguridad; con respecto al resto de las áreas, no se interfiere con su operación y existe separación de funciones, ya que el área de Operaciones de Seguridad realiza únicamente funciones de soporte al negocio y no interviene de forma directa en dichos procesos. Adicionalmente, la existencia de un área de Auditoría Interna separada permite una revisión imparcial de las funciones de Seguridad que dependa de cualquiera de las 3 áreas mostradas anteriormente. En ninguno de los casos anteriores la implementación y supervisión de controles de seguridad informática es un factor tan importante debido a su orientación a controlar; a diferencia del caso de Sistemas, donde su orientación es a producción.

De todas maneras, no hay un área ideal de dónde colgar al área de Seguridad Informática (si la hubiera, todo mundo lo haría así) quizás la dependencia directa de la Dirección General pero no es viable o fácil de lograrla en muchas empresas.

3. LA FORMACION EN SEGURIDAD INFORMÁTICA

Antes de entrar en materia, es menester recalcar que la seguridad informática tal y como hoy en día se reconoce, es un compendio de especialidades, técnicas, disciplinas, protocolos, etc. que van, desde lo más básico de la seguridad física de los sistemas informáticos, hasta temas de complejos protocolos criptográficos y técnicas de cifra aún sin una aplicación real o comercial, pasando por las políticas y planes de seguridad, recuperación ante desastres, auditoría y forensia informática, seguridad en redes y negocios, plataformas seguras, virología informática, cifra, firma digital, legislación sobre seguridad, etc. Por lo tanto, no se trata ya solamente de una ciencia asociada a las matemáticas y la criptografía, como podría pensarse hacia mediados del siglo pasado, sino un cúmulo de disciplinas en las que intervienen las matemáticas, la informática, las telecomunicaciones, la telemática, el derecho, la gestión de empresas, el análisis de riesgos, etc.

¿Cuál es la realidad en los países iberoamericanos en cuanto a la formación técnica universitaria? Si bien hay algunas excepciones dignas de detallar, la visión general en este aspecto es que aquel boom experimentado en las universidades españolas a mediados de los 90, que a la postre ha derivado en una oferta actual en torno a las 40 asignaturas y que en la practica no exista universidad con carreras tecnológicas de informática y/o telecomunicaciones que no incluya en su oferta asignaturas optativas relacionadas directamente con la seguridad informática y la criptografía, no ha llegado aún a estos países.

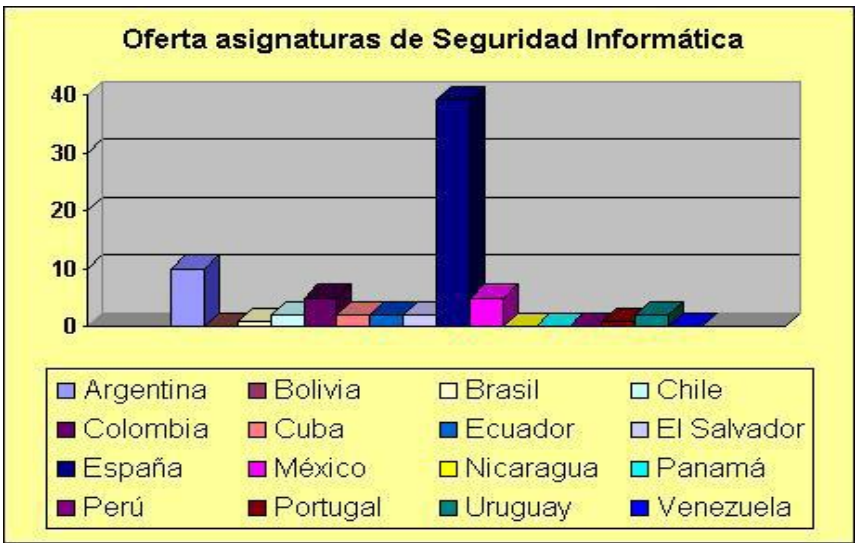
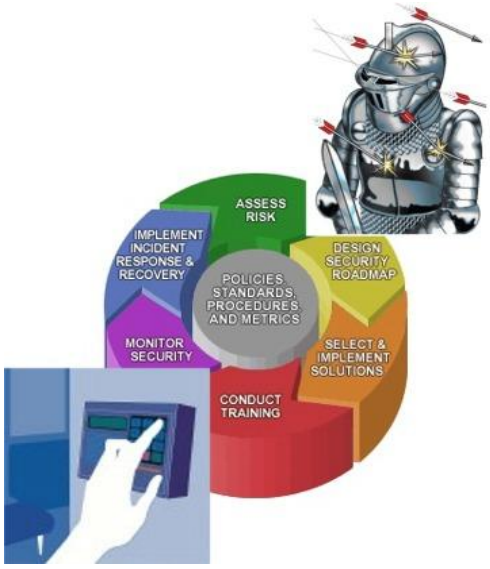


Figura 1: Oferta de formación de pregrado universitaria en Seguridad Informática.

La figura 1 muestra la oferta docente en asignaturas de pregrado para algunos países de Iberoamérica. No se han incluido aquellos países en los que no se tenía a mano una información fidedigna; no obstante en ellos cabe esperar un valor verdaderamente bajo en torno a dicha oferta docente, en algunos casos incluso ninguna. Asimismo, ciertos países que en la grafica muestran una oferta nula, podrían en realidad estar ofreciendo alguna asignatura pero, en todo caso, esto sería sólo anecdótico en el marco general y no cambiaría el primer golpe de efecto de la información que puede sacarse de ella, en cuanto a la comparación relativa entre España con un desarrollo docente muy importante, tres o cuatro países de Latinoamérica con un cierto desarrollo sostenido, y otros prácticamente en situación de inicio.

4. ¿EXPERTOS, ESPECIALISTAS O PROFESIONALES EN SEGURIDAD INFORMÁTICA?

Es frecuente escuchar los términos "experto en seguridad informática", "especialista en seguridad informática" o "profesional en seguridad informática", tres palabras, tres contextos que nos deben animar a una reflexión personal y profesional alrededor de aquellos interesados que enfrentan día a día los retos de la inseguridad informática. (HOWARD 2008, BRATUS 2007)



De acuerdo con el diccionario de la Real Academia Española - RAE, existen diferencias importantes entre las tres palabras: experto, especialista y profesional.

Para la RAE un experto, viene del latín expertus, alguien experimentado en algo, alguien que ha probado o tratado con algo. Se asocia generalmente a un perito. Un especialista, es alguien que cultiva o practica una rama determinada de un arte o una ciencia, de la que tiene particulares conocimientos y habilidades. Finalmente un profesional, es una persona que ejerce su profesión con relevante capacidad y aplicación.

Mirando estas tres definiciones se puede sugerir que los que se dedican a la seguridad informática (o inseguridad de la información), siendo estrictos en el manejo de las anteriores, responden a un proceso evolutivo que los cautiva y los lleva a explorar su propia curiosidad con eventos que desafían lo establecido, para generar nuevas inquietudes y así, continuar aprendiendo. Es un

proceso de desaprendizaje (POURDEHNAD, J., WARREN, B., WRIGHT, M. y MAIRANO, J. 2006) que invita a reconocer que no sabemos y que debemos estar atentos a descubrir las nuevas propuestas que nos ofrece el evento que se estudia.

Un experto en seguridad informática, siguiendo lo sugerido por la Real Academia, es alguien que se ha enfrentado a la inseguridad de la información, alguien que se ha enfrentado a la incertidumbre que genera la falla, a la presión que se manifiesta en ese momento para tomar acciones que ponen a prueba su conocimiento y experiencia previa en situaciones semejantes (nunca iguales). Las acciones acertadas o no, son el insumo de las futuras que esta persona enfrente, cuando nuevamente sea sorprendida por un nuevo episodio de la inseguridad informática.

Con el paso del tiempo este experto, desarrolla un instinto o intuición en el arte de conocer y descubrir la inseguridad; en ese momento se transforma en un ***especialista, no de seguridad informática, sino de inseguridad de la información***. El enfrentamiento constante con la inseguridad y la falla, genera en este personaje una mente más abierta y sistémica, más llevada por las relaciones y efectos emergentes, que por eventos puntales. El especialista estructura una red de conocimientos y prácticas que proponen soluciones emergentes, generalmente diferentes y alternas a las que pudiesen ofrecer lo que dicen las buenas prácticas actuales. Recordemos que las buenas prácticas, nacen del reconocimiento de acciones que han demostrado ser útiles en el tiempo.

Finalmente el ***profesional en seguridad informática***, sería una persona que ejerce una profesión, un oficio, que generalmente se encuentra estructurado bajo una serie de lineamientos y conceptos que son avalados y normados por entes reguladores en temas académicos o científicos. De esta forma, existen las profesiones como la ingeniería, el derecho, la medicina, entre otras.

En este contexto y considerando que a la fecha no existe un acuerdo nacional o internacional sobre currículos en seguridad de la información, tratar de responder la pregunta *¿qué debo estudiar para aprender seguridad informática?* es un reto que aún tenemos que enfrentar y donde tenemos grandes oportunidades para proponer y avanzar.

El profesional en seguridad informática actualmente es tema de discusión y análisis en diversos foros internacionales. Iniciativas como las efectuadas en la Universidad Politécnica de Madrid, orientada por el Dr. Jorge Ramio Aguirre (ver http://www.criptored.upm.es, sección docencia), las consideraciones de formación en seguridad informática (particularmente orientadas al desarrollo de software seguro) sugeridas por el Dr. Mattew Bishop (http://nob.cs.ucdavis.edu/bishop/papers/), de

la Universidad de California, en Davis, entre otras iniciativas (ver otras fuentes adicionales) son elementos que nos dicen que debemos continuar analizando posibilidades y estrategias para acercarnos cada vez más a un acuerdo base sobre lo que un profesional de seguridad informática debería estudiar.

La seguridad informática en su evolución desde los años 50's, ha venido mostrando patrones característicos e inquietudes particulares, generalmente atadas con la evolución de la inseguridad de la información. Si bien, cada vez que evolucionan las plataformas tecnológicas, la inseguridad se transforma, es importante observar que los profesionales de seguridad no lo hacen de la misma manera, pues, deben recorrer nuevamente la curva de aprendizaje que les exige el nuevo contexto computacional o de negocio que se enfrenta.

En razón a lo anterior y no obstante, los aspectos evolutivos de las tecnologías de información (ver publicación anterior de este blog), si se requiere adelantar un ejercicio de exploración y análisis sobre las prácticas de seguridad y los patrones que sugiere la inseguridad para delinear un perfil evolutivo de aprendizaje de la seguridad, que considere la exposición de los interesados sobre temas conocidos en seguridad, para avanzar y conocer comportamientos desconocidos ocasionados por la inseguridad. Esto permite disminuir el riesgo de que el experto (siguiendo la definición de RAE) sea víctima de "una falsa sensación de seguridad" y mantenga un mínimo de paranoia, requerida para mantenerse vigilante.

Si mantenemos a este experto, en proceso evolutivo de des aprendizaje, es decir, confrontando las buenas prácticas, los mecanismos de seguridad y sus procesos de construcción y afinamiento, inspeccionando código en búsqueda de funciones inseguras, analizando comportamientos adversos de personas en las organizaciones, entre otros elementos, pronto tendremos un especialista que de manera sistémica (KEILY, L y BENZEL, T. 2006) observe y diagnostique una situación antes de que ocurra. Si bien, no podrá anticiparse a todo lo que puede ocurrir, si estará atento a nuevas relaciones que la inseguridad pueda sugerir.

Como hemos visto hasta el momento y sabiendo que la inseguridad de la información es un "camino que se revela al andar", las personas que se dedican a la seguridad de la información, bien sean expertas, especialistas o profesionales siempre tendrán algo en común, una misión y deseo que los marca, una convicción de vida personal y profesional que los une: el reto de conocer, descubrir y aprender de la inseguridad de la información.

5. PERFIL DEL OFICIAL DE SEGURIDAD INFORMÁTICA - OSI

5.1 Definición

Por definición, el OSI es la persona responsable de planear, coordinar y administrar los procesos de seguridad informática en una organización.

De acuerdo con Gastón Tanoira, gerente de soluciones de Seguridad de Cisco Systems en América Latina, aunque el puesto de OSI aún es esporádico, cada día se va viendo más en las en las organizaciones para que haya soluciones integradas. "Antes había un jefe de seguridad de red, otro de aplicaciones, uno de infraestructura y ahora se busca una consolidación en una sola persona que atienda todas las necesidades de seguridad corporativa" comentó Tanoira, que bajo este cargo tiene la responsabilidad de liderar la estrategia del mercado de seguridad en América Latina y el desarrollo empresarial para este nicho.

5.2 Misión

El OSI 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.

El propósito de tener la figura del OSI es contar con 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 presentes.

5.3 Objetivos

Ahora bien entre los objetivos del OSI están:

- 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 auditorías 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.

En tanto, para Vincent Gullotto, vicepresidente de investigación de McAfee Avert, "actualmente existen cerca de 110.000 tipos de programas relacionados con vulnerabilidades, que incluyen: virus, spam, troyanos, gusanos y es muy importante destacar que se ha incrementado la cantidad; de 1998 a 1999 el aumento fue dramático y eso se debió a un creador de virus que hizo 15.000 él solo. La buena noticia es que todos estos virus eran variantes de uno solo creado un año atrás", comentó el experto, lo cual hace más urgente la necesidad de contar con una persona especializada en el área de seguridad informática.

5.4 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	Sistemas Operativos (Windows, Linux, UNIX) a nivel de administrador
Stack de TCP/IP	Protocolos de seguridad (IPSec)
Protocolos de comunicación (RPC, TCP, UDP)	Herramientas de Seguridad (scanners, firewalls, IDS)
Lenguajes de programación (C, C++)	Programación de sockets (RAW, TCP, UDP)
Legislación	Criptografías
	Mecanismos de Seguridad (firmas digitales, certificados)
	Conocimientos de estándares
	Programación del Shell
	Computo Forense

Cuadro 1: Conocimientos y experiencia en Seguridad Informática.

5.5 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
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 ene quipos 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

Cuadro 2: Habilidades Personales del OSI.

5.6 Deberes y responsabilidades

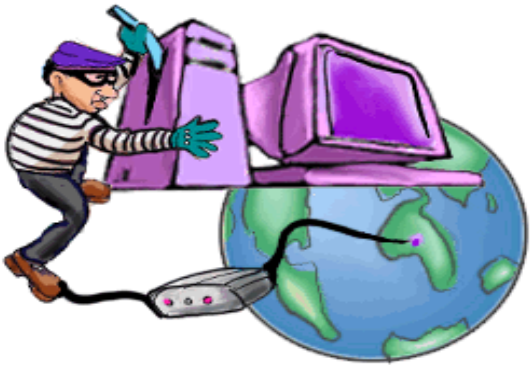
Los deberes y responsabilidades del OSI deben establecerse claramente y requieren ser aprobados por la administración y/o directivos.

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.
- 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 ISO 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 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.
- Es responsabilidad del OSI coordinar la realización periódica de auditorías a las prácticas de seguridad informática.
- 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 ISO debe establecer la misión y metas internas en cuanto a la seguridad de la información, de acuerdo a la misión y metas organizacionales.

A pesar de los esfuerzos de las corporaciones por adoptar de OSIs, de acuerdo con Tanoira, muchas empresas aún se conforman solo con poner un firewall y creen que con ello se soluciona el problema de la seguridad informática. "Las organizaciones latinoamericanas no están preparadas para defenderse de ataques informáticos. La seguridad debe ser parte del ADN de la red", comentó Tanoira.

Mientras, Gullotto considera que la mayoría de PCs no tienen la rutina de correr el escáner del antivirus. "La mayoría de usuarios creen que con solo la instalación del antivirus están protegidos y para complicar la cosa, la gente quiere conectarse todo el día a Internet y para terminar, la PC no tiene un firewall que la proteja. Por eso nosotros, los desarrolladores de antivirus tenemos que acelerar el paso, cada hora, cada día". De acuerdo con el vicepresidente de investigación de McAfee Avert, en la actualidad solo un 20 por ciento de las empresas a nivel mundial han adoptado la posición del OSI dentro de su estrategia de seguridad informática.



CONCLUSIONES

La Seguridad de la Información se ha convertido en un área clave en el mundo interconectado de hoy. Día a día, en los principales medios de comunicación se repiten los ataques de virus, hackers y otros peligros tecnológicos. Desde el ámbito corporativo y gubernamental**, la búsqueda de profesionales en Seguridad Informática** se ha duplicado y la tendencia sigue en **aumento**.

Es por eso que no basta con tener un adecuado conocimiento técnico de la Seguridad Informática para ser un profesional de éxito en la materia, sino que hay que dominar el desarrollo de estrategias de organización de Seguridad acordes para cada empresa y de los esquemas de control que verifiquen su cumplimiento.

La creciente exigencia del cumplimiento de estándares en Tecnología Informática en general y en Seguridad en particular hace del profesional, además del conocimiento técnico y de gestión de la Seguridad, deba tener un acabado dominio de normas como ISO-IEC 17799 (estándar mundial de la Seguridad Informática) y su nueva versión,

BIBLIOGRAFÍA

NORMAS:

- NTP-ISO/IEC 17799:2004.
  Tecnología de información. Código de buenas practicas para la gestión de la seguridad de la información.
- NTP-ISO /IEC 27001:2005
  Sistema de Gestión de Seguridad de Información
  www.shellsec.net

LIBROS TUTORIALES

- "Seguridad en redes de datos".
  Instituto Nacional de Estadística e Informática (INEI)
- "Conceptos sobre Seguridad de la Información".
  Instituto Nacional de Estadística e Informática (INEI)
- Introducción de las enseñanzas de seguridad informática en los planes de estudio de las Ingenierías del siglo XXI.
  http://www.criptored.upm.es/paginas/docencia.htm#gteoria
- Certificaciones en Seguridad Informática. Conceptos y Reflexiones.
  http://www.criptored.upm.es/paginas/docencia.htm#gteoria

SITIOS WEB

- La Seguridad Total
  http://members.xoom.com/segutot/la.htm
- Amenazas Deliberadas a la Seguridad de la Información
  http://www.iec.csic.es/criptonomicon/amenazas.html
- La Seguridad Informática en las Redes
  www.geocities.com/SiliconValley/Bit/7123/la.htm
- moon.act.uji.es/~inigo/seg-lfaq.html
- www.utp.ac.pa/seccion/topicos/seguridad/seguridad.html
- www.fciencias.unam.mx/revista/soluciones/30s/No33/seg-red.html
- www.geocities.com/SiliconValley/Drive/3491/_seguridad.html

- http://seguridad.internet2.ulsa.mx/congresos/2003/cudi1/perfil_osi.pdf
- http://www.tecnoempleo.com/oferta-empleo/consultor-seguridad-informatica/c807p954ajad2kba32a9
- www.criptored.upm.es/investigacion/agora_44_criptored.pdf
- www.whyfloss.com/pages/conference/static/editions/bsas07/charla18.pdf
- www.upb.edu.co/portal/page?_pageid=1134,32665698&_dad=portal&_schema=PORTAL
- candadodigital.blogspot.com/2007/10/la-funcin-de-seguridad-informtica-en-la.html
- www.upbbga.edu.co/programas/espseginfo/seginfo.html
- marianariva.blogspot.com/2007/07/perfiles-de-it-seguridad-informtica.html
- www.udi.edu/page.asp?page=sistseguridad
- www.ali.es/uploads/5019352c-44a3-6930.pdf
- www.silocal.org/perfiles/fichas/tic0012.pdf
- www.zonajobs.com.ar/trabajo=452532_ingeniero-de-seguridad-informatica.asp

ANEXOS

A. PRINCIPALES FUNCIONES PARA EL RESPONSABLE DE LA SEGURIDAD DE LA INFORMACION

A continuación se presenta una lista de principales funciones para el responsable de la seguridad de la información:

- Proveer un apoyo administrativo directo para la instalación de los sistemas de seguridad que aseguren el uso de todos los sistemas en línea.
- Establecer objetivos para el desarrollo futuro de los sistemas de seguridad a medida que vayan evolucionando los sistemas en línea.
- Determinar los requisitos de recursos especiales, tales como recursos humanos, capacitación, equipamiento y planes de desarrollo, programas de seguridad y los presupuestos relacionados a la seguridad.
- Negociar con niveles múltiples de programación de apoyo de la gerencia para asegurar la integración de los objetivos de seguridad asignados, con la estrategia de procesamiento de datos a largo alcance.
- Analizar continuamente y evaluar las alternativas de seguridad para determinar que línea de acción debe seguir basada en las implicaciones técnicas, conocimiento de los objetivos del negocio y la política de protección de activos corporativos, procedimientos y requerimientos.
- Asegurar que los proyectos asignados estén alineados con los objetivos de seguridad corporativa y sean completados de acuerdo con el programa dentro de los gastos consignados; informar a la gerencia tan pronto como sea posible de los problemas que podría materialmente afectar los objetivos, programas y gastos; sugerir soluciones alternativas.
- Supervisar el uso de todos los sistemas en línea para descubrir y actuar sobre los accesos desautorizados, y uso de los datos del propietario del negocio.
- Dirigir auditorías de seguridad, participar en evaluaciones de seguridad y proveer guía y asistencia, como es debido, para facilitar la realización de los programas de protección del patrimonio de la institución.
- Revisar los esfuerzos de documentación asociados con diversos sistemas de seguridad.

B. SISTEMAS CON ÉNFASIS EN SEGURIDAD INFORMÁTICA

¿Por qué estudiar Ingeniería de Sistemas con énfasis en Seguridad Informática en la UDI?

- Porque estamos viendo la era de la información y la tecnología es una herramienta fundamental del éxito profesional.
- Porque la UDI te permite, no solo conocer los aspectos de la tecnología de punta, sino estrategias gerenciales que complementen tu formación.
- Porque esta carrera te permite desarrollarte en un extensa gama de opciones laborales.
- Porque el mundo evoluciona día a día en lo que respecta a la tecnología. Por ende, siempre es necesario contar con profesionales idóneos que manejen sistemas.
- Porque el 85% de los estudiantes de Ing. de Sistemas que realizan práctica empresarial, se quedan laborando en la empresa donde realizaron la práctica.

Perfil del Estudiante de la Ingeniería de Sistemas (Seguridad Informática)

- Interés y aptitud numérica
- Detallista
- Paciente
- Cálculo numérico
- Alto nivel de razonamiento lógico
- Imaginación creadora

Oportunidades de Trabajo

Los egresados de la carrera pueden desempeñarse en cualquier empresa u organización sea pública o privada. Inicialmente podrán asumir cargos como: Analista Programador de Sistemas, Administración de Redes, Soporte Técnico, Asistente de Administración del Centro de Computo, Supervisor de Herramientas de Oficina, Administrador de Internet (WebMaster). A mediano plazo, se podrán desempeñar como Consultores y Ejecutivos Senior.

Plan de Estudios

Primer Cuatrimestre	**Sexto Cuatrimestre**
• Introducción a los Negocios • Inglés I • Informatica Básica • Programación I • Teoría de la Administración • Cálculo Diferencial e Integral	• PRODES • Contabilidad de Costos I • Análisis y Diseño de Sistemas I • Historia de Panamá • Métodos Númericos • Introducción a Redes
Segundo Cuatrimestre	**Séptimo Cuatrimestre**
• Inglés II • Programación II • Arquitectura de Computadores • Estructura de Datos • Cálculo Diferencial e Integral II • Programación Aplicada	• Metodología de la Investigación • Sistemas Operativos • Análisis y Diseños de Sistemas II • Problemática y Perfil del Emprendedor • Introducción a la Seguridad Informática • Inglés V
Tercer Cuatrimestre	**Octavo Cuatrimestre**
• Inglés III • Programación III • Estadística I • Contabilidad de Costos I • Física I • Álgebra Lineal • Dibujo Asistido por Computadora	• Recursos Humanos I • Mercadeo I • Derecho Intelectual y de la Propiedad Industrial • Diseño y Evaluación de Proyecto • Circuitos Lógicos • Inglés VI
Cuarto Cuatrimestre	**Noveno Cuatrimestre**
• Inglés IV • Programación IV • Ética Empresarial • Física II • Ecuaciones Diferenciales • Introducción a Base de Datos	• Organización de Empresas • Principio de Economía • Administración de Seguridad Informática • Continuidad de Negocios • Auditoría Informática • Investigación de Operaciones
Quinto Cuatrimestre	**Décimo Cuatrimestre**
• Programación V • Administración de Base de Datos • Geografía de Panamá • Contabilidad Básica • Mecánica • Español	• Prope • Ecología y Medio Ambiente • Laboratorio de Seguridad Informática • Sistemas Distribuidos • Administración de Tecnología de la Información **Total de Asignaturas:** 58 **Total de Créditos:** 183 **Titulo Otorgado:** Ingeniería en Sistemas con Énfasis en Seguridad Informática.

C. UNIVERSIDAD PONTIFICIA BOLIVARIANA

Perfil del Profesional del Especialista en Seguridad Informática

El especialista en Seguridad Informática debe ser un profesional con aptitud para aplicar y promover metodologías actualizadas que conduzcan a la práctica de una cultura de Seguridad Informática; capaz de discernir entre las ventajas y desventajas asociadas con el diseño y administración de políticas de seguridad para los recursos informáticos de una organización; capaz de diseñar estrategias que puedan garantizar la seguridad de los recursos informáticos de tal forma que se convierta en un valor agregado en los procesos de negocio entre cliente y empresa, basado en estándares nacionales e internacionales y aspectos éticos-legales que rigen la Seguridad Informática.

D. UNIVERSIDAD TECNOLÓGICA DEL PERU

Somos los primeros y únicos en Ingeniería de Seguridad Informática, para ello, la Universidad Tecnológica del Perú, cuenta con una plana docente altamente calificada, un innovador plan de estudios y múltiples laboratorios modernos que te permitirán desempeñarte con éxito en cualquier lugar del mundo, aplicando los conocimientos adquiridos durante los once ciclos de preparación universitaria en tecnologías de seguridad informática.

Ingeniería de Seguridad Informática

El Ingeniero en Seguridad Informática es un profesional de alta demanda en el mercado nacional e internacional, capaz de diseñar, construir y mantener en operación la seguridad de las sistemas tanto de área local como de área extendida, bajo altos estándares de calidad de servicio, respaldado por su formación en el área de las técnicas de seguridad y la profunda base en conocimientos de la Tecnología de la Información y Computacional, conocimientos que le permitirán afrontar las exigencias de cambio y desarrollo tecnológico acelerado.

E. PERFIL INGENIERO DE SEGURIDAD INFORMÁTICA

- Analizar y Gestionar los riesgos del sistema informático, determinar sus vulnerabilidades y establecer las medidas de salvaguarda que garanticen la confidencialidad, integridad y disponibilidad de la información de acuerdo a un riesgo residual asumido por la organización.
- Organización de la seguridad y clasificación de los recursos.
- Seguridad física y del entorno.
- Protección y control de acceso al sistema.
- Seguridad en las Comunicaciones.
- Seguridad en la operación y producción.
- Seguridad en el software tanto de los sistemas operativos, bases de datos y aplicaciones.
- Seguridad en las personas que le utilizan.
- Definir las especificaciones de seguridad para que los sistemas informáticos cumplan la legislación y normas estándar de seguridad nacionales e internacionales.
- Diseñar la seguridad del sistema informático según las especificaciones establecidas.
- Dirigir los proyectos de Seguridad basados en las leyes y normas estándar que permiten a la organizaciones Públicas y Privadas validar (ó certificar) su cumplimiento y obtener las acreditaciones de seguridad exigidas por ley y normas adoptadas.
- Gestionar el Plan de Seguridad Informática y mantenerle actualizado, muy especialmente el plan de continuidad del negocio.
- Velar por el cumplimiento legal de los sistemas informáticos utilizados en la organización: datos personales, propiedad intelectual, software legal, etc.
- Colaborar con la Dirección en la resolución de incidentes de seguridad y especialmente en aquellos que puedan dar origen a delitos y faltas tipificados en el derecho Penal, Civil, Convenios internacionales, etc.
- Colaborar con la Autoridad Judicial si los incidentes de seguridad acaecidos lo exigen en defensa de los intereses de la organización, ó si son críticos para el Estado: seguridad nacional, seguridad de las personas, medio ambiente, etc.

F. JEFE DE SEGURIDAD INFORMÁTICA

Función

- Mantener la integridad, disponibilidad y confidencialidad de la información de la empresa.

Obligaciones y responsabilidades

- Definir la política de seguridad informática a seguir por medio de normas y procedimientos que mantengan el grado de integridad, disponibilidad y confidencialidad de la información necesario para la misión de la empresa sin afectar la operatividad de los procesos de la misma. La política puede también ser fijada por una consultoría externa o por la casa matriz.
- Seleccionar herramientas y proveedores para llevar adelante las normas y procedimientos.
- Definir la estructura de restricciones y excepciones de acceso a la información de todo el personal, de acuerdo a las pautas de la política de seguridad y a las necesidades de acceso de los usuarios de acuerdo a su función.
- Diseñar el plan de contingencias de la empresa, implementarlo y ensayarlo periódicamente. Este plan también puede se provisto por una consultoría externa o por la casa matriz.
- Fijar junto con los otros jefes de área cuales son las necesidades, seleccionar a los proveedores y supervisar las instalaciones.

Interacción

- Gerente de sistemas, otros jefes de área y, en caso de necesidad, con todo el personal de la empresa

Conocimientos y habilidades requeridos

- Título universitario en análisis de sistemas, ciencias de la computación o ingeniería en sistemas con algún tipo de curso en seguridad informática (ya que por ahora no existen postgrados en el tema).
- Cuatro años de experiencia en el área de seguridad de sistemas, soporte técnico de herramientas de seguridad informática o similar

G. ESPECIALISTA EN SEGURIDAD INFORMÁTICA

OTRAS DENOMINACIONES

- Técnico Seguridad Informática; Técnico Sistemas Expertos en Seguridad; Consultor Seguridad/LOPD

FORMACIÓN REGLADA

- Ingeniería Técnica Informática o Equivalente

TAREAS

- Estudiar el mercado informático en referencia a nuevos productos, tendencias y servicios del ámbito de la seguridad informática.
- Realizar el análisis de riesgos
- Elaborar planes y políticas de seguridad de los sistemas de información de la organización.
- Desarrollar procedimientos y métodos de Seguridad
- Identificar, seleccionar, especificar, planificar e implantar los mecanismos de seguridad.
- Divulgar las políticas de seguridad, involucrando en ella a todos los miembros de la organización.
- Instalar y Configurar elementos de seguridad (Firewalls,…)
- Crear controles e indicadores para el mantenimiento del adecuado nivel de protección, revisándolos periódicamente (auditoría de seguridad).
- Analizar las Intrusiones en el Sistema Informático
- Colaborar con el responsable de sistemas en tareas de evaluación, planificación y coordinación de nuevas implantaciones.

COMPETENCIA TÉCNICA

Manejar

Red informática, ordenador personal, servidores, software de sistemas, periféricos, sistemas operativos de red, software específico, elementos de interconexión de redes, políticas de seguridad, mecanismos y procedimientos de seguridad, información técnica diversa,…

Conocer

Sistemas Informáticos; Redes y Comunicaciones; Arquitectura de ordenadores; Aplicaciones informáticas; Seguridad Informática; Amenazas y Riesgos de un Sistema Informático; Técnicas y

lenguajes de programación; Tendencias del sector; Normativa técnica; Inglés técnico; Seguridad e higiene; Estructura de la Organización.

COMPETENCIA ORGANIZATIVA Y ECONÓMICA

Capacidad para organizar y planificar en su ámbito de trabajo y en diferentes proyectos, optimizando los recursos disponibles, mostrando iniciativa, asumiendo decisiones y teniendo una visión de las diferentes especialidades de su área como un conjunto interrelacionado, conociendo y aplicando, o en su caso diseñando o adaptando, los procedimientos, herramientas y técnicas más adecuadas

COMPETENCIA DE COOPERACIÓN

Alta capacidad de comunicación y trabajo con el equipo, así como con el entorno exterior (clientes, proveedores, colaboradores…) y en diferentes proyectos, cooperando con la organización en la consecución de los objetivos establecidos, respetando los niveles de calidad y seguridad requeridos.

COMPETENCIA DE RESPUESTA A LAS CONTINGENCIAS

Alta capacidad de respuesta y resolución creativa a las incidencias que se produzcan tanto en los procedimientos, en equipos, en sistemas y en productos o servicios, atendiendo siempre a los niveles de calidad requeridos.