SEGURIDAD EN SISTEMAS DE INFORMACIÓN

PROGRAMA ANALÍTICO

PLAN DE ESTUDIOS	**2008**
ORDENANZA CSU. Nº	**1150**
HORAS/AÑO:	**64**
OBLIGATORIA	
ELECTIVA	**X**
ANUAL	
PRIMER CUATRIMESTRE	
SEGUNDO CUATRIMESTRE	**X**
NIVEL / AÑO	**3º**
HORAS CÁTEDRA SEMANALES	**4**

OBJETIVOS

OBJETIVO GENERAL

Concientizar sobre la importancia de la continuidad de procesos en la continuidad del "Negocio" en las empresas. Definir estándares para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad.

OBJETIVOS ESPECÍFICOS

a) Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
b) Implementar y operar controles para manejar los riesgos de la seguridad de la información.
c) Monitorear y revisar el desempeño y la efectividad del Plan de Contingencia.
d) Mejoramiento continúo en base a la medición del objetivo.

CONTENIDOS

CONTENIDOS SINTÉTICOS

1. La importancia de conocer los riesgos
2. Seguridad física de un centro de procesamiento de datos
3. Seguridad lógica de un centro de procesamiento de datos
4. Seguridad y organización de la empresa
5. Seguridad en Internet
6. Plan de contingencia

CONTENIDOS ANALÍTICOS

UNIDAD TEMÁTICA Nº 1. LA IMPORTANCIA DE CONOCER LOS RIESGOS

En esta introducción se explican los motivos por los cuales las fallas de Seguridad en los sistemas de información tienen cada vez mayor impacto en la eficiencia y rentabilidad de las empresas. Se fortalece el concepto de que la continuidad de negocios depende fuertemente de la continuidad operativa, confiabilidad y confidencialidad de los sistemas de información, relativizando el valor de los activos físicos y mostrando la gran importancia de la información para la toma de decisiones y actividades empresariales. Se dan definiciones sobre los conceptos claves y términos propios de la temática. Se capacita en los distintos tipos de riesgos a los que están sometidos los sistemas de información, presentando distintas visiones y clasificaciones. Se analizan casos reales en diversas industrias para ejemplificar y consolidar los conceptos. Se presentan diversas estrategias y técnicas de prevención, detección y corrección de las contingencias que se producen durante el ciclo de vida de un sistema de información. Se hace especial énfasis en la necesidad de una planificación previa que mejore las capacidades internas de la organización de responder exitosamente a contingencias potencialmente desastrosas.

Marco Conceptual

- **¿Para qué necesitamos la seguridad del SI?** Confidencialidad – Disponibilidad – Integridad – Protección de activos tangibles e intangibles (RRHH, datos críticos y estratégicos, hardware, software, confianza, giro comercial) Garantizar el servicio – Garantizar confiabilidad.
- **Objetivo:** Garantizar la continuidad operativa exitosa de los sistemas de información de la empresa.
- **Marco histórico**: Evolución desde los años 70 a los 90. Aumento de complejidad. Influencia de los SI en la continuidad del negocio. Nuevos requisitos de operación continúa.
- **Definiciones y conceptos clave**: Amenaza, riesgo y vulnerabilidad. Contingencia. Contingencias programadas y no programadas. Desastre y catástrofe, Sistemas y procesos críticos. Registros vitales y no vitales. Punto de recuperación. Ventana de vulnerabilidad. Control interno. Auditoria. Exposición al riesgo, frecuencia, pérdida unitaria, Medidas preventivas, detectivas y correctivas.

Factores de riesgo.

- **Clasificación de los riesgos: (En relación a los medios)** Físicos (accidentales o intencionales)- Fallas de equipos – Fallas de software – Fallas en RRHH (errores o fraude). (**En relación a la información**) Mal uso de la información – Pérdida o indisponibilidad – **(En relación al ciclo de vida de los sistemas de información)** Riesgos en la etapa de desarrollo (tiempos, resultados, costos, cancelación), en la implementación, en la explotación, en el mantenimiento.
- **Elementos necesarios para completar una amenaza intencional**: capacidad – motivación – oportunidad. Su importancia en el análisis de riesgos.
- **Errores de gerenciamiento**: subestimación de los riesgos – sobreestimación de los riesgos. Confiar en que recuperación será exitosa. (Prevención vs recuperación) ausencia de análisis y ponderación – falta de conciencia del impacto en empresa. Mala conducción de los proyectos informáticos.

Enfoque tradicional del análisis de riesgos

Diagnostico de las posibles causas de desastres. Establecer la probabilidad de ocurrencia. Frecuencia esperada: (datos históricos, probabilidad subjetiva. Estimación de pérdidas monetarias. Ranking en función al riesgo. Definir estrategias de prevención/recuperación. Problemas del análisis de riesgos: inexactitud de estimaciones, factores intangibles o de difícil medición. No es una ciencia exacta.

¿Cómo enfrentar los riesgos?

- **Estrategias de reducción de riesgos en función del análisis**: aceptación – transferencia – elusión o eliminación – reducción (disminuir la frecuencia FE o disminuir la perdida unitaria PU).

- **Respaldos y backups**: técnicas y metodologías – alcance – periodicidad – identificación de registros vitales – resguardo físico – duplicación – responsabilidad – testeo y simulación de la recuperación.
- **El factor humano**: separación de funciones y la contradicción con las nuevas tendencias. Organigrama. Estructura funcional. Concepto de control interno. Énfasis en la calidad como factor de prevención: en procedimientos, en los sistemas, en la selección de personal, en el entrenamiento, en la motivación, en el análisis de sistemas y proceso de desarrollo de software.
- **La redundancia como solución**: la baja de costos ayuda – las ventajas de estandarizar conceptos – convenios de Backup mutuo (ventajas, desventajas) – Mirroring – Duplexing – Sistemas múltiples y redundantes – Downsizing – distribución de procesos y datos – Centros de cómputos alternativos: Hot site y cold site. Servicios externos de prevención de contingencias. El problema de la obsolescencia – el problema de la vanguardia – en la redundancia vs la ventana de vulnerabilidad – importancia de identificar sistemas críticos y planificar la recuperación.
- **Plan de contingencia**: definiciones y objetivos. Concentrarse en los efectos no en las causas. Probabilidad de ocurrencia. Un desastre puede o no ocurrir. Considerar también las perdidas intangibles. Estimar costos de prevención y recuperación.
- **Factores a considerar para la elaboración de un plan de contingencia**: fuentes de amenazas – activos de la empresa a proteger – exposición a riesgo – atractivo – vulnerabilidad – medidas de prevención actuales – restricciones de tiempo, RRHH, presupuesto, técnicas, legales ambientales.

¿Prevención o recuperación? Grafico de costos de control y riesgo. Punto de razonabilidad. Conocer el inventario de software. Dinámica de la exposición al riesgo. Compromiso de los distintos niveles de la organización. ¿Puede generarse compromiso? El desafío de generar cultura. La paradoja de la prevención: creer que el proceso termina.

La administración de la seguridad

La administración de la seguridad como rol critico en la empresa. La línea está ocupada en el día a día. Necesidad de control en organizaciones dinámicas. Necesidad del know – how técnico y funcional. El mantenimiento y administración del cambio.

TIEMPO ASIGNADO: 8 HORAS

UNIDAD TEMÁTICA N° 2. SEGURIDAD FÍSICA DE UN CENTRO DE PROCESAMIENTO DE DATOS.

En esta unidad se presentan con mayor detalle los riesgos de naturaleza física (naturales, relativos a los activos materiales, casuales o intencionales), sus características y alternativas para reducir su impacto.

Control de acceso: sistemas de control de acceso y permanencia – registro de visitas – cámaras – niveles de restricción por áreas – salidas de emergencia: el valor del RRHH.

Sistemas de detección y alarmas: detección y corrección. Incendio, humo, humedad.

Sistemas de prevención: incendio, robo, acceso indebido.

Servicios: mantenimiento, UPS y gripo electrógeno, proveedores estratégicos, seguros, hot y cold site, servicios de asistencia, control de stocks, limpieza. Capacitación del personal.

Condiciones edilicias: ubicación geográfica, ubicación interna, ubicación de inflamables, vías de salida, procedimientos y prioridades.

Transmisión de datos: criptografía, medio físicos, topologías, seguridad del cableado, comparación de medios de comunicación.

Factores de evaluación de riesgo: identificación de recursos críticos: software, hardware, RRHH, datos.

Política de seguridad empresaria: normas internas, capacitación de usuarios, asignación de permiso de acceso, registración de acceso.

TIEMPO ASIGNADO: 8 HORAS

UNIDAD TEMÁTICA Nº 3. SEGURIDAD LÓGICA DE UN CENTRO DE PROCESAMIENTO DE DATOS

En esta unidad se hace una revisión general de los riesgos lógicos que pueden afectar los sistemas de información.

Riesgos en la etapa de desarrollo: el análisis de riesgo empieza en la etapa de diseño. Correcta definición de objetivos – el rol del auditor – importancia de las metodologías de diseño, desarrollo planeamiento – controles periódicos y revisión de objetivos – definición de estándares – administración de cambios – el testeo – el problema del cambio permanente en las herramientas de desarrollo.

Riesgos en la explotación: Control de acceso a los datos y registros – perfiles de seguridad y palabras clave – niveles de autorización – dígitos de auto verificación – balances y control de inconsistencias – control automático – registro de transacciones – copias de respaldo – integridad transaccional – integridad referencial – acceso a BD – acceso a bibliotecas – acceso a librerías de programas fuentes y objetos. Virus: concepto, clasificación, antivirus, políticas de prevención.

Riesgos en la fase de mantenimiento: Asignación de roles y responsabilidades – definición y aprobación de objetivos – planificación de cambios – testeo y participación del usuario – puesta en marcha – pase a producción – administración de versiones – independencia entre desarrollo y producción.

TIEMPO ASIGNADO: 8 HORAS

UNIDAD TEMÁTICA Nº 4. SEGURIDAD Y ORGANIZACIÓN DE LA EMPRESA

En esta unidad se analiza particularmente el rol de los RRHH, la organización funcional de la empresa. Se ve la influencia de la actitud gerencial en las políticas de seguridad y la necesidad de crear una cultura interna con conciencia de los riesgos y sus efectos, así como de los comportamientos esperables para su minimización.

Aspectos generales de la organización: Organigrama – la dirección de la empresa y el concepto de la seguridad – el rol del administrador de la seguridad de sistemas como recurso crítico – necesidad de control independiente – mantenimiento y administración del cambio.

Separación y oposición de funciones: Organización funcional de la gerencia de sistemas de información – separación de funciones – dependencia funcional del administrador de seguridad – política de personal – política presupuestaria y de costos – política de seguridad y confiabilidad – política de procedimientos generales de la organización – auditoría interna y externa.

TIEMPO ASIGNADO: 8 HORAS

UNIDAD TEMÁTICA Nº 5. SEGURIDAD EN INTERNET

Se discute el impacto de las nuevas tecnologías de comunicación e información (Internet) y los riesgos inherentes de la mayor exposición de los activos lógicos en ese nuevo contexto. Asimismo se exponen algunas de las técnicas actuales de prevención relacionadas.

El nuevo paradigma de la seguridad: usuarios internos conocidos vs usuarios externos desconocidos – los problemas que plantea el nuevo escenario: Business to consumer, business to business. Internet y extranet.

Nuevos riesgos: Mayor exposición, intrusión, nuevos virus, los problemas del código móvil.

Nuevas medidas: Cortafuegos, encripción, firmas digitales, certificados digitales, nuevos antivirus. Balance entre accesibilidad y seguridad. Restricciones al uso. Simulación de ataques.

TIEMPO ASIGNADO: 8 HORAS

UNIDAD TEMÁTICA Nº 6. PLAN DE CONTINGENCIA

Esta unidad presenta los elementos constitutivos de los planes de contingencia, su importancia, la forma de materializarlos en forma exitosa. Se procura consolidar estos conocimientos con el desarrollo de un trabajo práctico que consiste en la elaboración de un Plan de Contingencia. Este trabajo obliga al alumno a aplicar los conocimientos adquiridos

durante todo el curso, interactuando en equipo con los docentes. El TP se desarrolla a lo largo del último mes de cursada, realizando los docentes sucesivas observaciones a los alumnos en las que se evalúa la correcta interpretación de los conceptos brindados y la metodología aplicada.

Objetivos – contenidos y requerimientos básicos: escrito, público, completo y actualizado – requisitos para la recuperación – estrategias para la recuperación – procedimientos y medidas de seguridad – definición y asignación de responsabilidades – definición de instalaciones alternativas el rol y estructura del "equipo de recuperación de desastres" – prueba del plan de contingencia –simulacros en situación de desastres.

TIEMPO ASIGNADO: 24 HORAS

BIBLIOGRAFÍA

Juan Gaspar Martínez: *El plan de continuidad de negocio*, Díaz de Santos, 2006. Álvaro Gómez Vieites: *Enciclopedia de la seguridad informática*, Ra-Ma, 2006. IRAM-ISO/IEC: *NORMA 17799: Código de Práctica para la gestión de la seguridad de la información*, IRAM-ISO/IEC Primera edición, 2002. IRAM-ISO/IEC: E*stándar internacional. Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Información– Requerimientos*, IRAM-ISO/IEC Primera edición, 2005. Jon Erickson: *Hacking: The Art of Exploitation*, 2nd Edition, 2006.

CARACTERÍSTICAS DE LA ACTIVIDAD CURRICULAR

DESCRIPCIÓN

Se dictan clases presenciales, acorde a lo establecido en la reglamentación vigente. Son de carácter teórico y práctico. Se hace verdadero hincapié en ejemplos y se relaciona constantemente la teoría con la práctica. Se justifican los temas explicados. Se realiza un trabajo de confección de un "PLAN DE CONTINGENCIA" donde el alumno debe aplicar los conocimientos y metodologías adquiridos durante la primera parte del curso, integrando grupos de trabajo, con el fin de desarrollar experiencia de trabajo en equipo e interactuando en forma presencial y virtual con los docentes de la cátedra.

MODALIDAD DE LA ENSEÑANZA

Los docentes a cargo del curso desarrollan los temas del programa exponiendo los conceptos fundamentales de cada uno de ellos. Proponen, además, temas de interés y experiencias personales que debieron enfrentar a fin de proponer el debate de los tópicos tratados en clase. Para este último, punto se utilizará la bibliografía recomendada en el programa. Esta bibliografía es orientativa y se incentivará a los alumnos a investigar cualquier otra vinculada con los temas específicos.

EVALUACIÓN

Por cursada se realizan dos exámenes parciales, el primero teórico y el segundo se realiza con la entrega del "PLAN DE CONTINGENCIA" su presentación, explicación y detallando los fundamentos de acciones realizadas. Con los dos recuperatorios correspondientes por reglamento. En estos exámenes se evalúan los temas teóricos y la práctica. Se realizan evaluaciones continuas, tomando en cuenta las evaluaciones parciales, así como la participación en clase.

Requisitos de regularidad

- Cumplir con las condiciones de presentismo establecidas por la Facultad.
- Tener los exámenes parciales aprobados en alguna de sus instancias.
- Cumplir con las correlatividades solicitadas para la inscripción.

Requisitos de aprobación

Para aprobar la asignatura es necesario contar con las correlatividades correctas (tener aprobadas (con final) las materias requeridas). Además deberá aprobar un examen final conforme a las fechas establecidas por la Regional (para rendir e inscribirse).