Escuela Provincial de Educación Técnica Nº 1 " UNESCO"

PLANIFICACIÓN ANUAL 2015
Ciclo Superior Secundario

ESPACIO CURRICULAR: Seguridad Informática

DOCENTE: Báez, José Orlando – Martínez, Silvia Natalia

ESPECIALIDAD: Técnico en Informática Personal y Profesional.

CURSO: 5to **DIVISION: "E" y "F"**

HORAS SEMANALES: 3 hs.

FUNDAMENTACION

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

La misión de un administrador de sistemas en el plano de la seguridad, es garantizar la protección de la información crítica de la entidad en que trabaja. La información crítica es aquella cuyo deterioro pone en peligro la continuidad del negocio.

Toda organización tiene una misión. La misión es el objetivo mismo de la empresa. Si la información crítica de la organización se ve comprometida, el resultado puede ir desde un simple inconveniente hasta algo tan grave como la pérdida de la confianza del cliente.

Desgraciadamente, la seguridad no es tomada aún en serio en muchas organizaciones, por diferentes razones. En primer lugar,el coste de la seguridad (en formación, en restricciones, etc.) tiende a considerarse un factor de pérdida. Por otro lado, en muchas ocasiones, un Administrador de Sistemas es también responsable de seguridad de los mismos sistemas que administra. Esto lleva al trabajador a un dilema: por un lado, como administrador, busca la forma de mantener los servicios disponibles y fáciles de usar para los usuarios; por el otro, como responsable de seguridad debe limitar los servicios y restringir el acceso para asegurar la información. Por lo general, el administrador terminará superponiendo su tarea de administrador sobre su tarea de responsable de seguridad.

Esta materia se relaciona con Redes II.

OBJETIVOS

- Comprender los conceptos básicos de seguridad informática
- Describir los principales problemas de seguridad informática con los que se enfrentan los usuarios de computadoras.
- Conocer los conceptos de Integridad, confiabilidad y disponibilidad de la información.
- Conocer los factores de riegos.
- Reconocer e interpretar la seguridad lógica y fisca.
- Conocer los mecanismos de seguridad informática existentes.
- Concientizar sobre los riesgos a los que las organizaciones y usuarios de computadoras se enfrentan en materia de seguridad de la información.
- Ampliar o enriquecer los conocimientos a cerca de la seguridad informática.

CONTENIDOS CONCEPTUALES:
Distribución de unidades didácticas

UNIDAD I: Introducción

Informática, definición. Recursos y vulnerabilidades. Finalidad y Estrategia de la Seguridad Informática. Componentes de la Seguridad Informática. Disponibilidad, confiabilidad e integridad, concepto. Revisión de normativa vigente respecto del área de seguridad informática. Nacionales e Internacionales. Áreas en las que usualmente recae la responsabilidad de Seguridad, inconvenientes respecto a su control. Coordinación de Seguridad. Definición y objetivo.

Planificación, desarrollo, puesta en marcha y posterior verificación de las pautas de Seguridad. Coordinación interna y Asesoría externa, diferencia entre ambas. Organización del área. Dependencia. Responsabilidad. Actuación desde el diseño. Seguridad Física. Selección y diseño, metodología de evaluación. Protección de acceso. Medidas de resguardo de almacenamiento. Riesgos, distintos tipos, evaluación de ocurrencia. Seguridad Administrativa. Normas, su necesidad. Implementación y control de normas. Publicidad. Personal, reclutamiento y seguimiento. Contratos. División de responsabilidades. Seguridad Lógica. Concepto. Riesgos de Seguridad y problemas de protección. Recursos a proteger. Metodologías de uso común: identificación y autenticación de usuarios.

UNIDAD II: Redes.

Redes. LAN, WAN, de teleproceso. Componentes. Metodologías. Nociones de criptosistemas, propiedades. Interfases físicas y lógicas. Nociones de criptosistemas en redes. Malware, concepto y generalidades. Los cotos de una infección. Evolución del software dañino. Métodos de infección.

UNIDAD IV: Código Malicioso.

Código malicioso. Medidas preventivas. Que es un antivirus. Detención y prevención. Metodologías de comparación y heurística. Modelo antivirus. Estrategias de seguridad. Metodologías. Análisis de riesgos. Cuantificación de riesgos. Metodologías. Matrices. Bases económicas, políticas y sociales que respaldan la toma de medidas preventivas. Costo-beneficio.

CONTENIDOS ACTITUDINALES

- Valorar la importancia de la seguridad informática en la industria informática.
- Reconocer distintos tipos de códigos maliciosos.
- Analizar la seguridad lógica y física.
- Responsabilidad en la presentación de trabajos.
- Adquirir responsabilidad en interpretar realmente lo que aprende.
- Adoptar metodologías y criterios de organización en el trabajo.
- Interpretar documentación técnica relacionada.
- Buscar información en bibliografía especializada.
- Desarrollar su capacidad de análisis crítico e investigación.
- Respeto por el pensamiento ajeno.
- Valoración del intercambio de ideas como fuente de aprendizaje.
- Tolerancia y serenidad frente a resultados positivos o negativos de los proyectos en que participa.
- Valoración del equipo de trabajo y de las técnicas de organización y gestión en el diseño y realización de proyectos.
- Aprovechamiento de los aspectos positivos de la informática como herramienta para favorecer el desarrollo del pensamiento divergente.
- Manifestación de interés y preocupación por la asignatura.
- Actuar críticamente y demostrar un sentido reflexivo sobre los conocimientos adquiridos.

CONTENIDOS PROCEDIMENTALES

- Clasificar los distintos tipos de virus informáticos.
- Diferenciar la función realizada por los hackers de la realizada por los crakers y phreaker.
- Reflexionar y debatir sobre el proceder ético en el uso de aplicaciones informáticas.
- Operar software de detección y limpieza de virus informáticos, en discos, diskettes.
- Buscar información.
- Procesar información obtenida.

METODOLOGÍA DE ENSEÑANZA Y ACTIVIDADES DE APRENDIZAJE

. Resolución de problemas.
· Búsqueda bibliográfica.
· Lectura comprensiva.
· Estudio dirigido.
· Puesta en común de trabajos.
· Debates dirigidos.

· Investigación.
· Técnicas grupales.
· Exposición de actividades.
· Técnicas para interpretar textos.
· Confección de mapas conceptuales

ACTIVIDADES DE APRENDIZAJE

Elaboración de cuadro sinóptico sobre riesgos.
Elaboración de un mapa conceptual sobre seguridad informática.
Lectura y análisis de documentos.
Realizarán presentaciones conceptuales teóricas breves sobre cada tema y presentación de casos prácticos de aplicación.
Exposición de temas por parte de los alumnos.
Resolución de ejercicios propuestos a partir de una guía de trabajo.
Trabajos prácticos de investigación.

EVALUACIÓN

Evaluación inicial:
Observación directa. Indagación de conocimientos previos. Ejercicios. Actividades grupales.

Evaluación formativa:
Trabajos prácticos individuales y grupales. Indagación de saberes. Dialogo. Dinámicas grupales.

Evaluación sumativa:
Trabajos prácticos grupales. Exposición oral. Informes individuales y grupales. Examen escrito.

CRITERIOS DE EVALUACION

- La participación activa y constante del alumno en el curso.
- La buena predisposición en relación con los demás miembros del curso.
- La entrega en tiempo y condiciones de la carpeta y/o trabajos prácticos.
- Participación, interés, asistencia y colaboración con el equipo de trabajo al que pertenece.
- Habilidad para buscar, seleccionar y organizar La información.
- Entrega de trabajos prácticos(escritos y en la computadora) en tiempo y forma, aprobación de evaluaciones escritas u orales, carpeta completa.
- Utilización de vocabulario especifico.
- Capacidad para analizar y relacionar conocimientos.

INSTRUMENTOS DE EVALUACIÓN

- Narrativa, diálogos.
- Presentaciones con soportes informáticos/ audiovisuales, exposiciones orales
- Informes, trabajos monográficos.

- Pruebas escritas, registros.

RECURSOS

-Pizarra.
- Computadoras.
- Proyector.
- Microscopio, etc.
- USO DE LAS TIC's.
- Aula Virtual.

BIBLIOGRAFÍA

Apuntes de la materia.

Firma de los profesores:

Escuela Provincial de Educación Técnica Nº 1 " UNESCO"

Programa Anual 2015
Ciclo Superior Secundario

ESPECIALIDAD: Técnico en Informática Personal y Profesional.

ESPACIO CURRICULAR: Seguridad Informática

DOCENTE: Báez, José Orlando – Martínez, Silvia Natalia

CURSO: 5to **DIVISION: "E" y "F"**

Contenidos Conceptuales a Desarrollar:

UNIDAD I: Introducción

Informática, definición. Recursos y vulnerabilidades. Finalidad y Estrategia de la Seguridad Informática. Componentes de la Seguridad Informática. Disponibilidad, confiabilidad e integridad, concepto. Revisión de normativa vigente respecto del área de seguridad informática. Nacionales e Internacionales. Áreas en las que usualmente recae la responsabilidad de Seguridad, inconvenientes respecto a su control. Coordinación de Seguridad. Definición y objetivo.

Planificación, desarrollo, puesta en marcha y posterior verificación de las pautas de Seguridad. Coordinación interna y Asesoría externa, diferencia entre ambas. Organización del área. Dependencia. Responsabilidad. Actuación desde el diseño. Seguridad Física. Selección y diseño, metodología de evaluación. Protección de acceso. Medidas de resguardo de almacenamiento. Riesgos, distintos tipos, evaluación de ocurrencia. Seguridad Administrativa. Normas, su necesidad. Implementación y control de normas. Publicidad. Personal, reclutamiento y seguimiento. Contratos. División de responsabilidades. Seguridad Lógica. Concepto. Riesgos de Seguridad y problemas de protección. Recursos a proteger. Metodologías de uso común: identificación y autenticación de usuarios.

UNIDAD II: Redes.

Redes. LAN, WAN, de teleproceso. Componentes. Metodologías. Nociones de criptosistemas, propiedades. Interfases físicas y lógicas. Nociones de criptosistemas en redes. Malware, concepto y generalidades. Los cotos de una infección. Evolución del software dañino. Métodos de infección.

UNIDAD IV: Código Malicioso.

Código malicioso. Medidas preventivas. Que es un antivirus. Detención y prevención. Metodologías de comparación y heurística. Modelo antivirus. Estrategias de seguridad. Metodologías. Análisis de riesgos. Cuantificación de riesgos. Metodologías. Matrices. Bases económicas, políticas y sociales que respaldan la toma de medidas preventivas. Costo-beneficio.

Bibliografía:

Apuntes de la materia.

Criterios de Evaluación:

- La participación activa y constante del alumno en el curso.
- La buena predisposición en relación con los demás miembros del curso.
- La entrega en tiempo y condiciones de la carpeta y/o trabajos prácticos.

- Participación, interés, asistencia y colaboración con el equipo de trabajo al que pertenece.
- Habilidad para buscar, seleccionar y organizar La información.
- Entrega de trabajos prácticos (escritos y en la computadora) en tiempo y forma, aprobación de evaluaciones escritas u orales, carpeta completa.