Institución: Escuela Superior de Comercio Nro 43.

Carrera: Técnico Superior en Soporte de infraestructura de tecnología de la información.

Profesor: Norberto Juan Ignacio Tito

Unidad Curricular: Seguridad de los Sistemas

Campo de Formación: Específica

Formato: Taller

Régimen de cursado: Anual

Cantidad de horas: 5 Hs Semanales - 160 Hs Total.

Curso: 3er Año

Ciclo Lectivo: 2023

Plan Decreto: 2120/16

Fundamentación

La cátedra seguridad de los sistemas es fundamental para que a los estudiantes comprendan la importancia de proteger la información, los recursos y los procesos críticos de una organización. Los sistemas de información son vulnerables a diversas amenazas, como ataques cibernéticos, malware, robo de datos y desastres naturales, entre otros.
Esta unidad curricular brinda los conocimientos, habilidades y herramientas necesarios para proteger sus sistemas de información contra estas amenazas, implementar controles de seguridad efectivos, gestionar los riesgos de seguridad, y responder de manera adecuada a los incidentes de seguridad. Logrando una concientización y adopción de mejores prácticas de seguridad en el diseño, desarrollo y mantenimiento de los sistemas.
El desarrollo de esta asignatura, no solo podrán ser utilizados en otras áreas específicas de la carrera, sino que también revisten importancia significativa para que el futuro egresado pueda desempeñarse eficazmente en su ámbito laboral.

Propósitos

- Comprender los conceptos básicos de la seguridad de los sistemas, incluyendo los diferentes tipos de amenazas y vulnerabilidades.
- Identificar los riesgos de seguridad en los sistemas de información y aplicar estrategias para mitigarlos.
- Implementar medidas de seguridad para proteger la información, los recursos y los procesos críticos de la organización.
- Concientizar sobre la importancia de la seguridad en los sistemas de información y promover una cultura de seguridad en la organización.

Contenidos

Unidad 1: Estados de la información: transmisión, almacenamiento y procesamiento. Modelos de seguridad, dominios de seguridad, responsabilidades. Usuarios, sus derechos y

limitaciones. Servicios de seguridad: disponibilidad, integridad, confidencialidad, autenticación y no repudio. Mecanismos de implementación de diversos servicios de seguridad. Logs de eventos relacionados con la autoría y auditoría de procesos. Necesidad de proteger datos y programas, creación, identificación y administración o mantenimiento de archivos de respaldo (backups), así como su recuperación.
Parches para actualización de la seguridad de sistemas operativos y demás software de base. Software antivirus, antispam, antispyware y contra otro malware, su instalación, actualización y aplicación a nivel corporativo.

Unidad 2: Crear y administrar usuarios y grupos de usuarios aplicando políticas de seguridad. Automatizar rutinas de back up y recuperación. Verificar la ejecución de rutinas automáticas de aplicación de software para conjugar riesgos. Realizar recuperaciones de archivos. Aplicación de parches en sistemas operativos. Buscar en logs evidencias de intrusiones y analizarlas para describirlas.
Métodos de identificación positiva de usuarios. Algoritmos específicos para asegurar la integridad de los datos transmitidos. Mecanismos de control de recepción de los datos enviados.

Unidad 3: Fundamentos de criptografía, su aplicación a redes. Algoritmos de clave pública y privada. Protocolos de autenticación, firmas digitales, aplicaciones de Virtual Private Networks. Algoritmos de compresión de datos, algoritmos específicos para compresión de archivos digitales de imagen y sonido.
Capas de seguridad, protocolos y algoritmos más usados (http, https, SSLs). Detección de agujeros negros.
Riesgos que pueden afectar la continuidad del procesamiento.

Unidad 4: Conceptos fundamentales de seguridad: historia y terminología, conciencia de seguridad (paranoia razonada) principios de diseño (defensa profunda), ciclo de vida del sistema de seguridad, mecanismos de implementación de seguridad (puentes, patrullaje, criptografía), modelo de análisis de la seguridad de la información (MSR, amenazas, vulnerabilidades, ataques, contramedidas), recuperación de desastres (naturales y realizados por el hombre), análisis forense de acontecimientos.

Unidad 5:
Elementos y mecanismos de seguridad: criptosistemas, claves (simétricas, asimétricas), rendimiento (software, hardware), implementación. Proxies y firewalls.
Aspectos operativos: tendencias, auditoría, análisis de costo/beneficio, administración de activos, estándares, “enforcement”, aspectos legales, recuperación de desastres.
Servicios de Seguridad: disponibilidad, integridad, confidencialidad, autenticación, no repudio.
Políticas, estándares y buenas prácticas: creación, mantenimiento, prevención, “avoidance”, respuesta a incidentes, integración de dominios (físico, red, Internet), normas ITIL.
Vulnerabilidades: ataques internos, externos, lista blanca, lista negra, ignorancia, falta de cuidado, red, hardware, software, acceso físico.
Ataques: ingeniería social, negación de servicio, ataques a protocolos, ataques activos, ataques pasivos, ataques por overflow de buffers, malware (virus, troyanos, gusanos, bots, rootkits).
Análisis forense: sistemas legales, forénsica digital y su relación con otras disciplinas forénsicas, reglas de la evidencia, búsqueda y captura, evidencia digital, análisis de medios.

Estrategias Metodológicas

- Exposición didáctica.
- Estudios de caso
- Ejercicios de simulación
- Aprendizaje colaborativo
- Búsqueda de información en la web.
- Elaboración y presentación de informes.

Recursos

- Computadoras/Celulares. Internet. Proyector/TV
- Aula Virtual. Computadoras en red.
- Fotocopias, documentos digitales.
- Plataforma Classroom – distintas aplicaciones

MODALIDAD DE CURSADO

El taller de Seguridad de los Sistemas sólo admite el cursado regular presencial

EVALUACIÓN

La evaluación es continua, acompañada por un seguimiento exhaustivo del trabajo de cada estudiante. Se tienen en cuenta diferentes factores que hacen al conocimiento del docente respecto del desempeño personal de los estudiantes.

Instrumentos de evaluación:

- ❖ Trabajos prácticos.
- ❖ Elaboración de informes.
- ❖ Exposición y puesta en común de diferentes actividades.

Criterios de evaluación:

- ❖ Entrega en tiempo y forma de los trabajos prácticos en formato digital y papel.
- ❖ Asistencia a clases y a las actividades extra-áulicas organizada por el espacio curricular.
- ❖ Compromiso y responsabilidad en el desarrollo de los trabajos.

Regularización del taller:

a) Sólo admitirán el cursado regular presencial.

b) 75% de asistencia a las clases áulicas.

c) Aprobar el 100% de las instancias de evaluación previstas en la planificación anual.

Al cumplir con los requisitos a – b – c tiene derecho a una instancia final de integración que para aprobar deberá obtener nota de 6 (seis) o más sin centésimos.

El estudiante que no haya aprobado la instancia final de integración, podrá presentarse hasta dos turnos de exámenes consecutivos inmediatos posteriores a la finalización de la cursada.

Observación:

Debe tener **APROBADA:** Sistema Operativo

BIBLIOGRAFÍA

- Normas ISO 27000 link:
- Roa Buendia, J. (2013). Seguridad informática. Madrid: Mc GrawHill.
- Stallings, W. (2004). Fundamentos de Seguridad en Redes. Aplicaciones y estándares. Madrid: Pearson.
- Vieites A. (2010). Seguridad Informática Básico. Madrid: StarBook Editorial.
- Apunte Curso Cisco Cybersecurity Essentials (2023)