

Institución : Escuela Superior de Comercio Nro 43.

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

Profesor : Ariel Nardelli

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 : 2021

Plan Decreto : 2120/16

Fundamentación

La cátedra, estará orientada hacia los sistemas operativos, su instalación, configuración, mantenimiento y la realización de tareas habituales que se le pide a un sistema operativo a nivel de servidores. Proveer servicios a la red, permitir conectarse a internet y manejar los usuarios que puedan conectarse.

Esta unidad curricular brinda a los estudiantes los conocimientos necesarios para dotar a los sistemas de tecnología de la información, la seguridad necesaria para su adecuado funcionamiento.

A partir del conocimiento de la materia, el alumno es capaz de integrar conceptos y técnicas en la realización de procesos de investigación de mediano alcance de sistemas operativos de servidores ofrecidos actualmente en el mercado. En este marco los contenidos abordados durante 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

Facilitar la instalación, configuración y puesta a de un Sistema Operativo.

Posibilitar la comprensión del uso que se le da a los distintos Sistemas Operativos.

Desarrollar habilidades para desempeñarse como administrador de S. O.

Desarrollar el uso de los servicios dentro de la red de estos S.O.

Ofrecer la seguridad necesaria para el adecuado funcionamiento del S.O.

Contenidos

Unidad 1 : -Sistemas Operativos-

¿Qué es un Sistema Operativo? Concepto. Historia de los Sistemas Operativos. Tipos de Sistemas Operativos (Monousuario, Multiusuario, Monotareas y Multitareas). Sistemas de Archivos. Directorios y Archivos, su implementación. Virtualización y Docker, Diferencias e implementación.

Unidad 2 : -Seguridad-

Crear y administrar usuarios y grupos de usuarios aplicando políticas de seguridad. Riesgos que pueden afectar la continuidad del procesamiento. Conceptos fundamentales de seguridad: historia y terminología, conciencia de seguridad (paranoia razonada). Necesidad de proteger datos y programas, creación, identificación y administración o mantenimiento de archivos de respaldo (backups), así como su recuperación. 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.

Unidad 3 : -Ataques y Vulnerabilidades-

OSINT. ¿Qué es?. Técnicas y herramientas OSINT. Ingeniería Social. Ataques: Denegación de servicio, ataques a protocolos, ataques activos, ataques pasivos, ataques por overflow de buffers, malware (virus, troyanos, gusanos, bots, rootkits). Vulnerabilidades: ataques internos, externos, lista blanca, lista negra, ignorancia, falta de cuidado, red, hardware, software, acceso físico.

Unidad 4 : Sistema Operativo Windows. -Práctica-

Historia de Windows. Desde MS-DOS hasta Windows 10, Estructura del Sistema. Los procesos y administración de memoria en Windows. El sistema de archivo. Seguridad. Rendimiento. Mantenimiento. Configuración de la Red, Compartir archivos e Internet. Configuración DNS, DHCP y Proxy. Acceso a internet según grupo de equipos. Bloqueo de determinados sitios (Youtube, Instagram Facebook). Implementación de Firewalls.

Unidad 5 : Sistema Operativo Linux. -Práctica-

Historia de Unix a Linux. Generalidades de Linux. Los procesos y administración de Memoria en Linux. Sistemas de Archivo en Linux. Seguridad. Distribuciones, diferencias entre ellas. Instalación. Configuración básica. Entorno Gráfico. Rendimiento. Configuración de la Red, Compartir archivos e Internet. Configuración DNS, DHCP y Proxy. Acceso a internet según grupo de equipos. Bloqueo de determinados sitios (Youtube, Instagram y Facebook). Implementación de Firewalls.

Unidad 6 : Equipos Mikrotik . -Práctica-

Historia de Mikrotik. Generalidades. Seguridad nivel usuario y redes. Formas de instalación (En equipos o computadoras), diferencias entre ellas. Instalación. Configuración básica. Configuración de la Red, Compartir archivos e Internet. Configuración DNS, DHCP y Proxy. Acceso a internet según grupo de equipos. Bloqueo de determinados sitios (Youtube, Instagram y Facebook). Implementación de Firewalls.

Estrategias Metodológicas

Exposición didáctica.
Estudio dirigido.
Buceo bibliográfico.
Diálogo
Técnicas grupales.
Lectura comprensiva.
Búsqueda de información en la web.
Investigación.

Recursos

Pizarrón, Libros digitales, computadoras, videos, Aula Virtual. Computadoras en red.
Sistemas Operativos versión Servers. Dispositivos en hardware para comunicaciones.
Equipos Mikrotik.

Modalidad de cursado

Este taller permite al alumno solo la modalidades de cursado:

- Regular con cursado regular presencial.

De no poder dictar clases en forma presencial por cualquier motivo, el cursado se continúa de manera online, por classroom o cualquier medio electrónico que el docente o la institución consideren convenientes. Es obligatoria la participación de los alumnos en las clases virtuales y las evaluaciones se continuarán tomando en los formatos que el docente o la institución establezcan.

Evaluación

La evaluación será inicial y continua, a través de los diferentes trabajos desarrollados durante el ciclo lectivo.

Instrumentos de evaluación:

Trabajos prácticos.
Observación directa -por parte del docente- del trabajo grupal e individual.
Examen final integrador individual o grupal, si correspondiera.
Exposición y puesta en común de diferentes actividades.

Criterios de evaluación:

- Entrega en tiempo y forma de los trabajos prácticos y proyectos solicitados.
- Respeto por el trabajo y las opiniones del resto de los compañeros.
- Asistencia a clases y a las actividades organizadas en la cátedra para los alumnos regulares.
- Compromiso y responsabilidad en el desarrollo de los trabajos.
- Manejo del vocabulario específico.
- Participación en los trabajos grupales.
- Defensa y fundamentación de sus trabajos a partir de una base

conceptual sólida y correcta.

Regularización de la materia:

Para poder regularizar el taller el alumno deberá:

- Contar con el porcentaje de asistencia requerido, según la reglamentación vigente.
- Aprobar los trabajos prácticos. El alumno que no apruebe alguna de las instancias, tendrá derecho a un recuperatorio.

Trabajos Prácticos : Serán realizados en forma individual o grupal y entregados en tiempo y forma. En el aula virtual, se irá informando el contenido y la forma de presentación de cada trabajo.

Examen final : Será individual. Tendrá instancia escrita o oral, en caso que sea oral se deberá exponer un tema o unidad de la materia a elección y desarrollarlo en no más de 15 minutos, luego el docente realizará preguntas sobre el resto de las unidades del programa. Se deberá demostrar manejo de vocabulario específico de la materia.

Para regularizar la materia en forma **Regular presencial**, los alumnos deberán:

- Cumplir con el 75% de asistencia a clases. Para el alumno que presente certificado de trabajo y/o se encuentre en otras situaciones excepcionales como problemas de salud (debidamente comprobadas), el mínimo será de 50% de asistencia.
- Aprobar el 100% de los trabajos prácticos, entregados en tiempo y forma. El estudiante tendrá derecho a recuperatorios en todas las instancias de evaluación.
- Se regulará esta materia con una nota final con un mínimo de 6 (Seis). En caso de tener una nota menor, deberá recurrar la materia.

Aclaración : Si el alumno regulariza la materia, tiene derecho a un examen final en cualquiera de los turnos correspondientes, debiendo obtener una calificación mínima de 6 (Seis). ***Se mantiene la regularidad durante 2 (Dos) turnos Diciembre y Febrero/Marzo.***

Bibliografía:

- Tanenbaum, A. (2009 3ra Edición) - Sistemas Operativos Modernos.
Carletti (2017) - CiberSeguridad La 3ra Guerra Mundial.
Mario Carlos Ginzburg (2006 4ta Edición) La PC por Dentro.
Roa Buendia, J. (2013). Seguridad informática. Madrid: Mc GrawHill.
Stallings, W. (2004). Fundamentos de Seguridad en Redes. Aplicaciones y estándares. Madrid: Pearson.
Tenenbaum, A. (2013). Redes de computadores. México: PHH.
Vieites A. (2010). Seguridad Informática Básico. Madrid: StarBook Editorial.