INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

HOJA DE ASIGNATURA CON DESGLOSE DE UNIDADES TEMÁTICAS

1. Nombre de la asignatura	Seguridad de la Información
2. Competencias	Dirigir proyectos de tecnologías de información (T.I.) para contribuir a la productividad y logro de los objetivos estratégicos de las organizaciones utilizando las metodologías apropiadas. Evaluar sistemas de tecnologías de información (T.I.) para establecer acciones de mejora e innovación en las organizaciones mediante el uso de metodologías para auditoría.
3. Cuatrimestre	cuarto
4. Horas Prácticas	35
5. Horas Teóricas	40
6. Horas Totales	75
7. Horas Totales por Semana Cuatrimestre	5
8. Objetivo de la Asignatura	El alumno identificará las vulnerabilidades de los sistemas de información de una organización, para establecer los medios apropiados de protección que aseguren una eficaz gestión de las operaciones.

Unidades Temáticas	Horas		
	Prácticas	**Teóricas**	**Totales**
I. Introducción a la seguridad de la información.	7	9	16
II. Administración de la seguridad.	6	8	14
III. Métodos de autenticación.	7	6	13
IV. Firewalls.	4	3	7
V. VPN.	6	10	16
VI. Detección y prevención de intrusos.	5	4	9
Totales	**35**	**40**	**75**

SEGURIDAD DE LA INFORMACIÓN

UNIDADES TEMÁTICAS

1. Unidad Temática	I. Introducción a la Seguridad de la Información.
2. Horas Prácticas	7
3. Horas Teóricas	9
4. Horas Totales	16
5. Objetivo	El alumno implementará una política de seguridad para proteger la información de la organización apoyándose en las normas aplicables.

Temas	Saber	Saber hacer	Ser
Introducción a la Seguridad de la Información.	Describir los tipos de seguridad informática y los conceptos de disponibilidad, integridad, confidencialidad y control de acceso.		Sistemático. Creativo. Líder. Proactivo. Analítico.
Políticas de seguridad.	Identificar las características de una política de seguridad.	Elaborar políticas de seguridad identificando ventajas y desventajas de su implementación.	Sistemático. Creativo. Líder. Proactivo. Asertivo. Analítico. Hábil para el trabajo en equipo. Sociable.
Escenarios de ataques a redes.	Describir las amenazas a las que se enfrentan las redes modernas, detectando vulnerabilidades en capa 2 (MAC, ARP, VLAN, STP, CDP).	Configurar seguridad de puerto, deshabilitar auto trunking, habilitar BPDU Guard y Root Guard), deshabilitar protocolo CDP, en switches, considerando las buenas prácticas.	Sistemático. Creativo. Liderazgo. Proactivo. Hábil para el trabajo en equipo.

Temas	Saber	Saber hacer	Ser
Código malicioso.	Describir los métodos de mitigación para gusanos, virus, troyanos y ataques comunes a la red.	Establecer medidas preventivas y correctivas contra los gusanos, virus, troyanos y ataques comunes a la red.	Sistemático Creativo Líder Proactivo
Principios matemáticos para criptografía.	Identificar los principios matemáticos para criptografía simétrica y asimétrica.		Sistemático Proactivo Analítico
Algoritmos de criptografía.	Describir el funcionamiento de los algoritmos DES, 3DES, AES, RSA utilizados en seguridad informática.		Sistemático Proactivo Analítico
Normatividad nacional e internacional de seguridad.	Describir las características de la normatividad nacional e internacional en materia de seguridad. Identificar las características y aplicación de las normas ISO 27001, ISO 17799, COBIT, NIST y Systrust y Webtrust de AICPA (The American Institute of Certified Public Accountants).		Sistemático Proactivo Analítico

SEGURIDAD DE LA INFORMACIÓN

Proceso de evaluación		
Resultado de aprendizaje	**Secuencia de aprendizaje**	**Instrumentos y tipos de reactivos**
El alumno, a partir de un caso práctico, elaborará un reporte que incluya: • Política de seguridad. • Configuración de switches. • Medidas preventivas y correctivas contra código malicioso. • Listado de las normas aplicables.	1. Comprender los conceptos de disponibilidad, integridad, confidencialidad y control de acceso y los tipos de seguridad informática. 2. Determinar configuraciones para mitigar ataques a la Capa 2. 3. Comprender los métodos y medidas contra código malicioso. 4. Comprender el funcionamiento de los algoritmos DES, 3DES, AES, RSA. 5. Comprender la aplicación de las normas ISO 27001, ISO 17799, COBIT, NIST y Systrust y Webtrust de AICPA.	Estudio de Casos Lista de cotejo

SEGURIDAD DE LA INFORMACIÓN

Proceso enseñanza aprendizaje	
Métodos y técnicas de enseñanza	**Medios y materiales didácticos**
Aprendizaje basado en proyectos Práctica dirigida	Equipo de cómputo Internet Cañón Switches

Espacio Formativo		
Aula	**Laboratorio / Taller**	**Empresa**
	X	

SEGURIDAD DE LA INFORMACIÓN

UNIDADES TEMÁTICAS

1. Unidad Temática	II. Administración de la Seguridad.
2. Horas Prácticas	6
3. Horas Teóricas	8
4. Horas Totales	14
5. Objetivo	El alumno administrará la seguridad informática para garantizar la disponibilidad de la información.

Temas	Saber	Saber hacer	Ser
Administración de llaves públicas.	Identificar los mecanismos y relevancia de la administración de llaves públicas en un canal de comunicación seguro.	Configurar una entidad certificadora (servidor) con base en el estándar X.509 para llaves públicas.	Sistemático. Creativo. Proactivo.
Administración de riesgos y continuidad de actividades.	Describir los componentes generales de una Administración de Riesgos de la Información (ARI).	Elaborar una matriz de riesgos aplicada a la seguridad de la información.	Sistemático. Creativo Proactivo.
Prevención y recuperación de incidentes.	Explicar los planes de contingencia y procedimientos de recuperación.	Elaborar el esquema general de recuperación de incidentes conforme a las guías del NIST SP800 e ISO 17799.	Sistemático. Creativo. Líder. Proactivo.
Protección de Sistemas Operativos.	Identificar los elementos de seguridad en un SO de acuerdo al servicio que presta.	Implementar SSH ("Secure Shell") y SNMP.	Sistemático. Creativo. Líder. Proactivo.

Temas	Saber	Saber hacer	Ser
Protocolo SSL y SSL Handshake.	Identificar las funciones de SSL. Describir el proceso para establecer la comunicación entre el cliente y el servidor usando SSL Handshake.	Configurar el protocolo SSL.	Sistemático. Creativo. Líder. Proactivo.

SEGURIDAD DE LA INFORMACIÓN

Proceso de evaluación		
Resultado de aprendizaje	**Secuencia de aprendizaje**	**Instrumentos y tipos de reactivos**
El alumno, a partir de un caso de estudio, elaborará un plan de administración de la seguridad Informática en una organización que contenga: • Configuración de la entidad certificadora. • Esquema de recuperación de incidentes. • Matriz de riesgos. • Configuración de SSH y SNMP. • Configuración del protocolo SSL.	1. Comprender el procedimiento para habilitar una entidad certificadora y comprender la Administración de Riesgos de la Información (ARI). 2. Establecer un esquema de Recuperación de Incidentes (NIST SP800 e ISO 17799). 3. Comprender la implementación de SSH 4. Identificar los elementos de seguridad en SO. 5. Identificar la configuración del protocolo SSL.	Estudio de Casos Lista de cotejo

SEGURIDAD DE LA INFORMACIÓN

Proceso enseñanza aprendizaje	
Métodos y técnicas de enseñanza	**Medios y materiales didácticos**
Aprendizaje basado en proyectos. Práctica dirigida.	Equipo de cómputo Sistema operativo GNU/Linux Cañón Internet

Espacio Formativo		
Aula	**Laboratorio / Taller**	**Empresa**
	X	

SEGURIDAD DE LA INFORMACIÓN

UNIDADES TEMÁTICAS

1. Unidad Temática	III. Métodos de autenticación.
2. Horas Prácticas	7
3. Horas Teóricas	6
4. Horas Totales	13
5. Objetivo	El alumno implementará el método de autenticación adecuado para garantizar el acceso seguro a las aplicaciones y servicios informáticos de la organización.

Temas	Saber	Saber hacer	Ser
Servicios AAA.	Identificar las ventajas que ofrece el uso de servicio Radius, TACACS y Kerberos.	Configurar autenticación de usuarios utilizando RADIUS.	Sistemático Proactivo
Algoritmos de Hash MD5 y SHA-1.	Identificar las principales características de los algoritmos de Hash MD5 y SHA-1.		Sistemático Creativo Líder Proactivo
Certificados digitales.	Identificar los certificados digitales, asi como las entidades certificadoras.	Configurar el uso de certificados digitales en aplicaciones de correo electrónico.	Sistemático Creativo Líder Proactivo Hábil para el trabajo en equipo

SEGURIDAD DE LA INFORMACIÓN

Proceso de evaluación		
Resultado de aprendizaje	**Secuencia de aprendizaje**	**Instrumentos y tipos de reactivos**
El alumno, con base en un caso de estudio, elaborará un informe que incluya: • La comparación de los métodos de autenticación. • Configuración de autenticación con RADIUS • Descripción de la implementación de certificados digitales.	1. Comprender el procedimiento para la configuración de RADIUS. 2. Interpretar el funcionamiento de los Algoritmos de Hash. 3. Comprender el procedimiento para la configuración de certificados digitales para correo electrónico.	Estudio de Casos Lista de cotejo

SEGURIDAD DE LA INFORMACIÓN

Proceso enseñanza aprendizaje	
Métodos y técnicas de enseñanza	**Medios y materiales didácticos**
Aprendizaje basado en proyectos Práctica dirigida	Router Cisco 2811 con IOS Advance Secutiry Image. Router Cisco 1841 con IOS IP ADV Security. Equipo de Cómputo Sistema operativo Linux Cañón Internet

Espacio Formativo		
Aula	**Laboratorio / Taller**	**Empresa**
	X	

SEGURIDAD DE LA INFORMACIÓN

UNIDADES TEMÁTICAS

1. Unidad Temática	IV. Firewalls.
2. Horas Prácticas	4
3. Horas Teóricas	3
4. Horas Totales	7
5. Objetivo	El alumno implementará mecanismos de seguridad firewall, aplicando reglas de filtrado y directivas de control de acceso a redes para garantizar la seguridad de la información de la organización.

Temas	Saber	Saber hacer	Ser
Medidas de seguridad preventivas y correctivas aplicables a un Firewall.	Describir los mecanismos de seguridad preventiva y correctiva aplicables a un Firewall.	Establecer medidas preventivas y correctivas de seguridad e identificación de puertos TCP/UDP y zona desmilitarizada (DMZ).	Sistemático Creativo Líder Proactivo
Técnicas de implementación de Firewall.	Identificar las diferentes técnicas de implementación de firewall: Firewall a nivel de red, Firewall a nivel de aplicación.	Implementar un Firewall de filtrado de paquetes (a nivel de red aplicando Listas de Control de Acceso) y un Firewall Proxy de nivel de aplicación.	Analítico Creativo Innovador Sistemático Creativo Líder Proactivo Hábil para el trabajo en equipo

SEGURIDAD DE LA INFORMACIÓN

Proceso de evaluación		
Resultado de aprendizaje	**Secuencia de aprendizaje**	**Instrumentos y tipos de reactivos**
El alumno, solucionará un caso de estudio y elaborará un reporte que incluya el: • Diseño • Configuración • Pruebas para la implementación de un Firewall a nivel de red.	1. Comprender las medidas de seguridad aplicables a un Firewall. 2. Identificar los puertos vulnerables TCP/UDP. 3. Comprender las características de la Zona desmilitarizada. 4. Identificar el procedimiento para la implementación de un Firewall.	Estudio de Casos Lista de cotejo

SEGURIDAD DE LA INFORMACIÓN

Proceso enseñanza aprendizaje	
Métodos y técnicas de enseñanza	**Medios y materiales didácticos**
Aprendizaje basado en proyectos Práctica dirigida	Router Cisco 2811 con IOS Advance Security Image. Router Cisco 1841 con IOS IP ADV Security. Equipo de Cómputo. Sistema operativo Linux. Cañón. Internet. Appliance de seguridad (Firewall físico).

Espacio Formativo		
Aula	**Laboratorio / Taller**	**Empresa**
	X	

SEGURIDAD DE LA INFORMACIÓN

UNIDADES TEMÁTICAS

1. Unidad Temática	V. VPN.
2. Horas Prácticas	6
3. Horas Teóricas	10
4. Horas Totales	16
5. Objetivo	El alumno establecerá una conexión de red segura mediante VPNs, para transmitir con seguridad la información de la organización.

Temas	Saber	Saber hacer	Ser
Concepto y fundamentos de una VPN.	Describir las principales características de una VPN y la Seguridad en IP (IPSec).		Sistemático. Proactivo. Analítico. Objetivo. Asertivo.
Servicios de seguridad que presta una VPN.	Identificar los servicios de Seguridad de una VPN.		Sistemático. Proactivo. Analítico. Objetivo. Asertivo.
Tipos de VPNs.	Indicar los distintos tipos de VPN.		Sistemático. Proactivo. Analítico. Objetivo. Asertivo.
Protocolos que generan una VPN: PPTP, L2F, L2TP.	Describir los protocolos que generan una VPN.		Sistemático. Proactivo. Analítico. Objetivo. Asertivo.

Temas	Saber	Saber hacer	Ser
Configuración de una VPN.	Describir el procedimiento de configuración de una VPN.	Configurar una VPN.	Sistemático. Proactivo. Analítico. Objetivo. Asertivo. Creativo. Innovador. Líder. Responsable. Hábil para el trabajo en equipo.

SEGURIDAD DE LA INFORMACIÓN

Proceso de evaluación		
Resultado de aprendizaje	**Secuencia de aprendizaje**	**Instrumentos y tipos de reactivos**
El alumno, resolverá un caso de estudio y elaborará un reporte que incluya la configuración de routers y ASA para establecer una VPN.	1. Comprender el concepto de VPN. 2. Identificar los servicios de Seguridad de una VPN. 3. Identificar los tipos de VPN. 4. Comprender la operación de los protocolos PPTP, L2F, L2TP 5. Establecer la configuración de una VPN.	Estudio de Casos Lista de cotejo

SEGURIDAD DE LA INFORMACIÓN

Proceso enseñanza aprendizaje	
Métodos y técnicas de enseñanza	**Medios y materiales didácticos**
Aprendizaje basado en proyectos Práctica dirigida Análisis de casos	Router Cisco 2811 con IOS Advance Security Image Router Cisco 1841 con IOS IP ADV Security ASA 5510 Appliance with Advanced Inspection Prevention-Security Services Module Equipo de Cómputo Cañón Internet

Espacio Formativo		
Aula	**Laboratorio / Taller**	**Empresa**
	X	

SEGURIDAD DE LA INFORMACIÓN

UNIDADES TEMÁTICAS

1. Unidad Temática	VI. Detección y prevención de intrusos.
2. Horas Prácticas	5
3. Horas Teóricas	4
4. Horas Totales	9
5. Objetivo	El alumno implementará tecnologías y herramientas para la detección y prevención de intrusos para garantizar la seguridad de la red.

Temas	Saber	Saber hacer	Ser
Terminología y tecnologías de Sistemas de Detección de Intrusos.	Describir los términos y tecnologías de hardware y software referentes a la detección de intrusos.		Sistemático Proactivo Analítico Objetivo Asertivo
Tipos de sistemas de detección y prevención de intrusos.	Explicar las diferencias entre una detección de intrusiones de red/host (IDS) y la prevención de instrucciones (IPS).	Configurar la detección de intrusiones tanto en los host (software) como en soluciones appliance (hardware, Cisco ASA 5510, con módulo IPS).	Sistemático Proactivo Analítico Objetivo Asertivo Creativo Líder Hábil para el trabajo en equipo Ético Discreto

SEGURIDAD DE LA INFORMACIÓN

Proceso de evaluación		
Resultado de aprendizaje	**Secuencia de aprendizaje**	**Instrumentos y tipos de reactivos**
El alumno, resolverá un caso de estudio y elaborará un informe que incluya: • Diseño. • Configuración. • Pruebas para la implementación de un IPS.	1. Identificar las tecnologías IDS/IPS de Hardware y Software. 2. Comprender el procedimiento de implementación de un sistema de detección de intrusiones tanto en software y hardware.	Estudio de Casos Lista de cotejo

SEGURIDAD DE LA INFORMACIÓN

Proceso enseñanza aprendizaje	
Métodos y técnicas de enseñanza	**Medios y materiales didácticos**
Aprendizaje basado en proyectos Práctica dirigida Análisis de casos	Router Cisco 2811 con IOS Advance Security Image. Router Cisco 1841 con IOS IP ADV Security. Equipo de Cómputo. Sistema operativo Linux. Cañón. Internet. Software IDS/IPS (CISCO Security Agent).

Espacio Formativo		
Aula	**Laboratorio / Taller**	**Empresa**
	X	

SEGURIDAD DE LA INFORMACIÓN

CAPACIDADES DERIVADAS DE LAS COMPETENCIAS PROFESIONALES A LAS QUE CONTRIBUYE LA ASIGNATURA

Capacidad	Criterios de Desempeño
Estructurar aplicaciones Web avanzadas, móviles y de comercio electrónico, basados en métodos de ingeniería de software y web, con bases de datos para garantizar la calidad del proceso de desarrollo.	Genera documentos de especificación de requerimientos conforme a los estándares y metodologías establecidas para ello. Genera el análisis y modelado de la aplicación de acuerdo a los requerimientos con base en los estándares y metodologías (Patrones de diseño, Ingeniería de Software e Ingeniería Web). Genera la aplicación con base en el modelado previamente establecido. Ejecuta plan de pruebas para verificar funcionalidad. Documenta los resultados.
Implementar sistemas de telecomunicaciones apegándose a normas y estándares internacionales para alcanzar los objetivos de la organización.	Elabora el diseño del sistema de telecomunicaciones tomando en cuenta las condiciones requeridas (Redes convergentes, circuitos abiertos y seguridad) y considerando normas y estándares. Supervisa la instalación de la infraestructura física de telecomunicaciones apegándose al diseño. Configura los equipos y dispositivos que conforman los sistemas de telecomunicaciones con base a los requerimientos de la organización.
Estructurar la documentación que soporte la implementación del proyecto T.I. mediante el uso de metodologías y estándares correspondientes.	Elabora la documentación técnica y de usuario que soporte la implementación y operatividad del proyecto.

SEGURIDAD DE LA INFORMACIÓN

FUENTES BIBLIOGRÁFICAS

Autor	Año	Título del Documento	Ciudad	País	Editorial
Deal, Richard.	(2005)	*Complete Cisco VPN Configuration Guide, The*	Indianápolis	EE.UU.	Pearson Education, Cisco Press
Kaeo, Merike.	(2003)	*Designing Network Security, 2nd Edition*	Indianápolis	EE.UU.	Pearson Education, Cisco Press
Northcutt, Stephen, Frederick,Karen.	(2003)	*Inside Network Perimeter Security*	Indianápolis	EE.UU.	New Riders
Paquet, Catherine.	(2009)	*Implementing Cisco IOS Network Security (IINS): (CCNA Security exam 640-553) (Authorized Self-Study Guide), Rough Cuts*	Indianápolis	EE.UU.	Pearson Education, Cisco Press
Royer, Jean-Marc.	(2004)	*Seguridad en la informática de empresa: riesgos, amenazas, prevención y soluciones*	Paris	Francia	ENI Ediciones
Stallings ,William,	(2005)	*Cryptography and Network Security (4th Edition)*	Indianápolis	EE.UU.	Prentice Hall
Watkins, Michael.Wallace, Kevin.	(2008)	*CCNA Security Official Exam Certification Guide (Exam 640-553)*	Indianápolis	EE.UU.	Pearson Education, Cisco Press