UNIVERSIDAD RICARDO PALMA

FACULTAD DE INGENIERÍA

DEPARTAMENTO ACADEMICO DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE INFORMÁTICA

SÍLABO 2006-II

I. DATOS GENERALES

CURSO	: Seguridad y Protección Informática
CÓDIGO	: IF 1009
CICLO	: 10mo.
CRÉDITOS	3
CONDICIÓN	: Electivo
NATURALEZA	: Teórico-práctico
HORAS DE TEORÍA	: 2 horas
HORAS DE PRÁCTICA	: 3 horas
HORAS TOTALES	: 5 horas
REQUISITOS	: 180 créditos
COORDINADOR-PROFESOR	: Miguel Arrunátegui

II. SUMILLA

El curso consta de dos partes: teoría y práctica. En la parte teórica se presentan los conceptos, técnicas y métodos que permitan administrar la seguridad de la empresa en forma eficiente y minimizando riesgos que coloquen en peligro la continuidad operativa de la organización. Se complementa con casos prácticos orientadados al control de accesos y criptografía.

III. COMPETENCIAS DEL CURSO

Los alumnos estarán en la capacidad de analizar los conceptos de Seguridad necesarios para una correcta administración de los niveles de Seguridad en las corporaciones. El curso se enfoca en brindar y describir los diferentes dominios existentes en el Área de Seguridad de Tecnología de Información y cómo es su clasificación para que su aplicación esté correctamente identificada cuando sea necesario definir Políticas de Seguridad, controlar la inversión en el área de Seguridad y cumplir con los estándares de seguridad vigentes. Los logros a alcanzar son los siguientes:

- Comprender el alcance de la Ingeniería Administración de Seguridad y su interacción con los Procesos, Políticas y estándares corporativos.
- Conocer las metodologías para completar una Administración de seguridad eficiente.
- Conocer las diferentes áreas de seguridad y determinar que área corresponde a diferentes circunstancias asociadas a la presencia de incidentes de seguridad.

IV. PROGRAMACIÓN

Sem	Sesión / Tema	Actividades
1	Introducción: Control de Accesos	Control de Accesos. Acceso. Sujeto, Objeto. CIA Triad, Confidencialidad, Integridad, Disponibilidad. Categorías de control de Acceso. Control de Acceso Preventivo, Detectivo, Correctivo. Implementación de Control de Accesos: Administrativo, Lógico, Físico.
Sem	**Sesión / Tema**	**Actividades**
2	Técnicas de Control de Accesos	Identificación, Autenticación, Autorización. Técnicas de Identificación. Técnicas de Autenticación. Tipo 1: Algo que conoces, Tipo 2: Algo que tienes, Tipo 3: Algo que eres. Otros tipos de Autenticación.
Sem	**Sesión / Tema**	**Actividades**
3	Técnicas de Identific. y Autenticación.	Contraseñas. Debilidades, Tipos de contraseñas: dinámicas, estáticas, Pass Phrase, Password de conocimiento. Políticas de contraseñas. Métodos de ataques a contraseñas. Mejoras de seguridad en contraseñas. Análisis de Tráfico. Acceso a archivo de contraseñas, Ataques de Fuerza Bruta, Ataques de Diccionario, Ingeniería Social
Sem	**Sesión / Tema**	**Actividades**
4	Técnicas de Identific. y Autenticación.	Biométrico. Huella digital, Reconocimiento facial, Scan de Iris o Retina, Palma de la mano (topografía o geografía de la palma), Patrón de pulso/corazón, Patrón de Voz. Errores Tipo I, Tipo II, FAR, FRR, CER. Factores Negativos. TOKEN. OTP, Token estático, Token sincrónicos, Token asincrónicos, Token desafios-respuesta. Kerberos, KDC, TGS, AS, Tickets.
Sem	**Sesión / Tema**	**Actividades**
5	Seguridad en Redes	Modelo OSI. Protocolos. Niveles de Modelo OSI, Encapsulación, PDU, Segmento, Paquete, Frame, Datagrama. Nivel Físico: Especificaciones eléctricas, protocolos, interfaces, NIC, Hub, Repetidor. Nivel Enlace: Frame, Ethernet, Token Ring, ATM, FDDI, Protocolos, MAC Address, Switches.
Sem	**Sesión / Tema**	**Actividades**
6	Seguridad en Redes	Nivel Red: Información y Ruteo, Protocolos ICMP, RIP, IP, IPX, Routers. Nivel Transporte: Control de Sesiones, PDU, Reglas de sesión, servicios end-to-end, segmentación, optimización, protocolos TCP, UDP y SPX. Nivel Sesión: Gateway, Protocolos SSL, NFS, SQL, RPC, Simplex, Duplex. Nivel Presentacion: Transmisión archivos, HTTP, FTP, LPD, SMTP, Telnet. Nivel Aplicación: Protocolos TFTP, EDI, POP3, IMAP, SNMP.
Sem	**Sesión / Tema**	**Actividades**
7	Seguridad en Redes y Comunicaciones	LAN, WAN, Circuitos Privados PPP, SLIP, ISDN, DSL. Packet-switching, X.25, Frame Relay, ATM, SDLC, HDLC, HSSI. Cable Coaxil, Cableado de redes, STP, UTP. Tipos, EMI, distancia cubierta, característica de instalación. Degradación de señal. Regla 3-4-5.

Sem	Sesión / Tema	Actividades
9	Seguridad a nivel de Aplicaciones	Conceptos de Aplicaciones. Conceptos de Base de Datos, Conceptos de Sistemas Operativos. Conceptos de Programación Orientada a Objetos. Conceptos de Java. Vulnerabilidades, Amenazas. Seguridad en Base de Datos, Controles de Desarrollo de Sistemas.
Sem	**Sesión / Tema**	**Actividades**
10	Seguridad a nivel Operaciones	Gestión Administrativa. Posiciones administrativas que soportan las operaciones. Conceptos de Operaciones: Consolas, Almacenamiento, Programación automática de ejecución de procesos, Backups, Configuración, Contingencia. Protección de Recursos. Protección de Operaciones. Control de Operaciones.
Sem	**Sesión / Tema**	**Actividades**
11	Control de Ataques	Sistema Detección de Intrusos. IDS basado en conocimiento. IDS basado en comportamiento. IDS Host, IDS Red. IDS pasivo, IDS reactivo. Firewalls. Categorías de Firewalls. Firewall Packet-filter (Screening Router). Firewall Capa Aplicación (Proxy), Firewall Stateful Inspection, Firewall Dynamic packet- filtering.
Sem	**Sesión / Tema**	**Actividades**
12	Ataques	VPN. Point-to-Point Tunneling Protocol (PPTP). L2F (Layer 2 Forwarding), L2TP (Layer 2 Tunneling Protocol). IPSec. VPN Hardware, VPN Software. Tipos de Ataques. DoS – Flooding. DoS – Syn Flood. Smurf o Broadcast Store, Spoof Control Traffic Hijack, Snooping, Backdoors – Troyanos, Decoy, Sppofing, Port Scan, Password Cracking, SQL Injection.
Sem	**Sesión / Tema**	**Actividades**
13	Administración de Seguridad	Las áreas de Seguridad, Administración de Amenazas, Administración de Identidad y Acceso, Administración de Información de seguridad y la necesidad de una Consola centralizada de Seguridad. Revisión de la norma de Seguridad dictada por el Gobierno del Perú.
Sem	**Sesión / Tema**	**Actividades**
14	Administración de Identidades y Accesos	Aprovisionamiento de Usuarios, usuarios fantasmas, Roles, Administración de accesos basados en roles, usuario corporativo, Single Sign-On, Federación. Implementación de Federación por Navegación. Implementación de Federación por Documentos.

V. METODOLOGÍA

Las clases de la parte teórica se desarrollaran en aula; se presentaran conceptos, métodos y técnicas que permitan planificar, desarrollar y administrar aplicaciones informáticas para la empresa haciendo énfasis en aplicaciones concretas, y donde, el Profesor compartirá sus experiencias profesionales. Los

estudiantes desarrollarán. Paralelamente **se desarrollarán "<u>Trabajos Prácticos</u>" de "<u>Programación y Análisis</u>" sobre criptografía.**

VI. EVALUACIÓN

<u>Concepto</u>	**<u>Porcentaje</u>**	**<u>Compuesto</u>**	**<u>Responsable</u>**
Examen Parcial Teoría	**30%**	Examen Parcial.	Profesor de Teoría
Examen Final Teoría	**30%**	Examen Final.	Profesor de Teoría
Prácticas de Laboratorio	**40%**	• Desarrollo de Programas de Criptografía • Desarrollo de entornos • Ataques • Intervenciones en clase • Asistencia	Profesor de Teoría

(0.3 * EP) + (0.3 * EF) + 0.4 *((LAB1 + LAB2 + LAB3 + LAB4 + LAB5)/5)

EP : Examen Parcial
EF : Examen Final
LABx : Trabajos Laboratorio

VII. Referencias Bibliográficas

<u>Libros Texto</u>:

Information Security Management Handbook, 4th Ed.
by Harold F. Tipton and Micki Krause
CISSP Certified Information Systems
Security Professional
Study Guide

Bishop, Matt, Computer Security: Art and Science.
Addison-Wesley Professional. 1St. Edition
ISBN-10: 0201440997
ISBN-13: 978-0201440997