Federico Villarreal
Instituto de Educación Superior Tecnológico Privado

SYLLABUS
SEGURIDAD INFORMATICA

I. INFORMACION GENERAL

1.1.	**Carrera Profesional**	**:**	Computación e Informática
1.2.	**Ciclo Académico**	**:**	I
1.3.	**Semestre Lectivo**	**:**	2015-II
1.4.	**Carga Horaria Diaria**	**:**	3
1.5.	**Equipo Docente**	**:**	Ingeniero de Sistemas

II. SUMILLA

Permite al estudiante desarrollar un conocimiento amplio sobre conceptos de seguridad tanto para plataformas de sistemas operativos, redes y de gestión informática, y la capacidad de poder aplicar los conocimientos al desarrollo de una infraestructura segura en una empresa.
Se analizara las normas y estándares de seguridad informática, los tipos de delitos informáticos y los riesgos que ocasiona, lo cual desarrolla planes de contingencia en las redes de computadoras.

III. COMPETENCIAS

Administrar, gestionar e implementar el servicio de mantenimiento y operatividad de los recursos de hardware y software, redes de comunicación y los lineamientos y políticas de seguridad de la información, teniendo en cuenta los criterios y estándares vigentes.

IV. CAPACIDADES TERMINALES Y CRITERIOS DE EVALUACION

- Desarrollar el plan de aplicación de seguridad de información, de acuerdo a las medidas adoptadas por el área de soporte y mantenimiento.
- Aplica la seguridad en hardware, software y redes, estableciendo sus riesgos en cada uno de ellos.
- Describe los delitos informáticos, los tipos de virus y antivirus existentes en el mercado tecnológico.
- Aplica las normas ISO/EC para la seguridad informática.
- Realiza copy backup de los archivos importantes de una computadora y elabora los planes de seguridad en el Hardware y Software.

V. ORGANIZACIÓN DE ACTIVIDADES Y CONTENIDOS BASICOS

I UNIDAD DE FORMACION		
Día	**Fecha**	**Temas**
01		Seguridad Informática: Definición, objetivos. Amenazas, tipos de amenazas.
02		Seguridad física en los equipos de cómputo.
03		Seguridad lógica en el Software de aplicación, Base de Datos, Sistemas de Información.
04		Seguridad en las Redes: Cableado de Red, Dispositivos de Red.
05		Políticas y medidas de seguridad, análisis de riesgos
06		Delitos informáticos. Historia, casos Impacto y normatividad, prevención.
07		Robos Informáticos: Hacker, Cracker, Phreacker, Gamer, Piratas, Delincuentes Informáticos.
08		Virus informáticos: tipos, análisis de riesgos. Instalación y actualización.
09		Normas y estándares para la seguridad ISO/IEC. Normas peruanas
10		**Examen Parcial**
II UNIDAD DE FORMACION		
Día	**Fecha**	**Temas**
11		Políticas de seguridad. Niveles de acceso
12		Técnicas para asegurar la operatividad del sistema
13		Respaldo de la información. Plan de contingencias
14		Desarrollo de Planes de seguridad
15		Tipos de aplicaciones de Seguridad informática: En hardware, software, internet y redes.
16		Elaboración de informe de Seguridad informática.
17		Desarrollo de informe de seguridad informática en una empresa. Exposición del caso.
18		**Evaluación Final**

VI. METODOLOGIA

Para el desarrollo del curso se aplicaran los siguientes procedimientos didácticos:

a) **Clases teóricas:** Con exposición por parte del docente y la participación activa de los alumnos.
b) **Practica:** Se irán desarrollando talleres y casos prácticos según el tema tratado.
c) **Asesoría:** Se asesora la aplicación correcta de los conocimientos teóricos en la solución de un caso real administrado como un proyecto.

VII. EVALUACION

7.1. REQUISITOS DE APROBACION

a) La escala de calificación es vigesimal (0 a 20) y el calificativo mínimo Aprobatorio es Trece (13), en todos los casos la fracción 0,5 o más se considera como una unidad a favor del estudiante.

b) El estudiante que acumulara inasistencias injustificadas en número igual o Mayor al 30% de las sesiones de clase programadas, será desaprobado en Forma automática, sin derecho a recuperación.

c) Al Examen de Rezagados solo tendrán derecho los alumnos que no hayan Rendido algún Examen Parcial o Examen Final, el alumno que no asista a dos Exámenes parciales no podrá rendir examen de rezagados.

7.2. OBTENCION DEL PROMEDIO

a) POR UNIDAD DE FORMACION

El Promedio de cada Unidad de Formación (DOS), se obtiene de acuerdo a los siguientes criterios de evaluación:

A **Actitud**; consiste en Asistencia a clases, tardanzas, inasistencias, Uso del uniforme, respeto a las normas institucionales, participación En el aula, presentación personal, etc.

ED **Evaluación Diaria**; considera a las evaluaciones orales o escritas

EP **Evaluación Parcial**; por cada Unidad de formación Examen Parcial y Examen Final.

AP **Aptitud**; considera el desenvolvimiento del estudiante durante las Prácticas, examen práctico, revisión de examen práctico, etc.

$$\textbf{Promedio de UF} = \frac{\textbf{A+ED+EP+AP}}{\textbf{4}}$$

b) PROMEDIO FINAL

$$\textbf{Promedio Final} = \frac{\textbf{Promedio UF I + Promedio UF II}}{\textbf{2}}$$

VIII. RECURSO BIBLIOGRAFICO / BIBLIOGRAFIA

8.1. GOMEZ VIEITES, Alvaro Seguridad informática: básico
8.2. GOMEZ VIEITES, Alvaro Sistemas seguros de acceso y transmisión de datos
8.3. SCOLNIK, Hugo Qué es la seguridad informática
8.4. ANDERSON, Ross Ingeniería sobre seguridad informática
8.5. VELIZ DONOSO, Sebastian Python básico para hackers y pentester
8.6. SALAS, Antonio Los hombres que susurran a las máquinas: hackers, espías e intrusos en tu ordenador.
8.7. MITNICK, Kevin El Arte de la Intrusión: Como ser un hacker o evitarlos
8.8. AGUIAR, Edwar Seguridad informática para no informáticos