# SÍLABO:
## Seguridad Informática

## I. DATOS GENERALES:

| | | | |
|---|---|---|---|
| 1.1. | **Carrera Técnica Profesional** | : | Computación e Informática. |
| 1.2. | **Módulo Técnico Profesional** | : | Gestión del Soporte Técnico, Seguridad y Tecnología de la Información y Comunicación. |
| 1.3. | **Unidad Didáctica** | : | Seguridad Informática. |
| 1.4. | **Créditos** | : | 2 |
| 1.5. | **Año Académico** | : | |
| 1.6. | **Duración** | : | 18 Semanas |
| 1.7. | **Semestre Académico** | : | I |
| 1.8. | **Horario** | : | Jueves |
| 1.9. | **Nº Horas Semanales** | : | 03 |
| 1.10. | **Nº Horas Semestrales** | : | 54 |
| 1.11. | **Docente Responsable** | : | |

## II. COMPETENCIA DE LA CARRERA PROFESIONAL:

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.

## III. CAPACIDADES TERMINALES Y CRITERIOS DE EVALUACIÓN:

| CAPACIDAD TERMINAL | CRITERIOS DE EVALUACIÓN. |
|---|---|
| Ejecutar el plan de aplicación de seguridad de información de acuerdo a las medidas adoptadas por el oficial de seguridad | • Comunica y supervisa la aplicación de lineamientos y políticas de seguridad de la información por los usuarios finales.<br>• Reporta la ejecución de las políticas de seguridad |

## IV. ORGANIZACIÓN DE ACTIVIDADES Y CONTENIDOS BÁSICOS:

| Semanas/ Fecha | Elementos de Capacidad | Actividad de Aprendizaje | Contenidos Básicos. | Tareas Previas |
|---|---|---|---|---|
| (01) | Aplica los conceptos y los principios de la Seguridad Informática | Introducción a la Seguridad Informática. | Definiciones básicos:<br>✓ Definición.<br>✓ Objetivos de la Seguridad.<br>✓ Elementos de la Seguridad Informática<br>✓ Importancia de la seguridad de información.<br>✓ Las causas de inseguridad | Reconoce la importancia de la seguridad en el contexto personal y empresarial. |
| (02) | | | Trabajo Grupal Grupo 01 y 02 | |
| (03) | | Seguridad fisica | Amenazas<br>✓ Incendios<br>✓ Inundaciones<br>✓ Terremotos<br>✓ Trabajos no ergométricos<br>✓ Instalaciones eléctricas<br>• Estática<br>• Suministro ininterrumpido de corriente.<br>• Cableados defectuosos<br>✓ Seguridad del equipamiento | Advierte la presencia y/o factores que amenazan la seguridad. |
| (04) | | | Controles<br>✓ Sistemas de Alarma<br>✓ Control de personas<br>✓ Control de vehiculos<br>✓ Barreras infrarrojas-ultrasónicas<br>✓ Control de Hardware<br>✓ Controles biométricos<br>• Huellas digitales<br>• Control de voz<br>• Patrones oculares<br>• Verificación de firmas | |
| | | | Trabajo Grupal Grupo 03 y 04 | |

| | | | | |
|---|---|---|---|---|
| (05) | | Seguridad Lógica | ✓Principios de la seguridad lógica<br>✓Técnicas de control de acceso<br>•Identificación y autenticación<br>▪ Password seguras<br>•Roles<br>•Limitaciones a los servicios<br>•Modalidad de acceso<br>•Ubicación y horarios<br>✓Administración<br>• Administración del Personal Y Usuarios<br>✓Análisis de riesgo: plan estratégico de seguridad.<br>✓Normatividad y estándares de seguridad. | Actualizaciones del Sistema y Aplicaciones.<br><br>Elabora las políticas de seguridad informática y de la información. |
| (06) | | | | |
| | | | Evaluación Parcial de Seguridad Informática | |
| (07) | | Delitos Informáticos | ✓ Fraudes cometidos mediante manipulación<br>✓ de computadoras<br>✓ Daños a programas o datos almacenados<br>✓ Manipulación de datos de E/S<br>✓ Distribución de virus<br>✓ Espionaje<br>✓ Acceso no autorizado<br>✓ Reproducción y distribución de programas<br>✓ protegido por la ley | Aplica los principios de la seguridad informática según el escenario de amenazas y debilidades. |
| (08) | | | | |
| | | | Trabajo Grupal Grupo 05 y 06 | |
| (09) | | Amenazas Humanas | Tipos de Amenazas<br>• Internas<br>▪ Deshonestidad<br>▪ Errores<br>▪ Descuido<br>• Externas<br>▪ Seguridad Física<br>▪ Ataque Remotos<br>• Hacker<br>• Cracker<br>• Phreaker<br>• Pirata Informático<br>• Creador de virus<br>• Diseminadores de virus<br>• Insider | Aplica las medidas de prevención según los ataques, delitos |
| (10) | | | | |

| | | | | |
|---|---|---|---|---|
| | | | Trabajo Grupal Grupo 07 y 08 | |
| (11)<br>(12) | | Ataques | Tipos<br>Ingeniería Social<br>Social Inversa<br>Trashing<br>Vulnerabilidades propias de los sistemas | Aplica las medidas de prevención según los ataques, delitos |
| | | | Evaluación Parcial de Seguridad Informática | |
| (13)<br>(14) | | Virus y Antivirus | • Definición<br>• Tipos de Virus<br>• Carácter Vandálico<br>• Carácter Dirigido<br>• Programas que no cumplen con la definición de virus.<br>• Tipos de daños<br>Antivirus<br>• Definición<br>• Detección<br>• Identificación | Identifica los tipos de virus y sus variantes.<br>Implementación de corta fuego y antivirus corporativo. |
| | | | Trabajo Grupal Grupo 09 y 10 | |
| (15)<br>(16) | | Modelo de Protección | • Política de seguridad de la organización<br>• Auditorías permanentes<br>• Plan de respuestas a incidentes<br>• Sistema de seguridad a nivel físico<br>• Seguridad a nivel Router–Firewall<br>• Sistemas de detección de intrusos (IDS)<br>• Penetration Testing | Utiliza el cortafuego de Windows para la seguridad de la red. |
| | | | Trabajo Grupal Grupo 09 y 10 | |
| (17) | | Criptografía y Autenticación | • Definición<br>• Métodos Criptográficos<br>▪ Clásicos<br>▪ Modernos<br>• Utilidad de la Criptografía | Cifra y descifra mensajes escritos. |
| (18) | | | ➢ Evaluación Final (Elabora el plan de contingencia de seguridad informática y de la información.)<br>➢ Presentación de y Sustentación de Trabajos | |

Instituto de Educación Superior Tecnológico Público Cap. FAP José Abelardo Quiñones - Unidad Académica - Tumbes

## V. METODOLOGÍA:

**5.1.** Expositiva y participativa (Interacción permanente Docente – Alumno).
**5.2.** Cultura participativa y trabajo en equipo.
**5.3.** Análisis de lecturas y conversatorios, y debates; a fin de expresar los niveles de pensamiento creativo, crítico y reflexivo.
**5.4.** Investigación permanente y sustentación de propuestas.

## VI. EVALUACIÓN:

El proceso de evaluación será permanente y comprenderá:

6.1. Evaluación Formativa Interactiva: participación activa en las clases, conversatorios o debates.
6.2. En las exposiciones primara la capacidad reflexiva, la correlación de criterios, el análisis y pensamiento lógico.
6.3. Actividades de Aprendizaje: Análisis de lecturas, Trabajos Monográficos e Informenes de Investigación personal o grupal, elaboración de organizadores gráficos
6.4. De la asistencia: la falta a 5 Sesiones de Aprendizaje determinan la inhabilitación de la Unidad Didáctica y la justificación se hará únicamente con documentación oficial emitida a la Dirección del Instituto.
6.5. El calificativo mínimo aprobatorio es de trece (13), para el proceso de recuperación el estudiante deberá tener una nota desaprobatoria entre diez (10) y doce (12); el que obtenga una nota por debajo de diez (10) desaprueba la Unidad Didáctica.
6.6. El estudiante para ingresar al aula deberá estar adecuadamente uniformado.

## VII. REFERENCIAS BIBLIOGRÁFICAS:


**7.1. Impresos.**

- ✓ Arturo Hernández H. Virus informático. Computo Académico UNAM-2007.
- ✓ Purificación Aguilar López. Seguridad Informática. Editex -2011

**7.2. Digitales.(página WEB)**

- ✓ http://seguridadinformaticasmr.wikispaces.com/TEMA+7+-+CRIPTOGRAFIA
- ✓ http://www.segu-info.com.ar/fisica/seguridadfisica.htm
- ✓ https://seguridadinformaticasmr.wikispaces.com/TEMA+3+-+SEGURIDAD+L%C3%93GICA
- ✓ https://seguridadinformaticasmr.wikispaces.com/TEMA+3+-+SEGURIDAD+L%C3%93GICA


Instituto de Educación Superior Tecnológico Público Cap FAP José Abelardo Quiñones - Unidad Académica - Tumbes

I.E.S.T.P "CAP FAP JOSÉ A. QUIÑONES"
CPC. Eriberto Guerrero Mateo
Jefe (e) Unidad Académica