



SÍLABO:
Seguridad Informática

I. DATOS GENERALES:

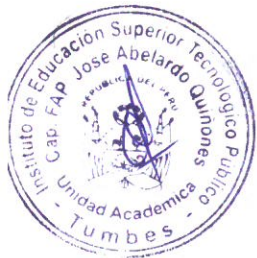
- 1.1. Carrera Técnica Profesional : Computación e Informática.
- 1.2. Módulo Técnico Profesional : Gestión del Soporte Técnico, Seguridad y Tecnología de la Información y Comunicación.
- 1.3. Unidad Didáctica : Seguridad Informática.
- 1.4. Créditos : 2
- 1.5. Año Académico :
- 1.6. Duración : 18 Semanas
- 1.7. Semestre Académico : I
- 1.8. Horario : Jueves
- 1.9. N° Horas Semanales : 03
- 1.10. N° 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	<ul style="list-style-type: none">• Comunica y supervisa la aplicación de lineamientos y políticas de seguridad de la información por los usuarios finales.• Reporta la ejecución de las políticas de seguridad

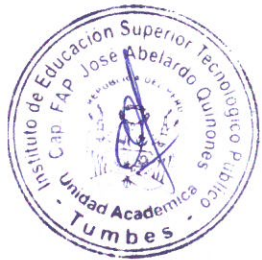




**IESTP "CAP. FAP. José Abelardo Quiñones"
TUMBES - PERÚ**

IV. ORGANIZACIÓN DE ACTIVIDADES Y CONTENIDOS BÁSICOS:

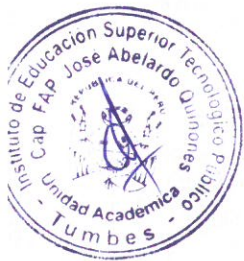
Semanas/ Fecha	Elementos de Capacidad	Actividad de Aprendizaje	Contenidos Básicos.	Tareas Previas
(01)	Aplica los conceptos y los principios de la Seguridad Informática	Introducción a la Seguridad Informática.	Definiciones básicas: ✓ Definición. ✓ Objetivos de la Seguridad. ✓ Elementos de la Seguridad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





**IESTP "CAP. FAP. José Abelardo Quiñones"
TUMBES - PERÚ**

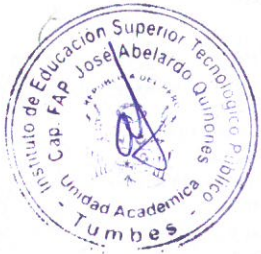
(05)		Seguridad Lógica	<ul style="list-style-type: none"> ✓ Principios de la seguridad lógica ✓ Técnicas de control de acceso <ul style="list-style-type: none"> • Identificación y autenticación <ul style="list-style-type: none"> ▪ Password seguras • Roles • Limitaciones a los servicios • Modalidad de acceso • Ubicación y horarios ✓ Administración <ul style="list-style-type: none"> • Administración del Personal Y Usuarios ✓ Análisis de riesgo: plan estratégico de seguridad. ✓ Normatividad y estándares de seguridad. 	Actualizaciones del Sistema y Aplicaciones.
(06)			Elabora las políticas de seguridad informática y de la información.	
Evaluación Parcial de Seguridad Informática				
(07)		Delitos Informáticos	<ul style="list-style-type: none"> ✓ Fraudes cometidos mediante manipulación ✓ de computadoras ✓ Daños a programas o datos almacenados ✓ Manipulación de datos de E/S ✓ Distribución de virus ✓ Espionaje ✓ Acceso no autorizado ✓ Reproducción y distribución de programas ✓ 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	<p>Tipos de Amenazas</p> <ul style="list-style-type: none"> • Internas <ul style="list-style-type: none"> ▪ Deshonestidad ▪ Errores ▪ Descuido • Externas <ul style="list-style-type: none"> ▪ Seguridad Física ▪ Ataque Remotos • Hacker • Cracker • Phreaker • Pirata Informático • Creador de virus • Diseminadores de virus • Insider 	Aplica las medidas de prevención según los ataques, delitos
(10)				





IESTP "CAP. FAP. José Abelardo Quiñones"
TUMBES - PERÚ

			Trabajo Grupal Grupo 07 y 08	
(11)		Ataques	Tipos Ingeniería Social Social Inversa Trashing Vulnerabilidades propias de los sistemas	Aplica las medidas de prevención según los ataques, delitos
(12)				
			Evaluación Parcial de Seguridad Informática	
(13)		Virus y Antivirus	<ul style="list-style-type: none"> • Definición • Tipos de Virus • Carácter Vandálico • Carácter Dirigido • Programas que no cumplen con la definición de virus. • Tipos de daños Antivirus	Identifica los tipos de virus y sus variantes. Implementación de corta fuego y antivirus corporativo.
(14)				
			Trabajo Grupal Grupo 09 y 10	
(15)		Modelo de Protección	<ul style="list-style-type: none"> • Política de seguridad de la organización • Auditorías permanentes • Plan de respuestas a incidentes • Sistema de seguridad a nivel físico • Seguridad a nivel Router-Firewall • Sistemas de detección de intrusos (IDS) • Penetration Testing 	Utiliza el cortafuego de Windows para la seguridad de la red.
(16)				
			Trabajo Grupal Grupo 09 y 10	
(17)		Criptografía y Autenticación	<ul style="list-style-type: none"> • Definición • Métodos Criptográficos <ul style="list-style-type: none"> ▪ Clásicos ▪ Modemos • Utilidad de la Criptografía 	Cifra y descifra mensajes escritos.
(18)			<ul style="list-style-type: none"> ➢ Evaluación Final (Elabora el plan de contingencia de seguridad informática y de la información.) ➢ Presentación de y Sustentación de Trabajos 	





IESTP "CAP. FAP. José Abelardo Quiñones"
TUMBES - PERÚ

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.

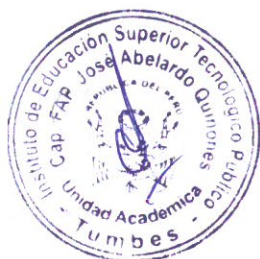
VI. EVALUACIÓN:

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. Edítex -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



IESTP
"CAP. FAP. JOSÉ A. QUINONES"
CPC. Eriberto Guerrero Mateo
Jefe (e) Unidad Académica



At the
of the
of the
of the