UNIVERSIDAD TECNOLÓGICA DEL VALLE DEL MEZQUITAL

PLANEACIÓN DIDÁCTICA DESDE LA ENSEÑANZA BASADA EN COMPETENCIAS

Programa Educativo: INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	**Facilitador: ING. EMILIANO BOMAYE ROQUE**
Cuatrimestre: 10 "B"	**Periodo Escolar: SEPTIEMBRE-DICIEMBRE-2020**

1. DATOS GENERALES DE LA ASIGNATURA

Nombre de la asignatura:	Seguridad de la Información				
Competencia(s) que desarrolla:	Dirigir proyectos de tecnologias de informacion (T.I.) para contribuir a la productividad y logro de los objetivos estrategicos de las organizaciones utilizando las metodologias apropiadas. evaluar sistemas de tecnologias de informacion (T.I.) para estab				
Horas prácticas:	35	**Horas teóricas:**	40	**Horas totales:**	75
Objetivo:	EL ALUMNO IDENTIFICAR LAS VULNERABILIDADES DE LOS SISTEMAS DE INFORMACION DE UNA ORGANIZACION# PARA ESTABLECER LOS MEDIOS APROPIADOS DE PROTECCION QUE ASEGUREN UNA EFICAZ GESTION DE LAS OPERACIONES.				
Nombre de las unidades temáticas:	1. Introducción a la seguridad de la información. 2. Administración de la seguridad. 3. Métodos de autenticación. 4. Firewalls. 5. VPN. 6. Detección y prevención de intrusos.				

2. DATOS DE LAS UNIDADES TEMÁTICAS

Número y nombre de la unidad temática	Objetivo general por unidad temática	Temas de cada unidad temática
1. Introducción a la seguridad de la información.	El alumno implementará una política de seguridad para proteger la información de la organización apoyándose en las normas aplicables.	Introducción a la Seguridad de la Información. Políticas de seguridad. Escenarios de ataques a redes. Código malicioso. Principios matemáticos para criptografía. Algoritmos de criptografía. Normatividad nacional e internacional de seguridad.
2. Administración de la seguridad.	El alumno administrará la seguridad informática para garantizar la disponibilidad de la información.	Administración de llaves públicas. Administración de riesgos y continuidad de actividades. Prevención y recuperación de incidentes. Protección de Sistemas Operativos. Protocolo SSL y SSL Handshake.
3. Métodos de autenticación.	El alumno implementará el método de autenticación adecuado para garantizar el acceso seguro a las aplicaciones y servicios informáticos de la organización.	Servicios AAA. Algoritmos de Hash MD5 y SHA-1. Certificados digitales.
4. Firewalls.	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.

Medidas de seguridad preventivas y

		correctivas aplicables a un Firewall. Técnicas de implementación de Firewall.

5. VPN.

	El alumno establecerá una conexión de red segura mediante VPNs, para transmitir con seguridad la información de la organización.

		Concepto y fundamentos de una VPN. Servicios de seguridad que presta una VPN. Tipos de VPNs. Protocolos que generan una VPN: PPTP, L2F, L2TP. Configuración de una VPN.
6. Detección y prevención de intrusos.	El alumno implementará tecnologías y herramientas para la detección y prevención de intrusos para garantizar la seguridad de la red.	Terminología y tecnologías de Sistemas de Detección de Intrusos. Tipos de sistemas de detección y prevención de intrusos.

3. SECUENCIA DIDÁCTICA POR UNIDAD TEMÁTICA(UNA TABLA POR UNIDAD DE CURSO)			
Unidad:	Introducción a la seguridad de la información.	**Duración (Horas)*:**	16
Objetivo de unidad:	El alumno implementará una política de seguridad para proteger la información de la organización apoyándose en las normas aplicables.		

Tipos de Saberes		
Saber	**Saber Hacer**	**Ser**
Describir los tipos de seguridad informática y los conceptos de disponibilidad, integridad, confidencialidad y control de acceso. Identificar las características de una política de seguridad.	Elaborar políticas de seguridad identificando ventajas y desventajas de su implementación. Configurar seguridad de puerto, deshabilitar auto trunking, habilitar BPDU Guard y Root Guard), des	Sistemático. Creativo. Líder. Proactivo. Analítico. Asertivo. Hábil para el trabajo en equipo. Sociable.

Resultado de la unidad de aprendizaje
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.

Secuencia didáctica		
Actividades iniciales	**Actividades de desarrollo**	**Actividades finales**
Presentación de la materia, entrega de temario, porcentajes y criterios de evaluación. Aplicación de examen diagnóstico. Leer el capítulo Amenazas modernas a la seguridad de las redes. Investigar elementos del protocolo CDP. Investigar políticas de seguridad y tipos de virus. Investigar características y aplicación de las normas ISO 27001 y ISO 17799	Presentación de vídeo motivacional Explicación de tema; Seguridad en redes, tipos de ataques en capa 2; Falsificación y DOS. Práctica demostrativa bloqueo de puertos. Elaborar en equipo un manual de políticas. Elaborar un mapa conceptual.	Elaborar práctica bloqueo de puertos. Elaborar práctica, deshabilitar protocolos CDP. Realizar evaluación de curso capítulo I.
Medios y materiales didácticos:	Computadora, Internet, Bibliografía, Software especializado	
Estrategias de enseñanza:	Aprendizaje basado en problemas	
Técnicas de enseñanza:	Lluvia de ideas, Interrogatorio, Equipos, Trabajo en binas	
Estrategias de aprendizaje:	Mapas conceptuales , Otros	
Evidencias de aprendizaje:	Portafolio de evidencias.	

4. DESCRIPCIÓN DEL SISTEMA DE EVALUACIÓN DE LA UNIDAD DE APRENDIZAJE			
Tipo de Evaluación	**Estrategia de Evaluación**	**Instrumento de Evaluación**	
Evaluación Diagnóstica:	Otro	**Tipo de Instrumento**	
		Examen	
Evaluación Formativa:		**Tipo de instrumento**	**Valor del instrumento (%)**
	Pruebas de Rendimiento	Lista de Cotejo o verificación	45 %
	Mapa conceptual	Lista de Cotejo o verificación	15 %
	Otro	Examen	40 %
			100 %
Evaluación Sumativa (Fecha de asignación de la calificación)	02/10/2020		

3. SECUENCIA DIDÁCTICA POR UNIDAD TEMÁTICA(UNA TABLA POR UNIDAD DE CURSO)			
Unidad:	Administración de la seguridad.	**Duración (Horas)*:**	14
Objetivo de unidad:	El alumno administrará la seguridad informática para garantizar la disponibilidad de la información.		

Tipos de Saberes		
Saber	**Saber Hacer**	**Ser**
Identificar los mecanismos y relevancia de la administración de llaves públicas en un canal de comunicación seguro. Describir los componentes generales de una Administración de Riesgos de la Información (ARI).	Configurar una entidad certificadora (servidor) con base en el estándar X.509 para llaves públicas. Elaborar una matriz de riesgos aplicada a la seguridad de la información.	Sistemático. Creativo. Proactivo. Líder.

Resultado de la unidad de aprendizaje
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. Configuraci

Secuencia didáctica		
Actividades iniciales	**Actividades de desarrollo**	**Actividades finales**
Investigar en que consiste el estándar x.509.	Explicación de tema y práctica demostrativa configuración de certificados.	Elaborar práctica de configuración de certificados.
En binas deberán investigar la administración de riesgos de la información.	Explicación de tema.	Elaborar una matriz de riesgos de seguridad informática.
Investigar en que consiste las guías NIST SP800 E ISO 17799.	Explicación de tema.	En binas deberán elaborar un plan de contingencia y procedimientos.
Leer el capítulo 2 protocolo de SSH, SSL y SSL Handshake.	Explicación de tema y práctica demostrativa	Elaborar práctica. Realizar evaluación de curso capítulo II y III.
Medios y materiales didácticos:	Computadora, Internet, Bibliografía, Software especializado	
Estrategias de enseñanza:	Aprendizaje basado en problemas	
Técnicas de enseñanza:	Lluvia de ideas, Interrogatorio, Equipos, Trabajo en binas	
Estrategias de aprendizaje:	Otros	
Evidencias de aprendizaje:	Portafolio de evidencias.	

4. DESCRIPCIÓN DEL SISTEMA DE EVALUACIÓN DE LA UNIDAD DE APRENDIZAJE			
Tipo de Evaluación	**Estrategia de Evaluación**	**Instrumento de Evaluación**	
Evaluación Diagnóstica:	Otro	**Tipo de Instrumento**	
		Examen	
Evaluación Formativa:		**Tipo de instrumento**	**Valor del instrumento (%)**
	Informes	Lista de Cotejo o verificación	15 %
	Pruebas de Rendimiento	Lista de Cotejo o verificación	45 %
	Otro	Examen	40 %
			100 %
Evaluación Sumativa (Fecha de asignación de la calificación)	30/10/2020		

3. SECUENCIA DIDÁCTICA POR UNIDAD TEMÁTICA(UNA TABLA POR UNIDAD DE CURSO)			
Unidad:	Métodos de autenticación.	**Duración (Horas)*:**	13
Objetivo de unidad:	El alumno implementará el método de autenticación adecuado para garantizar el acceso seguro a las aplicaciones y servicios informáticos de la organización.		

Tipos de Saberes		
Saber	**Saber Hacer**	**Ser**
Identificar las ventajas que ofrece el uso de servicio Radius, TACACS y Kerberos. Identificar las principales características de los algoritmos de Hash MD5 y SHA-1.	Configurar autenticación de usuarios utilizando RADIUS. Configurar el uso de certificados digitales en aplicaciones de correo electrónico.	Sistemático Proactivo Creativo Líder Hábil para el trabajo en equipo

Resultado de la unidad de aprendizaje
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.

Secuencia didáctica		
Actividades iniciales	**Actividades de desarrollo**	**Actividades finales**
Explicación de tema, servidores Radius y Keberos. Investigar y elaborar un mapa conceptual de los algoritmos HASH, MD5 y SHA-1. Investigar que son los certificados digitales.	En equipos deberán configurar el servidor de Radius. En binas deberán contestar un crucigrama. Explicación de tema	Elaborar un manual de instalación. Elaborar práctica de configuración de certificados.
Medios y materiales didácticos:	Computadora, Internet, Bibliografía, Software especializado	
Estrategias de enseñanza:	Aprendizaje basado en problemas	
Técnicas de enseñanza:	Lluvia de ideas, Interrogatorio, Equipos, Trabajo en binas	
Estrategias de aprendizaje:	Otros	
Evidencias de aprendizaje:	Portafolio de evidencias.	

4. DESCRIPCIÓN DEL SISTEMA DE EVALUACIÓN DE LA UNIDAD DE APRENDIZAJE			
Tipo de Evaluación	**Estrategia de Evaluación**	**Instrumento de Evaluación**	
Evaluación Diagnóstica:	Otro	**Tipo de Instrumento**	
		Examen	
Evaluación Formativa:		**Tipo de instrumento**	**Valor del instrumento (%)**
	Informes	Lista de Cotejo o verificación	10 %
	Pruebas de Rendimiento	Lista de Cotejo o verificación	50 %
	Otro	Examen	40 %
			100 %
Evaluación Sumativa (Fecha de asignación de la calificación)	20/11/2020		

3. SECUENCIA DIDÁCTICA POR UNIDAD TEMÁTICA(UNA TABLA POR UNIDAD DE CURSO)			
Unidad:	Firewalls.	**Duración (Horas)*:**	7
Objetivo de unidad:	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.		

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

Resultado de la unidad de aprendizaje
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.

Secuencia didáctica		
Actividades iniciales	**Actividades de desarrollo**	**Actividades finales**
Explicación de los mecanismos de seguridad de Firewalls. Investigar las técnicas de implementación a nivel de red y aplicación.	Elaborar una exposición incluir práctica demostrativa. Explicación mecanismos a nivel de red. Practica demostrativa.	Implementar la configuración. Práctica de configuración de listas de acceso. Evaluación del curso capítulo VI y VII.
Medios y materiales didácticos:	Computadora, Internet, Bibliografía, Software especializado	
Estrategias de enseñanza:	Aprendizaje basado en problemas	
Técnicas de enseñanza:	Lluvia de ideas, Interrogatorio, Equipos, Trabajo en binas	
Estrategias de aprendizaje:	Otros	
Evidencias de aprendizaje:	Portafolio de evidencia.	

4. DESCRIPCIÓN DEL SISTEMA DE EVALUACIÓN DE LA UNIDAD DE APRENDIZAJE			
Tipo de Evaluación	**Estrategia de Evaluación**	**Instrumento de Evaluación**	
Evaluación Diagnóstica:	Otro	**Tipo de Instrumento**	
		Examen	
Evaluación Formativa:		**Tipo de instrumento**	**Valor del instrumento (%)**
	Pruebas de Rendimiento	Lista de Cotejo o verificación	60 %
	Otro	Examen	40 %
			100 %
Evaluación Sumativa (Fecha de asignación de la calificación)	04/12/2020		

3. SECUENCIA DIDÁCTICA POR UNIDAD TEMÁTICA(UNA TABLA POR UNIDAD DE CURSO)			
Unidad:	VPN.	**Duración (Horas)*:**	16
Objetivo de unidad:	El alumno establecerá una conexión de red segura mediante VPNs, para transmitir con seguridad la información de la organización.		

Tipos de Saberes		
Saber	**Saber Hacer**	**Ser**
Describir las principales características de una VPN y la Seguridad en IP (IPSec). Identificar los servicios de Seguridad de una VPN.	Configurar una VPN.	Sistemático. Proactivo. Analítico. Objetivo. Asertivo. Creativo. Innovador. Líder. Responsable. Hábil para el trabajo en equipo.

Resultado de la unidad de aprendizaje
El alumno, resolverá un caso de estudio y elaborará un reporte que incluya la configuración de routers y ASA para establecer una VPN.

Secuencia didáctica		
Actividades iniciales	**Actividades de desarrollo**	**Actividades finales**
Investigar que son las VPN, servicios de seguridad, tipos y elaborar un mapa conceptual.	Explicación de tema. En binas deberán elaborar práctica demostrativa .	Elaborar la configuración de una VPN. Contestar cuestionario. Evaluación del curso capítulo VIII y IX.
Medios y materiales didácticos:	Computadora, Internet, Bibliografía, Software especializado	
Estrategias de enseñanza:	Aprendizaje basado en problemas	
Técnicas de enseñanza:	Lluvia de ideas, Interrogatorio, Equipos, Trabajo en binas	
Estrategias de aprendizaje:	Mapas conceptuales , Otros	
Evidencias de aprendizaje:	Portafolio de evidencias.	

4. DESCRIPCIÓN DEL SISTEMA DE EVALUACIÓN DE LA UNIDAD DE APRENDIZAJE			
Tipo de Evaluación	**Estrategia de Evaluación**	**Instrumento de Evaluación**	
Evaluación Diagnóstica:	Otro	**Tipo de Instrumento**	
		Examen	
Evaluación Formativa:		**Tipo de instrumento**	**Valor del instrumento (%)**
	Pruebas de Rendimiento	Lista de Cotejo o verificación	50 %
	Mapa conceptual	Lista de Cotejo o verificación	10 %
	Otro	Examen	40 %
			100 %
Evaluación Sumativa (Fecha de asignación de la calificación)	07/12/2020		

3. SECUENCIA DIDÁCTICA POR UNIDAD TEMÁTICA(UNA TABLA POR UNIDAD DE CURSO)			
Unidad:	Detección y prevención de intrusos.	**Duración (Horas)*:**	9
Objetivo de unidad:	El alumno implementará tecnologías y herramientas para la detección y prevención de intrusos para garantizar la seguridad de la red.		

Tipos de Saberes		
Saber	**Saber Hacer**	**Ser**
Describir los términos y tecnologías de hardware y software referentes a la detección de intrusos.	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

Resultado de la unidad de aprendizaje
El alumno, resolverá un caso de estudio y elaborará un informe que incluya: Diseño. Configuración. Pruebas para la implementación de un IPS.

Secuencia didáctica		
Actividades iniciales	**Actividades de desarrollo**	**Actividades finales**
Investigar las detenciones de intrusos IDS, IPS y elaborar un resumen.	Explicación de tema y practica demostrativa.	Elaborar práctica demostrativa. Evaluación curso capítulo X y XI
Medios y materiales didácticos:	Computadora, Internet, Bibliografía	
Estrategias de enseñanza:	Aprendizaje basado en problemas	
Técnicas de enseñanza:	Lluvia de ideas, Interrogatorio, Equipos, Trabajo en binas	
Estrategias de aprendizaje:	Resumen, Otros	
Evidencias de aprendizaje:	Portafolio de evidencias.	

4. DESCRIPCIÓN DEL SISTEMA DE EVALUACIÓN DE LA UNIDAD DE APRENDIZAJE			
Tipo de Evaluación	**Estrategia de Evaluación**	**Instrumento de Evaluación**	
Evaluación Diagnóstica:	Otro	**Tipo de Instrumento**	
		Examen	
Evaluación Formativa:		**Tipo de instrumento**	**Valor del instrumento (%)**
	Pruebas de Rendimiento	Lista de Cotejo o verificación	60 %
	Otro	Examen	40 %
			100 %
Evaluación Sumativa (Fecha de asignación de la calificación)	09/12/2020		

5. DESCRIPCIÓN DEL PROYECTO INTEGRADOR (Requisitar únicamente para asignaturas integradoras)	
Objetivo:	
Asignaturas que contribuyen a la competencia específica:	
Componentes del proyecto:	

ING. EMILIANO BOMAYE ROQUE	MTRA. GLORIA MARTÍNEZ MARTÍN
Elaboró	**Vo. Bo. del Director del PE**
El Nith, Ixmiquilpan, Hidalgo	04/09/2020
Lugar	**Fecha de elaboración**