ASIGNATURA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA

1. Competencias	Diseñar y optimizar soluciones de redes digitales, a través de la administración y dirección de proyectos tecnológicos, alineados a normas y estándares vigentes, para contribuir a la continuidad del negocio.
2. Cuatrimestre	Octavo
3. Horas Teóricas	25
4. Horas Prácticas	50
5. Horas Totales	75
6. Horas Totales por Semana Cuatrimestre	5
7. Objetivo de aprendizaje	El alumno identificará las vulnerabilidades de los sistemas de información para establecer los medios apropiados de seguridad, que contribuyan a la continuidad de negocio.

Unidades de Aprendizaje	Horas		
	Teóricas	**Prácticas**	**Totales**
I. Seguridad de los dispositivos de red	5	10	15
II. Dispositivos y Servicios de Seguridad	5	15	20
III. Criptografía y Redes privadas virtuales VPNs	5	10	15
IV. Implementación de Dispositivos especializados	5	10	15
V. Administración de redes seguras	5	5	10
Totales	**25**	**50**	**75**

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**I. Seguridad de los dispositivos de red**
2. Horas Teóricas	5
3. Horas Prácticas	10
4. Horas Totales	15
5. Objetivo de la Unidad de Aprendizaje	El alumno implementará la seguridad en dispositivos de red para contribuir a la continuidad del negocio

Temas	Saber	Saber hacer	Ser
Fundamentos de Seguridad	Definir los conceptos de confidencialidad, integridad, disponibilidad Identificar los conceptos asociados al cubo de destrezas de la ciberseguridad		Analítico Proactivo Pensamiento lógico Autodidacta Ordenado Capacidad para investigar Capacidad de abstracción
Vulnerabilidades y Amenazas de Red	Identificar las vulnerabilidades y amenazas de red Identificar técnicas de mitigación de ataques comunes de red	Proponer las técnicas de mitigación de acuerdo a las vulnerabilidades y amenazas de red	Analítico Proactivo Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad

Temas	Saber	Saber hacer	Ser
Aseguramiento de dispositivos de borde de red	Identificar las áreas de aseguramiento de los ruteadores de borde Identificar las tareas de aseguramiento de los accesos administrativos a los ruteadores Identificar las opciones seguras de accesos local y remoto a los dispositivos de borde	Configurar el acceso administrativo seguro Configurar las características mejoradas de inicio de sesión Configurar conexiones remotas seguras, SSH Configurar el acceso a la interfaz de línea de comandos basado en roles	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad
Seguridad de dispositivos finales	Identificar las tareas de aseguramiento de los accesos administrativos a los dispositivos finales Identificar las opciones seguras de accesos local y remoto a los dispositivos finales	Configurar el acceso administrativo seguro Configurar servicios de seguridad antimalware Configurar servicios de seguridad de conexión remota	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad
Monitoreo y administración de dispositivos	Distinguir las medidas de aseguramiento del sistema operativo y el archivo de configuración de los dispositivos de borde Identificar las características de las herramientas de administración y monitoreo de red	Configurar funciones de recuperación y aseguramiento del sistema operativo Configurar la función de copia segura de archivos de los dispositivos de borde Configurar el protocolo de registro de sistema, Syslog Configurar el protocolo simple de administración de red, SNMP	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad

Temas	Saber	Saber hacer	Ser
Seguridad de sistemas operativos	Distinguir las funciones de un sistema operativo Diferenciar tipos de sistemas operativos Identificar mecanismos de control de acceso a sistemas operativos	Proponer mecanismos de control de acceso a sistemas operativos Configurar perfiles de privilegios de usuarios y dispositivos Programar actualizaciones y aplicación de parches a los sistemas operativos	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
A partir de un caso práctico, elabora y presenta una memoria técnica y una simulación que incluya: Memoria técnica - Análisis de vulnerabilidades y amenazas - Propuesta de técnicas de mitigación - Descripción de estrategias para aseguramiento de dispositivos de borde, dispositivos finales y sistemas operativos - Scripts de configuración Simulación - Configuración de acceso administrativo seguro - Configuración de las características mejoradas de inicio de sesión - Configuración de conexiones remotas seguras, SSH - Configuración del acceso a la interfaz de línea de comandos basado en roles - Configuración las funciones de recuperación y aseguramiento del sistema operativo	1. Identificar los fundamentos de seguridad 2. Identificar las amenazas, vulnerabilidades y técnicas de mitigación 3. Identificar las técnicas de aseguramiento de dispositivos de borde, finales y sistemas operativos 4. Explicar las configuraciones del aseguramiento de dispositivos de borde, finales y sistemas operativos	1. Proyecto 2. Lista de cotejo

- Configuración de la función de copia segura de archivos de los dispositivos de borde - Configuración del protocolo de registro de sistema, Syslog - Configuración del protocolo simple de administración de red, SNMP		

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Aprendizaje basado en proyectos -Equipos colaborativos -Estudio de casos	-Equipo de computo -Acceso a internet -Cañón -Ruteadores -Switches -Simulador de redes

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X		

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**II. Dispositivos y Servicios de Seguridad**
2. Horas Teóricas	5
3. Horas Prácticas	15
4. Horas Totales	20
5. Objetivo de la Unidad de Aprendizaje	El alumno implementará métodos de acceso seguro, tecnologías de cortafuegos y sistemas de prevención de intrusos para resguardar los recursos de la organización.

Temas	Saber	Saber hacer	Ser
Autenticación, Autorización y Contabilidad AAA	Identificar las características de los servicios AAA Identificar las características de la Autenticación AAA local y basada en servidor Diferenciar las funciones de los protocolos de AAA basada en servidor	Configurar servicios de Autenticación AAA local basada en interfaz de línea de comandos. Configurar servicios AAA basados en servidor.	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad
Tecnologías de cortafuegos	Identificar los beneficios y las limitaciones de tecnologías de cortafuegos Comparar tipos de tecnologías de cortafuegos	Establecer medidas de seguridad basadas en identificación de puertos y establecimiento de zona desmilitarizada. Implementar tecnologías de firewalls de filtrado de paquetes y firewalls de políticas basadas en zonas.	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad

Temas	Saber	Saber hacer	Ser
IDS e IPS	Identificar las características de sistemas IDS e IPS Identificar las características de IPS basado en host e IPS basado en red	Configurar Sistemas IPS basados en host. Configurar Sistemas IPS basados en red.	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
A partir de un caso práctico, elabora y presenta una memoria técnica y una simulación que incluya: Memoria técnica -Identificar las técnicas de acceso seguro -Descripción de las tecnologías de seguridad implementadas -Topología lógica de red -Tabla de direccionamiento -Scripts de configuración -Pruebas de conectividad Simulación -Configuración de acceso administrativo seguro -Configuración de servicios AAA -Configuración del rutedor como firewall -Configuración del rutedor como IDS -Configuración del rutedor como IPS	1.-Identificar los servicios AAA 2.-Explicar el funcionamiento de los tipos de firewall 3.-Explicar el funcionamiento de IDS e IPS 4.-Explicar las configuraciones del aseguramiento de la red por medio de los servicios AAA, Firewall, IDS e IPS	1. Proyecto 2. Lista de cotejo

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Aprendizaje basado en proyectos -Equipos colaborativos -Estudio de casos	-Equipo de computo -Acceso a internet -Cañón -Ruteadores -Switches -Simulador de redes -Firewalls basados en hardware

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**III. Criptografía y Redes privadas virtuales VPNs**
2. Horas Teóricas	5
3. Horas Prácticas	10
4. Horas Totales	15
5. Objetivo de la Unidad de Aprendizaje	El alumno implementará métodos de seguridad para proteger la integridad, autenticación y confidencialidad del tráfico de datos en la red.

Temas	Saber	Saber hacer	Ser
Criptografía	Identificar principios para la criptografía simétrica y asimétrica Describir el funcionamiento de algoritmos de cifrado utilizados en seguridad informática	Crear mensajes cifrados utilizando herramientas basadas en algoritmos criptográficos	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad
VPNs	Identificar las características de las VPNs Identificar los distintos tipos de VPN Identificar las características del Framework de IPSec	Configurar VPNs IPSec de sitio a sitio con interfaz de línea de comando	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
A partir de un caso práctico, elabora y presenta una memoria técnica y una simulación que incluya: Memoria técnica -Identificar las técnicas de acceso seguro -Identificar los algoritmos criptográficos -Describir las comunicaciones seguras utilizando herramientas basadas en algoritmos criptográficos -Describir las características de configuración de VPNs -Topología lógica de red -Tabla de direccionamiento -Scripts de configuración -Pruebas de conectividad Simulación -Configuración de acceso administrativo seguro -Configurar comunicaciones seguras utilizando herramientas basadas en algoritmos criptográficos -Configurar VPNs	1.-Identificar los algoritmos criptográficos 2.-Explicar el funcionamiento de las conexiones seguras 3.-Explicar el funcionamiento de las VPNs sitio a sitio 4.-Explicar la configuración de las VPNs de sitio a sitio	1. Proyecto 2. Lista de cotejo

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Aprendizaje basado en proyectos -Equipos colaborativos -Estudio de casos	-Equipo de computo -Acceso a internet -Cañón -Ruteadores -Switches -Simulador de redes -Emulador de equipos de red

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**IV. Implementación de Dispositivos especializados de seguridad**
2. Horas Teóricas	5
3. Horas Prácticas	10
4. Horas Totales	15
5. Objetivo de la Unidad de Aprendizaje	El alumno implementará configuraciones en sistemas especializados de seguridad para resguardar los recursos de la organización.

Temas	Saber	Saber hacer	Ser
Introducción a los Dispositivos especializados de seguridad	Identificar las características de los dispositivos especializados de seguridad de red Identificar los modos de operación de los dispositivos especializados de seguridad de red		Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad
Configuración Básica de Dispositivos especializados de seguridad	Identificar los comandos básicos de configuración de dispositivos especializados de seguridad	Establecer la configuración básica de dispositivos especializados de seguridad de red	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad

Temas	Saber	Saber hacer	Ser
Configuraciones Avanzadas en Dispositivos especializados de seguridad	Identificar los comandos avanzados de configuración de dispositivos especializados de seguridad	Establecer la configuración avanzada de dispositivos especializados de seguridad de red Establecer la configuración de listas de accesos en dispositivos especializados de seguridad de red Establecer la configuración de servicios NAT y AAA en dispositivos especializados de seguridad de red	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
A partir de un caso práctico, elabora y presenta una memoria técnica y una simulación que incluya: Memoria técnica -Identificar las técnicas de acceso seguro -Identificar los dispositivos especializados de seguridad de red -Describir las características de configuración de los dispositivos especializados de seguridad de red -Topología lógica de red -Tabla de direccionamiento -Scripts de configuración -Pruebas de conectividad Simulación -Configuración de acceso administrativo seguro -Configurar dispositivos especializados de seguridad de red	1. Identificar los dispositivos especializados de seguridad de red 2. Explicar el funcionamiento de los dispositivos especializados de seguridad de red 3. Explicar la configuración de los dispositivos especializados de seguridad de red	1. Proyecto 2. Lista de cotejo

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Aprendizaje basado en proyectos -Equipos colaborativos -Estudio de casos	-Equipo de computo -Acceso a internet -Cañón -Ruteadores -Switches -Simulador de redes -Emulador de equipos de red -Firewall basados en hardware

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**V. Administración de redes seguras**
2. Horas Teóricas	5
3. Horas Prácticas	10
4. Horas Totales	15
5. Objetivo de la Unidad de Aprendizaje	El alumno implementará una política de seguridad para proteger los recursos de la organización apoyándose en normas y estándares vigentes

Temas	Saber	Saber hacer	Ser
Políticas de seguridad	Identificar las características de las políticas de seguridad	Elaborar políticas de seguridad identificando ventajas y desventajas de su implementación	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad
Estándares , Guías y procedimientos para seguridad de redes	Diferenciar las especificaciones, funciones y objetivos de los Estándares, Guías y Procedimientos para la seguridad de redes		Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad

Temas	Saber	Saber hacer	Ser
Roles y responsabilidades para la seguridad de redes	Identificar roles y responsabilidades de los participantes en el plan de continuidad de negocio.	Elaborar una matriz de roles y responsabilidades de los participantes en el plan de continuidad de negocio	Analítico Pensamiento lógico Autodidacta Ordenado Honestidad Capacidad para investigar Capacidad de abstracción Hábil para planificar Responsabilidad

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
A partir de un caso práctico, elabora y presenta una memoria técnica y una simulación que incluya: Memoria técnica -Identificar el objetivo de negocio de la organización -Matriz de análisis de riesgos -Determinar el plan de continuidad de negocio -Matriz de roles y responsabilidades de los participantes -Política de seguridad de la organización Simulación -Configuración de una topología en la que se implementen los puntos de la política de seguridad de la organización	1.-Identificar los objetivos de negocio de la organización 2.-Explicar el plan de continuidad de negocio de la organización 3.-Explicar las políticas de seguridad de la organización	1. Proyecto 2. Lista de cotejo

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Aprendizaje basado en proyectos -Equipos colaborativos -Estudio de casos	-Equipo de computo -Acceso a internet -Cañón -Ruteadores -Switches -Simulador de redes -Emulador de equipos de red -Firewall basados en hardware

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

CAPACIDADES DERIVADAS DE LAS COMPETENCIAS PROFESIONALES A LAS QUE CONTRIBUYE LA ASIGNATURA

Capacidad	Criterios de Desempeño
Diagnosticar riesgos y vulnerabilidades en la seguridad de información a partir del análisis del entorno de las organizaciones, para desarrollar estrategias que permitan su mitigación.	Entrega un reporte técnico que incluya lo siguiente: - Análisis del contexto del negocio. - Listado requerimientos funcionales y no funcionales. - Análisis de la situación actual de la seguridad de información de la organización
Establecer políticas de seguridad de información mediante estándares y procedimientos vigentes aplicables al entorno de la organización, para establecer las bases de continuidad de negocio.	Entrega un documento con la política de seguridad de información que considere los siguientes puntos: - Matriz de riesgos y vulnerabilidades. - Procesos de continuidad del negocio. - Políticas de salvaguarda de los activos de la organización. - Identificación y clasificación de los activos de la organización.
Seleccionar herramientas y servicios para la seguridad de información mediante la aplicación de estándares, para dar cumplimiento a las políticas de seguridad de las organizaciones.	Entrega una propuesta de solución que incluye lo siguiente: - Tabla comparativa de la evaluación de alternativas de solución. - Arquitectura de la solución propuesta. - Análisis del retorno de la inversión. - Hoja técnica de la solución propuesta
Planear las estrategias de implementación de políticas, herramientas y servicios de seguridad de información a partir del análisis del entorno, para salvaguardar los activos de las organizaciones.	Entrega un plan de trabajo que incluye lo siguiente: - Actividades a desarrollar. - Responsables. - Tiempos asignados a cada tarea.
Implementar las soluciones de seguridad de información a partir de los lineamientos organizacionales y en apego a los procedimientos y estándares aplicables a las tecnologías seleccionadas, para salvaguardar los activos de las organizaciones.	Entrega una memoria técnica que integre lo siguiente: - Línea base del servicio. - Bitácora de implementación. - Pruebas de la implementación.

Capacidad	Criterios de Desempeño
Evaluar la implementación de soluciones de seguridad de información mediante la aplicación de auditorías, pruebas e interpretación de métricas, para determinar áreas de oportunidad en los procesos de continuidad de negocio.	Entrega un reporte de auditoria de seguridad que incluye los siguiente: - Resultados de pruebas de penetración. - Análisis de vulnerabilidades. - Propuesta de mejoras a la política de seguridad de la organización.
Monitorear la implementación de soluciones y políticas de seguridad de información a través del análisis de los resultados de auditorías, para optimizar los procesos de continuidad del negocio.	Entrega un reporte técnico que incluye lo siguiente: - Bitácora de eventos. - Lista de verificación de las políticas de seguridad de la organización. - Reportes de rendimiento y eficiencia de la solución.

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

FUENTES BIBLIOGRÁFICAS

Autor	Año	Título del Documento	Ciudad	País	Editorial
Santos Omar, John Stuppi	2017 ISBN-13: 978-1-58720-608-5	*CCNA Security 210-260 Pearson uCertify Course and Textbook Bundle*	USA	USA	Cisco Press
Gerardus Blokdyk	ISBN-13 : 978-0655925781	*CCNA Security A Complete Guide - 2020 Edition*	USA	USA	5STARCooks
Wendell Odom	2019 ISBN-13 : 978-0135792735	*CCNA 200-301 Official Cert Guide, Volume 1*	USA	USA	Cisco Press; 1er edición
William Stallings	2016 ISBN-13 : 978-0134527338	*Network Security Essentials: Applications and Standards*	USA	USA	Pearson
William Stallings	2016 ISBN-13 : 978-0134444284	*Cryptography and Network Security: Principles and Practice*	USA	USA	Pearson
Lee Brotherston	2017 ISBN-13 : 978-1491960387	*Defensive Security Handbook: Best Practices for Securing Infrastructure*	USA	USA	O'Reilly Media
William Stallings	2016 ISBN-13 : 978-9352866601	*Network Security Essentials :Application And Standards, 6Th Edition*	USA	USA	Pearson