FORMATO SYLLABUS

PERTENECE AL PROCEDIMIENTO: IDENTIFICACIÓN DEL CURSO

CLASIFICACIÓN: USO INTERNO

NOMBRE CURSO:	CIBERSEGURIDAD
NIVEL:	BÁSICO
DURACIÓN TÉCNICA:	108 HORAS

DESCRIPCIÓN DEL CURSO	
MODALIDAD DE FORMACIÓN	VIRTUAL/PRESENCIAL
METODOLOGÍA	TUTORIZADA: VIRTUAL SINCRÓNICA
PERFIL DEL TUTOR / EJECUTOR:	Profesional con experiencia en ciberseguridad, especializado en la implementación y gestión de políticas de seguridad de la información. Con conocimientos sólidos en redes, sistemas de detección de intrusiones y análisis de riesgos. Habilidad para enseñar y guiar a estudiantes a través de metodologías prácticas y basadas en problemas reales.

RESULTADOS DE APRENDIZAJE ESPERADOS
• Conocer los conceptos relacionados con ciberseguridad. • Reconocer los conceptos fundamentales de los modelos de seguridad en la red. • Reconocer las acciones de higiene digital que se deben tener en cuenta para el aseguramiento de la confidencialidad, integridad y disponibilidad de los activos de información.

- Reconocer los conceptos de vulnerabilidad, amenaza y riesgo, aplicado en entorno digitales.
- Reconocer medios de transmisión, mecanismos de autenticación de redes.
- Hacer la configuración de redes Lan y Vlan.
- Reconocer el concepto de política de seguridad de la información para garantizar la confidencialidad, integridad y disponibilidad de los recursos informáticos de una empresa.

COMPETENCIAS

Al finalizar el curso, los estudiantes serán capaces de aplicar de manera integral los conocimientos y habilidades adquiridos para diseñar, implementar y gestionar un plan de seguridad de la información que garantice la protección de los activos digitales de una organización. Esto incluye la identificación de amenazas y vulnerabilidades, la configuración segura de redes, la implementación de políticas de seguridad y la respuesta efectiva a incidentes de seguridad.

Competencias:

- Capacidad para Identificar y Evaluar Amenazas y Vulnerabilidades en Sistemas y Redes
- Habilidad para Implementar Prácticas de Higiene Digital y Configurar Redes Seguras.
- Capacidad para Desarrollar e Implementar Políticas de Seguridad de la Información.

ESTRATEGIAS METODOLÓGICAS

Aprendizaje Basado en Proyectos

Los estudiantes trabajan en proyectos prácticos desde el inicio del curso. Cada módulo incluye proyectos incrementales que culminan en un proyecto final integrador.

La implementación de la estrategia para cada módulo se realizaría así:

- Módulo 1: Crear un sitio web personal utilizando HTML, CSS y JavaScript.
- Módulo 2: Desarrollar un programa en Python que realice análisis y visualización de datos de un conjunto de datos específico.
- Módulo 3: Desarrollar una aplicación web que integre las habilidades de frontend y backend para mostrar visualizaciones de datos dinámicas

Estudios de Caso y Resolución de Problemas

Se implementa a través de:

- Análisis de Brechas de Seguridad: Presentar estudios de caso de brechas de seguridad famosas y pedir a los estudiantes que analicen lo que salió mal y cómo se podría haber evitado.
- Soluciones Creativas: Desafiar a los estudiantes a idear soluciones innovadoras para problemas de seguridad complejos presentados en los estudios de caso.
- Documentación y Reportes: Enseñar a los estudiantes a documentar y reportar sus análisis y soluciones de manera profesional.

Talleres y Laboratorios

Se implementa a través de:

- Talleres Prácticos: Organizar talleres sobre temas específicos, como la configuración de seguridad en sistemas operativos, el uso de herramientas de análisis de red, y la implementación de controles de acceso.
- Laboratorios Virtuales: Utilizar laboratorios virtuales para que los estudiantes practiquen configuraciones y pruebas de seguridad en un entorno seguro y controlado.
- Sesiones de Q&A: Incluir sesiones de preguntas y respuestas al final de cada taller o laboratorio para resolver dudas y reforzar el aprendizaje

Aprendizaje Colaborativo

Se fomenta la colaboración entre los estudiantes a través de proyectos en equipo y actividades de pair programming. Esta estrategia se implementa a través de:

- Proyectos en Equipo: Algunos proyectos se diseñan para ser realizados en equipos, promoviendo la colaboración y la comunicación.
- Pair Programming: Actividades regulares donde los estudiantes trabajan en parejas para resolver problemas de programación.

- Hackathons y Coding Challenges: Eventos especiales donde los estudiantes colaboran para resolver problemas o desarrollar aplicaciones en un tiempo limitado.

Aprendizaje Basado en Problemas

Los estudiantes aprenden resolviendo problemas complejos y reales que requieren la aplicación de múltiples conceptos y habilidades. Esta se puede implementar a través de:

- Desafíos Semanales: Presentar un problema al inicio de la semana que los estudiantes deben resolver utilizando las habilidades adquiridas hasta ese momento.
- Grupos de Discusión: Facilitar grupos de discusión donde los estudiantes pueden compartir sus enfoques y soluciones al problema.
- Presentaciones de Soluciones: Al final de la semana, los estudiantes presentan sus soluciones y discuten los diferentes enfoques utilizados.

MATERIAL PEDAGÓGICO POR MÓDULO

Módulo 1: Fundamentos de la Ciberseguridad

Material Pedagógico:

1. **Textos y Lecturas:**
    - Material de lectura que presenta los conceptos básicos y la historia de la ciberseguridad.
2. **Presentaciones y Videos:**
    - Presentaciones multimedia y videos que explican visualmente los modelos de seguridad y los conceptos clave.
3. **Cuestionarios y Evaluaciones:**
    - Herramientas de evaluación para medir la comprensión de los fundamentos teóricos.
4. **Proyectos Iniciales:**

- Proyectos prácticos para aplicar los conceptos básicos en un contexto realista.

Módulo 2: Higiene Digital y Seguridad en Redes

Material Pedagógico:

1. **Guías y Manuales:**
   - Documentos detallados que explican las mejores prácticas de higiene digital y configuraciones de seguridad.
2. **Simulaciones y Entornos Virtuales:**
   - Simulaciones de redes y laboratorios virtuales donde los estudiantes pueden practicar configuraciones seguras.
3. **Estudios de Caso:**
   - Casos prácticos que permiten a los estudiantes analizar y resolver problemas de seguridad en redes.
4. **Actividades Prácticas:**
   - Ejercicios y talleres donde los estudiantes configuran y aseguran redes LAN y VLAN.

Módulo 3: Políticas de Seguridad de la Información

Material Pedagógico:

1. **Documentación Normativa:**
   - Acceso a políticas de seguridad y normativas estándar para estudio y referencia.
2. **Talleres de Desarrollo de Políticas:**
   - Talleres interactivos para la creación y revisión de políticas de seguridad.
3. **Herramientas de Gestión de Seguridad:**
   - Software y herramientas para la implementación y monitoreo de políticas de seguridad.
4. **Proyectos Finales:**

○ Proyectos integradores donde los estudiantes diseñan e implementan un plan de seguridad completo para una organización.

ESTRUCTURA DEL CURSO

Módulo 1: Fundamentos de la Ciberseguridad	
Nombre de la lección	**Subtemas**
Introducción a la Ciberseguridad	• Definición de ciberseguridad. • Importancia de la ciberseguridad en el mundo actual. • Principales objetivos de la ciberseguridad: confidencialidad, integridad y disponibilidad. • Historia de la ciberseguridad. • Evolución de las amenazas cibernéticas. • Casos históricos de ciberataques.
Modelos de Seguridad en la Red	• Capas del modelo OSI. • Función de cada capa en la seguridad de la red. • Comparación entre OSI y TCP/IP. • Firewall, IDS/IPS. • VPNs y su uso en la protección de datos. • Segmentación de redes y DMZ.
Vulnerabilidades, Amenazas y Riesgos	• Vulnerabilidad: tipos comunes y cómo identificarlas.

	• Amenaza: internas vs. externas, ejemplos de amenazas comunes. • Riesgo: cómo evaluar y gestionar riesgos en entornos digitales. • Evaluación de riesgos. • Análisis de impacto. • Planes de mitigación y contingencia.

Módulo 2: Higiene Digital y Seguridad en Redes	
Nombre de la lección	**Subtemas**
Higiene Digital	• Gestión de contraseñas: creación y almacenamiento seguro. • Autenticación multifactor (MFA). • Actualización y parcheo de software. • Encriptación de datos. • Uso de herramientas de privacidad en línea (VPN, navegadores seguros).
Medios de Transmisión y Autenticación de Redes	• Tipos de medios: cableados e inalámbricos. • Vulnerabilidades asociadas a cada tipo de medio. • Autenticación basada en certificados. • Autenticación biométrica. • Protocolo de autenticación en redes (WPA2, WPA3).
Configuración de Redes LAN y VLAN	• Configuración básica de una LAN.

	• Asignación de direcciones IP y subredes. • Concepto de VLAN y su importancia. • Configuración de VLANs en un switch. • Ventajas de usar VLANs para la segmentación de redes.

Módulo 3: Políticas de Seguridad de la Información	
Nombre de la lección	**Subtemas**
Concepto de Política de Seguridad	• Qué es una política de seguridad de la información. • Importancia de las políticas de seguridad en una organización. • Componentes esenciales de una política de seguridad. • Pasos para crear una política de seguridad efectiva. • Involucramiento de stakeholders.
Implementación de Políticas de Seguridad	• Implementación de políticas en sistemas y redes. • Monitoreo y cumplimiento. • Herramientas para la gestión de políticas de seguridad. • Ejemplos Prácticos: • Ejemplos de políticas de uso aceptable. • Políticas de acceso y control de usuarios.
Garantizar Confidencialidad,	• Técnicas de cifrado.

	Integridad y Disponibilidad	• Control de acceso basado en roles (RBAC). • Hashing y verificación de integridad. • Sistemas de detección de intrusos (IDS). • Planificación de continuidad del negocio. • Recuperación ante desastres. • Balanceo de carga y redundancia.	

INTENSIDAD HORARIA		
Módulo	**Lección**	**Duración (hrs)**
Fundamentos de la Ciberseguridad	Introducción a la Ciberseguridad	10
	Modelos de Seguridad en la Red	12
	Vulnerabilidades, Amenazas y Riesgos	8
Higiene Digital y Seguridad en Redes	Higiene Digital	14
	Medios de Transmisión y Autenticación de Redes	9
	Configuración de Redes LAN y VLAN	12
Políticas de Seguridad de la Información	Concepto de Política de Seguridad	13
	Implementación de Políticas de Seguridad	15
	Garantizar Confidencialidad, Integridad y Disponibilidad	15
TOTAL		105

RÚBRICA DE EVALUACIÓN GENERAL DEL CURSO			
COMPETENCIA	ESCALA DE CALIFICACIÓN		
	NO CUMPLE	A MEJORAR	CUMPLE
	01- 30	31-89	90-100
Aplicar de manera integral los conocimientos y habilidades adquiridos para diseñar, implementar y gestionar un plan de seguridad de la información que garantice la protección de los activos digitales de una organización. Esto incluye la identificación de amenazas y vulnerabilidades, la configuración segura de redes, la implementación de políticas de seguridad y la respuesta efectiva a incidentes de seguridad.	Debe darse alguna de las siguientes dificultades en el conocimiento:	Deben mejorarse, algunos o varios de los siguientes conocimientos parciales:	Deben cumplirse a satisfacción uno o varios de los siguientes conocimientos:
	El estudiante tiene dificultades significativas para identificar amenazas y vulnerabilidades en sistemas.	El estudiante puede identificar algunas amenazas y vulnerabilidades, pero carece de un enfoque sistemático.	El estudiante identifica de manera completa y precisa las amenazas y vulnerabilidades relevantes.
	El estudiante muestra dificultades para configurar redes LAN y VLAN de manera segura, incluyendo errores básicos.	El estudiante configura redes LAN y VLAN con algunas medidas de seguridad, pero con áreas que requieren mejora.	El estudiante configura redes LAN y VLAN de manera completa y segura, implementando todas las medidas necesarias.
	El estudiante presenta dificultades para desarrollar políticas de seguridad claras y coherentes.	El estudiante desarrolla políticas de seguridad básicas, pero faltan algunos componentes clave o detalles específicos.	El estudiante desarrolla e implementa políticas de seguridad completas, claras y detalladas, cubriendo todos los aspectos.
	El estudiante tiene dificultades para responder a incidentes de	El estudiante responde a incidentes de seguridad con	El estudiante responde a incidentes de seguridad de manera

	seguridad de manera efectiva y ordenada.	efectividad parcial, pero falta claridad en algunos procedimientos.	efectiva y ordenada, siguiendo todos los protocolos adecuados.
	El estudiante presenta dificultades significativas en la documentación y presentación de su trabajo, con errores y omisiones.	El estudiante documenta y presenta su trabajo de manera adecuada, pero con algunos detalles que requieren mayor claridad.	El estudiante documenta y presenta su trabajo de manera clara, completa y profesional, cubriendo todos los aspectos relevantes.