GUÍA DE CLASES PRÁCTICA DE LA ASIGNATURA	
CARRERA: TECNOLOGÍA SUPERIOR EN ENERGÍAS ALTERNATIVAS	**ASIGNATURA:** COMPUTACIÓN IV
UNIDAD 1: SEGURIDAD EN REDES CORPORATIVAS	
TÍTULO DE LA CLASE PRÁCTICA: Introducción al cifrado de datos	
OBJETIVO: Comprender la importancia de los puertos de comunicaciones y las amenazas existentes en protocolos poco seguros	
TIEMPO DE DURACIÓN: 14 HORAS	

1. **FUNDAMENTOS:**

   La aplicación de los conocimientos básicos sobre la resolución de problemas y evaluación de herramientas de seguridad informática permite a los estudiantes desarrollar habilidades clave para identificar y mitigar amenazas en los sistemas de red. Esto los capacita para ser el primer punto de apoyo en la identificación de riesgos potenciales, utilizando sistemas de detección de intrusos y evaluando su efectividad. Estas competencias son esenciales para garantizar la seguridad de las comunicaciones en la red, asegurando que las comunicaciones sean seguras y que se mantenga la integridad de la información en entornos digitales. La habilidad para tomar decisiones rápidas y efectivas frente a incidentes de seguridad es fundamental para proteger los datos y las infraestructuras críticas.

2. **OBJETIVOS A ALCANZAR:**

   En la clase práctica sobre seguridad informática, los estudiantes deberán familiarizarse con los conceptos clave sobre ataques y amenazas, así como las herramientas y métodos para prevenirlos. Se enfocarán en el uso de sistemas de detección de intrusos para identificar accesos no autorizados en redes y sistemas.

   - Identificación de amenazas: Utilizar sistemas de detección de intrusos para detectar actividades sospechosas en redes.
   - Evaluación de riesgos: Analizar los riesgos potenciales en los servicios de red y aplicar medidas preventivas.
   - Protección de comunicaciones: Aplicar técnicas de cifrado y establecer redes seguras para garantizar la confidencialidad.
   - Simulación de incidentes: Resolver casos prácticos simulando situaciones de ataques informáticos y respondiendo de manera efectiva.

3. BREVE DESCRIPCIÓN DE LAS CAPACIDADES PRÁCTICAS A DESARROLLAR:

Habilidades de pensamiento: Los estudiantes deben desarrollar habilidades de pensamiento crítico y analítico para identificar y evaluar amenazas en redes y sistemas informáticos. Esto implica analizar patrones de comportamiento en el tráfico de red, detectar vulnerabilidades potenciales y tomar decisiones rápidas y fundamentadas para mitigar riesgos. La capacidad de pensar de manera estratégica y proactiva es esencial para proteger las infraestructuras digitales y prevenir posibles intrusiones o ataques.

Destrezas sensoriales: Las destrezas sensoriales en este contexto requieren que los estudiantes afiancen su capacidad para detectar señales visuales y auditivas que indiquen anomalías o intrusiones en los sistemas de red. Esto incluye interpretar alertas en tiempo real de los sistemas de monitoreo, identificar cambios en patrones de tráfico o reconocer notificaciones de posibles vulnerabilidades. La capacidad para distinguir entre datos normales y potencialmente peligrosos es fundamental para una gestión eficiente de la seguridad informática.

Destrezas motoras: Las destrezas motoras en seguridad informática están relacionadas con la operación precisa y eficiente de herramientas de seguridad, como sistemas de detección de intrusos (IDS), plataformas de análisis forense y software de cifrado. Los estudiantes deben ser capaces de navegar rápidamente por interfaces técnicas, ejecutar configuraciones adecuadas y aplicar medidas correctivas o preventivas con exactitud. Esta habilidad asegura que puedan reaccionar ante incidentes de manera efectiva, minimizando el impacto de cualquier ataque.

4. EVALUACIÓN DEL APRENDIZAJE:

- **Cuestionarios de evaluación teórica:** Para verificar la comprensión de los conceptos impartidos en clase que permiten un mejor aprendizaje autodidáctico del estudiante.

- **Ejercicios Prácticos:** Trabajar en el área práctica de sobre la edición de correos electrónicos para beneficio del estudiante con la clase impartida para un mejor tratamiento de datos en el entorno tanto personal como laboral.

5. PREPARACIÓN PREVIA DEL ESTUDIANTE:

El docente organizará un taller para abordar los nuevos temas. El estudiante adquirirá los fundamentos teóricos mediante la investigación y el análisis de diversas fuentes bibliográficas, complementando su aprendizaje con la elaboración de un organizador gráfico que resuma los contenidos. Este material será enriquecido con la retroalimentación del docente y las discusiones realizadas en el aula.

6. PROCEDIMIENTOS A EMPLEAR:
Explicación sobre Seguridad Informática

Introducción teórica:

- Iniciar con una explicación detallada sobre los tipos de ataques y amenazas comunes en redes y sistemas informáticos, abordando conceptos como ataques de denegación de servicio (DDoS), phishing y malware. Además, se discutirá el rol de los sistemas de detección de intrusos (IDS) y su aplicación en la identificación de actividades sospechosas.

Demostración práctica:

- Mostrar a los estudiantes cómo configurar y utilizar herramientas de IDS para detectar y alertar sobre accesos no autorizados en un entorno de red simulado. Se explicará el proceso de monitoreo y análisis de logs, enseñando a identificar patrones sospechosos.

Evaluación de riesgos potenciales:

Los estudiantes analizarán una red o sistema específico, identificando posibles vulnerabilidades y evaluando los riesgos asociados. Luego, deberán proponer y aplicar medidas de seguridad, como el cifrado de comunicaciones y la implementación de redes privadas virtuales (VPN) para proteger los datos.

7. NORMAS DE SEGURIDAD:
Seguridad: La seguridad es primordial. Los ambientes de práctica deben cumplir con regulaciones de seguridad y salud en el trabajo. Esto incluye la identificación de riesgos potenciales, la provisión de equipo de protección personal cuando sea necesario y la implementación de protocolos de seguridad.

Supervisión: Los estudiantes en prácticas suelen requerir supervisión adecuada para asegurarse de que están realizando las tareas de manera segura y correcta. Los docentes han de asumir la función de supervisores, por lo que deben estar disponibles para responder preguntas, proporcionar orientación y evaluar el progreso del estudiante.

8. FORMACIÓN EN VALORES Y DESARROLLO DE HABILIDADES BLANDAS:

En la asignatura Computación IV, los estudiantes fortalecen su capacidad de trabajo en equipo, resolución de problemas y colaboración en proyectos tecnológicos. Se promueven valores como el respeto, la solidaridad y la ética en el uso de herramientas y plataformas tecnológicas fundamentales para su éxito académico y profesional en el ámbito de seguridad y prevención de riesgos laborales

9. CONCLUSIONES:

El conocimiento y uso adecuado de las herramientas de seguridad informática son fundamentales para proteger las redes y los sistemas ante amenazas y ataques. La aplicación de sistemas de detección de intrusos y la correcta evaluación de riesgos permiten mitigar vulnerabilidades y mantener la seguridad de la información. Las simulaciones prácticas ofrecen una experiencia valiosa para responder eficazmente a incidentes de seguridad en entornos controlados.

10. RECOMENDACIONES:

Se recomienda a los estudiantes practicar regularmente con herramientas de seguridad y mantenerse actualizados sobre las últimas amenazas y soluciones de ciberseguridad. Además, es crucial reforzar la comprensión sobre la importancia de las comunicaciones seguras y aplicar el cifrado en todas las interacciones digitales. También es beneficioso realizar simulaciones periódicas de ataques para mejorar la respuesta ante incidentes reales.

TECNOLÓGICO DE FORMACIÓN
CONDICIÓN UNIVERSITARIO
CÓDIGO SENESCYT 2258

GUÍA DE CLASES PRÁCTICA DE LA ASIGNATURA	
CARRERA: TECNOLOGÍA SUPERIOR EN ENERGÍAS ALTERNATIVAS	**ASIGNATURA:** COMPUTACIÓN IV
UNIDAD 2: NORMATIVA LEGAL EN MATERIA DE SEGURIDAD INFORMÁTICA	
TÍTULO DE LA CLASE PRÁCTICA: Tratamiento de los datos en la web.	
OBJETIVO: Comprender las principales normativas y leyes que regulan la seguridad informática, evaluando su impacto en la protección de datos y sistemas, y examinando cómo estas normativas contribuyen a la creación de un entorno digital seguro y conforme a los estándares legales.	
TIEMPO DE DURACIÓN: 14 HORAS	

1. **FUNDAMENTOS:**

   La aplicación de los conocimientos básicos sobre la resolución de problemas y evaluación de herramientas de seguridad informática permite a los estudiantes desarrollar habilidades clave para identificar y mitigar amenazas en los sistemas de red. Esto los capacita para ser el primer punto de apoyo en la identificación de riesgos potenciales, utilizando sistemas de detección de intrusos y evaluando su efectividad. Estas competencias son esenciales para garantizar la seguridad de las comunicaciones en la red, asegurando que las comunicaciones sean seguras y que se mantenga la integridad de la información en entornos digitales. La habilidad para tomar decisiones rápidas y efectivas frente a incidentes de seguridad es fundamental para proteger los datos y las infraestructuras críticas.

2. **OBJETIVOS A ALCANZAR:**

   En la clase práctica sobre seguridad informática, los estudiantes deberán familiarizarse con los conceptos clave sobre ataques y amenazas, así como las herramientas y métodos para prevenirlos. Se enfocarán en el uso de sistemas de detección de intrusos para identificar accesos no autorizados en redes y sistemas. Además, aprenderán a evaluar los riesgos potenciales en los servicios de red, analizando vulnerabilidades y tomando decisiones para mitigarlas. Se proporcionarán casos prácticos donde los estudiantes podrán aplicar técnicas de protección, como el cifrado de comunicaciones y el establecimiento de redes seguras.

   - Identificación de amenazas: Utilizar sistemas de detección de intrusos para detectar actividades sospechosas en redes.
   - Evaluación de riesgos: Analizar los riesgos potenciales en los servicios de red y aplicar medidas preventivas.
   - Protección de comunicaciones: Aplicar técnicas de cifrado y establecer redes seguras para garantizar la confidencialidad.
   - Simulación de incidentes: Resolver casos prácticos simulando situaciones de ataques informáticos y respondiendo de manera efectiva.

3. BREVE DESCRIPCIÓN DE LAS CAPACIDADES PRÁCTICAS A DESARROLLAR:

Habilidades de pensamiento: Los estudiantes deben desarrollar habilidades de pensamiento crítico y analítico para identificar y evaluar amenazas en redes y sistemas informáticos. Esto implica analizar patrones de comportamiento en el tráfico de red, detectar vulnerabilidades potenciales y tomar decisiones rápidas y fundamentadas para mitigar riesgos. La capacidad de pensar de manera estratégica y proactiva es esencial para proteger las infraestructuras digitales y prevenir posibles intrusiones o ataques.

Destrezas sensoriales: Los estudiantes deben afianzar su capacidad para detectar señales visuales y auditivas que indiquen anomalías o intrusiones en los sistemas de red. Esto incluye interpretar alertas en tiempo real de los sistemas de monitoreo, identificar cambios en patrones de tráfico o reconocer notificaciones de posibles vulnerabilidades. La capacidad para distinguir entre datos normales y potencialmente peligrosos es fundamental para una gestión eficiente de la seguridad informática.

Destrezas motoras: Las destrezas motoras en seguridad informática están relacionadas con la operación precisa y eficiente de herramientas de seguridad, como sistemas de detección de intrusos (IDS), plataformas de análisis forense y software de cifrado. Los estudiantes deben ser capaces de navegar rápidamente por interfaces técnicas, ejecutar configuraciones adecuadas y aplicar medidas correctivas o preventivas con exactitud. Esta habilidad asegura que puedan reaccionar ante incidentes de manera efectiva, minimizando el impacto de cualquier ataque.

4. EVALUACIÓN DEL APRENDIZAJE:

- **Cuestionarios de evaluación teórica:** Para verificar la comprensión de los conceptos impartidos en clase que permiten un mejor aprendizaje autodidáctico del estudiante.

- **Ejercicios Prácticos:** Trabajar en el área práctica de Google Workspace para beneficio del estudiante con la clase impartida para un mejor tratamiento de datos en el entorno tanto personal como laboral.

5. PREPARACIÓN PREVIA DEL ESTUDIANTE:

El docente organizará un taller para abordar los nuevos temas. El estudiante adquirirá los fundamentos teóricos mediante la investigación y el análisis de diversas fuentes bibliográficas, complementando su aprendizaje con la elaboración de un organizador gráfico que resuma los contenidos. Este material será enriquecido con la retroalimentación del docente y las discusiones realizadas en el aula.

6. PROCEDIMIENTOS A EMPLEAR: Explicación sobre Tratamiento de los datos

Introducción teórica:

- Iniciar con una explicación detallada sobre los tipos de ataques y amenazas comunes en redes y sistemas informáticos, abordando conceptos como ataques de denegación de servicio (DDoS), phishing y malware. Además, se discutirá el rol de los sistemas de detección de intrusos (IDS) y su aplicación en la identificación de actividades sospechosas.

Demostración práctica:

- Mostrar a los estudiantes cómo configurar y utilizar herramientas de IDS para detectar y alertar sobre accesos no autorizados en un entorno de red simulado. Se explicará el proceso de monitoreo y análisis de logs, enseñando a identificar patrones sospechosos.

Evaluación de riesgos potenciales:

Los estudiantes analizarán una red o sistema específico, identificando posibles vulnerabilidades y evaluando los riesgos asociados. Luego, deberán proponer y aplicar medidas de seguridad, como el cifrado de comunicaciones y la implementación de redes privadas virtuales (VPN) para proteger los datos.

7. NORMAS DE SEGURIDAD:

Seguridad: La seguridad es primordial. Los ambientes de práctica deben cumplir con regulaciones de seguridad y salud en el trabajo. Esto incluye la identificación de riesgos potenciales, la provisión de equipo de protección personal cuando sea necesario y la implementación de protocolos de seguridad.
Supervisión: Los estudiantes en prácticas suelen requerir supervisión adecuada para asegurarse de que están realizando las tareas de manera segura y correcta. Los docentes han de asumir la función de supervisores, por lo que deben estar disponibles para responder preguntas, proporcionar orientación y evaluar el progreso del estudiante.

8. FORMACIÓN EN VALORES Y DESARROLLO DE HABILIDADES BLANDAS:

En la asignatura Computación IV, los estudiantes fortalecen su capacidad de trabajo en equipo, resolución de problemas y colaboración en proyectos tecnológicos. Se promueven valores como el respeto, la solidaridad y la ética en el uso de herramientas y plataformas tecnológicas fundamentales para su éxito académico y profesional en el ámbito de seguridad y prevención de riesgos laborales.

9. CONCLUSIONES:

El conocimiento y uso adecuado de las herramientas de seguridad informática son fundamentales para proteger las redes y los sistemas ante amenazas y ataques. La aplicación

de sistemas de detección de intrusos y la correcta evaluación de riesgos permiten mitigar vulnerabilidades y mantener la seguridad de la información. Las simulaciones prácticas ofrecen una experiencia valiosa para responder eficazmente a incidentes de seguridad en entornos controlados.

10. RECOMENDACIONES:

Se recomienda a los estudiantes practicar regularmente con herramientas de seguridad y mantenerse actualizados sobre las últimas amenazas y soluciones de ciberseguridad. Además, es crucial reforzar la comprensión sobre la importancia de las comunicaciones seguras y aplicar el cifrado en todas las interacciones digitales. También es beneficioso realizar simulaciones periódicas de ataques para mejorar la respuesta ante incidentes reales.