

Navegación Segura y Ciberseguridad: Dominando Herramientas Digitales en la Ingeniería de Sistemas

Ingeniería | Ingeniería de sistemas | Aprendizaje Basado en Problemas

Descripción

En este plan de clase los estudiantes de Ingeniería de Sistemas aprenderán a navegar de forma segura en internet, utilizar plataformas en la nube como Google Drive y OneDrive, y aplicar prácticas básicas de ciberseguridad y ética digital. El propósito es que comprendan la evolución histórica de la informática y cómo los componentes físicos y lógicos conforman los sistemas computacionales actuales. Además, desarrollarán habilidades prácticas para configurar sistemas operativos, organizar y respaldar información digital, y emplear herramientas de productividad esenciales. Este aprendizaje es fundamental para su formación profesional, ya que el manejo seguro y eficiente de la información digital es una competencia clave en la ingeniería moderna. A través de actividades basadas en problemas reales, los estudiantes fortalecerán su pensamiento crítico y estarán preparados para enfrentar desafíos cotidianos relacionados con la seguridad informática y la ética digital, conectando su aprendizaje con contextos actuales y su vida académica y profesional.

Objetivos de Aprendizaje

- Reconocer la evolución histórica de la informática y su impacto en la sociedad actual.
- Identificar los componentes físicos (hardware) y lógicos (software) de un sistema computacional.
- Configurar y personalizar el entorno de trabajo de un sistema operativo (Windows/Linux).
- Aplicar técnicas de organización, gestión y respaldo de información digital.
- Utilizar herramientas de productividad (procesador de texto, hoja de cálculo, presentaciones).
- Desarrollar habilidades de navegación segura en internet y uso de plataformas colaborativas.
- Implementar prácticas básicas de ciberseguridad y ética digital.

Recursos Necesarios

- Computadoras con acceso a internet (1 por estudiante o pareja)
- Proyector y pantalla para presentaciones
- Acceso a plataformas Google Drive y OneDrive
- Material impreso con esquema de evolución histórica de la informática (1 por estudiante)
- Acceso a navegadores web actualizados (Chrome, Firefox, Edge)
- Videos cortos sobre phishing y ética digital (aprox. 5 minutos cada uno)
- Guía digital con pasos para configuración básica de Windows y Linux

- Lista de verificación para creación de contraseñas seguras
- Herramientas digitales para creación de mapas mentales o resúmenes (opcional)

Requisitos Previos

- Conocimientos básicos de informática general y uso de computadoras
- Familiaridad con sistemas operativos Windows o Linux
- Habilidades básicas para buscar información en internet
- Experiencia previa con alguna herramienta ofimática (procesador de texto o presentaciones)

Actividades

Fase de Inicio

Tiempo estimado: 20 minutos

Propósito de la sesión:

Docente: Explica que en la sesión se abordará cómo navegar de forma segura, usar la nube para gestionar información y aplicar prácticas de ciberseguridad y ética digital, habilidades fundamentales para su futuro profesional en ingeniería de sistemas.

Activación de conocimientos previos:

Docente: Propone el siguiente caso para reflexión rápida:

- “Imagina que tienes que compartir un documento importante con tu equipo de trabajo, ¿qué plataforma usarías y por qué? ¿Qué medidas tomarías para proteger esa información?”

Estudiantes: Responden en plenaria, compartiendo experiencias o expectativas.

Motivación y enganche:

Docente: Presenta un dato impactante: “El 90% de los ciberataques comienzan con un error humano. Hoy aprenderán a evitar esos errores y usar herramientas que protejan su información y su carrera profesional.”

Contextualización:

Docente: Conecta el tema con la vida diaria y profesional de los estudiantes, enfatizando que la ingeniería de sistemas exige competencias sólidas en seguridad digital y manejo de la nube para colaborar efectivamente en proyectos y proteger activos digitales.

Fase de Desarrollo

Tiempo estimado: 80 minutos

Presentación del contenido:

Docente: Introduce brevemente la evolución histórica de la informática usando un esquema visual. Luego, plantea un desafío basado en problemas reales: “Un equipo de trabajo ha sufrido pérdida de información y ataques de phishing. Deben diseñar un plan para mejorar su navegación segura, uso de la nube y prácticas de ciberseguridad.”

Actividad 1: Análisis de caso y búsqueda avanzada en navegadores

- **Objetivo:** Desarrollar habilidades de búsqueda avanzada y reconocer amenazas comunes en la navegación.
- **Instrucciones:**
 - Se divide a los estudiantes en grupos de 3-4 personas.
 - Se entrega un caso de phishing simulado.
 - Cada grupo debe usar motores de búsqueda avanzada para investigar señales y ejemplos de phishing y cómo evitarlos.
 - El grupo prepara una lista de indicadores de phishing y recomendaciones para navegación segura.
- **Organización:** Grupos de 3-4
- **Producto:** Lista con indicadores y recomendaciones
- **Tiempo:** 25 minutos
- **Rol docente:** Circula entre grupos, formula preguntas como “¿Qué señales identifican como sospechosas?”, “¿Qué estrategias usaron para filtrar información confiable?” y guía la discusión.

Actividad 2: Uso práctico de Google Drive / OneDrive y organización digital

- **Objetivo:** Aplicar técnicas de organización, gestión y respaldo de información digital usando plataformas colaborativas.
- **Instrucciones:**
 - En parejas, acceden a Google Drive o OneDrive.
 - Crean una carpeta compartida, suben documentos de ejemplo, crean un documento colaborativo y configuran permisos de acceso.
 - Practican la organización con subcarpetas y etiquetado.
 - Simulan un respaldo y recuperación de información.
- **Organización:** Parejas
- **Producto:** Carpeta organizada y documento colaborativo realizado
- **Tiempo:** 30 minutos
- **Rol docente:** Apoya con dudas técnicas, verifica correcta configuración y fomenta buenas prácticas de seguridad en permisos y respaldo.

Actividad 3: Creación de contraseñas seguras y ética digital

- **Objetivo:** Implementar prácticas básicas de seguridad y ética digital relacionadas con contraseñas y manejo responsable de la información.
- **Instrucciones:**
 - Individualmente, cada estudiante crea 3 contraseñas seguras siguiendo criterios proporcionados.
 - Luego, se visualiza un video corto sobre phishing y ética digital.
 - En plenaria, discuten cómo las contraseñas y la ética digital previenen riesgos y fortalecen la seguridad.
- **Organización:** Individual y plenaria
- **Producto:** Contraseñas creadas y respuestas a preguntas de reflexión ética
- **Tiempo:** 25 minutos
- **Rol docente:** Verifica la calidad de las contraseñas, modera discusión y refuerza conceptos clave.

Diferenciación

- **Para estudiantes que terminan antes:** Explorar opciones avanzadas de configuración en Google Drive o investigar técnicas adicionales de búsqueda avanzada y compartir brevemente en plenaria.
- **Para estudiantes que requieren más apoyo:** Atención personalizada para guiar paso a paso en la configuración y creación de contraseñas, uso de ejemplos prácticos y recursos visuales adicionales.

Transiciones

- Al terminar el análisis de phishing, el docente conecta con la necesidad de proteger información en la nube.
- Tras la práctica en Google Drive, se introduce la relevancia de contraseñas seguras para evitar ataques.
- Luego de la reflexión ética, se prepara la síntesis para consolidar aprendizajes.

Fase de Cierre

Tiempo estimado: 20 minutos

Síntesis:

Docente: Propone un mapa mental colectivo en la pizarra digital donde los estudiantes aportan ideas claves sobre navegación segura, uso de la nube, contraseñas y ética digital, organizados en categorías.

Estudiantes: Contribuyen activamente, sintetizando lo aprendido.

Reflexión metacognitiva:

- ¿Cómo aplicarías hoy mismo las técnicas aprendidas para proteger tu información personal y profesional?
- ¿Qué señales de phishing te parecen más difíciles de detectar y cómo planeas afrontarlas?
- ¿De qué manera la ética digital influye en tu desempeño como futuro ingeniero de sistemas?

Estudiantes: Responden de forma escrita breve o verbal.

Retroalimentación:

Docente: Proporciona comentarios inmediatos sobre las contribuciones al mapa mental y las reflexiones, destacando aciertos y áreas para profundizar.

Transferencia:

Docente: Conecta lo aprendido con la importancia de la seguridad digital en proyectos reales de ingeniería y anuncia que en futuras sesiones se profundizará en configuración avanzada y análisis de riesgos.

Tarea o reto:

Docente: Asigna la tarea de implementar una gestión segura de información personal en la nube y redactar un breve informe sobre medidas tomadas y dificultades encontradas, para discutir en la próxima clase.

Evaluación

Tipo de evaluación: Diagnóstica en la fase de inicio (activación de conocimientos), formativa durante el desarrollo (observación y revisión de productos de actividades), y sumativa en el cierre (mapa mental colectivo y reflexiones escritas).

Criterios de evaluación:

- Capacidad para identificar amenazas y prácticas de navegación segura (objetivo: desarrollar habilidades de navegación segura y ciberseguridad).
- Correcta aplicación de técnicas de organización y uso de plataformas en la nube (objetivo: aplicar técnicas de organización y herramientas de productividad).
- Generación de contraseñas seguras y comprensión de ética digital (objetivo: implementar prácticas básicas de ciberseguridad y ética).
- Participación activa en actividades colaborativas y reflexión crítica (objetivo: desarrollo de competencias integrales).

Instrumentos sugeridos: Lista de cotejo para evidenciar cumplimiento de actividades, observación directa durante el desarrollo, rúbrica para evaluar calidad de productos digitales y reflexiones, y autoevaluación al cierre.

Evidencias de aprendizaje: Listas de indicadores y recomendaciones, carpetas organizadas en plataformas de nube, contraseñas creadas, aportes al mapa mental colectivo y respuestas a preguntas de reflexión metacognitiva.