

Ecosistemas Digitales y Ciberseguridad: Navegando el Mundo Digital con Confianza

Ingeniería | Ingeniería de sistemas | Diseño Universal para el Aprendizaje

Descripción

Este plan de clase está diseñado para estudiantes universitarios de Ingeniería de Sistemas y tiene como propósito fundamental que comprendan y apliquen los conceptos esenciales relacionados con los ecosistemas digitales y la ciberseguridad. A lo largo de dos sesiones de trabajo activo, los estudiantes aprenderán a diferenciar entre hardware, software local y computación en la nube; utilizarán plataformas SaaS para colaborar eficazmente; y aplicarán prácticas básicas de identidad digital, privacidad y ciberseguridad en contextos académicos y profesionales.

La relevancia de este tema radica en la integración creciente de tecnologías digitales en todos los ámbitos de la vida y el trabajo, lo que demanda un manejo crítico y seguro de estas herramientas. Además, el plan conecta directamente con la realidad cotidiana y futura profesional de los estudiantes, preparándolos para enfrentar retos tecnológicos con responsabilidad y competencia. Se utilizará la metodología del Diseño Universal para el Aprendizaje, garantizando que el proceso sea inclusivo y motivador, atendiendo distintas formas de aprendizaje y expresión.

Objetivos de Aprendizaje

- Explicar las diferencias entre hardware, software local y computación en la nube.
- Utilizar plataformas SaaS para colaborar de manera eficiente en entornos digitales.
- Aplicar prácticas básicas de identidad digital, privacidad y ciberseguridad en contextos académicos y profesionales.

Recursos Necesarios

- Computadoras o laptops con acceso a internet (1 por estudiante o pareja).
- Proyector y pantalla para presentaciones.
- Plataformas SaaS para colaboración (Google Workspace, Microsoft 365, u otra similar).
- Material impreso con esquemas comparativos de hardware, software local y computación en la nube.
- Video corto introductorio sobre ciberseguridad (duración 5 minutos).
- Herramientas digitales para mapas mentales (ej. Coggle, MindMeister) o papel y marcadores para mapas mentales manuales.
- Encuesta digital rápida (Google Forms o similar) para activación de conocimientos.
- Documento guía con preguntas para reflexión y discusión.

Requisitos Previos

- Conocimientos básicos de informática y sistemas operativos.
- Familiaridad previa con conceptos tecnológicos generales (hardware y software).
- Habilidades básicas para navegar en internet y manejo elemental de plataformas digitales.
- Experiencia mínima en trabajo colaborativo en entornos digitales (recomendable, no excluyente).

Actividades

Plan de Actividades para Ecosistemas Digitales y Ciberseguridad

Sesión 1: Introducción a los Ecosistemas Digitales y Computación en la Nube

Fase de Inicio

Tiempo estimado: 15 minutos

Propósito de la sesión:

Conectar con conocimientos previos y presentar el objetivo de comprender las diferencias entre hardware, software local y computación en la nube, y la importancia de estos conceptos en la ingeniería de sistemas.

Activación de conocimientos previos:

- **Docente:** Saluda a los estudiantes y plantea la pregunta inicial: "*¿Qué entienden por hardware, software local y computación en la nube? ¿Pueden dar ejemplos de cada uno?*"
- **Estudiantes:** Responden en una lluvia de ideas rápida (3-5 minutos), participando oralmente o por chat si es virtual.
- **Docente:** Registra las respuestas en pantalla o pizarra para luego compararlas con la información oficial.

Motivación y enganche:

- **Docente:** Presenta un dato curioso: "*En 2023, más del 80% de las empresas en el mundo utilizan servicios en la nube para almacenar sus datos y operar. ¿Qué riesgos y beneficios creen que esto implica?*"
- **Estudiantes:** Reflexionan brevemente y comparten opiniones iniciales.

Contextualización:

- **Docente:** Explica cómo estos conceptos impactan directamente en la vida académica y profesional de los estudiantes, por ejemplo, al elegir dónde guardar sus proyectos o cómo colaborar en equipo.
- **Estudiantes:** Escuchan y anotan puntos clave para vincular el aprendizaje con su realidad.

Fase de Desarrollo

Tiempo estimado: 95 minutos

Presentación del contenido:

Se introduce el contenido mediante recursos visuales, esquemas comparativos, y videos cortos, evitando exposiciones magistrales largas. Se promueve la interacción constante para mantener la atención y el aprendizaje activo.

Actividad 1: Comparación y clasificación de conceptos

- **Objetivo:** Explicar las diferencias entre hardware, software local y computación en la nube.
- **Instrucciones:**
 - **Docente:** Divide a los estudiantes en grupos de 3-4. Entrega material impreso con definiciones breves y ejemplos variados.
 - Solicita que trabajen juntos para clasificar cada ejemplo bajo hardware, software local o computación en la nube, y que justifiquen cada clasificación.
 - Luego, cada grupo presenta un ejemplo y su clasificación, generando debate.
- **Organización:** Grupos de 3-4 estudiantes.
- **Producto/Evidencia:** Tabla clasificada con ejemplos y justificaciones.
- **Tiempo:** 30 minutos.
- **Rol del docente:** Facilita la dinámica, observa la participación, formula preguntas para profundizar, y guía la discusión.

Actividad 2: Exploración práctica de plataformas SaaS

- **Objetivo:** Utilizar plataformas SaaS para colaborar de manera eficiente.
- **Instrucciones:**
 - **Docente:** Asigna parejas y presenta una breve demo de una plataforma SaaS (Google Docs, Microsoft Teams, etc.).
 - Indica que los estudiantes deben crear un documento colaborativo donde respondan a preguntas sobre la sesión y agreguen comentarios.
 - Invita a experimentar funciones como compartir, comentar y editar simultáneamente.
- **Organización:** Parejas.
- **Producto/Evidencia:** Documento colaborativo con respuestas y comentarios.
- **Tiempo:** 40 minutos.
- **Rol del docente:** Supervisa el uso de la plataforma, brinda apoyo técnico, y fomenta la colaboración.

Actividad 3: Video y debate sobre ciberseguridad básica

- **Objetivo:** Introducir prácticas básicas de identidad digital, privacidad y ciberseguridad.

- **Instrucciones:**

- **Docente:** Proyecta un video corto de 5 minutos que muestre casos reales de ciberataques y buenas prácticas.
- Luego, lanza preguntas para debate guiado, por ejemplo: "*¿Qué riesgos identifican en los casos? ¿Cómo podrían protegerse mejor?*"
- **Estudiantes:** Participan en debate abierto, exponiendo ideas y experiencias.

- **Organización:** Plenaria.

- **Producto/Evidencia:** Notas de debate y conclusiones.

- **Tiempo:** 25 minutos.

- **Rol del docente:** Modera el debate, fomenta participación equitativa, sintetiza ideas clave.

Diferenciación:

- Para estudiantes que terminan antes: Invitar a investigar herramientas adicionales de computación en la nube y anotar ventajas/desventajas para compartir.
- Para estudiantes que requieren apoyo: Brindar guías escritas claras y apoyo individual, además de permitir respuestas orales o visuales en lugar de escritas si es necesario.

Transiciones:

El docente conecta cada actividad destacando cómo lo aprendido en la anterior fundamenta la siguiente para construir un entendimiento sólido y aplicado del tema.

Fase de Cierre

Tiempo estimado: 10 minutos

Síntesis:

- **Docente:** Propone que cada estudiante escriba en un "ticket de salida" tres ideas clave que aprendieron sobre ecosistemas digitales y ciberseguridad.
- **Estudiantes:** Escriben y entregan sus tickets.

Reflexión metacognitiva:

- ¿Cómo puedo aplicar lo aprendido hoy en mi vida académica o profesional?
- ¿Qué concepto me resultó más desafiante y cómo puedo profundizar en él?
- ¿Qué prácticas de ciberseguridad considero esenciales para proteger mi identidad digital?

Retroalimentación:

El docente lee varios tickets en voz alta, ofrece retroalimentación positiva y orienta sobre cómo seguir mejorando.

Transferencia:

Se anticipa que en la siguiente sesión se profundizará en la aplicación práctica de la ciberseguridad en entornos colaborativos digitales.

Sesión 2: Colaboración en la Nube y Seguridad Digital Práctica

Fase de Inicio

Tiempo estimado: 10 minutos

Propósito de la sesión:

Conectar con la sesión anterior y preparar a los estudiantes para aplicar prácticas de identidad digital y ciberseguridad mientras colaboran en entornos SaaS.

Activación de conocimientos previos:

- **Docente:** Presenta una encuesta rápida digital con preguntas sobre conceptos clave vistos en la sesión anterior.
- **Estudiantes:** Responden la encuesta en 5 minutos.
- **Docente:** Comenta resultados y aclara dudas rápidas.

Motivación y enganche:

- **Docente:** Propone un reto: *"Imagina que tu equipo debe diseñar una guía rápida de buenas prácticas de seguridad para compartir con nuevos estudiantes. ¿Qué incluirías?"*
- **Estudiantes:** Reflexionan y anticipan la actividad principal del día.

Contextualización:

El docente explica la importancia de la seguridad digital para proteger información personal y profesional en un mundo cada vez más conectado.

Fase de Desarrollo

Tiempo estimado: 100 minutos

Actividad 1: Creación colaborativa de guía de buenas prácticas de ciberseguridad

- **Objetivo:** Aplicar prácticas básicas de identidad digital, privacidad y ciberseguridad.
- **Instrucciones:**
 - **Docente:** Divide a los estudiantes en grupos de 4. Cada grupo accede a un documento compartido en una plataforma SaaS.
 - Solicita que elaboren una guía con al menos 8 recomendaciones prácticas para proteger la identidad digital y la privacidad en ambientes académicos y profesionales.
 - Los grupos deben usar funciones colaborativas para comentar y editar en tiempo real.

- **Organización:** Grupos de 4 estudiantes.
- **Producto/Evidencia:** Documento colaborativo con guía de buenas prácticas.
- **Tiempo:** 60 minutos.
- **Rol del docente:** Facilita la colaboración, responde preguntas, sugiere puntos clave y fomenta la inclusión de ejemplos reales.

Actividad 2: Simulación de escenarios de riesgo y toma de decisiones

- **Objetivo:** Evaluar y aplicar prácticas de ciberseguridad en contextos reales.
- **Instrucciones:**
 - **Docente:** Presenta 3 escenarios escritos breves que incluyen riesgos típicos de seguridad digital (phishing, contraseñas débiles, uso inadecuado de redes públicas).
 - Los grupos discuten cuál sería la mejor respuesta y escriben un plan de acción para cada escenario.
 - Se realiza puesta en común y debate sobre las decisiones tomadas.
- **Organización:** Mismos grupos de actividad 1.
- **Producto/Evidencia:** Plan de acción escrito para cada escenario.
- **Tiempo:** 35 minutos.
- **Rol del docente:** Modera la discusión, plantea preguntas guía como: "*¿Qué consecuencias se evitarían con esta acción?*", y resalta buenas prácticas.

Diferenciación:

- Para estudiantes avanzados: Proponer que integren herramientas digitales específicas para reforzar la seguridad (autenticación multifactor, gestores de contraseñas).
- Para estudiantes que requieren apoyo: Proveer ejemplos concretos y ofrecer asistencia en la redacción y organización de ideas.

Transiciones:

El docente conecta la simulación con el cierre, invitando a reflexionar sobre la importancia de la seguridad digital en la colaboración diaria.

Fase de Cierre

Tiempo estimado: 10 minutos

Síntesis:

- **Docente:** Solicita a cada grupo compartir oralmente una recomendación clave de su guía y una lección aprendida del ejercicio de simulación.
- **Estudiantes:** Exponen sus aportes brevemente.

Reflexión metacognitiva:

- ¿Cómo cambió mi percepción sobre la seguridad digital después de estas actividades?
- ¿Qué práctica de identidad digital implementaré de inmediato en mi vida académica o profesional?
- ¿Qué dudas o inquietudes me gustaría resolver en futuras sesiones?

Retroalimentación:

El docente ofrece comentarios positivos sobre la colaboración y la calidad de las guías, además de sugerir recursos para profundizar.

Transferencia:

Invita a aplicar las guías elaboradas en proyectos futuros y a compartirlas con compañeros que no participaron.

Tarea o reto:

- Los estudiantes deben implementar al menos tres recomendaciones de seguridad en sus cuentas personales y redactar un breve informe sobre su experiencia para la próxima clase.

Evaluación

Tipo de evaluación:

- **Diagnóstica:** Activación de conocimientos previos en la sesión 1 (fase de inicio).
- **Formativa:** Observación y retroalimentación durante actividades colaborativas y debates en ambas sesiones.
- **Sumativa:** Productos finales como tabla comparativa, documentos colaborativos, planes de acción y reflexión escrita/ticket de salida.

Criterios de evaluación:

- Capacidad para explicar con claridad y precisión las diferencias entre hardware, software local y computación en la nube.
- Dominio en el uso de plataformas SaaS para colaborar eficazmente en equipo.
- Aplicación correcta de prácticas básicas de identidad digital, privacidad y ciberseguridad en contextos académicos y profesionales.

Instrumentos sugeridos:

- Rúbrica de evaluación para documentos colaborativos y planes de acción.
- Lista de cotejo para participación activa y calidad de aportes en debates.
- Observación directa durante actividades prácticas.
- Autoevaluación y coevaluación mediante cuestionarios breves.

Evidencias de aprendizaje:

- Tabla comparativa con clasificaciones y justificaciones.

- Documento colaborativo con guía de buenas prácticas.
- Plan de acción para escenarios de riesgo.
- Ticket de salida con síntesis individual.
- Informe de aplicación de recomendaciones de seguridad en la tarea.