

# Explorando la Seguridad Computacional: Definiciones, Políticas y Ética en Acción

Ingeniería | Ingeniería de sistemas | Aprendizaje Basado en Problemas

## Descripción

Este plan de clase tiene como propósito que los estudiantes universitarios de Ingeniería de Sistemas comprendan los fundamentos esenciales de la seguridad computacional, incluyendo definiciones clave, políticas informales y formales, diferencias entre seguridad computacional y seguridad comercial, y consideraciones éticas relevantes. A través de un enfoque activo basado en la metodología Aprendizaje Basado en Problemas (ABP), los estudiantes analizarán casos reales y simulados para desarrollar pensamiento crítico y habilidades para diseñar y evaluar políticas de seguridad efectivas.

La seguridad computacional es un área crucial en la ingeniería moderna, no solo para proteger sistemas y datos, sino también para garantizar el cumplimiento ético y legal en el manejo de la información. Este conocimiento es relevante para los futuros ingenieros de sistemas, quienes serán responsables de diseñar, implementar y mantener infraestructuras seguras en organizaciones de diversos sectores. El aprendizaje se conecta con su vida profesional y cotidiana, pues la protección de datos y la ética en tecnología son temas de creciente importancia global.

## Objetivos de Aprendizaje

- Analizar las definiciones y conceptos fundamentales de la seguridad computacional.
- Diferenciar entre políticas informales y formales de seguridad, identificando sus características y aplicaciones.
- Comparar la seguridad computacional con la seguridad comercial para entender sus ámbitos y objetivos.
- Argumentar sobre las consideraciones éticas implicadas en la seguridad computacional.
- Aplicar el método de Aprendizaje Basado en Problemas para resolver casos relacionados con seguridad computacional.

## Recursos Necesarios

- Proyector y computadora para presentaciones.
- Acceso a internet para consulta en línea.
- Material impreso: casos de estudio sobre seguridad computacional (2 copias por grupo).
- Plataforma digital para trabajo colaborativo (ej. Google Drive o Microsoft Teams).
- Pizarras o rotafolios con marcadores para trabajo en grupo.
- Videos breves sobre incidentes reales de seguridad informática (3 videos de 3-5 minutos).
- Cuadernos y bolígrafos para toma de notas.

## Requisitos Previos

- Conocimientos básicos de sistemas informáticos y redes.
- Familiaridad con conceptos elementales de seguridad informática.
- Habilidades básicas para trabajo en equipo y análisis crítico.
- Experiencia previa en lectura y análisis de textos técnicos.

## Actividades

# Plan de Actividades para Seguridad Computacional

### Sesión 1: Fundamentos y Políticas de Seguridad Computacional

#### Fase de Inicio

**Tiempo estimado: 15 minutos**

#### Propósito de la sesión:

**Docente:** Explica que en esta sesión se introducirán las definiciones básicas y el concepto de políticas de seguridad, esenciales para entender cómo proteger sistemas de información. Subraya la importancia de comprender estos conceptos para aplicar soluciones reales en su futura profesión.

#### Activación de conocimientos previos:

**Docente:** Plantea la pregunta detonadora a los estudiantes: "¿Qué entienden por seguridad computacional y por qué creen que es importante en las organizaciones actuales?"

**Estudiantes:** Responden individualmente con ideas breves y luego comparten en plenaria durante 5 minutos, el docente toma nota de ideas clave en la pizarra.

#### Motivación y enganche:

**Docente:** Presenta un video corto (3 min) sobre un incidente real de ciberataque a una empresa conocida, mostrando las consecuencias.

**Estudiantes:** Observan el video y reflexionan brevemente sobre el impacto.

#### Contextualización:

**Docente:** Conecta el tema con la vida diaria y futura profesional de los estudiantes, explicando cómo la seguridad computacional protege tanto datos personales como información crítica en empresas y gobiernos.

**Estudiantes:** Escuchan y participan con preguntas o comentarios.

#### Fase de Desarrollo

**Tiempo estimado: 90 minutos**

### **Presentación del contenido:**

**Docente:** Introduce brevemente las definiciones clave de seguridad computacional, políticas informales y formales, y las diferencias entre seguridad computacional y comercial a través de una lectura guiada (material impreso entregado).

### **Actividad 1: Análisis de Definiciones y Políticas**

- **Objetivo:** Analizar conceptos y diferenciar tipos de políticas de seguridad.
- **Instrucciones:**
  - **Docente:** Divide la clase en grupos de 4. Cada grupo recibe un conjunto de definiciones y ejemplos de políticas informales y formales para analizar.
  - Los grupos deben discutir y clasificar cada política como formal o informal, y justificar sus elecciones.
  - Luego, preparan una breve presentación de 5 minutos.
- **Organización:** Grupos de 4 estudiantes.
- **Producto:** Presentación grupal y lista clasificada de políticas.
- **Tiempo:** 40 minutos.
- **Rol del docente:** Observa las discusiones, formula preguntas guía como "¿Qué características identifican a una política formal?" y "¿Por qué algunas políticas son informales?", además de apoyar con ejemplos si es necesario.

### **Actividad 2: Debate Comparativo**

- **Objetivo:** Comparar seguridad computacional y seguridad comercial.
- **Instrucciones:**
  - **Docente:** Propone un debate en plenaria con la consigna: "¿En qué se diferencian y se parecen la seguridad computacional y la seguridad comercial?"
  - Organiza a los estudiantes en dos grupos que defienden cada tipo de seguridad.
  - Cada grupo prepara argumentos basados en los materiales y el conocimiento previo.
  - Se realiza el debate durante 25 minutos, seguida de una reflexión conjunta.
- **Organización:** Plenaria dividida en dos grupos.
- **Producto:** Argumentos escritos y debate oral.
- **Tiempo:** 30 minutos.
- **Rol del docente:** Modera el debate, incentiva la participación equitativa, y plantea preguntas para profundizar el análisis.

### **Diferenciación:**

- Para estudiantes que terminan antes: Se les invita a investigar un caso adicional de política formal en línea y preparar un breve resumen para compartir en la siguiente sesión.
- Para estudiantes que requieren más apoyo: Se ofrece una guía con definiciones simplificadas y ejemplos adicionales, y se promueve el trabajo colaborativo en grupos heterogéneos.

### **Transición:**

**Docente:** Resume las diferencias y similitudes discutidas y anuncia que en la siguiente sesión se abordarán las consideraciones éticas y se aplicarán todos los conceptos en un caso práctico.

## **Fase de Cierre**

**Tiempo estimado: 15 minutos**

### **Síntesis:**

**Docente:** Invita a los estudiantes a crear un mapa mental colectivo en la pizarra con los conceptos clave y las relaciones entre definiciones, políticas y tipos de seguridad.

**Estudiantes:** Participan aportando ideas y conceptos para el mapa mental.

### **Reflexión metacognitiva:**

- ¿Cómo diferenciarías una política formal de una informal en un entorno empresarial?
- ¿Por qué es importante entender la diferencia entre seguridad computacional y seguridad comercial?
- ¿Qué relevancia tiene para ti el conocimiento adquirido sobre seguridad computacional?

### **Retroalimentación:**

**Docente:** Proporciona comentarios inmediatos sobre las presentaciones y participación, destacando fortalezas y áreas de mejora.

### **Transferencia:**

**Docente:** Explica que en la próxima sesión aplicarán estos conceptos en un escenario real para profundizar en las implicaciones éticas y prácticas.

## **Sesión 2: Ética y Aplicación Práctica en Seguridad Computacional**

### **Fase de Inicio**

**Tiempo estimado: 10 minutos**

### **Propósito de la sesión:**

**Docente:** Recuerda brevemente lo visto en la sesión anterior, enfatizando los conceptos clave y objetivos. Presenta que hoy se explorarán las consideraciones éticas y se resolverá un caso práctico aplicando todo lo aprendido.

### **Activación de conocimientos previos:**

**Docente:** Plantea la pregunta para discusión rápida en parejas: "¿Qué situaciones éticas crees que pueden surgir en la gestión de la seguridad computacional?"

**Estudiantes:** Discuten en parejas durante 5 minutos y comparten algunas ideas en plenaria.

### **Motivación y enganche:**

**Docente:** Muestra un segundo video (4 minutos) sobre un dilema ético real en seguridad informática, invitando a reflexionar sobre las decisiones tomadas.

### **Contextualización:**

**Docente:** Relaciona el tema ético con el rol profesional del ingeniero, destacando la responsabilidad social y legal.

## **Fase de Desarrollo**

### **Tiempo estimado: 95 minutos**

#### **Presentación del contenido:**

**Docente:** Introduce las consideraciones éticas en seguridad computacional con ejemplos concretos y normativa aplicable, apoyándose en un resumen impreso.

### **Actividad 3: Resolución de Caso Ético**

- **Objetivo:** Argumentar sobre consideraciones éticas y aplicar conceptos de seguridad computacional.
- **Instrucciones:**
  - **Docente:** Presenta un caso real o simulado que involucra un dilema ético relacionado con la seguridad de la información.
  - Los estudiantes trabajan en grupos de 4 para analizar el caso, identificar problemas, proponer soluciones y justificar sus decisiones éticas.
  - Preparan una presentación grupal (7 minutos) para compartir sus conclusiones.
- **Organización:** Grupos de 4 estudiantes.
- **Producto:** Informe y presentación grupal.
- **Tiempo:** 60 minutos.
- **Rol del docente:** Facilita el análisis con preguntas guía: "¿Qué valores están en conflicto?", "¿Cómo afectaría esta decisión a los usuarios y a la empresa?", "¿Qué políticas podrían prevenir esta situación?"

### **Actividad 4: Síntesis y Debate Final**

- **Objetivo:** Consolidar aprendizajes y reflexionar críticamente.
- **Instrucciones:**

- **Docente:** Propone un debate en plenaria sobre el impacto de las políticas y la ética en la seguridad computacional, tomando como base las presentaciones de los grupos.
- Los estudiantes participan expresando sus puntos de vista y construyendo consensos.
- **Organización:** Plenaria.
- **Producto:** Debate oral y conclusiones escritas breves.
- **Tiempo:** 30 minutos.
- **Rol del docente:** Modera, fomenta la participación respetuosa y destaca las conexiones con los objetivos de aprendizaje.

### **Diferenciación:**

- Para estudiantes adelantados: Se les invita a relacionar el caso con normativas internacionales y preparar una breve comparación para compartir.
- Para estudiantes con dificultades: Se les proporciona una guía con preguntas estructuradas para apoyar el análisis y se fomenta la colaboración cercana en su grupo.

### **Transición:**

**Docente:** Resume los aprendizajes logrados y enfatiza la importancia de aplicar estos conocimientos en su desarrollo profesional y ético.

### **Fase de Cierre**

**Tiempo estimado: 15 minutos**

### **Síntesis:**

**Docente:** Solicita a cada estudiante escribir en una tarjeta tres ideas clave que se llevan de la unidad y cómo piensan aplicarlas en su carrera.

### **Reflexión metacognitiva:**

- ¿Cómo aplicarías una política formal para mejorar la seguridad en un sistema que diseñes?
- ¿Qué aprendiste sobre la importancia de la ética en la seguridad computacional?
- ¿De qué manera el aprendizaje basado en problemas te ayudó a comprender mejor el tema?

### **Retroalimentación:**

**Docente:** Recoge las tarjetas, comenta las ideas más recurrentes o innovadoras, y brinda retroalimentación positiva y constructiva final.

### **Transferencia:**

**Docente:** Invita a los estudiantes a aplicar lo aprendido en la elaboración de futuros proyectos y en su vida profesional, recordando la responsabilidad ética y técnica.

## Tarea o reto:

**Docente:** Propone investigar una política de seguridad formal vigente en una empresa o gobierno, y redactar un breve informe crítico para presentar en la próxima clase.

## Evaluación

# Estrategia de Evaluación

### • Tipo de evaluación:

- Diagnóstica: en la fase de inicio de la sesión 1, mediante la pregunta detonadora para valorar conocimientos previos.
- Formativa: durante las actividades de análisis grupal, debate y resolución de casos en ambas sesiones, con observación y retroalimentación continua.
- Sumativa: en el cierre de la sesión 2, a través del informe del caso ético, presentaciones grupales y las reflexiones individuales en tarjetas.

### • Criterios de evaluación:

- Capacidad para analizar y explicar definiciones y conceptos clave de seguridad computacional.
- Habilidad para diferenciar y clasificar políticas informales y formales con justificación adecuada.
- Claridad y coherencia en la comparación entre seguridad computacional y comercial.
- Argumentación fundamentada sobre aspectos éticos y aplicación en casos prácticos.
- Participación activa y colaborativa en actividades de aprendizaje basado en problemas.

### • Instrumentos sugeridos:

- Lista de cotejo para participación y trabajo en equipo.
- Rúbrica para evaluación de presentaciones grupales e informes escritos.
- Observación directa durante debates y actividades.
- Autoevaluación y coevaluación al final de la segunda sesión.

### • Evidencias de aprendizaje:

- Presentaciones grupales sobre políticas y casos éticos.
- Listas clasificadas y mapas mentales elaborados en clase.
- Informes escritos y reflexiones individuales.
- Participación activa en debates y discusiones.