

Descubriendo la privacidad en Data Science: Ética y protección en el manejo de datos

Tecnologías Emergentes e Impacto Social | Privacidad de Datos y Seguridad Informática | Design Thinking

Descripción

Este plan de clase está diseñado para que adultos en educación para el trabajo comprendan y apliquen los principios fundamentales de la privacidad de datos en el contexto del Data Science. Los estudiantes aprenderán cómo proteger la información confidencial durante todo el ciclo de vida del análisis de datos, desde la recolección hasta la presentación de resultados, asegurando un manejo ético y legal. La privacidad de datos es un tema crucial en la era digital actual, donde la información personal se usa para tomar decisiones que pueden afectar vidas y negocios. Este aprendizaje es relevante para cualquier persona que maneje datos o esté interesada en tecnología, ya que les proporcionará herramientas prácticas para garantizar que el uso de los datos respete la privacidad y cumpla con normativas vigentes. A través de una metodología activa basada en Design Thinking, los estudiantes podrán empatizar con usuarios afectados, identificar problemas, proponer soluciones y evaluar el impacto de sus decisiones en la privacidad de los datos. Esto los prepara para enfrentar retos reales en ambientes laborales donde el uso responsable de la información es clave.

Objetivos de Aprendizaje

- Analizar las etapas del ciclo de vida del Data Science con enfoque en privacidad de datos.
- Aplicar principios fundamentales de privacidad en la recolección, almacenamiento y uso de datos.
- Diseñar estrategias prácticas para garantizar el uso ético y legal de información confidencial.
- Evaluar casos reales de violaciones a la privacidad y proponer soluciones basadas en buenas prácticas.

Recursos Necesarios

- Pizarra o rotafolio con marcadores.
- Computadoras o tablets con acceso a internet (1 por cada 2 estudiantes).
- Presentación digital (PowerPoint o equivalente) con conceptos clave y casos.
- Hojas impresas con guías para actividades de ideación y prototipado.
- Material para prototipado: papel, lápices, post-its, marcadores.
- Videos cortos sobre privacidad de datos y Data Science (2 videos de 3-5 minutos).
- Formulario de autoevaluación impreso o digital.

Requisitos Previos

- Conocimientos básicos de informática y manejo de datos.
- Familiaridad con conceptos generales de tecnología y uso de internet.
- Experiencia previa en análisis o manejo sencillo de información (aunque sea personal o laboral).
- Habilidades básicas de lectura y expresión oral para participar en debates y exposiciones.

Actividades

Sesión 1: Entendiendo el valor y los riesgos de la privacidad en Data Science

Fase de Inicio

Tiempo estimado: 15 minutos

Propósito de la sesión:

Conectar a los estudiantes con el tema de privacidad en el manejo de datos, motivarlos a identificar la importancia y los riesgos relacionados con su información personal en el contexto del Data Science.

Activación de conocimientos previos:

- **Docente:** Pregunta inicial para toda la clase: “¿Han escuchado o vivido alguna situación donde sus datos personales hayan sido usados sin su permiso? ¿Qué consecuencias tuvo eso?”
- **Estudiantes:** Responden oralmente compartiendo alguna experiencia o percepción, el docente escribe palabras clave en la pizarra para luego retomar.

Motivación y enganche:

- **Docente:** Presenta un dato curioso: “Cada día, más de 2.5 quintillones de bytes de datos se generan en el mundo. ¿Sabían que gran parte de esos datos son sobre ustedes, sobre sus hábitos y preferencias?”
- **Estudiantes:** Reflexionan brevemente sobre la magnitud del dato y su implicación personal.

Contextualización:

- **Docente:** Explica que la clase tratará sobre cómo proteger la privacidad cuando se trabaja con datos y por qué es importante para ellos, ya sea en su vida personal o en futuros empleos.
- **Estudiantes:** Escuchan y preparan preguntas o comentarios.

Fase de Desarrollo

Tiempo estimado: 95 minutos

Presentación del contenido:

El docente introduce el ciclo de vida del Data Science, destacando cada etapa y los riesgos de privacidad asociados. Para cada etapa, se muestra un ejemplo real y se invita a los estudiantes a reflexionar sobre posibles vulnerabilidades.

Actividad 1: Mapeo colectivo del ciclo de vida del Data Science

- **Objetivo:** Analizar las etapas del ciclo de vida con enfoque en privacidad.
- **Instrucciones:**
 - **Docente:** Divide la pizarra o rotafolio en cinco secciones: Recolección, Limpieza, Análisis, Almacenamiento, Presentación.
 - Solicita que en grupos de 3-4, los estudiantes escriban en post-its ejemplos o riesgos de privacidad que conocen o imaginan para cada etapa.
 - Los grupos van colocando sus post-its en la sección correspondiente mientras explican su idea.
 - El docente organiza y complementa la información para clarificar conceptos.
- **Organización:** Grupos de 3-4 estudiantes.
- **Producto:** Mapa visual en la pizarra con riesgos y ejemplos por etapa.
- **Tiempo:** 35 minutos.
- **Rol docente:** Facilita, pregunta: “¿Por qué creen que este riesgo es importante aquí?”, “¿Qué pasaría si no se controla?”

Actividad 2: Video y debate: Casos reales de violación de privacidad

- **Objetivo:** Evaluar casos reales y comprender consecuencias.
- **Instrucciones:**
 - **Docente:** Muestra dos videos cortos con casos reales de mal manejo de datos y breves consecuencias legales/sociales.
 - Pide que los estudiantes formen parejas para responder: “¿Qué principios de privacidad se violaron?”, “¿Cómo evitarían ese problema?”
 - Invita a compartir las respuestas en plenaria y genera discusión moderada.
- **Organización:** Parejas y plenaria.
- **Producto:** Lista colectiva de principios violados y propuestas para corregir.
- **Tiempo:** 40 minutos.
- **Rol docente:** Guía preguntas para profundizar en aspectos éticos y legales.

Actividad 3: Ideación - Diseñando prácticas para proteger datos

- **Objetivo:** Diseñar estrategias prácticas para privacidad y uso ético.
- **Instrucciones:**
 - **Docente:** Entrega hoja guía con preguntas: “¿Qué puedo hacer en cada etapa para proteger datos?”, “¿Qué herramientas o reglas aplicaría?”

- En grupos, idean al menos 3 prácticas concretas que podrían implementar.
- Comparten en plenaria y el docente anota para referencia futura.
- **Organización:** Grupos de 3-4 estudiantes.
- **Producto:** Lista de estrategias prácticas.
- **Tiempo:** 20 minutos.
- **Rol docente:** Estimula creatividad, pregunta: “¿Cómo aplicarían esta práctica en su trabajo o vida?”

Diferenciación

- Para estudiantes que terminan antes: Proporcionar un breve artículo digital con regulaciones vigentes (por ejemplo, GDPR o leyes locales) para que identifiquen un principio adicional.
- Para estudiantes que necesitan apoyo: Ofrecer resumen visual del ciclo de vida y ejemplos concretos para facilitar comprensión, apoyo individual durante actividades grupales.

Transiciones

- Al terminar la ideación, el docente conecta: “En la próxima sesión pondremos a prueba estas ideas creando prototipos y evaluando su impacto en casos específicos.”

Fase de Cierre

Tiempo estimado: 10 minutos

Síntesis:

- **Docente:** Solicita que cada estudiante escriba en un papel tres ideas claves aprendidas sobre privacidad en Data Science.
- **Estudiantes:** Escriben y comparten al menos una idea con un compañero.

Reflexión metacognitiva:

- ¿Qué etapa del ciclo de Data Science me parece más vulnerable en términos de privacidad y por qué?
- ¿Cómo puedo aplicar hoy lo aprendido para proteger mis datos personales?
- ¿Qué dudas o preguntas tengo para aclarar en la siguiente sesión?

Retroalimentación:

- **Docente:** Escucha las respuestas, brinda comentarios positivos y aclara dudas inmediatas.

Transferencia:

- Explica que en la siguiente sesión se trabajará en soluciones concretas para garantizar privacidad y seguridad en proyectos de Data Science.

Sesión 2: Prototipando soluciones éticas y legales para la privacidad en Data Science

Fase de Inicio

Tiempo estimado: 10 minutos

Propósito de la sesión:

Recordar lo aprendido, preparar a los estudiantes para diseñar y evaluar soluciones que garanticen la privacidad en el ciclo de Data Science.

Activación de conocimientos previos:

- **Docente:** Pregunta rápida en plenaria: “¿Cuál fue la práctica que más les gustó de las que diseñaron la clase pasada? ¿Por qué?”
- **Estudiantes:** Responden y comentan experiencias.

Motivación y enganche:

- **Docente:** Presenta un breve escenario: “Imagina que trabajas en un equipo que maneja datos de clientes. ¿Qué harías para proteger la privacidad y cumplir con la ley?”
- **Estudiantes:** Reflexionan y preparan ideas para compartir.

Contextualización:

- **Docente:** Explica que ahora aplicarán Design Thinking para crear prototipos de soluciones concretas.
- **Estudiantes:** Se organizan en grupos para iniciar la actividad.

Fase de Desarrollo

Tiempo estimado: 95 minutos

Presentación del contenido:

Breve revisión de buenas prácticas legales y éticas, introducción a herramientas básicas para proteger datos (anonimización, consentimiento informado, almacenamiento seguro).

Actividad 1: Prototipado de soluciones para cada etapa del ciclo

- **Objetivo:** Aplicar principios de privacidad diseñando soluciones prácticas.
- **Instrucciones:**
 - **Docente:** Entrega a cada grupo una hoja con las etapas del ciclo y espacio para anotar ideas.
 - Pide que elijan una etapa y diseñen un prototipo de solución que incluya medidas para proteger datos y cumplir con la ley.
 - El prototipo puede ser un procedimiento, una política, una herramienta sencilla o un flujo de trabajo.

- Los grupos preparan una breve explicación para presentar a la clase.
- **Organización:** Grupos de 3-4 estudiantes.
- **Producto:** Prototipo en papel con explicación oral.
- **Tiempo:** 50 minutos.
- **Rol docente:** Observa, formula preguntas: “¿Cómo garantizan el consentimiento?”, “¿Qué pasa si alguien incumple esta medida?”

Actividad 2: Evaluación entre pares y mejora del prototipo

- **Objetivo:** Evaluar y mejorar soluciones con enfoque crítico y colaborativo.
- **Instrucciones:**
 - Cada grupo presenta su prototipo frente a otro grupo.
 - El grupo que escucha debe identificar puntos fuertes y áreas de mejora, usando una guía sencilla entregada por el docente.
 - Luego, los grupos regresan para mejorar su propuesta incorporando retroalimentación.
- **Organización:** Grupos en parejas para evaluación y luego trabajo interno.
- **Producto:** Prototipo mejorado y lista de mejoras recibidas.
- **Tiempo:** 35 minutos.
- **Rol docente:** Facilita la discusión, asegura respeto y enfoque constructivo.

Diferenciación

- Estudiantes avanzados pueden apoyar a grupos que se atasquen, sugiriendo recursos o ejemplos.
- Para quienes necesiten más apoyo, ofrecer ejemplos de prototipos simples y acompañamiento directo.

Transiciones

- Al concluir, el docente conecta: “Terminamos con un cierre para consolidar y reflexionar sobre lo aprendido.”

Fase de Cierre

Tiempo estimado: 15 minutos

Síntesis:

- **Docente:** Solicita que cada estudiante complete un “ticket de salida” con tres ideas clave que aplicará para proteger la privacidad en el manejo de datos.
- **Estudiantes:** Escriben y entregan al docente.

Reflexión metacognitiva:

- ¿Qué principio fundamental de privacidad me parece más importante y por qué?

- ¿Cómo puedo garantizar que mis acciones sean éticas y legales al manejar datos?
- ¿Qué desafío veo para aplicar hoy estas prácticas en mi entorno?

Retroalimentación:

- **Docente:** Lee algunas respuestas en voz alta, felicita ideas originales y aclara dudas finales.

Transferencia:

- Invita a aplicar estas prácticas en su vida laboral o personal y a compartir con otros lo aprendido.

Tarea o reto:

- Observar en su entorno un caso donde se manejen datos y hacer una lista breve de recomendaciones para proteger la privacidad según lo aprendido.

Evaluación

Tipo de evaluación:

- **Diagnóstica:** En la Sesión 1, fase de inicio, mediante la activación de conocimientos previos al compartir experiencias.
- **Formativa:** Durante el desarrollo en ambas sesiones, observación directa de participación en actividades grupales, mapeo, ideación, prototipado y debate.
- **Sumativa:** En la fase de cierre de la Sesión 2, con el ticket de salida y la calidad de prototipos diseñados y mejorados.

Criterios de evaluación:

- Relaciona correctamente las etapas del ciclo de Data Science con riesgos y principios de privacidad (Objetivo 1).
- Propone y aplica prácticas claras para proteger datos en contextos específicos (Objetivo 2 y 3).
- Demuestra capacidad crítica para evaluar casos y soluciones desde el enfoque ético y legal (Objetivo 4).

Instrumentos sugeridos:

- Lista de cotejo para participación en actividades grupales.
- Rúbrica para evaluar prototipos: claridad, aplicabilidad, enfoque ético y legal.
- Autoevaluación mediante preguntas de reflexión metacognitiva.

Evidencias de aprendizaje:

- Mapa visual colectivo del ciclo de vida y riesgos.
- Listas de prácticas y estrategias diseñadas.
- Prototipos de soluciones creados y mejorados en grupo.
- Respuestas escritas en tickets de salida y reflexiones finales.

Enriquecimientos

Recomendaciones - Tic_ia

Inicio

- **Herramienta:** Mentimeter (Sustitución)

Implementación: Utilizar Mentimeter para realizar la pregunta inicial sobre experiencias con el uso no autorizado de datos personales. Los estudiantes pueden responder desde sus dispositivos móviles o computadoras, y el docente proyecta las respuestas en tiempo real.

Contribución al objetivo: Facilita la activación de conocimientos previos de manera interactiva y visual, motivando la participación y el análisis de riesgos de privacidad.

- **Herramienta:** Video explicativo breve en YouTube o similar (Aumento)

Implementación: Presentar un video corto y sencillo que explique la magnitud de los datos generados diariamente y su relación con la privacidad, seguido de una breve reflexión guiada por el docente.

Contribución al objetivo: Complementa la motivación con información visual y auditiva que ayuda a contextualizar la importancia de la privacidad en Data Science para adultos con diferentes estilos de aprendizaje.

Desarrollo

- **Herramienta:** Jamboard o Google Jamboard (Modificación)

Implementación: En lugar de usar post-its físicos, los grupos colaboran en un Jamboard digital dividido en las cinco etapas del ciclo de vida del Data Science. Cada grupo añade notas virtuales con ejemplos y riesgos de privacidad.

Contribución al objetivo: Permite una colaboración en tiempo real y organiza visualmente las ideas, facilitando el análisis del ciclo de vida con enfoque en privacidad y fomentando el trabajo en equipo digital.

- **Herramienta:** ChatGPT o IA conversacional (Aumento)

Implementación: Los estudiantes pueden formular preguntas específicas sobre conceptos éticos o riesgos de privacidad durante la sesión, y el docente usa ChatGPT para proporcionar respuestas claras y contextualizadas en lenguaje accesible.

Contribución al objetivo: Mejora la comprensión de conceptos complejos y fomenta la curiosidad, apoyando el aprendizaje autónomo y la aclaración inmediata de dudas.

Cierre

- **Herramienta:** Google Forms con retroalimentación automática (Sustitución)

Implementación: Aplicar un cuestionario digital que evalúe la comprensión de los principios fundamentales de privacidad y ética en Data Science. El formulario incluye preguntas de opción múltiple y de reflexión breve.

Contribución al objetivo: Permite valorar el aprendizaje y reforzar los conceptos clave con retroalimentación inmediata, facilitando la autoevaluación de los estudiantes.

- **Herramienta:** Padlet para reflexión final (Redefinición)

Implementación: Invitar a los estudiantes a publicar en un Padlet sus compromisos personales o ideas para aplicar la privacidad en su entorno laboral o personal, generando un mural digital compartido.

Contribución al objetivo: Fomenta una reflexión profunda y colectiva, creando un espacio para compartir y visualizar compromisos éticos, lo que fortalece la internalización y aplicación práctica del aprendizaje.