Ciberseguridad: Protegiendo tu Mundo Digital

Tecnología e Informática | Manejo de Información | para estudiantes de secundaria (12-15 años) | 20 semanas

Descripción del Curso

Este curso tiene como propósito principal introducir a los estudiantes de secundaria en el fascinante mundo de la ciberseguridad, enfocándose en el manejo seguro y responsable de la información digital. A lo largo de 20 semanas, los alumnos explorarán conceptos clave relacionados con la protección de datos personales, el reconocimiento de amenazas cibernéticas como estafas y spam, y el entendimiento básico de cómo funcionan los algoritmos que influyen en sus experiencias en línea.

Dirigido a estudiantes de 12 a 15 años, el curso utiliza una metodología participativa y práctica que combina actividades colaborativas, análisis de casos reales y ejercicios interactivos, fomentando el pensamiento crítico y el desarrollo de habilidades digitales esenciales para su vida diaria y académica.

Al finalizar, los estudiantes serán capaces de identificar riesgos en entornos digitales, aplicar buenas prácticas para proteger su información, reconocer intentos de fraude y manipulación, y entender la importancia del control sobre los algoritmos que afectan su navegación, promoviendo así un uso más seguro, consciente y ético de la tecnología.

Objetivos Generales

- Describir los conceptos fundamentales de la ciberseguridad y su importancia en la vida diaria.
- Identificar y diferenciar tipos comunes de amenazas digitales y sus características.
- Aplicar medidas básicas de protección para resguardar la información personal en línea.
- Analizar el impacto de los algoritmos en la selección y presentación de información digital.
- Evaluar y comunicar prácticas seguras para navegar y utilizar tecnologías digitales de forma responsable.

Competencias

- Identificar y analizar diferentes tipos de amenazas digitales como estafas, spam y malware.
- Aplicar estrategias básicas para proteger la información personal y la privacidad en entornos digitales.
- Reconocer y evaluar el funcionamiento y la influencia de algoritmos en plataformas digitales.
- Desarrollar habilidades para un uso responsable y seguro de las tecnologías de información.
- Comunicar de manera efectiva recomendaciones y buenas prácticas en ciberseguridad.

Requerimientos

- Conocimientos básicos de uso de computadoras e internet.
- Acceso a un dispositivo con conexión a internet para actividades prácticas.

- Material didáctico proporcionado, incluyendo guías, videos y casos de estudio.
- Habilidades básicas de lectura y comprensión en español.

Unidades del Curso

Unidad 1: Introducción a la Ciberseguridad

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de definir los conceptos básicos de ciberseguridad y explicar su importancia en la vida diaria mediante ejemplos cotidianos.
- Al finalizar la unidad, el estudiante será capaz de identificar y clasificar tipos comunes de amenazas digitales, como virus, phishing y malware, a partir de situaciones simuladas.
- Al finalizar la unidad, el estudiante será capaz de describir cómo la ciberseguridad afecta la privacidad y la seguridad personal en línea, analizando casos sencillos.
- Al finalizar la unidad, el estudiante será capaz de explicar la relación entre la protección de datos personales y el uso responsable de tecnologías digitales, justificando buenas prácticas básicas.

Contenidos Temáticos

1. Conceptos básicos de ciberseguridad

- Definición de ciberseguridad: qué es y para qué sirve.
- Importancia de la ciberseguridad en la vida diaria: ejemplos cotidianos de protección digital.
- Elementos fundamentales: privacidad, confidencialidad, integridad y disponibilidad de la información.

2. Tipos comunes de amenazas digitales

- Virus: qué son, cómo se propagan y ejemplos simples.
- Malware: definición general y tipos comunes (troyanos, spyware, ransomware).
- Phishing: qué es, cómo reconocerlo y efectos en la seguridad personal.
- Otras amenazas básicas: spam, ataques de ingeniería social, contraseñas débiles.

3. Impacto de la ciberseguridad en la privacidad y seguridad personal en línea

- Qué es la privacidad en internet y por qué es importante.
- Cómo las amenazas digitales pueden afectar la información personal.
- Casos sencillos de violación de privacidad y consecuencias.

4. Protección de datos personales y uso responsable de tecnologías digitales

- Concepto de datos personales y ejemplos relevantes para estudiantes.

- Buenas prácticas para proteger datos personales en línea: uso de contraseñas seguras, actualización de software, cuidado al compartir información.
- Responsabilidad digital: comportamiento respetuoso y seguro en redes sociales y plataformas digitales.
- Relación entre protección de datos y hábitos seguros para prevenir riesgos.

Actividades

Actividad 1: "Definiendo la ciberseguridad con ejemplos de mi día a día"

Objetivo: Contribuir al primer objetivo de la unidad: definir conceptos básicos y explicar su importancia con ejemplos cotidianos.

Descripción paso a paso:

- El docente inicia con una breve explicación sobre qué es la ciberseguridad.
- Los estudiantes piensan y anotan ejemplos de cómo usan tecnología en su vida diaria (smartphones, juegos, redes sociales).
- En parejas, discuten cómo la ciberseguridad puede ayudar a proteger esos usos.
- Cada pareja comparte uno o dos ejemplos con el grupo.
- El docente complementa con una síntesis y ejemplos adicionales para reforzar la idea.

Organización: individual y parejas

Producto esperado: lista de ejemplos cotidianos relacionados con la ciberseguridad.

Duración estimada: 40 minutos

Actividad 2: "Identificando amenazas digitales en situaciones simuladas"

Objetivo: Identificar y clasificar tipos comunes de amenazas digitales como virus, phishing y malware.

Descripción paso a paso:

- El docente presenta situaciones simuladas o relatos cortos donde se describen casos de virus, phishing, malware.
- En grupos pequeños, los estudiantes leen las situaciones y discuten qué tipo de amenaza representa cada una.
- Cada grupo clasifica y justifica su respuesta.
- Se realiza puesta en común para corregir y aclarar dudas.

Organización: grupos pequeños

Producto esperado: lista clasificada de amenazas con justificación.

Duración estimada: 50 minutos

Actividad 3: "Analizando casos sencillos de privacidad y seguridad en línea"

Objetivo: Describir cómo la ciberseguridad afecta la privacidad y seguridad personal en línea.

Descripción paso a paso:

- El docente presenta dos o tres casos sencillos (por ejemplo, alguien comparte demasiada información personal en redes sociales, o recibe mensajes sospechosos).
- Los estudiantes, en parejas, analizan qué riesgos o problemas de privacidad pueden existir en cada caso.
- Discuten posibles soluciones o recomendaciones para proteger su privacidad.
- Se comparten conclusiones en plenaria y el docente refuerza conceptos clave.

Organización: parejas

Producto esperado: análisis escrito o verbal de riesgos y recomendaciones.

Duración estimada: 45 minutos

Actividad 4: "Buenas prácticas para proteger mis datos personales en línea"

Objetivo: Explicar la relación entre protección de datos personales y uso responsable de tecnologías digitales.

Descripción paso a paso:

- El docente introduce el concepto de datos personales y ejemplos.
- Los estudiantes elaboran una lista de buenas prácticas para proteger sus datos, basándose en lo que han aprendido.
- En grupos, comparan listas y eligen las más importantes.
- Se crea un cartel o presentación sencilla con las buenas prácticas para compartir con toda la clase.

Organización: individual y grupos

Producto esperado: cartel o presentación con buenas prácticas para proteger datos personales.

Duración estimada: 60 minutos

Evaluación

Evaluación diagnóstica

Se evalúa el conocimiento previo sobre ciberseguridad y amenazas digitales.

- **Cómo se evalúa:** cuestionario interactivo breve con preguntas abiertas y de opción múltiple sobre conceptos básicos y experiencias previas.
- **Instrumento sugerido:** cuestionario en papel o digital (5-7 preguntas).

Evaluación formativa

Se evalúa el progreso en la comprensión de conceptos y habilidades para identificar amenazas y proponer buenas prácticas.

- **Cómo se evalúa:** observación durante actividades, revisión de productos parciales (listas, análisis, clasificaciones) y retroalimentación continua.
- **Instrumento sugerido:** rúbrica simple para valorar participación, claridad en justificaciones y calidad de productos.

Evaluación sumativa

Se evalúa la adquisición integral de los objetivos al final de la unidad.

- **Cómo se evalúa:** prueba escrita con preguntas que incluyen definición de conceptos, clasificación de amenazas, análisis de casos y justificación de buenas prácticas.
- **Instrumento sugerido:** examen escrito o digital con preguntas de desarrollo y selección múltiple (15-20 preguntas).

Unidad 2: Entendiendo la Información Digital

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar los diferentes tipos de información digital presentes en entornos en línea mediante ejemplos concretos.
- Al finalizar la unidad, el estudiante será capaz de explicar la importancia de manejar la información digital de forma segura, resaltando las consecuencias de una mala gestión.
- Al finalizar la unidad, el estudiante será capaz de clasificar datos personales y datos públicos, diferenciando su nivel de sensibilidad y riesgo asociado.
- Al finalizar la unidad, el estudiante será capaz de aplicar prácticas básicas para proteger la información digital en situaciones simuladas, como el uso de contraseñas seguras y configuraciones de privacidad.
- Al finalizar la unidad, el estudiante será capaz de evaluar situaciones cotidianas para identificar riesgos potenciales relacionados con el manejo inadecuado de la información digital.

Contenidos Temáticos

1. Introducción a la Información Digital

- Definición de información digital: Qué es y dónde se encuentra en el entorno digital.
- Tipos de información digital: texto, imágenes, videos, audio, datos personales y otros formatos.
- Ejemplos concretos de información digital en redes sociales, aplicaciones y sitios web.

2. Importancia de manejar la información digital de forma segura

- Razones para proteger la información digital: privacidad, reputación, seguridad personal y familiar.
- Consecuencias de una mala gestión: robo de identidad, fraude, pérdida de datos y daño a la imagen personal.
- Casos reales y ejemplos que muestran el impacto de no proteger la información digital.

3. Clasificación de datos: personales y públicos

- Definición y ejemplos de datos personales: nombre, dirección, número telefónico, contraseñas.
- Definición y ejemplos de datos públicos: información compartida en redes sociales, datos de contacto de empresas.
- Nivel de sensibilidad y riesgo asociado a cada tipo de dato.

- Cómo identificar qué información es segura para compartir y cuál no.

4. Prácticas básicas para proteger la información digital

- Uso de contraseñas seguras: características y creación de contraseñas fuertes.
- Configuración de privacidad en redes sociales y aplicaciones.
- Reconocimiento de señales de alerta: enlaces sospechosos, solicitudes inusuales de información.
- Simulaciones prácticas sobre protección de la información digital.

5. Evaluación de riesgos en situaciones cotidianas

- Identificación de riesgos potenciales en ejemplos diarios: chats, juegos en línea, correos electrónicos.
- Análisis crítico de situaciones para detectar manejo inadecuado de información digital.
- Recomendaciones para actuar ante posibles riesgos.

Actividades

Actividad 1: Mapa de Información Digital

Objetivo: Identificar los diferentes tipos de información digital presentes en entornos en línea mediante ejemplos concretos.

Descripción:

- Los estudiantes investigan en parejas ejemplos de información digital que ellos mismos usan o conocen (mensajes, fotos, videos, datos personales).
- Crean un mapa visual o esquema clasificando la información encontrada por tipo (texto, imagen, audio, datos personales, etc.).
- Presentan el mapa a la clase explicando los ejemplos y su clasificación.

Organización: Parejas

Producto esperado: Mapa visual o esquema clasificado con ejemplos concretos.

Duración estimada: 45 minutos

Actividad 2: Debate sobre la importancia de proteger la información digital

Objetivo: Explicar la importancia de manejar la información digital de forma segura y las consecuencias de una mala gestión.

Descripción:

- Se divide la clase en dos grupos: uno argumenta sobre la importancia de proteger la información digital y el otro expone posibles consecuencias de no hacerlo.
- Se prepara un debate guiado con preguntas clave para promover la participación.
- Cierre con reflexión grupal sobre aprendizajes y aplicación en la vida diaria.

Organización: Grupos grandes

Producto esperado: Participación activa en debate y reflexión escrita individual.

Duración estimada: 50 minutos

Actividad 3: Clasificación de datos personales y públicos

Objetivo: Clasificar datos personales y datos públicos, diferenciando su nivel de sensibilidad y riesgo.

Descripción:

- Se entrega a cada estudiante un listado con diferentes tipos de datos (ejemplos variados).
- Indican si cada dato es personal o público y justifican su respuesta.
- Discusión en grupo para comparar clasificaciones y debatir niveles de riesgo asociados.

Organización: Individual y luego grupal

Producto esperado: Lista clasificada y justificada por cada estudiante.

Duración estimada: 40 minutos

Actividad 4: Taller Práctico de Protección Digital

Objetivo: Aplicar prácticas básicas para proteger la información digital en situaciones simuladas.

Descripción:

- Simulación en la que los estudiantes crean contraseñas seguras para diferentes perfiles ficticios.
- Configuración de privacidad en redes sociales mediante ejemplos de perfiles simulados.
- Identificación de riesgos en correos electrónicos o mensajes simulados con enlaces o solicitudes sospechosas.

Organización: Individual y parejas

Producto esperado: Contraseñas creadas, configuraciones de privacidad aplicadas y análisis de riesgos.

Duración estimada: 60 minutos

Actividad 5: Análisis de Riesgos en Situaciones Cotidianas

Objetivo: Evaluar situaciones cotidianas para identificar riesgos potenciales relacionados con el manejo inadecuado de la información digital.

Descripción:

- Se presentan diferentes escenarios cotidianos (por ejemplo, compartir ubicación en redes, responder a desconocidos, descargar apps).
- En grupos, analizan cada situación para identificar posibles riesgos y proponen medidas de protección.
- Se realiza una puesta en común para compartir conclusiones y recomendaciones.

Organización: Grupos pequeños

Producto esperado: Informe grupal con análisis y recomendaciones.

Duración estimada: 50 minutos

Evaluación

Evaluación diagnóstica

Qué se evalúa: Conocimientos previos sobre tipos de información digital y percepción de riesgos.

Cómo se evalúa: Cuestionario breve con preguntas abiertas y de opción múltiple sobre conceptos básicos.

Instrumento sugerido: Cuestionario escrito o digital de 10 preguntas.

Evaluación formativa

Qué se evalúa: Comprensión y aplicación de conceptos durante las actividades (identificación, clasificación, protección y análisis de riesgos).

Cómo se evalúa: Observación de participación en actividades, revisión de productos elaborados (mapas, listas, análisis, configuraciones).

Instrumento sugerido: Rúbrica de evaluación para cada actividad y registros de observación docente.

Evaluación sumativa

Qué se evalúa: Capacidad para identificar tipos de información digital, explicar la importancia de su protección, clasificar datos, aplicar prácticas básicas y evaluar riesgos.

Cómo se evalúa: Examen escrito y práctico que incluye:

- Preguntas de identificación y clasificación de información.
- Explicación escrita sobre importancia y consecuencias.
- Ejercicios de creación de contraseñas y configuración de privacidad.
- Análisis de escenarios de riesgo.

Instrumento sugerido: Prueba combinada escrita y práctica con rúbrica detallada.

Unidad 3: Amenazas Digitales Comunes

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar las características principales de estafas, spam, phishing y malware mediante ejemplos concretos.
- Al finalizar la unidad, el estudiante será capaz de diferenciar entre tipos de amenazas digitales comunes al analizar situaciones simuladas en entornos digitales.
- Al finalizar la unidad, el estudiante será capaz de describir los riesgos asociados a cada tipo de amenaza digital y explicar su impacto en la seguridad personal en línea.
- Al finalizar la unidad, el estudiante será capaz de clasificar mensajes y contenidos en línea como seguros o potencialmente peligrosos utilizando criterios establecidos durante la unidad.
- Al finalizar la unidad, el estudiante será capaz de elaborar recomendaciones básicas para protegerse contra estafas, spam, phishing y malware en su vida digital cotidiana.

Unidad 4: Protección de Datos Personales

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar los diferentes tipos de datos personales que deben protegerse al usar internet.
- Al finalizar la unidad, el estudiante será capaz de describir las principales estrategias y herramientas para proteger la privacidad en línea, como contraseñas seguras y configuración de privacidad en redes sociales.
- Al finalizar la unidad, el estudiante será capaz de analizar situaciones cotidianas para reconocer riesgos de exposición de información personal y proponer acciones preventivas adecuadas.
- Al finalizar la unidad, el estudiante será capaz de aplicar medidas básicas para proteger sus datos personales en plataformas digitales durante actividades prácticas guiadas.
- Al finalizar la unidad, el estudiante será capaz de evaluar la importancia de la protección de datos personales y comunicar buenas prácticas de privacidad a sus pares mediante presentaciones o debates.

Contenidos Temáticos

1. Introducción a los Datos Personales

- Definición de datos personales: qué son y por qué son importantes.
- Tipos de datos personales: datos identificativos, sensibles, financieros, de ubicación, entre otros.
- Ejemplos comunes de datos personales en la vida digital cotidiana.

2. Riesgos y Consecuencias de la Exposición de Datos Personales

- Riesgos principales: robo de identidad, fraude, acoso y pérdida de privacidad.
- Situaciones cotidianas donde se pueden exponer datos personales sin darse cuenta.
- Impacto personal y social de no proteger adecuadamente los datos.

3. Estrategias y Herramientas para Proteger la Privacidad en Línea

- Contraseñas seguras: características, creación y gestión.
- Uso de autenticación de dos factores (2FA).
- Configuración de privacidad en redes sociales: cómo ajustar permisos y limitar el acceso a información personal.
- Reconocimiento de mensajes y sitios web sospechosos para evitar phishing y fraudes.

4. Medidas Prácticas para la Protección de Datos Personales

- Buenas prácticas al compartir información en línea.
- Configuración de privacidad en diferentes plataformas digitales comunes (redes sociales, correo electrónico, aplicaciones).
- Uso responsable de dispositivos y redes Wi-Fi públicas.
- Actualización y uso de software de seguridad básico (antivirus, firewalls).

5. Comunicación y Conciencia sobre la Protección de Datos Personales

- Importancia de la educación y el diálogo sobre privacidad entre pares.
- Elaboración de mensajes claros y efectivos para promover buenas prácticas de privacidad.
- Presentaciones y debates sobre casos reales y estrategias de protección.
- Reflexión sobre el valor de la información personal y la responsabilidad digital.

Actividades

Actividad 1: Identificación de Datos Personales

Objetivo: Identificar los diferentes tipos de datos personales que deben protegerse al usar internet.

Descripción:

- El docente presenta ejemplos de situaciones en línea (registro en redes sociales, compras en línea, uso de aplicaciones).
- Los estudiantes, en grupos, listan qué datos personales se solicitan o se pueden compartir en cada situación.
- Discusión guiada sobre qué datos son sensibles y por qué deben protegerse.

Organización: Grupos de 3-4 estudiantes.

Producto esperado: Lista organizada de tipos de datos personales con ejemplos.

Duración: 45 minutos.

Actividad 2: Creación de Contraseñas Seguras y Simulación de Configuración de Privacidad

Objetivo: Describir y aplicar estrategias para proteger la privacidad en línea, como contraseñas seguras y configuración de privacidad en redes sociales.

Descripción:

- El docente explica qué es una contraseña segura y muestra ejemplos.
- Los estudiantes crean varias contraseñas seguras siguiendo criterios dados.
- Simulan en una plantilla o en dispositivos (si es posible) la configuración de privacidad básica en una red social ficticia.

Organización: Individual o parejas.

Producto esperado: Contraseñas creadas y plantilla de configuración de privacidad completada.

Duración: 60 minutos.

Actividad 3: Análisis de Riesgos y Propuestas Preventivas

Objetivo: Analizar situaciones cotidianas para reconocer riesgos de exposición de información personal y proponer acciones preventivas adecuadas.

Descripción:

- Se presentan casos reales o hipotéticos donde se expone información personal (por ejemplo, aceptar solicitudes de desconocidos, compartir fotos con ubicación).

- Los estudiantes, en grupos, identifican los riesgos y discuten posibles soluciones o medidas preventivas.
- Cada grupo presenta sus conclusiones al resto de la clase para generar debate.

Organización: Grupos de 4 estudiantes.

Producto esperado: Lista de riesgos y propuestas de medidas preventivas documentadas y expuestas oralmente.

Duración: 60 minutos.

Actividad 4: Presentación y Debate sobre la Importancia de Proteger Datos Personales

Objetivo: Evaluar la importancia de la protección de datos personales y comunicar buenas prácticas de privacidad a sus pares.

Descripción:

- Los estudiantes preparan, individualmente o en parejas, una presentación breve (5 minutos) o un cartel sobre la importancia de proteger datos personales y consejos prácticos.
- Se organiza un debate o foro donde se exponen las presentaciones y se discuten ideas.
- El docente guía la reflexión final y resalta los puntos clave aprendidos.

Organización: Individual o parejas; presentación en grupo clase.

Producto esperado: Presentación oral o cartel informativo y participación en debate.

Duración: 90 minutos (preparación y exposición).

Evaluación

Evaluación Diagnóstica

Qué se evalúa: Conocimientos previos sobre qué son los datos personales y su importancia.

Cómo se evalúa: Cuestionario breve con preguntas abiertas y de selección múltiple sobre conceptos básicos de datos personales y riesgos en línea.

Instrumento sugerido: Cuestionario impreso o digital al inicio de la unidad.

Evaluación Formativa

Qué se evalúa: Progreso en la identificación de datos personales, uso de estrategias de protección y análisis de riesgos durante las actividades.

Cómo se evalúa: Observación directa del trabajo en actividades grupales e individuales, revisión de productos como listas, configuraciones y propuestas.

Instrumento sugerido: Rúbrica de evaluación con criterios de comprensión, aplicación y análisis; notas anecdóticas.

Evaluación Sumativa

Qué se evalúa: Capacidad para aplicar medidas básicas de protección, comunicar buenas prácticas y reflexionar sobre la importancia de la privacidad.

Cómo se evalúa: Presentación o debate final, con evaluación de contenido, claridad, argumentación y participación.

Instrumento sugerido: Rúbrica para presentaciones orales y participación en debate; prueba escrita de cierre con preguntas de reflexión.

Unidad 5: Contraseñas y Autenticación Segura

Unidad 6: Uso Seguro de Redes Sociales

Unidad 7: Reconocimiento y Manejo del Spam

Unidad 8: Introducción a los Algoritmos en Internet

Unidad 9: Control y Privacidad frente a Algoritmos

Unidad 10: Herramientas y Recursos para la Ciberseguridad

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar diferentes tipos de software y recursos de ciberseguridad disponibles para proteger la información personal en línea.
- Al finalizar la unidad, el estudiante será capaz de explicar el funcionamiento básico de herramientas como antivirus, firewalls y gestores de contraseñas, describiendo su importancia en la protección digital.
- Al finalizar la unidad, el estudiante será capaz de aplicar configuraciones básicas en programas de seguridad para resguardar datos personales en dispositivos digitales.
- Al finalizar la unidad, el estudiante será capaz de evaluar la efectividad de diferentes recursos de ciberseguridad mediante la comparación de sus características y funcionalidades.
- Al finalizar la unidad, el estudiante será capaz de comunicar recomendaciones para el uso seguro de herramientas digitales enfocadas en la protección de la información personal.

Unidad 11: Ética y Responsabilidad Digital

Unidad 12: Resolución de Problemas y Casos Prácticos

Unidad 13: Análisis de Casos de Estafas y Fraudes Digitales

Unidad 14: Seguridad en Dispositivos y Redes

Unidad 15: Navegación Segura y Protección Contra Malware

Unidad 16: Gestión de la Identidad Digital

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de describir qué es la identidad digital y explicar su importancia en la protección de la información personal en línea.
- Al finalizar la unidad, el estudiante será capaz de identificar y analizar los riesgos asociados con compartir información personal en diferentes plataformas digitales.
- Al finalizar la unidad, el estudiante será capaz de aplicar estrategias para construir una identidad digital segura y positiva mediante la configuración adecuada de privacidad en redes sociales y otras plataformas.
- Al finalizar la unidad, el estudiante será capaz de evaluar diferentes prácticas de seguridad para proteger sus contraseñas y datos personales en entornos digitales.
- Al finalizar la unidad, el estudiante será capaz de comunicar recomendaciones para mantener una identidad digital responsable y segura en su entorno escolar y social.

Unidad 17: Introducción a la Seguridad en Aplicaciones y Juegos

Unidad 18: Derechos y Responsabilidades en el Mundo Digital

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar los principales derechos digitales que protegen su privacidad y seguridad en línea mediante ejemplos prácticos.
- Al finalizar la unidad, el estudiante será capaz de explicar las responsabilidades que tiene al utilizar tecnologías digitales de forma ética y segura en diferentes contextos escolares y personales.
- Al finalizar la unidad, el estudiante será capaz de analizar situaciones comunes en el entorno digital para distinguir comportamientos responsables de aquellos que pueden comprometer la seguridad personal.
- Al finalizar la unidad, el estudiante será capaz de aplicar normas básicas de conducta digital responsable para prevenir riesgos y proteger su información personal en actividades en línea.
- Al finalizar la unidad, el estudiante será capaz de comunicar la importancia de respetar los derechos digitales propios y ajenos a través de presentaciones o debates en clase.

Unidad 19: Proyecto Final: Diseñando un Plan de Ciberseguridad Personal

Unidad 20: Evaluación y Reflexión Final

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de resumir los conceptos fundamentales de la ciberseguridad aprendidos durante el curso mediante un examen escrito.
- Al finalizar la unidad, el estudiante será capaz de identificar y explicar al menos tres tipos comunes de amenazas digitales y sus características a través de una presentación grupal.

- Al finalizar la unidad, el estudiante será capaz de evaluar prácticas personales y grupales de seguridad digital utilizando una lista de cotejo para reflexionar sobre su efectividad.
- Al finalizar la unidad, el estudiante será capaz de elaborar un plan personal de medidas básicas para proteger su información en línea, aplicando criterios de seguridad vistos en el curso.
- Al finalizar la unidad, el estudiante será capaz de comunicar la importancia de la ciberseguridad en la vida cotidiana mediante un ensayo reflexivo que incluya ejemplos concretos.