

CyberDefensores: La Misión Contra el Ciberdelito y la Violencia Digital

Gamificación Estructural | Ciencias Sociales y Humanas | Derecho | Tema: Ciberdelito y violencia digital en argentina

Contexto Narrativo

Contexto Narrativo

En el año 2024, Argentina enfrenta una creciente ola de ciberdelitos y violencia digital que afecta a ciudadanos, instituciones y organizaciones. Desde fraudes electrónicos y suplantación de identidad hasta ataques de odio en redes sociales y grooming, la sociedad enfrenta retos inéditos en el ámbito digital. En este escenario, un grupo de estudiantes técnicos y tecnólogos es convocado para formar parte de la unidad especial “CyberDefensores”. Su misión: convertirse en expertos en derecho digital para proteger a la comunidad y promover una cultura responsable y segura en el mundo online.

Los estudiantes asumen roles de agentes especializados, que combinan conocimientos técnicos y jurídicos para investigar casos reales y resolver conflictos relacionados con ciberdelito y violencia digital. A través de la experiencia, deberán analizar normativas vigentes, identificar riesgos y proponer soluciones innovadoras, siempre desde una perspectiva ética e inclusiva.

Ambientación

La experiencia se desarrolla en un aula transformada en un centro de operaciones digital. En cada sesión, los participantes reciben informes, evidencias y desafíos reales o simulados relacionados con delitos informáticos y violencia en entornos digitales. El aula contará con estaciones de trabajo con computadoras y acceso a recursos digitales oficiales, normativas actualizadas y materiales multimedia. En paralelo, los estudiantes crearán un “Mapa de Riesgos Digitales” que irá creciendo con cada misión cumplida.

Roles de los Estudiantes

- **Investigador Jurídico:** Especialista en normativas de derecho digital, encargado de analizar leyes y decretos nacionales y provinciales.
- **Analista Técnico:** Experto en herramientas digitales y ciberseguridad, responsable de identificar vulnerabilidades y evidencias técnicas.
- **Comunicación y Prevención:** Diseñador de campañas de concientización inclusivas, que promueve el respeto y la equidad en ambientes digitales.
- **Moderador Ético:** Asegura que las soluciones propuestas respeten los derechos humanos, la diversidad y la inclusión.

Misión Principal

La unidad CyberDefensores debe resolver una serie de casos relacionados con ciberdelito y violencia digital en Argentina, aplicando la legislación vigente, desarrollando estrategias de prevención y proponiendo acciones concretas para proteger a las víctimas y promover un entorno digital seguro y justo. Para ello, deberán avanzar en niveles de complejidad creciente, enfrentándose a retos que ponen a prueba su pensamiento crítico, creatividad, colaboración y autonomía.

Conexión con el Tema de Aprendizaje

Esta experiencia gamificada integra contenidos de derecho vinculados a ciberdelito y violencia digital, tales como el análisis de la Ley 27.078 de Delitos Informáticos, la Ley 26.485 de Protección Integral a las Mujeres, y normativas relacionadas con privacidad y protección de datos personales. Al mismo tiempo, se abordan las dimensiones sociales y éticas del problema, fomentando la reflexión crítica sobre el impacto de las conductas digitales en la convivencia y los derechos humanos. La narrativa facilita que los estudiantes comprendan el alcance de la legislación, su aplicación práctica y la importancia de una cultura digital responsable y respetuosa.

La experiencia se estructura en torno a misiones y casos concretos que simulan situaciones reales en Argentina, promoviendo un aprendizaje significativo y conectado con el contexto local y tecnológico de los estudiantes de educación técnica/tecnológica.

Mecánicas de Juego

Mecánicas de Juego

Sistema de Puntos

Los estudiantes ganan puntos por cada actividad completada con éxito, con criterios que valoran la precisión jurídica, la creatividad en soluciones, la colaboración efectiva y la inclusión en las propuestas. Los puntos se asignan individualmente y también en equipo, fomentando tanto el esfuerzo personal como el trabajo colaborativo.

- Investigación jurídica correcta: 10 puntos
- Identificación acertada de evidencias técnicas: 8 puntos
- Propuesta de campaña inclusiva: 12 puntos
- Participación activa y colaboración: hasta 5 puntos por sesión
- Resolución creativa y ética del caso: 15 puntos

Niveles

La experiencia se organiza en 4 niveles de complejidad creciente:

- **Nivel 1 - Detectives Digitales:** Casos básicos de ciberdelito (phishing, suplantación).
- **Nivel 2 - Analistas de Conflictos:** Casos de violencia digital y delitos más complejos (ciberacoso, grooming).
- **Nivel 3 - Estrategas de la Prevención:** Diseño de campañas y propuestas legales para la prevención.

- **Nivel 4 - Expertos CyberDefensores:** Resolución integral de casos complejos, elaboración de informes para autoridades.

Para avanzar de nivel, los estudiantes deben acumular un mínimo de puntos y demostrar dominio de los contenidos y habilidades.

Insignias

Las insignias son reconocimientos visibles que se otorgan al cumplir hitos específicos:

- *“Detective Legal”*: por completar con éxito el primer caso jurídico.
- *“Guardián de la Equidad”*: por propuestas inclusivas destacadas.
- *“Innovador Digital”*: por soluciones creativas e innovadoras.
- *“Líder Colaborativo”*: por destacado trabajo en equipo y coordinación.
- *“CyberDefensor Completo”*: al terminar todos los niveles y misiones.

Las insignias se muestran en un mural digital o físico visible en el aula.

Retos y Recompensas

Cada misión presenta un reto con un caso o problema específico. Al superarlo, el equipo recibe puntos y recompensas adicionales, como acceso a recursos exclusivos, pistas para futuros casos o tiempo extra para diseñar propuestas.

Progresión

Los estudiantes ven su progreso reflejado en una tabla de clasificación, que puede estar en un tablero visible en el aula o en una plataforma digital. Esto genera motivación sana y competitividad constructiva. Además, cada nivel desbloquea nuevas herramientas y materiales para las siguientes misiones.

Retroalimentación Inmediata

Después de cada actividad, los docentes y compañeros ofrecen retroalimentación estructurada, destacando fortalezas y áreas de mejora. También se utilizan cuestionarios interactivos y simulaciones que entregan resultados al instante para que los estudiantes ajusten estrategias.

Actividades Gamificadas

Actividades Gamificadas Paso a Paso

Actividad 1: “Caso Phishing en la Red”

Descripción: Los estudiantes investigan un caso simulado de phishing dirigido a usuarios argentinos. Deben identificar las características del delito, analizar la legislación aplicable y proponer medidas legales y técnicas.

Instrucciones:

- Formar equipos de 4 integrantes, cada uno asumiendo un rol (Investigador Jurídico, Analista Técnico, Comunicación y Prevención, Moderador Ético).

- Recibir el informe con el caso simulado que incluye capturas de pantalla, correos electrónicos y testimonios.
- Investigar la Ley 27.078 y otras normativas relacionadas al ciberdelito.
- Analizar las evidencias técnicas para identificar el modus operandi.
- Redactar un informe conjunto que contenga: descripción del delito, legislación aplicable, recomendaciones prácticas y una campaña breve para alertar a la comunidad.
- Presentar el informe al resto del grupo y recibir retroalimentación.

Tiempo estimado: 90 minutos

Materiales: Computadoras con acceso a internet, recursos digitales oficiales, plantillas de informe, proyector o pantalla para presentaciones.

Integración con mecánicas: Se otorgan puntos por investigación correcta, análisis técnico, calidad del informe y creatividad en la campaña. Se puede ganar la insignia “Detective Legal”.

Actividad 2: “Mapa de Riesgos y Violencia Digital”

Descripción: Los estudiantes identifican tipos de violencia digital presentes en Argentina, analizando casos reales y elaboran un “Mapa de Riesgos” que localiza zonas, plataformas y perfiles vulnerables.

Instrucciones:

- Revisar noticias, informes y datos oficiales sobre violencia digital en Argentina (ciberacoso, grooming, discriminación online).
- Dividirse en equipos para investigar diferentes regiones y plataformas digitales.
- Crear un mapa visual (digital o físico) donde se señalen los principales riesgos y casos emblemáticos.
- Proponer recomendaciones para prevención y protección desde el marco jurídico.
- Compartir el mapa con el grupo y discutir desafíos y estrategias.

Tiempo estimado: 120 minutos

Materiales: Mapas de Argentina impresos o digitales, acceso a internet, materiales para collage o programas de diseño simples (Canva, Google Slides).

Integración con mecánicas: Se asignan puntos por profundidad de investigación, creatividad en el mapa y propuestas inclusivas. Se puede obtener la insignia “Guardían de la Equidad”.

Actividad 3: “Simulación de Juicio Digital”

Descripción: Se simula un juicio donde un caso de violencia digital es juzgado. Los estudiantes deben defender sus posiciones según el rol asignado y aplicar conceptos jurídicos y éticos.

Instrucciones:

- Preparar roles: fiscal, defensor, juez, víctimas y testigos (pueden rotar o asignarse por equipo).
- Revisar el caso asignado, leyes y jurisprudencia relevante.
- Cada parte prepara sus argumentos, evidencias y contraargumentos.
- Realizar la simulación ante el grupo, con tiempos asignados para cada intervención.

- El juez dicta una sentencia fundamentada.
- Reflexionar en grupo sobre el proceso y las decisiones.

Tiempo estimado: 150 minutos

Materiales: Documentos del caso, legislación impresa o digital, cronómetro, espacio para la simulación.

Integración con mecánicas: Puntos por argumentación jurídica, ética y colaboración. Reconocimiento “Innovador Digital” para propuestas creativas y “Líder Colaborativo” para coordinación eficaz.

Actividad 4: “Campaña Inclusiva de Prevención”

Descripción: Los estudiantes diseñan una campaña digital para prevenir ciberdelitos y violencia digital, con enfoque en diversidad, equidad e inclusión.

Instrucciones:

- Investigar grupos vulnerables y cómo la violencia digital los afecta.
- Definir objetivos claros para la campaña.
- Crear contenido visual y textual que promueva respeto, inclusión y prevención.
- Utilizar herramientas digitales accesibles para diseñar posters, videos cortos o infografías.
- Presentar la campaña, explicando el enfoque y la estrategia de difusión.

Tiempo estimado: 120 minutos

Materiales: Computadoras, programas gratuitos de diseño (Canva, Piktochart), acceso a internet.

Integración con mecánicas: Puntos por creatividad, inclusión y aplicabilidad. Insignia “Guardían de la Equidad” y “Innovador Digital”.

Actividad 5: “Informe Final y Propuesta Integral”

Descripción: En equipos, los estudiantes elaboran un informe final que integra aprendizajes previos y propone una solución integral para un caso complejo de ciberdelito y violencia digital. Este informe simula una presentación ante autoridades o comunidad.

Instrucciones:

- Recopilar y sintetizar información de actividades anteriores.
- Redactar un documento que incluya descripción del problema, análisis jurídico, propuestas técnicas y de prevención, y un plan de acción inclusivo.
- Preparar una presentación clara y convincente.
- Exponer ante el grupo y recibir retroalimentación.

Tiempo estimado: 180 minutos en dos sesiones

Materiales: Computadoras, plantillas para informes, programa de presentación (PowerPoint, Google Slides).

Integración con mecánicas: Puntos elevados por excelencia, integración y liderazgo. Insignia “CyberDefensor Completo”.

Estas actividades permiten desarrollar competencias del siglo XXI como creatividad, pensamiento crítico, colaboración, autonomía, adaptabilidad y curiosidad, mediante un diseño gamificado que motiva y guía el aprendizaje.

Reglas y Condiciones

Reglas del Juego CyberDefensores

Condiciones de Victoria

- Completar los 4 niveles acumulando al menos 250 puntos.
- Obtener las insignias principales: “Detective Legal”, “Guardían de la Equidad”, “Innovador Digital” y “CyberDefensor Completo”.
- Demostrar comprensión práctica y ética de los contenidos.
- Realizar una presentación final convincente y coherente.

Penalizaciones

- Faltas reiteradas de respeto o inclusión: pérdida de 5 puntos.
- No cumplir con el rol asignado: reducción de puntos individuales.
- Entrega tardía o incompleta de informes: descuento del 10% de puntos en la actividad.

Turnos y Roles

- Las actividades grupales se distribuyen en turnos para asegurar participación equitativa.
- Cada estudiante debe cumplir su rol, pero se fomentan rotaciones para desarrollar todas las habilidades.
- Se promueve la escucha activa y el respeto en todas las intervenciones.

Restricciones

- Uso responsable de dispositivos digitales, sin distracciones ajenas a la actividad.
- Prohibición de contenidos ofensivos, discriminatorios o violentos en las propuestas.
- Se respeta la privacidad y se evita compartir datos personales reales.

Tabla de Puntos (Ejemplo)

Actividad	Investigación Jurídica	Análisis Técnico	Creatividad/Propuesta	Colaboración	Total Máximo
Caso Phishing	10	8	12	5	35
Mapa de Riesgos	12	7	15	5	39
Juicio Digital	15	10	15	5	45

Actividad	Investigación Jurídica	Análisis Técnico	Creatividad/Propuesta	Colaboración	Total Máximo
Campaña Inclusiva	8	5	20	5	38
Informe Final	20	15	25	10	70

Sistema de Logros

- Al alcanzar ciertos puntos o cumplir objetivos, se entregan insignias y medallas digitales o físicas.
- Los logros se registran en un mural para motivar y reconocer el esfuerzo.
- Se fomenta el feedback positivo y el apoyo mutuo.

Evaluación Gamificada

Evaluación Gamificada del Aprendizaje

Criterios de Evaluación

- **Dominio conceptual:** comprensión de leyes y normativas sobre ciberdelito y violencia digital.
- **Aplicación práctica:** capacidad para analizar casos y proponer soluciones reales.
- **Creatividad e innovación:** originalidad en campañas y estrategias preventivas.
- **Colaboración y comunicación:** trabajo en equipo, respeto y participación activa.
- **Inclusión y ética:** integración de criterios DEI en propuestas y reflexiones.
- **Autonomía y adaptabilidad:** capacidad para autogestionar tareas y responder a cambios o desafíos.

Rúbricas Integradas

Se utiliza una rúbrica por actividad con indicadores para cada criterio, evaluada por docente y auto/coevaluación entre pares.

Criterio	Excelente (4)	Bueno (3)	Aceptable (2)	Insuficiente (1)
Dominio Conceptual	Explica con precisión y profundidad los conceptos y leyes.	Explica correctamente pero con detalles limitados.	Entiende parcialmente, con errores menores.	Confusión evidente y errores graves.
Aplicación Práctica	Resuelve casos complejos con argumentos sólidos y claros.	Resuelve casos básicos con argumentos adecuados.	Resuelve casos simples con dificultad.	No logra resolver casos o argumentos incorrectos.

Criterio	Excelente (4)	Bueno (3)	Aceptable (2)	Insuficiente (1)
Creatividad e Innovación	Propuestas originales y efectivas.	Propuestas adecuadas, poco originales.	Propuestas poco claras o poco innovadoras.	Sin propuestas creativas.
Colaboración y Comunicación	Participa activamente y fomenta el trabajo en equipo.	Participa pero con aportes limitados.	Participa esporádicamente.	No participa o dificulta el trabajo.
Inclusión y Ética	Integra plenamente criterios DEI y valores éticos.	Considera algunos aspectos DEI.	Considera superficialmente.	No considera o contradice valores DEI.
Autonomía y Adaptabilidad	Gestiona tareas con iniciativa y se adapta fácilmente.	Gestiona tareas con supervisión mínima.	Necesita supervisión frecuente.	No muestra autonomía ni adaptación.

Evidencias de Aprendizaje

- Informes escritos y presentaciones orales.
- Mapas de riesgo y campañas digitales.
- Participación en simulaciones y debates.
- Reflexiones individuales y grupales al final de cada nivel.

Reflexión Final y Cierre de la Narrativa

Al concluir la experiencia, cada estudiante escribe una reflexión personal sobre lo aprendido, los desafíos enfrentados y cómo aplicará ese conocimiento en su vida profesional y personal. En sesión plenaria, se realiza un cierre narrativo donde la unidad CyberDefensores presenta su informe final a una audiencia simulada (puede incluir otros docentes o familias), reforzando el sentido de misión cumplida y el compromiso social.

Recomendaciones Logísticas

Recomendaciones para la Implementación

Tiempo Necesario

- La experiencia completa puede desarrollarse en 8 a 10 sesiones de 90 a 120 minutos cada una.
- Se recomienda distribuir las actividades para no saturar y permitir reflexión y trabajo en equipo.

Espacio Físico

- Aula con disposición flexible para trabajo colaborativo en equipo.
- Estaciones o rincones para roles específicos (jurídico, técnico, comunicación).

- Zona para exposiciones o simulaciones (juicio digital).

Materiales y Herramientas TIC

- Computadoras con acceso estable a internet.
- Proyector o pantalla grande para presentaciones y visualización de contenidos.
- Software gratuito para diseño gráfico y presentaciones (Canva, Google Slides, Piktochart).
- Recursos digitales oficiales y bases de datos legislativas accesibles en línea.
- Materiales impresos para mapas o plantillas si se trabaja parcialmente offline.

Tamaño del Grupo

- Ideal entre 16 y 24 estudiantes para facilitar la formación de equipos de 4 integrantes.
- Posibilidad de adaptar la experiencia para grupos más pequeños o grandes ajustando roles y tiempos.

Preparación Previa del Docente

- Estudio de la legislación vigente y actualización en temas de ciberdelito y violencia digital.
- Familiarización con herramientas digitales propuestas y plataformas para gamificación.
- Preparación de materiales, casos y recursos para cada actividad.
- Planificación de la distribución de roles y diseño del espacio.
- Preparación para la evaluación y retroalimentación estructurada.

Posibles Dificultades y Soluciones

- **Desigualdad en acceso a TIC:** proporcionar materiales impresos, facilitar acceso en aula o bibliotecas.
- **Resistencia a roles o trabajo en equipo:** realizar actividades iniciales de integración y sensibilización.
- **Complejidad jurídica:** simplificar lenguaje, utilizar ejemplos claros y apoyo docente constante.
- **Distracciones digitales:** establecer normas claras de uso y supervisión activa.
- **Dificultades para inclusión:** monitorear participación, adaptar roles y contenidos para diversidad funcional y cultural.

Con estas recomendaciones, la experiencia CyberDefensores se convierte en una herramienta poderosa, motivadora y efectiva para abordar temas críticos de la sociedad digital argentina desde el aula técnica y tecnológica, desarrollando competencias transversales y valores fundamentales.