

# CiberGuardianes: La Aventura Digital para Proteger la Red

*Gamificación Completa | Tecnología e Informática | Pensamiento Computacional | Tema: Ciberseguridad*

## Contexto Narrativo

### Contexto Narrativo: Bienvenidos a CiberGuardianes

En un futuro cercano, el mundo está conectado de forma más intensa que nunca. La red digital se ha convertido en la columna vertebral de la comunicación, el aprendizaje y el entretenimiento. Sin embargo, esta conectividad trae consigo grandes riesgos: virus informáticos, robo de datos, suplantación de identidad y amenazas invisibles acechan a cada usuario.

Los estudiantes entran al aula no solo como aprendices, sino como *CiberGuardianes*, un grupo élite de protectores digitales encargados de defender la red contra estas amenazas. Su misión principal es aprender y aplicar conductas seguras para proteger su identidad digital, mantener la privacidad de sus datos y respetar los derechos de autor en el intercambio de información.

La ambientación es una ciudad futurista llamada **Netópolis**, un lugar virtual donde la información fluye como energía vital. En esta ciudad, las calles son redes, los edificios son servidores y los ciudadanos son usuarios digitales. Los CiberGuardianes deben explorar diferentes zonas de Netópolis para cumplir misiones específicas que los ayudarán a convertirlos en expertos en ciberseguridad.

Los estudiantes adoptan roles dentro del equipo, tales como:

- **Analista de Seguridad:** Especialista en detectar amenazas y vulnerabilidades.
- **Criptógrafo:** Encargado de proteger la información mediante técnicas de cifrado básico.
- **Comunicador Seguro:** Responsable de transmitir información segura y clara.
- **Defensor de la Privacidad:** Experto en proteger datos personales y entender derechos digitales.

La misión principal de los CiberGuardianes es completar una serie de retos y desafíos para asegurar que Netópolis permanezca segura. Cada misión está directamente conectada con los objetivos de aprendizaje del docente: adoptar conductas seguras, manejar información de forma responsable, comprender derechos digitales y aplicar medidas de seguridad activa y pasiva.

Esta narrativa envuelve a los estudiantes en una experiencia de aprendizaje significativa, donde cada paso que dan en el juego representa un avance real en sus competencias digitales y cívicas.

### Conexión con el Aprendizaje

Los desafíos que enfrentan en la narrativa se basan en problemas reales de ciberseguridad, presentados en formatos lúdicos y colaborativos. Por ejemplo, para proteger un servidor de Netópolis, deben identificar ataques de phishing; para proteger la privacidad de un usuario, deben configurar correctamente sus ajustes de seguridad; para compartir

información, deben respetar las licencias de uso y derechos de autor.

La narrativa facilita que los estudiantes internalicen la importancia de la ciberseguridad, al tiempo que desarrollan competencias del siglo XXI como pensamiento crítico, creatividad, colaboración y comunicación.

Además, la historia incorpora elementos de diversidad, equidad e inclusión: los personajes y escenarios representan múltiples culturas, géneros y capacidades, asegurando que todos los estudiantes se sientan representados y valorados dentro de esta aventura digital.

En resumen, **CiberGuardianes: La Aventura Digital para Proteger la Red** es mucho más que un juego; es una experiencia educativa transformadora que da sentido y propósito al aprendizaje del pensamiento computacional aplicado a la ciberseguridad.

## Mecánicas de Juego

### Mecánicas de Juego Integradas

Para hacer de *CiberGuardianes* una experiencia motivadora y efectiva, se implementan las siguientes mecánicas de juego:

- **Sistema de Puntos (CiberPuntos):** Cada actividad y reto completado otorga CiberPuntos, que representan el progreso individual y grupal. Se usan para desbloquear niveles y recompensas.
- **Niveles de CiberGuardianes:** Hay 5 niveles de dominio: Novato, Explorador, Protector, Defensor, Maestro CiberGuardián. Los estudiantes suben de nivel acumulando puntos y completando misiones clave.
- **Insignias Temáticas:** Se entregan insignias digitales por logros específicos, por ejemplo: *Detective de Phishing*, *Maestro de Privacidad*, *Comunicador Seguro*. Las insignias se muestran en el perfil virtual del estudiante y fomentan el orgullo y la competencia sana.
- **Retos y Misiones:** Las actividades están diseñadas como misiones con objetivos claros y desafíos que requieren aplicar lo aprendido. Algunos retos tienen tiempo límite para generar dinamismo.
- **Recompensas y Privilegios:** Además de puntos e insignias, los equipos pueden obtener privilegios dentro del aula, como elegir la siguiente actividad, obtener pistas extra, o ser líderes de equipo.
- **Progresión y Retroalimentación Inmediata:** Se utiliza un tablero visible en el aula (físico o digital) donde se actualizan los puntos, niveles y premios constantemente. El docente da retroalimentación en tiempo real para reforzar aprendizajes y corregir errores.
- **Trabajo en Equipo y Roles:** Los estudiantes trabajan en equipos con roles asignados que rotan para fomentar la colaboración y desarrollar diferentes habilidades.
- **Desafíos de Adaptabilidad:** El juego incluye eventos sorpresa que requieren que los equipos adapten su estrategia, promoviendo flexibilidad y pensamiento crítico.
- **Elementos Narrativos:** Se usan relatos, vídeos y personajes virtuales que guían las misiones y mantienen el interés.

### Implementación Detallada

**Sistema de Puntos:** Cada tarea tiene asignado un valor de CiberPuntos entre 5 y 20, dependiendo de la dificultad. Por ejemplo, identificar un correo phishing correcto vale 10 puntos, mientras que diseñar una infografía sobre privacidad vale 20.

**Niveles:** - Novato: 0-50 puntos

- Explorador: 51-100 puntos

- Protector: 101-150 puntos

- Defensor: 151-200 puntos

- Maestro: 201+ puntos

**Insignias:** Se crean en formato digital con herramientas como Canva, y se entregan en formato PDF o imagen para que los estudiantes las guarden o impriman.

**Retos:** Se diseñan con instrucciones claras, recursos accesibles y criterios de éxito bien definidos para facilitar la evaluación.

**Recompensas:** Pueden incluir tiempo extra para actividades creativas, oportunidades para enseñar a otros, o pequeños reconocimientos físicos como stickers o certificados.

**Tablero de Progreso:** Puede ser una pizarra física con tarjetas o una hoja de cálculo compartida proyectada en clase.

**Roles:** Se asignan al inicio de cada misión y rotan para asegurar que cada estudiante desarrolle todas las competencias.

**Eventos Sorpresa:** Por ejemplo, un mensaje de alerta en Netópolis que obliga a los equipos a replantear su estrategia de protección.

Estas mecánicas están diseñadas para mantener el interés, fomentar la colaboración y asegurar que el aprendizaje sea activo, reflexivo y contextualizado.

## Actividades Gamificadas

### Actividades Gamificadas Paso a Paso

#### 1. Misión Inicial: Detectives de Phishing

**Descripción:** Los estudiantes aprenden a identificar correos electrónicos sospechosos para evitar fraudes.

**Instrucciones:**

- Se divide a la clase en equipos de 4 personas, cada uno con roles asignados.
- Se entrega a cada equipo una carpeta con 10 correos electrónicos impresos o digitales (mezcla de reales y phishing).
- El equipo debe analizar cada correo, discutir y decidir si es seguro o phishing.
- Por cada correo correctamente identificado, obtienen 10 CiberPuntos.
- Se asigna un tiempo límite de 40 minutos.

**Materiales:** Ejemplos de correos, hojas de trabajo, dispositivos para acceso digital opcional.

**Integración con mecánicas:** Puntos asignados, roles activos, trabajo colaborativo. El docente da retroalimentación inmediata sobre cada correo.

## **2. Misión Criptógrafo: Cifrado Básico**

**Descripción:** Los estudiantes crean y descifran mensajes usando cifrados simples (César, sustitución).

### **Instrucciones:**

- Los equipos reciben un mensaje secreto que deben descifrar usando la clave proporcionada.
- Luego, deben crear su propio mensaje cifrado para que otro equipo lo descifre.
- Cada mensaje descifrado correctamente vale 15 puntos; crear uno comprensible vale 10 puntos.
- Tiempo estimado: 50 minutos.

**Materiales:** Plantillas de cifrados, hojas de papel, computadoras o tablets.

**Integración con mecánicas:** Retos por equipo, roles de criptógrafo activos, recompensa por creatividad y precisión.

## **3. Misión Comunicador Seguro: Diseño de Campaña Informativa**

**Descripción:** Los estudiantes diseñan una mini campaña para informar sobre buenas prácticas de seguridad digital.

### **Instrucciones:**

- En equipos, eligen uno de los temas discutidos (protección de datos, privacidad, uso responsable).
- Crean un cartel digital o físico, un vídeo corto o una presentación para compartir con la comunidad escolar.
- Presentan su campaña y responden preguntas del resto de la clase.
- Se otorgan hasta 20 puntos por creatividad, claridad y pertinencia.
- Tiempo estimado: 2 sesiones de 45 minutos.

**Materiales:** Computadoras con acceso a Canva o PowerPoint, materiales para cartelera, cámaras para vídeo (opcional).

**Integración con mecánicas:** Roles de comunicador, colaboración, recompensas por presentación, uso de insignias.

## **4. Misión Defensor de la Privacidad: Configuración de Perfiles y Derechos Digitales**

**Descripción:** Los estudiantes revisan configuraciones de privacidad en redes sociales simuladas y analizan derechos de autor.

### **Instrucciones:**

- Se presenta un simulador o ejemplos de perfiles con configuraciones variadas.
- Los equipos deben identificar riesgos y proponer configuraciones seguras.
- Discuten casos de uso responsable y respeto a derechos digitales.
- Se asignan 15 puntos por cada configuración correcta y explicación clara.

- Tiempo estimado: 60 minutos.

**Materiales:** Computadoras, simuladores online (ej. PrivacyCheck), hojas guía.

**Integración con mecánicas:** Retos, trabajo en equipo, retroalimentación inmediata.

## 5. Evento Sorpresa: Ciberataque en Netópolis

**Descripción:** Aparece un ataque digital en la ciudad virtual que pone a prueba todo lo aprendido.

### Instrucciones:

- El docente presenta un escenario con múltiples amenazas simultáneas (phishing, robo de datos, fake news).
- Los equipos deben priorizar acciones, distribuir roles y aplicar estrategias para defender Netópolis.
- Cada decisión acertada otorga puntos extra y avanza el nivel del equipo.
- Tiempo estimado: 45 minutos.

**Materiales:** Guion preparado con escenarios, recursos visuales.

**Integración con mecánicas:** Adaptabilidad, pensamiento crítico, roles rotativos, recompensas por estrategia.

## 6. Misión Final: Presentación del Proyecto CiberGuardían

**Descripción:** Cada equipo elabora un proyecto final que integre los aprendizajes sobre ciberseguridad en un formato creativo.

### Instrucciones:

- Los equipos eligen un formato: video, podcast, cómic digital, presentación multimedia.
- El proyecto debe incluir recomendaciones para protegerse en la red, derechos digitales y hábitos seguros.
- Presentan su proyecto al grupo y reciben retroalimentación.
- Se asignan hasta 30 puntos por calidad, creatividad y aplicación práctica.
- Tiempo estimado: 3 sesiones de 45 minutos.

**Materiales:** Software de edición básica, recursos gráficos, guías para guionización.

**Integración con mecánicas:** Uso de insignias, subida de nivel a Maestro CiberGuardían, evaluación colaborativa.

## Consideraciones para DEI

- Actividades diseñadas para que todos los estudiantes participen según sus fortalezas y necesidades.
- Materiales visuales y auditivos para diversidad de estilos de aprendizaje.
- Opciones para adaptar tiempos y roles según capacidades.
- Temas y personajes inclusivos y representativos culturalmente.

## Reglas y Condiciones

### Reglas Claras del Juego CiberGuardianes

- **Condiciones de Victoria:** Un equipo gana al alcanzar el nivel de Maestro CiberGuardián (201 puntos o más) y completar satisfactoriamente la Misión Final.
- **Turnos:** Cada reto permite que los equipos trabajen simultáneamente; para actividades con roles rotativos, cada estudiante asume su rol en cada misión.
- **Penalizaciones:** Se restan 5 puntos por respuestas incorrectas cuando se detecte falta de análisis o no se respeten las reglas de trabajo en equipo (por ejemplo, no respetar turnos para hablar).
- **Roles:** Los roles se asignan al inicio de cada misión y deben rotar para que todos experimenten diversas competencias.
- **Restricciones:** El uso de dispositivos debe ser responsable y limitado a actividades indicadas; copiar respuestas sin análisis será penalizado con pérdida de puntos y advertencia.
- **Tabla de Puntos:**

| Actividad                   | Puntos por Correcto | Penalización                  |
|-----------------------------|---------------------|-------------------------------|
| Identificación de Phishing  | 10                  | -5 por error                  |
| Cifrado y Descifrado        | 15 / 10             | -5 por mensaje incomprensible |
| Campaña Informativa         | 20                  | -5 por falta de claridad      |
| Configuración de Privacidad | 15                  | -5 por configuración insegura |
| Evento Sorpresa             | Variable (10-20)    | -10 por mala estrategia       |
| Proyecto Final              | 30                  | -10 por falta de integración  |

- **Sistema de Logros:** Para obtener insignias, los equipos deben cumplir criterios específicos, por ejemplo: acertar 9 de 10 correos en la misión phishing para la insignia *Detective de Phishing*.
- **Comportamiento:** Se promueven valores de respeto, colaboración y responsabilidad; faltas graves pueden implicar suspensión temporal del rol.

## Evaluación Gamificada

### Evaluación Gamificada Integrada

La evaluación se realiza de forma continua y formativa, integrando evidencias dentro del sistema de juego para motivar y orientar el aprendizaje.

#### Criterios de Evaluación

- **Comprensión de conductas seguras (Objetivo 6.1):** Capacidad para identificar riesgos y adoptar hábitos de protección en la red.

- **Uso responsable de servicios digitales (Objetivo 6.2):** Aplicación de criterios básicos de seguridad al acceder y compartir información.
- **Reconocimiento de derechos digitales (Objetivo 6.3):** Entendimiento y respeto a derechos de autor y propiedad intelectual.
- **Aplicación de seguridad activa y pasiva (Objetivo 6.4):** Uso de métodos para proteger datos personales y comunicación.
- **Competencias siglo XXI:** Evidencias de pensamiento crítico, creatividad, colaboración, comunicación, adaptabilidad y responsabilidad en las tareas.
- **Inclusión y respeto:** Participación equitativa y respeto a la diversidad dentro de los equipos.

#### Rúbrica Integrada

| Criterio                                                    | Excelente (4)                                                          | Bueno (3)                                                     | Regular (2)                                           | Insuficiente (1)                                |
|-------------------------------------------------------------|------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------------|-------------------------------------------------|
| Identificación de riesgos y conductas seguras               | Identifica y explica todos los riesgos con evidencia clara.            | Identifica la mayoría de riesgos con explicación adecuada.    | Reconoce algunos riesgos con explicaciones básicas.   | No identifica ni explica riesgos correctamente. |
| Aplicación de criterios de seguridad en servicios digitales | Aplica criterios rigurosamente en todas las actividades.               | Aplica criterios en la mayoría de actividades.                | Aplica criterios de forma limitada.                   | No aplica criterios o lo hace incorrectamente.  |
| Reconocimiento de derechos digitales                        | Demuestra comprensión profunda y respeta derechos en todas las tareas. | Muestra comprensión general y respeta la mayoría de derechos. | Demuestra comprensión parcial con errores en respeto. | No demuestra comprensión ni respeta derechos.   |
| Participación y colaboración                                | Participa activamente y fomenta un ambiente inclusivo.                 | Participa y colabora adecuadamente.                           | Participa de forma pasiva o limitada.                 | No participa o genera conflictos.               |

#### Evidencias de Aprendizaje

- Resultados en retos y misiones (puntos y desempeño).
- Proyectos finales y campañas informativas presentadas.
- Participación en debates y análisis de casos.
- Reflexiones individuales y grupales al final de cada misión.

#### Reflexión Final y Cierre de la Narrativa

Al concluir la experiencia, los estudiantes participan en una sesión de reflexión donde comparten:

- Qué aprendieron sobre la protección en la red y su importancia.
- Cómo aplicarán estos conocimientos en su vida diaria.
- Qué rol disfrutaron más y por qué.
- Cómo la experiencia los preparó para ser ciudadanos digitales responsables.

El docente cierra la narrativa destacando el papel de los CiberGuardianes en la construcción de un entorno digital seguro y respetuoso, motivando a que continúen siendo protectores activos fuera del aula.

## Recomendaciones Logísticas

### Recomendaciones para la Implementación

- **Tiempo necesario:** La experiencia completa puede planificarse en 3 a 4 semanas, con sesiones de 45 a 60 minutos, incluyendo actividades, eventos sorpresa y proyectos finales.
- **Espacio físico:** Aula con disposición flexible para trabajo en equipo; espacio para tablero de progreso visible; zona para presentaciones y debates.
- **Materiales y herramientas TIC:**
  - Computadoras o tablets con acceso a internet para simuladores, creación de campañas y proyectos.
  - Software gratuito: Canva, PowerPoint, herramientas básicas de edición de video o audio.
  - Impresiones de correos y materiales para actividades offline.
  - Pizarra o proyector para mostrar tablero de puntos y materiales visuales.
- **Tamaño del grupo:** Ideal entre 16 y 30 estudiantes para facilitar el trabajo en equipos y rotación de roles.
- **Preparación previa del docente:**
  - Familiarizarse con conceptos básicos de ciberseguridad y pensamiento computacional.
  - Preparar materiales y ejemplos adaptados al contexto local y cultural.
  - Crear o adaptar las insignias digitales y tablero de puntos.
  - Planificar la asignación de roles y dinámica de rotación.
  - Probar simuladores y herramientas TIC para asegurar su funcionamiento.
- **Posibles dificultades y soluciones:**
  - *Desigualdad en acceso a dispositivos:* Alternar actividades digitales con impresas y trabajo colaborativo para compensar.
  - *Falta de motivación:* Usar la narrativa y recompensas para mantener el interés; adaptar retos al nivel del grupo.
  - *Dificultades técnicas:* Tener plan B con materiales offline y apoyo técnico disponible.
  - *Problemas de convivencia o colaboración:* Establecer normas claras desde el inicio y mediar conflictos rápidamente.

Siguiendo estas recomendaciones, el docente podrá implementar *CiberGuardianes* de forma fluida, creando un ambiente de aprendizaje dinámico, inclusivo y significativo para los estudiantes de secundaria.