ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE

Periodo Académico: 2025-B **Fecha de Entrega:** 17/11/2025

Asignatura: Desarrollo de Juegos Interactivos **Grupo:** GR1SW

Integrantes: Guerra Sebastián, Morales Anthony

Taller Clase 006

1. Ficha de Diseño Dual

Concepto Núcleo del Juego:

Un simulador de ciberseguridad donde el jugador gestiona las defensas de una red corporativa para detectar y neutralizar amenazas digitales en tiempo real.

Tabla Comparativa de Diseño

Característica de Diseño	Versión 1: Juego de Entretenimiento	Versión 2: Juego Serio
Título (Sugerido)	Cyber Defense: Neon Walls	SecureNet Simulator: Entrenamiento de Protocolos ISO 27001
Estética MDA (Propósito)	• **Fantasía:** Ser un "Hacker de Élite" (estilo película). • **Sensation:** Visuales neón, explosiones digitales. • **Desafío:** Reflejos rápidos para detener ataques.	• **Educación:** Entrenar a nuevos SysAdmins en detección real de amenazas. • **Realismo:** Simular entornos de estrés controlado. • **Cumplimiento:** Certificar conocimiento de normas.

Bucle de Juego (Core Loop)	1. Recibir Alerta Visual. 2. Jugar Minijuego de "Disparo/Puzzle" (arcade) para destruir el virus. 3. Recibir "Cripto-Monedas". 4. Mejorar Firewall (Estadísticas).	1. Analizar Logs del Sistema (Lectura). 2. Identificar Anomalía según Matriz de Riesgo. 3. Seleccionar Protocolo de Respuesta (ej. Aislar Puerto). 4. Verificar Integridad del Sistema.
Modelo de Negocio / Financiación	• **Free-to-Play (F2P):** Descarga gratuita para masificar usuarios en móviles.	• **Licencia B2B:** Venta de licencias anuales a departamentos de RRHH o TI de grandes empresas.
Mecánicas de Monetización	• **Micro transacciones:** Venta de "Skins" para el avatar o la interfaz. • **Pases de Batalla:** Recompensas exclusivas por jugar mucho. • **Anuncios:** Ver video para revivir.	• **Reducción de Riesgo:** El "ingreso" para el cliente es evitar una multa por brecha de datos. • **Ahorro en Capacitación:** Más barato que un taller presencial con instructor.
Mecánicas de Ludificación (Gamificación)	• **Rachas Diarias:** "Conéctate 7 días seguidos para un bono". • **Leaderboards Globales:** "¿Quién tiene el puntaje más alto del mundo?". • **Energía:** Limita el juego para generar deseo.	• **Insignias de Competencia:** "Experto en Phishing" (Certificación visual). • **Barra de Progreso:** % del curso completado. • **Feedback Inmediato:** Explicación de *por qué* falló la defensa (Corrección de error).
Métrica de Éxito (KPI)	• **Retención D30:** % de usuarios que	• **Transferencia de Aprendizaje:**

	siguen jugando al mes. • **ARPU:** Ingreso promedio por usuario.	Reducción de incidentes de seguridad reales en la empresa post-juego. • **Tasa de Aprobación:** % de usuarios que pasan el examen final.

2. Análisis Comparativo (Preguntas)

2.1 Impacto del Modelo F2P (Versión Entretenimiento)

La elección del modelo Free-to-Play nos obligó a introducir fricción artificial en el bucle de juego. Para monetizar, no basta con que el juego sea divertido; el jugador debe necesitar algo.

- **Cambio de Diseño:** Tuvimos que implementar un sistema de "Energía" (CPU Cycles). Cada vez que el jugador defiende un ataque, gasta energía. Cuando se acaba, debe esperar (tiempo de espera) o pagar para seguir jugando.

- **Consecuencia:** Esto rompe la inmersión a cambio de rentabilidad. Además, añadimos mecánicas de "Pay-to-Win" (potenciadores de defensa) que permiten superar niveles difíciles pagando, algo que altera el equilibrio de habilidad pura.

2.2 Impacto del Propósito Serio (Versión Seria)

El objetivo pedagógico de enseñar protocolos reales (como NIST) restringió severamente la "espectacularidad" del juego.

- Mecánicas Eliminadas: Tuvimos que eliminar el minijuego de "disparar a los virus" (tipo arcade) porque eso enseña una falsedad: la ciberseguridad no es disparar, es analizar.

- Nuevo Diseño: Fue reemplazado por la lectura de Logs y Dashboards. Esto es "aburrido" comparado con la versión comercial, pero es necesario para la fidelidad del aprendizaje. La tensión ya no viene de la velocidad de los dedos, sino de la presión de tomar la decisión correcta bajo un límite de tiempo realista, simulando el estrés de un *Centro de Operaciones de Seguridad (SOC)*.

2.3 El Doble Rol de la Ludificación

Aunque usamos elementos similares (Puntos y Rankings), su función psicológica es opuesta:

- **En la Versión Comercial (Entretenimiento):** Los *Leaderboards* y *Rachas* apelan al ego y al miedo a perderse algo (FOMO). Su fin es la Adicción y el Estatus Social. Queremos que el jugador vuelva mañana para no perder su racha.

- **En la Versión Seria (Educativa):** Las *Insignias* y *Barras de Progreso* actúan como marcadores de competencia y autoevaluación. Su fin es la Motivación Intrínseca y el

Sentido de Logro. Cuando el jugador recibe la insignia de "Experto en Phishing", no es para presumir ante extraños, sino para validar que ha adquirido una habilidad profesional útil para su carrera.