ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA DE SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

Materia

Desarrollo de Juegos Interactivos

Elemento de Evaluación

Taller 06

Integrantes

Josue Peralta
Ariel Sánchez

Taller: El Diseño de Doble Propósito

Tema: El "Por Qué" y el "Para Qué" - Modelos de Negocio y Aplicaciones

Objetivo del Taller

- **Primario**: Diseñar un concepto de juego único y adaptarlo a dos contextos: (1) Entretenimiento (comercial) y (2) Serio (aplicado).
- **Secundario**: Analizar cómo la elección del Modelo de Negocio (ej. F2P) impacta directamente en las Mecánicas de Monetización (ej. Pases de Batalla) y en el diseño del bucle de juego.
- **Terciario**: Diferenciar cómo las Mecánicas de Ludificación se usan para (1) impulsar la retención/monetización versus (2) reforzar los objetivos de aprendizaje/impacto.

Ficha de Diseño Dual

Concepto Núcleo del Juego: Un simulador de gestión de red informática donde el jugador asume el rol de un operador de ciberseguridad que debe monitorear tráfico, detectar intrusiones y proteger datos sensibles contra ataques externos.

Tabla Comparativa de Diseño

Característica de Diseño	Versión 1: Juego de Entretenimiento	Versión 2: Juego Serio
Título (Sugerido)	Cyber Defender: Neon Wars	InfoSec Guardian: Protocolo Corporativo

Estética MDA (Propósito)	Fantasía y Competencia. El objetivo es sentirse un "hacker de élite" en un mundo cyberpunk estilizado. La diversión proviene de la adrenalina visual y el dominio sobre oponentes.	Educación y Entrenamiento. El objetivo es simplificar conceptos complejos de seguridad (phishing, malware) y formar habilidades prácticas de detección para empleados reales.
Bucle de Juego (Core Loop)	1. Recibir oleada de ataques (virus visuales). 2. Desplegar defensas (torretas/firewalls). 3. Ganar "Crypto-Monedas" al destruir virus. 4. Mejorar defensas para la siguiente oleada.	1. Recibir correo o alerta de sistema. 2. Analizar indicadores (remitente, URL, adjunto). 3. Decidir (Reportar / Abrir / Borrar). 4. Feedback inmediato (Infección simulada o Felicitación).
Modelo de Negocio / Financiación	Free-to-Play (F2P). Juego gratuito para atraer una gran base de usuarios con barrera de entrada nula.	Venta B2B (Licenciamiento). Venta de licencias corporativas a empresas que necesitan capacitar a su personal (Modelo Premium para la empresa).
Mecánicas de Monetización	Mecánicas Internas (Micropagos). 1. Energy System: Pagar para recargar energía y seguir jugando. 2. Skins: Comprar diseños neón para las torretas.	ROI (Retorno de Inversión). No cobra al usuario. Su valor económico se justifica en la reducción de incidentes de seguridad reales en la empresa cliente, ahorrando costos operativos y legales.

	3. Loot Boxes: Cajas aleatorias con defensas raras.	
Mecánicas de Ludificación (Gamificación)	Fidelización y Retención. 1. Rachas Diarias: Bonos por entrar 7 días seguidos (hábito). 2. Ligas (Leaderboards): Ranking mundial de mejores defensores. 3. Eventos Temporales: Pases de batalla con recompensas limitadas.	Motivación y Progreso. 1. Barras de Progreso: Visualizar el avance del curso de inducción. 2. Insignias (Badges): Certificado digital al completar módulos (ej: "Escudo Anti-Phishing"). 3. Feedback: Puntos por respuestas correctas para incentivar la práctica.
Métrica de Éxito (KPI)	Retención y LTV. Tasa de Retención D30 (Jugadores activos al mes) y Lifetime Value (Cuánto gasta un jugador en total).	Efectividad del Aprendizaje. Tasa de reducción de clics en correos de phishing reales post-entrenamiento y porcentaje de completitud del curso.

Análisis Comparativo

1. **Impacto del Modelo F2P en la Versión 1**

   En Cyber Defender: Neon Wars, la elección del modelo Free-to-Play forzó la introducción de fricción artificial en el bucle de juego. Para que las microtransacciones sean deseables, tuvimos que diseñar "tiempos de espera" (ej. esperar 30 minutos para mejorar un firewall) o limitar la "energía" de juego. Esto cambia el diseño: no se busca la experiencia más fluida posible, sino una que genere la necesidad de pagar para eliminar interrupciones, un riesgo asociado al F2P donde se busca rentabilidad a través de mecánicas internas. Si fuera un juego Premium, el bucle sería continuo y basado puramente en habilidad.

2. **Impacto del Propósito Serio en la Versión 2**

En InfoSec Guardian, el objetivo pedagógico de "formar habilidades prácticas" restringió severamente la libertad creativa. Tuvimos que eliminar la estética "Cyberpunk" y las mecánicas de "torretas disparando láseres" porque, aunque divertidas, no enseñan cómo se ve una amenaza real en una oficina. El diseño tuvo que volverse realista y aburrido (leer correos, revisar URLs), priorizando la precisión técnica sobre la espectacularidad visual. El "juego" se subordinó completamente a la simulación de un entorno laboral real.

3. El Doble Rol de la Ludificación

Las mecánicas de gamificación cambian drásticamente de función según el contexto:

- **En Entretenimiento (V1):** Los puntos y leaderboards sirven para generar competitividad y adicción (engagement), buscando que el usuario pase más tiempo en la app para monetizarlo.

- **En Juego Serio (V2):** Las barras de progreso e insignias actúan como andamiaje motivacional. Dado que la tarea (aprender protocolos de seguridad) puede ser tediosa, la gamificación provee una estructura de recompensa extrínseca para mantener al usuario enfocado hasta completar el objetivo educativo. En V1 la gamificación es el fin (ganar), en V2 es el medio (aprender).