**CIBERATAQUE: Blue Team en Alerta Máxima - Edición de Éxito**

**(Logotipo del juego, ahora con un diseño más impactante y moderno)**

**Manual de Juego - ¡Prepárate para la Ciberdescarga!**

**Índice**

1. **¡INICIO DE SESIÓN!** - Introducción al Juego
2. **CARGA DE DATOS** - Componentes del Juego
3. **OBJETIVO: CERO VULNERABILIDADES** - El Propósito de la Misión
4. **CONFIGURACIÓN INICIAL: DESPLIEGUE DEL BLUE TEAM** - Preparación de la Partida
5. **PROTOCOLO DE ACTUACIÓN: DESARROLLO DE LA PARTIDA**
   * **FASE 1: INTRUSIÓN RED TEAM - LA BRECHA INICIAL**
   * **FASE 2: DESPLIEGUE BLUE TEAM - CONTENCIÓN Y MITIGACIÓN**
   * **FASE 3: EVALUACIÓN DE IMPACTO - CONSECUENCIAS Y APRENDIZAJE**
6. **PERFILES BLUE TEAM: TUS AGENTES DE CIBERDEFENSA**
7. **CONTRAMEDIDAS: TU ARSENAL DE SEGURIDAD**
8. **EVENTOS RED TEAM: LA INTELIGENCIA DE AMENAZAS**
9. **GLOSARIO CRÍTICO: DESCODIFICANDO LA CIBERSEGURIDAD (CCN-CERT & CISSP CBK)**
10. **¡SISTEMA SEGURO!** - Condiciones de Victoria
11. **¡FALLO CRÍTICO!** - Condiciones de Derrota
12. **MECÁNICAS DE ALTO OCTANAJE: ADRENALINA CIBERNÉTICA**
13. **DESAFÍOS ADICIONALES: EXPANDIENDO EL CAMPO DE BATALLA**
14. **CRÉDITOS Y AGRADECIMIENTOS**

**1. ¡INICIO DE SESIÓN!** - Introducción al Juego

Bienvenido al corazón de la ciberdefensa con **CIBERATAQUE!** Olvídate de juegos pasivos; esto es una inmersión total en la adrenalínica batalla entre el Blue Team y las implacables fuerzas del Red Team. Como parte de un equipo de élite, cada decisión cuenta mientras te enfrentas a ciberataques dinámicos y evolutivos. Utiliza la sinergia de tus perfiles Blue Team, despliega contramedidas estratégicas y anticipa los movimientos del adversario. **CIBERATAQUE** no es solo un juego; es una simulación de crisis en tiempo real que te mantendrá al borde del asiento. ¿Tienes lo que se necesita para defender la fortaleza digital?

**Mecánica Clave para el Éxito:** La mecánica central de **CIBERATAQUE** se basa en la **gestión de riesgos asimétrica y la resolución cooperativa bajo presión**. Cada Evento Red Team presenta un desafío único con consecuencias inmediatas y a largo plazo, obligando al Blue Team a priorizar amenazas, coordinar sus acciones y optimizar sus recursos limitados. La incertidumbre de los próximos ataques y la necesidad de adaptarse constantemente crean una experiencia de juego tensa y altamente rejugable.

**2. CARGA DE DATOS** - Componentes del Juego

* **Mazo de Cartas de Perfil Blue Team (X cartas):** Cada perfil (p. ej., *Cazador de Amenazas Proactivo*, *Especialista en Forense Digital*, *Arquitecto de Resiliencia*) no solo tiene áreas de habilidad, sino también una **"Puntuación de Alerta"** que influye en su capacidad para detectar amenazas tempranamente y una **"Capacidad de Intervención"** que limita cuántas contramedidas puede apoyar efectivamente por ronda.
* **Mazo de Cartas de Contramedida (Y cartas):** Las contramedidas (p. ej., *Despliegue de Honeypots Avanzados*, *Implementación de Zero Trust Networking*, *Orquestación de Respuesta Automatizada*) ahora tienen un **"Coste de Activación"** en Puntos de Acción, una **"Ventana de Oportunidad"** (la fase en la que son más efectivas) y un **"Nivel de Mitigación Escalable"** (su efectividad puede aumentar si se invierten más PA o se combinan con otros perfiles/contramedidas).
* **Mazo de Cartas de Evento Red Team (Z cartas):** Los eventos (p. ej., *Ataque de Phishing Spear con Carga Útil Persistente*, *Movimiento Lateral Avanzado a través de Canales Cifrados*, *Exfiltración de Datos Sensibles mediante DNS Tunneling*) incluyen ahora un **"Índice de Persistencia"** (que indica si la amenaza persiste en rondas futuras si no se mitiga completamente) y un **"Potencial de Escalada"** (la amenaza puede volverse más severa con el tiempo).
* **Fichas de Punto de Acción (PA) (N fichas):** El recurso principal para desplegar defensas y activar habilidades. La gestión eficiente de PA es crucial.
* **Tablero de Nivel de Alerta:** Un track que representa la creciente sofisticación y frecuencia de los ataques del Red Team. Alcanzar ciertos niveles desbloquea nuevas reglas o intensifica los eventos.
* **Marcador de Integridad del Sistema:** La representación de la salud de la infraestructura crítica. Comienza en un valor alto y disminuye con los ataques no mitigados.
* **Marcadores de Persistencia de Amenaza:** Para recordar qué amenazas siguen activas y sus efectos continuos.
* **Este Manual de Juego.**

**3. OBJETIVO: CERO VULNERABILIDADES** - El Propósito de la Misión

El objetivo cooperativo es **mantener la Integridad del Sistema por encima de cero** hasta que se agote el mazo de Evento Red Team, demostrando la resiliencia del Blue Team ante una campaña de ciberataques sostenida y sofisticada. La verdadera victoria radica en la **maestría de la anticipación y la neutralización proactiva** de las amenazas.

**4. CONFIGURACIÓN INICIAL: DESPLIEGUE DEL BLUE TEAM** - Preparación de la Partida

1. **Baraja los mazos:** Asegúrate de una mezcla aleatoria para cada desafío.
2. **Selección Estratégica de Perfiles:** Cada jugador elige **X** cartas de Perfil Blue Team. La composición del equipo es vital; la sinergia entre diferentes habilidades será clave para la supervivencia.
3. **Mano de Contramedidas Inicial:** Cada jugador comienza con **Y** cartas de Contramedida. Esta es tu reserva inicial de defensas.
4. **Preparación del Red Team:** Coloca el mazo de Evento Red Team boca abajo. La incertidumbre de lo que vendrá es parte del desafío.
5. **Nivel de Alerta Inicial:** Comienza en el nivel más bajo del Tablero de Nivel de Alerta.
6. **Integridad del Sistema:** Establece el marcador en el valor inicial.
7. **Coordinador de la Primera Ronda:** Decidir quién liderará la primera respuesta.

**5. PROTOCOLO DE ACTUACIÓN: DESARROLLO DE LA PARTIDA**

Cada ronda se desarrolla en tres fases críticas:

**FASE 1: INTRUSIÓN RED TEAM - LA BRECHA INICIAL**

1. El coordinador roba la carta superior de Evento Red Team y la revela. ¡El ataque comienza!
2. Se analiza el Evento: Tipo de ataque, vector, impacto potencial, severidad e **Índice de Persistencia**.
3. **Puntuación de Alerta:** Los jugadores comparan la **Puntuación de Alerta** de sus Perfiles Blue Team activos con la severidad del Evento Red Team. Si la puntuación total del equipo supera la severidad, pueden obtener una visión temprana del ataque, lo que podría otorgar una bonificación en la Fase de Despliegue (ej. PA adicional, robar una carta de Contramedida extra).

**FASE 2: DESPLIEGUE BLUE TEAM - CONTENCIÓN Y MITIGACIÓN**

1. El equipo discute y decide qué Contramedidas desplegar. La comunicación y la comprensión de las sinergias son esenciales.
2. Para desplegar una Contramedida, un Perfil Blue Team activo debe tener una habilidad coincidente con los requisitos.
3. Se pagan los **Costes de Activación** en Puntos de Acción de la reserva común. La gestión de PA es un factor limitante clave.
4. Los jugadores deben considerar la **Ventana de Oportunidad** de cada Contramedida para maximizar su efectividad contra el Evento Red Team actual.
5. Se pueden combinar múltiples Contramedidas y la inversión adicional de PA puede aumentar el **Nivel de Mitigación Escalable** de una Contramedida.
6. Los Perfiles Blue Team pueden usar sus habilidades especiales (con posibles costes o límites de uso) para influir en la mitigación.

**FASE 3: EVALUACIÓN DE IMPACTO - CONSECUENCIAS Y APRENDIZAJE**

1. Se compara la efectividad de las Contramedidas desplegadas con el Evento Red Team.
2. Si el ataque no se mitiga completamente, se reduce la Integridad del Sistema según el impacto restante.
3. Si el Evento Red Team tiene un **Índice de Persistencia**, se coloca un Marcador de Persistencia en el tablero, recordando al equipo los efectos continuos en rondas futuras.
4. Se ajusta el Tablero de Nivel de Alerta según las reglas del juego (aumenta con el tiempo o la severidad de los ataques).
5. Los jugadores roban cartas de Contramedida para reponer sus manos hasta un límite.
6. El rol de coordinador pasa al siguiente jugador.

**6. PERFILES BLUE TEAM: TUS AGENTES DE CIBERDEFENSA**

Cada carta de Perfil Blue Team detalla:

* **Nombre y Especialización:** (Ej. Analista de Tráfico de Red - Especialista en Detección de Anomalías)
* **Áreas de Habilidad (ENISA):** Las competencias clave del perfil.
* **Puntuación de Alerta:** Su capacidad para anticipar amenazas.
* **Capacidad de Intervención:** Cuántas Contramedidas puede apoyar por ronda.
* **Habilidad Especial:** Una acción única y poderosa que puede realizar.
* **(Nueva Mecánica) Enlace de Habilidades:** Algunos perfiles tienen habilidades que se potencian si se despliegan junto a otros perfiles específicos, fomentando la construcción de un equipo sinérgico.

**7. CONTRAMEDIDAS: TU ARSENAL DE SEGURIDAD**

Cada carta de Contramedida detalla:

* **Nombre y Descripción:** (Ej. Análisis de Comportamiento de Usuarios y Entidades (UEBA) - Detecta actividades anómalas que podrían indicar una brecha)
* **Nivel ENS:** Su alineación con los estándares de seguridad.
* **Habilidades Blue Team Requeridas:** Los perfiles necesarios para su implementación.
* **Coste de Activación (PA):** El recurso necesario para desplegarla.
* **Ventana de Oportunidad:** La fase del ataque donde es más efectiva.
* **Nivel de Mitigación Escalable:** Cómo su efectividad puede aumentar con inversión adicional.
* **Sinergia de Contramedida:** Algunas contramedidas se vuelven más poderosas si se despliegan junto a otras específicas.

**8. EVENTOS RED TEAM: LA INTELIGENCIA DE AMENAZAS**

Cada carta de Evento Red Team detalla:

* **Nombre del Evento:** (Ej. Campaña de Watering Hole Dirigida a Proveedores)
* **Tipo de Ataque (Guía Nacional):** La clasificación del incidente.
* **Vector de Ataque:** Cómo se está llevando a cabo la intrusión.
* **Impacto Potencial:** Las áreas de la infraestructura en riesgo (Confidencialidad, Integridad, Disponibilidad).
* **Severidad (Guía Nacional):** La gravedad del ataque.
* **Índice de Persistencia:** Si la amenaza persiste y requiere contención continua.
* **Potencial de Escalada:** Cómo la amenaza puede intensificarse en rondas futuras si no se neutraliza.
* **(Nueva Mecánica) Patrones de Ataque:** Algunos eventos pertenecen a un "Patrón de Ataque" (ej. Amenazas Persistentes Avanzadas - APT). Si el equipo no logra mitigar varios eventos del mismo patrón, se activan efectos negativos adicionales.

**9. GLOSARIO CRÍTICO: DESCODIFICANDO LA CIBERSEGURIDAD (CCN-CERT & CISSP CBK)**

*(Se mantiene el glosario anterior, enfatizando la importancia de estos términos en el contexto estratégico del juego).*

**10. ¡SISTEMA SEGURO!** - Condiciones de Victoria

El equipo Blue Team celebra la victoria si logra **agotar el mazo de Evento Red Team** manteniendo la Integridad del Sistema por encima de cero, demostrando una defensa sólida y adaptable contra una campaña de ciberataques sostenida.

**11. ¡FALLO CRÍTICO!** - Condiciones de Derrota

La partida termina en derrota si la Integridad del Sistema llega a cero en cualquier momento, indicando una brecha catastrófica en la defensa.

**12. MECÁNICAS DE ALTO OCTANAJE: ADRENALINA CIBERNÉTICA**

* **Gestión de Crisis en Tiempo Real:** La naturaleza impredecible del mazo de Evento Red Team y la necesidad de tomar decisiones rápidas bajo presión simulan la realidad de la respuesta a incidentes.
* **Sinergia de Equipo Obligatoria:** Ningún jugador puede ganar por sí solo. La comunicación constante, la planificación coordinada y la comprensión de las fortalezas de cada perfil son cruciales para la supervivencia.
* **Riesgo vs. Recompensa:** Decidir si invertir más PA en una mitigación más fuerte o conservar recursos para futuras amenazas crea decisiones tácticas significativas.
* **Progresión y Maestría:** A medida que los jugadores aprenden las sinergias entre perfiles y contramedidas, y anticipan los Patrones de Ataque del Red Team, su eficiencia y capacidad para manejar crisis aumentan, brindando una sensación de progresión y maestría.
* **Elementos Sorpresa:** Las cartas de Evento Red Team con **Potencial de Escalada** y los **Patrones de Ataque** mantienen la incertidumbre y obligan al equipo a adaptarse constantemente.

**13. DESAFÍOS ADICIONALES: EXPANDIENDO EL CAMPO DE BATALLA**

* **Módulos de Expansión:** Introducir mazos de Evento Red Team temáticos (ej. Ataques a Infraestructuras Críticas Específicas, Amenazas Internas) y nuevos perfiles y contramedidas.
* **Cartas de "Tecnología en Evolución":** Cartas que representan nuevas tecnologías de ataque o defensa, alterando las reglas del juego o introduciendo nuevas mecánicas.
* **Modo Campaña:** Jugar una serie de escenarios conectados con objetivos específicos y consecuencias persistentes.

**14. CRÉDITOS Y AGRADECIMIENTOS**

*(Se mantiene la sección de créditos, enfatizando la base educativa del juego).*