🛡️ Ejercicio de Juego de Rol: Respuesta a un Incidente de Ciberseguridad

Introducción: ¿Estáis Preparados?

Objetivo del Juego: Ha ocurrido un incidente de seguridad en nuestra empresa. Vuestro equipo de respuesta ante incidentes debe **averiguar qué ha pasado** y **establecer los pasos para remediarlo**[1].

Duración Estimada: 60 - 90 minutos (ajustable según el debate).

🛠️ Material Necesario

- Un equipo de **personas** para debatir sobre el incidente y su resolución.
- Una **pizarra** o un lugar donde pegar notas (*post-its*) para anotar conclusiones.
- Esta guía y la descripción del incidente.
- (Opcional) Un PC con conexión a Internet para consultar guías de apoyo.

🏢 Escenario de la Empresa (Activos y Entorno)

Nuestra empresa, **"MY SHOP"**, es una PYME con la siguiente infraestructura y activos:

Activos Físicos y Lógicos

Tipo de Activo	Ejemplos
Puestos de Trabajo	PCs, impresoras, teléfonos fijos.
Dispositivos Móviles	Portátiles, móviles, tabletas.
Almacenamiento Local	Discos duros externos, *pendrives*.

Tipo de Activo	Ejemplos
Servidores e Infraestructura	Servidores de correo, servidores de archivos/aplicaciones, *routers* con conexión WiFi.
Activos Lógicos	Datos personales de clientes, propiedad intelectual, procesos internos (CRM, ERP), programas.

Servicios Externalizados y en la Nube

Utilizamos servicios externos para aspectos clave del negocio:

- **Servicios en la Nube:** Almacenamiento (ej. Dropbox), aplicaciones (ej. Gmail, Office 365, Salesforce).
- **Web/Tienda Online:** Una página web/tienda online alojada en un proveedor externo.
- **Redes Sociales:** Uso activo de redes sociales como herramienta de comunicación y marketing.

🚨 Fase 1: ¿Qué ha Pasado? (El Incidente)

*(El moderador debe leer la descripción del incidente en este momento. **Aclaración: El documento fuente no proporciona un incidente específico. Debes crear uno, como el siguiente ejemplo**).*

PLANTEAMIENTO DEL INCIDENTE (Ejemplo para el Ejercicio)

"A las 10:00 AM, el Director de Marketing reporta que la **tienda online está inaccesible** y devuelve un error al intentar cargar. Casi al mismo tiempo, el departamento de Contabilidad informa que no pueden acceder a los **archivos compartidos** en el servidor de archivos local.

Poco después, varios empleados reciben un **correo electrónico interno** aparentemente legítimo de la gerencia, que en realidad contiene un archivo adjunto malicioso. Tres empleados lo han abierto. Ahora, en el servidor de archivos y en algunos puestos de trabajo aparece una pantalla con un mensaje que dice: **'SYSTEM BARCE'** y un **símbolo de extorsión/peligro**, solicitando un rescate en criptomonedas para liberar los archivos cifrados."

📝 Preguntas Guía para el Debate (30 min)

Debatid y anotad las posibles respuestas a las siguientes preguntas:

1. **¿Qué ha ocurrido y dónde?** ¿Qué tipo de incidentes se han manifestado (ej. *malware*, denegación de servicio, robo de datos)? ¿Qué dispositivos están afectados (servidores, puestos de trabajo, *cloud*)?.
2. **¿Cuándo/Desde Cuándo Ocurre?** (Estimar el punto de origen).
3. **¿Quién ha podido hacerlo?** ¿Es un error interno (despiste, descontento) o un ataque externo (ciberdelincuente, ex-empleado)?.
4. **¿Cuáles son las consecuencias (daños)?** Valora los daños materiales, económicos (coste de reparación, interrupción del servicio) y personales/reputacionales. (Usar tabla de apoyo 3).
5. **Implicaciones Legales y Comunicación:** ¿Tenemos que avisar a clientes o usuarios? ¿Tiene implicaciones legales (RGPD, denuncias)?.

📊 Tabla de Apoyo 1: Posibles Incidentes vs. Activos

Marquen las casillas que consideren afectadas por el incidente planteado:

Incidente / Activo	**Robo o Pérdida**	**Avería**	**Infección por Malware**	**Infección con Extorsión (Ransomware)**	**Denegación de Servicio (DDoS)**
Puesto de trabajo					
Servidores y redes					
Página web / Cloud					

❌ Fase 2: ¿Qué ha Fallado? (Identificación de Errores)

Una vez que han identificado el incidente, el equipo debe debatir sobre **qué mecanismo o protocolo de seguridad ha fallado** y ha permitido que ocurra el ataque.

📝 Preguntas Guía para el Debate (20 min)

1. ¿Qué errores técnicos o de procedimiento permitieron la infección por *malware* o la extorsión?
2. ¿Qué fallos de seguridad permitieron que la tienda online cayera o que el correo malicioso fuera enviado/abierto?

📊 Tabla de Apoyo 2: Posibles Fallos de Seguridad

Marquen la(s) casilla(s) que probablemente fallaron en este incidente:

Fallo de Seguridad	**Robo o Pérdida**	**Infección por Malware**	**Infección con Extorsión**	**Denegación de Servicio**
Uso de equipos o servicios no autorizados				
Contraseña poco segura / por defecto				
Víctima de engaños de **Ingeniería Social**				
Mala configuración de equipos/dispositivos				
Equipos con **software no actualizado**				

Fallo de Seguridad	Robo o Pérdida	Infección por Malware	Infección con Extorsión	Denegación de Servicio
Mala gestión de usuarios (permisos excesivos)				
Routers o redes con **contraseña por defecto**				
Procedimiento de **copias de seguridad** ausente/fallido				

✅ Fase 3: ¿Cómo Salimos de Esta? (Resolución y Prevención)

Ahora hay que resolver el incidente, contenerlo y planificar cómo evitarlo en el futuro.

📝 Preguntas Guía para el Debate (25 min)

1. **Contención y Recuperación:** ¿Tenemos que **detener el incidente** y evitar que se propague? ¿Cómo? ¿Podemos recuperar la información afectada (ej. ¿tenemos copias de seguridad?)?.
2. **Asistencia:** ¿A quién debemos avisar primero (soporte interno/externo, perito forense, policía)?.
3. **Prevención:** ¿Qué debemos hacer para evitar que vuelva a suceder? (Tecnologías, procedimientos, formación).

📊 Tabla de Apoyo 3: Medidas a Implementar para Evitarlo

Identifica las medidas clave que faltan o fallaron y que deben implementarse en los activos afectados:

Medida Preventiva	Puesto de Trabajo	Servidores y Redes	Pág. Web / Cloud	Varios Activos
Actualizaciones de *software*				
Antimalware / Cortafuegos				
Control de Accesos Lógico				
Procedimiento Copias de Seguridad				
Formación Ingeniería Social				
Formación Cuentas y Contraseñas				

💡 Fase 4: ¿Qué Hemos Aprendido?

Es el momento de repasar las conclusiones.

1. **Revisión:** Comprobad que habéis respondido a todas las preguntas y que hay consenso en las respuestas clave.
2. **Lecciones Aprendidas:** Repasad los **fallos técnicos, de procedimiento o de formación** que permitieron el incidente.
3. **Plan de Acción:** Listad las actuaciones que vais a poner en marcha para que el incidente no vuelva a ocurrir (p. ej., "Implementar copias de seguridad diarias", "Formar a empleados en *phishing*", "Contratar soporte legal").
4. **Estructura:** Recordad la necesidad de definir un **Plan de Respuesta ante Incidentes** y un **responsable** para estas circunstancias.

💣 Escenario de Incidente Complejo: "El Ataque del Doble Venganza"

🗓️ Cronología del Incidente

Hora (Aprox.)	Evento	Estado
08:30 AM	El equipo de Marketing se conecta y detecta que el **portal web de noticias** (alojado externamente) tiene su **página de inicio desfigurada** con un mensaje político y una calavera.	**Visible (Público)**
09:00 AM	El responsable de TI recibe una alerta de que el **Servidor de Archivos local** y el **Servidor de Aplicaciones (ERP/CRM)** están inaccesibles. Todos los archivos tienen una nueva extensión y una nota de rescate en el escritorio.	**Crítico (Interno)**
09:15 AM	Se recibe un correo electrónico de un atacante ("El Doble Venganza") que indica que no solo han cifrado los datos, sino que **han extraído una copia** de la **base de datos de clientes** (nombres, correos electrónicos, historiales de compra) y **documentos de Propiedad Intelectual** antes de cifrar los servidores.	**Fuga de Datos Confirmada**
09:30 AM	Un cliente clave llama a la oficina para informar que el **móvil de un empleado** (que utiliza Salesforce) ha sido **bloqueado** remotamente, y que han intentado usar la cuenta de ese empleado para enviar *phishing* a sus contactos.	**Impacto en Movilidad y Terceros**
10:00 AM	Se intenta acceder al **servicio de *cloud* (Dropbox/Office 365)** para revisar copias de seguridad, pero se descubre que la cuenta del administrador tiene la **contraseña cambiada** y no se puede ingresar.	**Pérdida de Control en la Nube**

📝 Resumen del Incidente

La empresa se enfrenta a un ataque complejo que combina:

1. **Denegación de Servicio/Vandalismo:** La web pública está caída/alterada.
2. ***Ransomware* con Extorsión:** Los sistemas críticos internos (ERP/CRM y Archivos) están cifrados y se exige un rescate.
3. **Filtración de Datos (Exfiltración):** Los datos personales de clientes y propiedad intelectual han sido robados.
4. **Compromiso de Cuentas:** Se ha perdido el acceso al entorno *cloud* y se ha comprometido un dispositivo móvil.

❓ Puntos Clave para el Debate

- **RTO vs. RPO en Múltiples Puntos:** ¿Qué se debe restaurar primero (el ERP, los archivos, el acceso al *cloud*)? ¿Cuál es la pérdida de datos más crítica?
- **Decisión Crítica:** ¿Se debe pagar el rescate, sabiendo que ya han robado los datos?
- **Obligación Legal (GDPR/LOPD):** Dada la fuga de datos personales, ¿quién debe ser notificado, y en qué plazo? (Autoridad de Protección de Datos y clientes).
- **Comunicación en Crisis:** ¿Qué mensaje se envía al cliente que llamó? ¿Qué se le dice al público sobre la web desfigurada? ¿Y a los empleados?

Este escenario requiere que el equipo de respuesta utilice las tablas de la guía original, marcando múltiples casillas para los tipos de incidente y los activos afectados, y forzando a priorizar acciones bajo una presión extrema de tiempo y legales.