Paso 1: Identificación de Activos Críticos

Objetivo: Identificar los activos críticos que requieren protección.
Actividades:

1. **Explicación:**
    - Definición de activos críticos: Elementos esenciales para la operación (ej. bases de datos, servidores).
    - Impacto de su compromiso: Pérdida de confianza, multas legales, interrupción del negocio.
2. **Ejercicio Grupal:**
    - Listar activos: Bases de datos de clientes, servidores web, sistemas de pago, claves API, información financiera.
3. **Discusión:**
    - Clasificar por criticidad:
        - **Alto:** Bases de datos, sistemas de pago.
        - **Medio:** Servidores web.
        - **Bajo:** Registros de marketing.

Resultado Esperado: Lista priorizada de activos críticos.

Paso 2: Análisis de Amenazas y Riesgos

Objetivo: Evaluar amenazas y riesgos para los activos.
Actividades:

1. **Explicación:**
    - Amenazas comunes: Phishing, malware, ransomware, DDoS.
2. **Ejercicio Grupal:**
    - Mapear amenazas por activo:
        - Ejemplo: Bases de datos → Ransomware (impacto alto, probabilidad media).
3. **Discusión:**
    - Priorizar con matriz de riesgo:
        - **Alto riesgo:** Ransomware en bases de datos.
        - **Impactos:** Pérdida de ingresos, daño reputacional.

Resultado Esperado: Tabla de amenazas priorizadas.

Paso 3: Equipo de Respuesta a Incidentes

Objetivo: Definir roles del equipo.
Actividades:

1. **Explicación:**
    - Roles clave:
        - **Responsable de Comunicaciones:** Coordina mensajes internos/externos.
        - **Técnico de Sistemas:** Mitiga el incidente técnicamente.
        - **Legal:** Gestiona implicaciones regulatorias.
2. **Ejercicio Grupal:**
    - Asignar roles y crear lista de contactos de emergencia (ej. proveedor de hosting, abogado).
3. **Discusión:**
    - Validar responsabilidades y canales de comunicación.

Resultado Esperado: Estructura del equipo con roles definidos.

Paso 4: Procedimientos de Detección

Objetivo: Diseñar monitoreo proactivo.
Actividades:

1. **Explicación:**
    - Herramientas: IDS, análisis de logs (ej. acceso no autorizado), alertas en tiempo real.
2. **Demostración:**
    - Simular revisión de logs (ej. intentos de acceso fallidos).
3. **Ejercicio Grupal:**
    - Crear checklist de monitoreo diario:
        - Revisar logs de autenticación.
        - Configurar alertas para transacciones sospechosas.

Resultado Esperado: Procedimiento básico de detección.

Paso 5: Plan de Contención

Objetivo: Acciones inmediatas para mitigar daños.
Actividades:

1. **Explicación:**
    - Ejemplos: Aislar servidores afectados, bloquear IPs maliciosas.
2. **Ejercicio Grupal:**
    - Diseñar plan para las primeras 24 horas:
        - Paso 1: Desconectar sistemas comprometidos.
        - Paso 2: Notificar al equipo legal.
3. **Discusión:**
    - Retroalimentación sobre viabilidad del plan.

Resultado Esperado: Plan de contención con pasos claros.

Paso 6: Plan de Recuperación y Continuidad

Objetivo: Restaurar operaciones y comunicar a clientes.
Actividades:

1. **Explicación:**
    - Mejores prácticas: Copias de seguridad diarias, comunicación transparente.
2. **Ejercicio Grupal:**
    - Elaborar plan:
        - Restaurar datos desde backups.
        - Mensaje a clientes: "Hemos detectado una incidencia y sus datos están seguros".
3. **Simulación:**
    - Escenario: Ataque de ransomware. Evaluar respuesta del grupo.

Resultado Esperado: Plan de recuperación con enfoque técnico y comunicacional.

Paso 7: Conclusiones y Preguntas

Objetivo: Sintetizar aprendizajes.
Actividades:

- Resumen de pasos clave: Desde identificación de activos hasta recuperación.
- Q&A: Aclarar dudas sobre roles o procedimientos.
- **Material entregable:** Plantilla de plan de respuesta a incidentes.