**Paso 1: Identificación de Activos Críticos**

En esta etapa se identificaron los activos más importantes dentro de una empresa. Para ello, primero se explicó qué se considera un activo crítico: cualquier recurso físico o digital cuya pérdida o mal funcionamiento afectaría gravemente las operaciones.

Como actividad, se hizo una lista de activos comunes, tales como:

* Bases de datos de clientes
* Servidores de aplicaciones
* Sitio web corporativo
* Sistemas de nómina
* Equipos de red (routers, firewalls)

Luego, se clasificaron por nivel de criticidad. Por ejemplo, las bases de datos de clientes se consideraron de alta prioridad debido a que contienen información confidencial. El sitio web también fue considerado crítico, especialmente si se usa para ventas.

Finalmente, se priorizó la protección de aquellos activos que combinaban alta dependencia con alta sensibilidad de los datos.

**Paso 2: Análisis de Amenazas y Riesgos**

En esta fase se analizaron las amenazas que podrían comprometer los activos críticos identificados anteriormente.

Primero se revisaron ejemplos de amenazas frecuentes:

* Phishing: suplantación mediante correos engañosos
* Malware y ransomware: software que puede dañar o cifrar la información
* Ataques DDoS: afectan la disponibilidad de servicios en línea
* Acceso no autorizado: compromete la confidencialidad y control de los sistemas

Luego, se relacionó cada amenaza con los activos. Por ejemplo, el servidor de correo electrónico podría ser el medio para un ataque de phishing, mientras que las bases de datos son vulnerables ante accesos no autorizados.

Se utilizó una matriz simple para evaluar la probabilidad e impacto de cada amenaza sobre cada activo, clasificando los riesgos como altos, medios o bajos. Así se priorizó la gestión de amenazas de mayor impacto, como el ransomware sobre la base de datos principal.

**Paso 3: Formación del Equipo de Respuesta a Incidentes**

Se desarrolló una estructura básica de un equipo de respuesta ante incidentes, con roles definidos y responsabilidades específicas. La actividad consistió en simular la creación de este equipo con los siguientes roles:

* Coordinador general: dirige las acciones durante el incidente
* Técnico de sistemas: identifica, aísla y mitiga amenazas técnicas
* Responsable legal: asegura el cumplimiento normativo
* Encargado de comunicaciones: gestiona la información hacia usuarios y clientes
* Analista de seguridad: evalúa el origen y el impacto del incidente

También se elaboró un pequeño directorio con nombres ficticios y contactos de emergencia. Esta información serviría para una rápida activación del equipo en caso de detectarse un incidente de seguridad.

**Paso 4: Desarrollo de Procedimientos de Detección**

Se estudiaron los métodos que permiten detectar incidentes a tiempo. Para esto, se analizaron logs de eventos, sistemas de monitoreo y herramientas de detección de intrusiones.

En la demostración técnica se observaron logs del sistema operativo (Windows y Linux) y logs de firewall. Se identificaron entradas sospechosas como múltiples intentos fallidos de acceso o conexiones desde direcciones IP inusuales.

Como parte del ejercicio, se propuso un procedimiento de monitoreo que incluye:

* Revisión diaria de logs del servidor
* Revisión semanal de logs del correo electrónico
* Configuración de alertas automáticas ante ciertos eventos críticos
* Asignación de una persona responsable de esta revisión

**Paso 5: Elaboración del Plan de Contención**

En esta etapa se construyó un plan básico para contener un incidente y evitar que se propague. Se explicó que la contención es clave para limitar los daños.

Se trabajó en un escenario hipotético de infección por ransomware en un servidor. El plan de contención incluyó:

* Desconectar el servidor infectado de la red
* Comunicar inmediatamente al equipo de respuesta
* Guardar una copia de los logs y archivos comprometidos como evidencia
* Activar el protocolo de aislamiento de sistemas relacionados
* Notificar a los usuarios sobre posibles interrupciones del servicio

Este ejercicio ayudó a comprender la necesidad de actuar rápidamente y con un plan estructurado para evitar la escalada del incidente.

**Paso 6: Plan de Recuperación y Continuidad del Negocio**

Por último, se abordó la fase de recuperación posterior al incidente. Se analizaron métodos para restaurar la operación normal y garantizar la continuidad del negocio.

Se elaboró un pequeño plan de recuperación que consideró lo siguiente:

* Verificación del estado de las copias de seguridad
* Restauración de los sistemas comprometidos desde los respaldos
* Validación de la integridad de los datos recuperados
* Comunicación a los clientes sobre la reanudación del servicio
* Revisión y actualización de los sistemas de seguridad afectados

Finalmente, se simuló una situación donde, tras un ataque, los sistemas eran recuperados desde backups. Se evaluó el tiempo de respuesta y la claridad de los procedimientos establecidos, destacando la importancia de tener estos planes preparados de antemano.