Unidad 1: Protección y Seguridad

1. **Seguridad Informática vs. Seguridad de la Información**:
    - **Seguridad Informática**: Protege hardware, software, redes y datos contra amenazas tecnológicas.
    - **Seguridad de la Información**: Protege toda la información de la empresa, incluyendo documentos físicos.
2. **Vulnerabilidades en TI**:
    - **Vulnerabilidad**: Cualquier debilidad del sistema que puede ser explotada.
    - **Amenaza**: Algo que aprovecha una vulnerabilidad.
    - **Impacto**: Consecuencias del daño si una vulnerabilidad es explotada.
3. **Triángulo de la Seguridad**:
    - **Confidencialidad**: Solo los autorizados pueden acceder a la información.
    - **Disponibilidad**: Los recursos están disponibles cuando son necesarios.
    - **Integridad**: Los datos no han sido modificados sin autorización.
4. **Copias de Seguridad**:
    - **Completa**: Copia de todos los datos.
    - **Incremental**: Solo los cambios desde la última copia.
    - **Diferencial**: Cambios desde la última copia completa.
5. **Planes de Recuperación**:
    - **Plan de Continuidad de Negocio**: Mantener las operaciones durante un desastre.
    - **Plan de Contingencia**: Respuesta inmediata para restaurar operaciones.

Unidad 2: Auditoría Informática

1. **Concepto de Auditoría Informática**:
    - Revisión de controles de seguridad, tanto tecnológicos como de procesos y personal.
    - Recopilación de evidencias para garantizar la protección de los activos empresariales.
2. **Tipos de Auditoría**:
    - **Por sujeto**: Interna (personal de la empresa) o externa (empresa externa).
    - **Por amplitud**: Total (todos los elementos tecnológicos) o parcial (una parte específica).

- **Por frecuencia**: Permanente (continua) o ocasional (en momentos específicos).

3. **Funciones y Objetivos**:
   - Asegurar la operatividad y calidad de los sistemas.
   - Alinear los sistemas de TI con los objetivos empresariales.
4. **Evolución de la Auditoría Informática**:
   - Edad Media: Detección de fraudes financieros.
   - Actualidad: Auditoría integral con estándares como ISO 27001.
5. **Técnicas de Auditoría**:
   - **Clásica (manual)**: Entrevistas y observación.
   - **Asistida por computadora (TAC)**: Uso de programas para analizar sistemas.
6. **Delitos Informáticos en Bolivia**:
   - Daños informáticos, fraudes en línea, trata de personas, pornografía infantil, ciberbullying.

Unidad 3: Auditoría de Sistemas

1. **Definición y Objetivo**:
   - Verificación de controles en el procesamiento de información y la instalación de sistemas.
   - Evaluar la efectividad, eficiencia y seguridad de los sistemas.
2. **Pasos de la Auditoría de Sistemas**:
   - Investigación preliminar y detallada.
   - Pruebas sustantivas para verificar la eficacia de los controles.
   - Emisión de opinión sobre la seguridad y eficiencia.
3. **Objetivos**:
   - Mejorar la relación coste-beneficio del sistema de información.
   - Incrementar la satisfacción y seguridad de los usuarios.
   - Minimizar la exposición a riesgos como virus y hackers.
4. **Vulnerabilidades de los Sistemas**:
   - **Diseño y protocolos**: Debilidades en los protocolos de red.
   - **Implementación**: Errores de programación.
   - **Día cero**: Vulnerabilidades sin solución conocida.
5. **Pruebas a los Sistemas**:

- **Caja blanca**: Evaluación del código fuente.
- **Caja negra**: Pruebas basadas en entradas y salidas sin conocer la lógica interna.

6. **Informe de Auditoría**:
    - Incluye título, alcance, opinión del auditor, párrafos de énfasis y salvedades.