**ACTIVIDAD: ANÁLISIS Y DISEÑO DE ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN**

**Instrucciones**

1. **Formación de equipos:** se trabajará en equipos de 3 personas.
2. **Distribución del caso:** Cada equipo tendrá un caso descrito más adelante.
3. **Fase 1: Análisis del caso**
   * Identificar los riesgos asociados al modelo operativo del caso (On-Premise, Cloud o Alta Disponibilidad).
   * Mapear las vulnerabilidades principales y los activos críticos involucrados.
4. **Fase 2: Diseño de controles informáticos**
   * Diseñar **3 controles informáticos clave** para mitigar los riesgos identificados. Ejemplo de controles:
     + Políticas de acceso y cifrado para datos sensibles.
     + Implementación de firewalls y sistemas de detección de intrusos.
     + Configuración de backups automáticos y recuperación en caso de fallo.
5. **Fase 3: Desarrollo de Planes de Contingencia**
   * Elaborar un esquema inicial para los siguientes planes:
     + **BIA (Business Impact Analysis):** Identificar procesos críticos y tiempo máximo tolerable de interrupción (MTTI).
     + **BCP (Business Continuity Plan):** Proponer un plan que permita mantener las operaciones clave tras un evento crítico.
     + **DRP (Disaster Recovery Plan):** Diseñar una estrategia para restaurar sistemas y datos tras un desastre.
6. **Fase 4: Presentación**
   * Cada equipo presentará su análisis y propuestas en una sesión de 10 minutos, destacando:
     + Riesgos identificados.
     + Controles diseñados.
     + Esquema de los planes BIA, BCP y DRP.

**CASOS**

**Caso 1: Empresa mediana con infraestructura On-Premise**

Una empresa de manufactura que opera en un mercado competitivo administra toda su infraestructura tecnológica de manera On-Premise, incluyendo servidores, bases de datos y aplicaciones críticas para el control de inventarios y producción.

Recientemente, la empresa ha sufrido un ataque de ransomware que cifró los datos de sus servidores, afectando sus operaciones por tres días. Además, los equipos de TI identificaron que los sistemas de respaldo no estaban configurados adecuadamente, dejando a la empresa sin acceso a copias recientes de sus datos.

Requerimientos:

* Diseñar controles para proteger la infraestructura de futuros ataques de ransomware.
* Identificar las áreas de mayor impacto en el negocio y proponer un esquema para el BIA.
* Elaborar un BCP que permita a la empresa continuar operando en caso de nuevos incidentes.
* Diseñar un DRP para restaurar la infraestructura y los datos críticos rápidamente.

**Caso 2: Startup en la nube**

Una startup tecnológica gestiona todos sus servicios en la nube, utilizando plataformas como AWS y Azure para bases de datos, aplicaciones web y almacenamiento de datos de clientes. La startup ha experimentado interrupciones frecuentes debido a fallas en el proveedor de servicios en la nube, lo que ha resultado en que sus clientes no puedan acceder a sus aplicaciones por varias horas.

Además, la startup está preocupada por las posibles brechas de seguridad en la transferencia de datos sensibles y la falta de un plan formal para manejar estos incidentes.

Requerimientos:

* Diseñar controles para asegurar la disponibilidad y protección de los datos almacenados en la nube.
* Identificar los riesgos asociados con el proveedor y proponer un esquema para el BIA.
* Elaborar un BCP que permita a la startup garantizar la continuidad de los servicios, incluso si el proveedor tiene fallas.
* Diseñar un DRP para migrar servicios a otro proveedor en caso de incidentes graves.

**Caso 3: Organización financiera con alta disponibilidad**

Una institución financiera debe garantizar la alta disponibilidad de sus servicios digitales, como aplicaciones de banca en línea, cajeros automáticos y sistemas de pago. Por regulaciones legales, cualquier interrupción en los servicios debe ser menor a 30 minutos.

Recientemente, un fallo en su sistema redundante causó una interrupción de 1 hora, lo que generó pérdidas económicas y multas regulatorias. Además, el análisis post-incidente reveló que la organización no tiene un plan claro para recuperación de desastres ni un proceso formal de análisis de impacto en el negocio.

Requerimientos:

* Diseñar controles para garantizar la redundancia y disponibilidad continua de los servicios críticos.
* Identificar los procesos más críticos y desarrollar un esquema para el BIA.
* Elaborar un BCP para que la institución pueda mantener los servicios activos durante fallos de infraestructura.
* Diseñar un DRP que permita recuperar los servicios en menos de 30 minutos en caso de desastres.

**Criterios de Evaluación**

* **Análisis del caso (20%):** Identificación adecuada de riesgos y activos críticos.
* **Diseño de controles (30%):** Relevancia y calidad de los controles propuestos.
* **Planes de contingencia (30%):** Complejidad y aplicabilidad de los planes BIA, BCP y DRP.
* **Presentación y argumentación (20%):** Claridad, organización y defensa de las propuestas.