# Ejercicio Evaluativo Individual: Gestión de Riesgos y Requisitos CID

**Introducción**

Este ejercicio tiene como objetivo consolidar su comprensión sobre la Tríada de la Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad - CID), la gestión de riesgos y la priorización de recursos en un entorno empresarial real. Deberá actuar como un consultor de seguridad independiente contratado para analizar la infraestructura de la empresa ficticia "TechSoluciones Innovadoras".

**Instrucciones:** Lea detenidamente el caso de estudio de la empresa y luego complete las cinco (5) fases del ejercicio, elaborando un informe detallado que responda a todas las preguntas planteadas.

## Caso de Estudio: TechSoluciones Innovadoras S.A.

**Empresa:** TechSoluciones Innovadoras S.A. **Sector:** Desarrollo de software y consultoría tecnológica (tamaño PYME). **Personal:** 50 empleados (Desarrolladores, Consultores, Ventas y Administración).

**Presupuesto de Seguridad:** El presupuesto asignado para seguridad de la información es limitado, requiriendo una justificación clara de la inversión y la priorización de las medidas de protección.

**Recursos de Información Críticos (Sistemas)**

La infraestructura de TechSoluciones se compone de cuatro sistemas principales:

| ID del Sistema | Nombre del Sistema | Descripción y Función Crítica | Datos Manejados | Ubicación |
|---|---|---|---|---|
| **SISTEMA A** | CRM y Ventas | Gestión de relaciones con clientes, seguimiento de oportunidades y contratos. Es vital para la generación de ingresos. | Nombres, contactos, historial de compras, información de contratos. | Centro de Datos Local (Virtualizado) |
| **SISTEMA B** | Servidor de Desarrollo | Almacena y gestiona el código fuente propietario y los repositorios de desarrollo de software. Interrupción = Parada de la producción. | Código Fuente, Propiedad Intelectual. | Centro de Datos Local (Virtualizado) |
| **SISTEMA C** | Nóminas y RR.HH. | Procesamiento de nóminas, gestión de vacaciones y datos personales de los empleados. | Salarios, Cuentas Bancarias, Historial Médico Básico, Información Personal Sensible. | Centro de Datos Local (Virtualizado) |
| **SISTEMA D** | Portal Web Público | Aloja el sitio web corporativo, blog y el portal de atención al cliente no logueado. | Información de Marketing, Contactos de prospectos. | Nube Pública (AWS) |

## Obligaciones Legales y Regulatorias

La empresa opera en un entorno que exige estricto cumplimiento con la **Protección de Datos Personales** (similar a GDPR o legislación local de privacidad), tanto para los datos de los clientes (SISTEMA A) como para los datos sensibles de los empleados (SISTEMA C). Cualquier filtración de estos datos conlleva multas elevadas y daño reputacional.

## Fases del Ejercicio Evaluativo

A continuación, se detallan las tareas que debe completar para elaborar su informe.

**FASE 1: Análisis de Requisitos de Seguridad (CID e Impacto)**

En esta fase, usted identificará la importancia de cada sistema.

1. **Análisis de Impacto y Requisitos CID (Puntos 7 y 1):**
    - Identifique los **procesos críticos** que dependen de cada uno de los cuatro sistemas (A, B, C, D).
    - Para cada sistema, asigne el nivel de requisito CID (Confidencialidad, Integridad, Disponibilidad) necesario, utilizando la siguiente escala:
        - **Alto (A):** Pérdida o interrupción catastrófica.
        - **Medio (M):** Impacto significativo, pero no detiene completamente el negocio.
        - **Bajo (B):** Poco impacto operacional o financiero.
    - Justifique brevemente su asignación de CID para cada sistema, haciendo referencia a las **obligaciones legales o regulatorias** cuando sea aplicable (Sistemas A y C).
2. **Creación de la Matriz CID (Punto 2):**
    - Cree una tabla (Matriz CID) que resuma las asignaciones de requisitos de CID para cada sistema (A, B, C, D).

| ID del Sistema | Confidencialidad (C) | Integridad (I) | Disponibilidad (D) | Justificación (Legal/Operacional) |
|---|---|---|---|---|
| SISTEMA A | | | | |
| SISTEMA B | | | | |
| SISTEMA C | | | | |
| SISTEMA D | | | | |

**FASE 2: Identificación y Análisis de Riesgos**

En esta fase, explorará cómo evaluar los riesgos para la empresa.

3. **Metodologías de Riesgo (Punto 9):**
    - Seleccione una de las metodologías de gestión de riesgo mencionadas (NIST SP 800-30, Magerit, ISO 31000) y explique por qué sería la más adecuada para "TechSoluciones Innovadoras", considerando el tamaño y recursos de la empresa.
4. **Análisis Cuantitativo vs. Cualitativo (Punto 10):**
    - Discuta las diferencias entre el análisis de riesgos cualitativo (basado en opiniones y escalas) y el cuantitativo (basado en cálculos de costo/probabilidad).
    - Explique cuándo y cómo cada enfoque podría ser útil para la gestión de seguridad de TechSoluciones.
5. **Creación de Escenarios (Punto 11):**
    - Cree un escenario de riesgo específico para el **SISTEMA B (Servidor de Desarrollo)** que requiera tomar decisiones de mitigación urgentes. Describa brevemente el ataque o interrupción.

**FASE 3: Priorización de Recursos y Estrategia**

En esta fase, tomará decisiones estratégicas bajo la restricción presupuestaria.

6. **Priorización de Recursos y Compromisos (Punto 3):**
    - Basándose en su Matriz CID de la Fase 1, priorice los cuatro sistemas del más crítico al menos crítico.
    - Asigne una porción del **5% del Presupuesto de Seguridad** a los sistemas A, B y C. Justifique la distribución, considerando cómo debe balancear las exigencias de seguridad (ej. control de acceso, cifrado) frente a las de recuperación (ej. copias de seguridad, redundancia).
    - *Ejemplo de asignación:* 40% a Sistema X, 30% a Sistema Y, etc.
7. **Herramientas de Seguridad y Estrategia Integral (Puntos 14 y 8):**
    - Investigue y proponga **dos herramientas de seguridad** (ej. *firewalls*, *antivirus*, *RBAC*) específicas para proteger el **SISTEMA C (Nóminas/RR.HH.)**.
    - Discuta la importancia de un **enfoque integral** para la seguridad de TechSoluciones, que combine estas herramientas tecnológicas con la formación del personal (factor humano) y la gestión de políticas (factor organizativo).

**FASE 4: Planificación de Mitigación y Respuesta a Incidentes**

En esta fase, diseñará respuestas a los riesgos.

8. **Desarrollo de un Plan de Control de Daños (Punto 4):**
    - Cree un **plan simple de control de daños** para una interrupción total del **SISTEMA A (CRM/Ventas)** (por ejemplo, fallo del disco duro o ataque de ransomware).
    - El plan debe incluir:

        - Medidas preventivas (ej. respaldos, redundancia).
        - Procedimientos para restaurar operaciones después de la falla.

9. **Plan de Acción y Mitigación Específica (Punto 12):**
    - Diseñe y presente un **Plan de Mitigación específico** para el escenario de riesgo que creó en el **Punto 5 (Sistema B).**
    - Su plan debe incluir al menos una **medida técnica** (ej. implementación de RBAC, cifrado de repositorios) y una **medida operacional** (ej. realización de ejercicios de recuperación o capacitación).

**FASE 5: Revisión y Lecciones Aprendidas**

En la fase final, aplicará el conocimiento a escenarios externos y propondrá la mejora continua.

10. **Ejemplos Prácticos y Casos Reales (Puntos 5 y 13):**
    - Investigue un **ejemplo real de un ciberataque** ocurrido en los últimos tres años (ej. *filtración de datos*, *ransomware* o *ataque de denegación de servicio*).
    - Describa brevemente el ataque y, utilizando las herramientas y principios vistos, discuta cómo el impacto de ese ataque pudo haber sido **evitado o mitigado** si hubiera afectado a TechSoluciones Innovadoras.

11. **Gestión Continua (Punto 6):**
    - Discuta cómo "TechSoluciones Innovadoras" puede implementar un ciclo de **mejora continua** para su gestión de riesgos y medidas de protección.
    - Mencione tres prácticas clave para garantizar que la gestión de riesgos no sea un proceso estático, incluyendo la adaptación a nuevas tecnologías y amenazas emergentes.

**Formato de Entrega:** El ejercicio debe entregarse como un informe escrito y estructurado, utilizando títulos y subtítulos claros para cada fase y punto.

**Extensión Recomendada:** Aproximadamente 1200 - 1500 palabras en total.