



UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES "ARAGÓN"

SISTEMAS DE INFORMACIÓN

ALUMNOS:

EMILIANO CARMONA RUIZ

OBET PEREZ HERNANDEZ

LEONARDO ARIEL ARRIAGA DIEGO

LIVEWORKSHEET

EQUIPO 5

LIVEWORKSHEETS

PARTE I.

Instrucciones: Selecciona únicamente la opción correcta para cada una de las siguientes preguntas.

1. ¿Qué estrategia de tratamiento de riesgo se está aplicando si una empresa decide contratar una póliza de seguro contra ciberataques o externalizar sus servidores a la nube?

(a) Mitigar

(b) Aceptar

(c) Transferir

2. Dentro de la Tríada de Seguridad de la Información (CID), ¿qué elemento garantiza que la información solo sea accesible para las personas autorizadas (por ejemplo, implementando el modelo Zero Trust)?

(a) Disponibilidad

(b) Confidencialidad

(c) Integridad

3. ¿Cuál es el enfoque principal de un Plan de Continuidad del Negocio (BCP)?

(a) Mantener las funciones críticas operando y generando ingresos durante una falla tecnológica.

(b) Reparar físicamente los servidores dañados por un desastre natural.

(c) Calcular el costo total de las licencias de software de la empresa.

LIVEWORKSHEETS

4. En la gestión de recursos financieros, ¿qué métrica se utiliza para evaluar no solo el precio de compra de un software, sino también sus costos de mantenimiento, capacitación y soporte a largo plazo?

(a) OPEX (Gasto Operativo)

(b) TCO (Costo Total de Propiedad)

(c) CAPEX (Gasto de Capital)

5. En los planes de recuperación, ¿qué indicador clave define el tiempo máximo que el negocio puede sobrevivir sin el sistema operativo antes de sufrir daños financieros irreparables?

(a) RPO (Objetivo de Punto de Recuperación)

(b) SLA (Acuerdo de Nivel de Servicio)

(c) RTO (Objetivo de Tiempo de Recuperación)

PARTE II.

Instrucciones: Une con una línea el concepto de la Columna A con su definición o ejemplo correcto en la Columna B

Columna A: Concepto		Columna B: Definición / Ejemplo
6. Riesgo Operativo		Asegurar que los datos sean precisos y no sufran alteraciones no autorizadas
7. Mitigar (Estrategia)		Define cuánta pérdida de datos históricos es tolerable antes de requerir un respaldo (backup)
8. Integridad (Tríada CID)		Fallas de hardware, caídas de red o errores humanos en la configuración

LIVEWORKSHEETS

9. OPEX (Recursos Financieros)		Implementar controles (ej. firewalls y capacitación) para disminuir la probabilidad del riesgo
10. RPO (Métrica de Continuidad)		Gasto operativo flexible, como pagar suscripciones mensuales por servicios en la nube

PARTE III.

Instrucciones: escoge la opción correcta de la lista desplegable para completar o responder cada inciso.

(11) ¿Qué tipo de riesgo de TI implica el incumplimiento de normativas (como el GDPR) que pueden generar multas y auditorías fallidas?

[Menú desplegable ▼]

-Riesgo Estratégico

-Riesgo Legal y de Cumplimiento (Compliance)

-Riesgo Operativo

(12) En la evaluación de riesgos, ¿qué tipo de evaluación asigna valores financieros reales calculando la expectativa de pérdida anual?

[Menú desplegable ▼]

-Evaluación Cualitativa

-Evaluación Cuantitativa

-Evaluación Estratégica

LIVEWORKSHEETS

(13) ¿Qué elemento de la Tríada CID se encarga de mantener los sistemas y servidores accesibles para el negocio en todo momento, mitigando ataques DDoS?

[Menú desplegable ▼]

-Confidencialidad

-Integridad

-Disponibilidad)

(14) En la administración de recursos humanos de TI, ¿qué práctica es crucial para evitar fraudes internos y reducir la dependencia de "personal clave"?

[Menú desplegable ▼]

-Segregación de funciones (SoD)

-Transición de CAPEX a OPEX

-Evaluación cualitativa)

(15) ¿Qué plan es un subconjunto técnico diseñado específicamente para que el equipo de TI restaure los servidores, redes y bases de datos tras un desastre?

[Menú desplegable ▼]

-BCP (Business Continuity Plan)

-DRP (Disaster Recovery Plan)

-SLA (Service Level Agreement))

LIVEWORKSHEETS