UNIVERSIDAD NACIONAL AUTÓNOMA DE

MÉXICO FACULTAD DE ESTUDIOS SUPERIORES

ARAGÓN

INSTRUCCIONES GENERALES:

Lee con atención cada sección y resuelve los 15 reactivos
interactivos. Revisa tus respuestas antes de hacer clic en "Terminar".

SECCIÓN I. OPCIÓN MÚLTIPLE

Instrucciones: Haz clic sobre la letra correspondiente a la respuesta correcta.

1. ¿Cuál es el primer paso crítico en el ciclo de gestión de riesgos de TI, según normas como ISO 31000 e ISO/IEC 27005?

a) Contratar una póliza de seguro de ciberseguridad antes de evaluar cualquier amenaza.

b) La identificación precisa y exhaustiva de amenazas y vulnerabilidades, apoyada en un inventario de activos.

c) Eliminar todos los sistemas heredados de la organización.

d) Aceptar formalmente todos los riesgos con una firma de la alta dirección.

Equipo 13
Marlon Giovanni Cortés Sepúlveda
Iván roberto Cruz Trejo
Salvador Flores Hernandez

LIVEWORKSHEETS

2. ¿Qué busca la evaluación cuantitativa de riesgos tecnológicos?

a) Clasificar las amenazas únicamente con escalas descriptivas como Bajo, Medio o Alto.

b) Sustituir el inventario de activos por una matriz de colores.

c) Asignar un valor monetario directo a las posibles pérdidas y a los costos de mitigación.

d) Eliminar el juicio de expertos de la gestión de riesgos.

3. ¿Qué componentes integran la Tríada CIA de la seguridad de la información?

a) Control, Inventario y Auditoría.

b) Cifrado, Identidad y Acceso.

c) Continuidad, Impacto y Análisis.

d) Confidencialidad, Integridad y Disponibilidad.

Equipo 13
Marlon Giovanni Cortés Sepúlveda
Iván roberto Cruz Trejo
Salvador Flores Hernandez

LIVEWORKSHEETS

SECCIÓN II. UNIR CON FLECHAS

Instrucciones: Arrastra una flecha desde cada estrategia de tratamiento de riesgos hasta su definición correcta.

4. Mitigar (o Reducir)	⚫	⚫ Implementar controles físicos, técnicos o administrativos para disminuir la probabilidad o el impacto de la amenaza.
5. Transferir (o Compartir)	⚫	⚫ Trasladar el impacto financiero del riesgo a un tercero, por ejemplo, mediante un seguro de ciberseguridad.
6. Evitar	⚫	⚫ Detener o no iniciar la actividad que genera el riesgo.

Equipo 13
Marlon Giovanni Cortés Sepúlveda
Iván roberto Cruz Trejo
Salvador Flores Hernandez

LIVEWORKSHEETS

SECCIÓN III. COMPLETAR MEDIANTE LISTA DESPLEGABLE

Instrucciones: Despliega el menú en cada espacio y selecciona el término correcto.

7. La evaluación cualitativa utiliza matrices de riesgo que cruzan la probabilidad de ocurrencia de un evento con el [ ] potencial en el negocio.

8. Cuando el costo de mitigar un riesgo supera las posibles pérdidas, la alta dirección puede [ ] formalmente el riesgo, dejando una decisión estrictamente documentada.

9. El principio de [ ] establece que cada usuario y sistema tiene únicamente los permisos estrictamente necesarios para cumplir su función.

10. El Plan de Continuidad del Negocio (BCP) inicia con el [ ], que identifica los procesos críticos y el impacto financiero y operativo de su interrupción.

Equipo 13
Marlon Giovanni Cortés Sepúlveda
Iván roberto Cruz Trejo
Salvador Flores Hernandez

LIVEWORKSHEETS

SECCIÓN IV. TEXTO EXACTO

Instrucciones: Escribe la palabra o siglas correctas en el recuadro asignado.

11. Escribe las siglas de la métrica que define cuánto tiempo puede tolerar el negocio que un sistema esté inactivo antes de sufrir daños irreversibles:

Respuesta: [ ]

12. Escribe las siglas en inglés de la métrica que proyecta el costo de un riesgo a lo largo de un año (Annualized Loss Expectancy):

Respuesta: [ ]

Equipo 13
Marlon Giovanni Cortés Sepúlveda
Iván roberto Cruz Trejo
Salvador Flores Hernandez

LIVEWORKSHEETS

SECCIÓN V. ARRASTRAR Y SOLTAR

Instrucciones: Arrastra la etiqueta de la caja de conceptos hacia su definición o recuadro correspondiente.

CAJA DE CONCEPTOS A ARRASTRAR:

[Shadow IT] **[DRP]** **[Zero Trust]**

13. Adopción de hardware o software por parte de los departamentos sin el conocimiento explícito del área de TI, lo que genera riesgos de seguridad e ineficiencias:

Respuesta: [ ].

14. Brazo técnico del BCP: manual paso a paso para restaurar servidores, redes, bases de datos y aplicaciones críticas mediante sitios alternos (Cold, Warm o Hot Sites):

Respuesta: [ ]

15. Arquitectura de seguridad que no confía por defecto en ninguna conexión, incluso si proviene del interior de la red corporativa:

Respuesta: [ ]

Equipo 13
Marlon Giovanni Cortés Sepúlveda
Iván roberto Cruz Trejo
Salvador Flores Hernandez

LIVEWORKSHEETS