PREGUNTAS – ACTIVIDAD SEMANA 1

1. ¿Cuál de los siguientes factores es **MÁS** importante determinar a la hora de definir estrategias de gestión de riesgos?

   A. Criterios de evaluación de riesgos
   B. Complejidad de la arquitectura de TI
   C. Un Plan de Recuperación de Desastres (PRD)
   D. Objetivos organizacionales

2. ¿Cuál de los siguientes elementos brinda la **MEJOR** perspectiva de la gestión de riesgo?
   A. Un equipo interdisciplinario
   B. Un proveedor externo de evaluación de riesgo
   C. El departamento de TI de la organización
   D. El departamento de cumplimiento de la organización

3. Una organización terceriza gran parte de su departamento de TI, y los servidores del proveedor están en otro país. ¿Cuál de las siguientes consideraciones acerca de la seguridad es la **MÁS** crítica?
   A. Las notificaciones de violación de la seguridad pueden retrasarse por la diferencia horaria.
   B. Deben instalarse sensores adicionales para detección de intrusos, lo que genera costos adicionales.
   C. Es posible que la organización no pueda monitorear el cumplimiento con sus pautas internas de seguridad y privacidad.
   D. Las leyes y regulaciones del país de origen pueden no aplicarse en el otro país.

4. ¿Cuál de los siguientes es el objetivo **PRINCIPAL** del programa de gestión de riesgo?
   A. Mantener el riesgo residual a un nivel aceptable
   B. Instaurar controles preventivos para todas las amenazas
   C. Eliminar todo el riesgo inherente
   D. Reducir el riesgo inherente a cero

5. ¿Cuál es el método **MÁS** eficaz para evaluar el impacto potencial de los requisitos jurídicos, regulatorios y contractuales en los objetivos de negocio?
   A. Un análisis de brecha orientado al cumplimiento.
   B. Entrevistas con las partes interesadas en los procesos de negocio.
   C. Un mapeo de los requisitos de cumplimiento de políticas y procedimientos.
   D. Un análisis de impacto en el negocio (BIA) orientado al cumplimiento.

6. La falta de controles adecuados representa:
   A. Una vulnerabilidad
   B. Un impacto
   C. Un activo

D. Una amenaza

7. El foco **PRINCIPAL** de gestionar el riesgo de negocios relacionado con TI es proteger:
   A. La información
   B. El hardware
   C. Las aplicaciones
   D. Las bases de datos

8. El objetivo **PRINCIPAL** de la gestión de riesgo de TI es:
   A. Prevenir la pérdida de activos de TI
   B. Presentar informes de gestión puntuales
   C. Garantizar el cumplimiento de la regulación
   D. Permitir que se tomen decisiones de negocios con conciencia del riesgo

9. Una organización se entera de una violación de la seguridad ocurrida en otra entidad que utiliza tecnología similar. La medida **MÁS** importante que debe tomar el profesional de riesgo es:
   A. Evaluar la probabilidad de que el mismo incidente ocurra en su organización
   B. Discontinuar el uso de la tecnología vulnerable
   C. Informar a la Alta Dirección de que la organización no se vio afectada
   D. Recordar al personal que no ocurrieron violaciones similares a la seguridad

10. ¿Cuál de las siguientes es la **MEJOR** técnica de identificación de riesgo para una organización que permite a sus empleados identificar el riesgo de manera anónima?
    A. La técnica Delphi
    B. Grupos piloto aislados
    C. Un análisis de fortalezas, debilidades, oportunidades y amenazas (FODA)
    D. Un análisis causa-raíz

TriLabs CYBERSEGURIDAD