**Seguridad de la información**

**Instrucción:** Es tiempo de validar el conocimiento y poner a prueba lo aprendido. Por ello, indique la opción que considera da respuesta a cada interrogante.

Pregunta 1: **¿Qué se conoce como riesgo?**

1. Posibilidad que ocurra un incidente.
2. Todo aquel suceso que ocurre.
3. Son los sucesos que no ocurren.
4. Sucesos ocurridos en un tiempo determinado.

**Retroalimentación positiva:** Muy bien, has acertado. Recuerda que un incidente es la posibilidad que un suceso ocurra y que podemos prevenirlo o mitigarlo.

**Retroalimentación negativa:** Lastimosamente no has acertado, te invitamos a repasar de nuevo el componente formativo en los conceptos de manejo de riesgos y contingencia.

Pregunta 2: **Según la matriz de riesgo trabajada a cuánto corresponde un riesgo de magnitud alta.**

1. 4
2. 3
3. 5
4. 6

**Retroalimentación positiva:** Muy bien, has acertado. Recuerda que en la escala de valoración este componente corresponde a un 4, esto debido a la incidencia y gravedad que se pueda presentar.

**Retroalimentación negativa:** Lastimosamente no has acertado, te invitamos a repasar el componente formativo en los conceptos de matriz de riesgo y su escala de valoración.

**Pregunta 3: ¿Qué se entiende por seguridad física?**

1. Conjunto de medidas que permiten garantizar el acceso y control de los lugares de la empresa y dispositivos y personas.
2. Conjunto de medidas para proteger solo el ingreso del personal a la empresa.
3. Conjunto de medidas que protegen las cámaras de seguridad y al personal que ingresa a la empresa.
4. Es todo lo que debo bloquear en la empresa para que no ingrese.

**Retroalimentación positiva:** Muy bien, has acertado. Recuerda que la seguridad física establece los controles para el acceso de dispositivos y lugares que se deben proteger dentro de la organización.

**Retroalimentación negativa:** Lastimosamente no has acertado, te invitamos a repasar el componente formativo en los conceptos seguridad física y control de acceso.

**Pregunta 4: ¿Cuáles son los tipos de riesgo que se contemplan en el estándar ISO 27001?**

1. Confidencialidad, Integridad, Disponibilidad.
2. Información, Datos personas.
3. Confidencialidad, Integridad e información.
4. Personas, confidencialidad, disponibilidad.

**Retroalimentación positiva:** Muy bien, has acertado, recuerda que los riesgos asociados de acuerdo al estándar ISO 27001 son la confidencialidad, disponibilidad e integridad de la información.

**Retroalimentación negativa:** Lastimosamente no has acertado, te invitamos a repasar el componente formativo en los conceptos del estándar ISO 27001.

Pregunta 5: ¿Qué es DRP?

1. Plan de recuperación de desastres.
2. Plan de recuperación en producción.
3. Plan de propiedad y recursos.
4. Plan de recursos y procesos.

**Retroalimentación positiva:** Muy bien, has acertado, tengamos en cuenta que DRP son las siglas de plan de recuperación de desastres.

**Retroalimentación negativa:** Lastimosamente no has acertado, te invitamos a repasar el componente formativo en los conceptos de Plan de recuperación de desastres y contingencias.

**Pregunta 6: ¿Cuáles son los niveles de contingencia de acuerdo a un DRP?**

1. Menor, Mayor, Catastrófica.
2. Terrible, Irrecuperable, Pérdida total.
3. Baja, Media, Alta.
4. Poca incidencia, Media incidencia, Alta incidencia.

**Retroalimentación positiva:** Muy bien, has acertado. Recordemos que para las empresas es importante establecer los niveles de contingencia ya que estos determinan la gravedad del suceso y su tratamiento.

**Retroalimentación negativa:** Lastimosamente no has acertado, te invitamos a repasar el componente formativo en los conceptos de niveles de contingencia en los DRP.

**Pregunta 7: ¿Cuántos principios tiene COBIT?**

1. 5
2. 6
3. 10
4. 4

**Retroalimentación positiva:** Muy bien, has acertado. Tengamos en cuenta que estos principios son la base fundamental de la administración de tecnología en la organización.

**Retroalimentación negativa:** Lastimosamente no has acertado, te invitamos a repasar el componente formativo en la temática COBIT y buenas prácticas en el uso de tecnología en las organizaciones.