



1. El objetivo principal de un programa de concientización sobre la seguridad informática es
- A) comunicar los procedimientos de seguridad.
  - B) proponer la gestión de riesgos como parte de todas las actividades del negocio.
  - C) fomentar la conciencia del riesgo potencial y la exposición. \*
  - D) evitar la divulgación de información confidencial en las redes sociales.

Referencia bibliográfica: Norma NTP-ISO/IEC 27002

2. Respecto de la Seguridad de Información, señale la alternativa INCORRECTA.
- A) No importa el tamaño de la empresa o el costo de las medidas de seguridad implantadas, toda organización necesita un Plan de Continuidad del Negocio.
  - B) Las empresas deben establecer un periodo de recuperación mínimo para garantizar la continuidad del negocio.
  - C) El SGSI debe ser revisado periódicamente para asegurar que se cumplan los objetivos marcados por la organización.
  - D) A mayores controles implementados en la organización, mayor será la seguridad y la eficiencia en la empresa. \*

Referencia bibliográfica: Norma NTP-ISO/IEC 27002

3. De acuerdo con las funciones de Gestión del Riesgo, marque la alternativa CORRECTA.
- A) El proceso de identificación de riesgos solo implica identificar algunos activos de información que tienen valor monetario para la organización.
  - B) Una amenaza se puede definir como cualquier evento que afecta los activos de información y se relaciona principalmente con recursos humanos o fallas técnicas.
  - C) Una adecuada gestión de riesgos es aquella que permite a las organizaciones conocer cuáles son algunas vulnerabilidades de sus activos.
  - D) No se puede eliminar totalmente el riesgo, ya que, muchas veces, no es posible ni rentable, solo se reduce su posibilidad de ocurrencia. \*

Referencia bibliográfica: Norma NTP-ISO/IEC 27002

4. Respecto de la NTP-ISO/IEC 27002, ¿qué alternativa corresponde al control Recolección de evidencia?
- A) Correctivo\*
  - B) Preventivo
  - C) Paliativo
  - D) Detectivo

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002



5. Respecto de la NTP-ISO/IEC 27002, ¿qué alternativa corresponde al control Monitoreo de seguridad física?

- A) Preventivo y correctivo
- B) Preventivo y detectivo\*
- C) Correctivo y detectivo
- D) Preventivo, correctivo y detectivo

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002

6. Respecto de la NTP-ISO/IEC 27002, ¿qué alternativa corresponde al control Actividades de monitoreo?

- A) Correctivo y preventivo
- B) Detectivo y preventivo
- C) Detectivo y correctivo\*
- D) Preventivo, correctivo y detectivo

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002

7. De acuerdo con la NTP-ISO/IEC 27002, ¿qué alternativa corresponde al control Protección contra *software* malicioso?

- A) Preventivo y correctivo
- B) Correctivo y detectivo
- C) Preventivo
- D) Preventivo, correctivo y detectivo\*

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002

8. Respecto de la NTP-ISO/IEC 27002, ¿qué alternativa corresponde a la propiedad de seguridad de la información bajo el control Preparación de las TIC para la continuidad del negocio?

- A) Disponibilidad\*
- B) Integridad
- C) Confidencialidad
- D) Responsabilidad

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002

9. De acuerdo con la NTP-ISO/IEC 27002, ¿qué alternativa corresponde a la propiedad de seguridad de la información bajo el control Eliminación segura o reutilización de equipos?

- A) Confidencialidad\*
- B) Disponibilidad
- C) Responsabilidad
- D) Integridad

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002



- 10.** Respecto de la NTP-ISO/IEC 27002, ¿qué alternativa corresponde a la propiedad de seguridad de la información bajo el control Sincronización de reloj?
- A) Responsabilidad
  - B) Confidencialidad
  - C) Integridad\*
  - D) Disponibilidad

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002

- 11.** De acuerdo con la NTP-ISO/IEC 27002, ¿qué alternativa corresponde a la propiedad de seguridad de la información bajo el control Servicios de suministro?
- A) Integridad y confidencialidad
  - B) Integridad y disponibilidad\*
  - C) Responsabilidad e integridad
  - D) Disponibilidad y confidencialidad

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002

- 12.** Respecto de la NTP-ISO/IEC 27002, ¿qué alternativa corresponde a la propiedad de seguridad de la información bajo el control Seguridad del cableado?
- A) Confidencialidad y disponibilidad\*
  - B) Disponibilidad y responsabilidad
  - C) Confidencialidad e integridad
  - D) Integridad y disponibilidad

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002

- 13.** De acuerdo con la NTP-ISO/IEC 27002, ¿qué alternativa corresponde a la propiedad de seguridad de la información bajo el control Gestión de la capacidad?
- A) Integridad y confidencialidad
  - B) Confidencialidad y disponibilidad
  - C) Disponibilidad e integridad\*
  - D) Responsabilidad y disponibilidad

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002

- 14.** Respecto de la NTP-ISO/IEC 27002, ¿qué alternativa corresponde a la propiedad de seguridad de la información bajo el control Respaldo de la información?
- A) Integridad y responsabilidad
  - B) Integridad y confidencialidad
  - C) Integridad y disponibilidad\*
  - D) Confidencialidad y disponibilidad



Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002

- 15.** Respecto de la NTP-ISO/IEC 27002, ¿qué alternativa corresponde a la propiedad de seguridad de la información bajo el control Trabajo remoto?
- A) Confidencialidad y disponibilidad
  - B) Confidencialidad e integridad
  - C) Disponibilidad y responsabilidad
  - D) Confidencialidad, integridad y disponibilidad\*

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002

- 16.** De acuerdo con la NTP-ISO/IEC 27001, ¿qué alternativa NO forma parte de la política de seguridad de la información?
- A) Los controles implementados\*
  - B) Los objetivos de seguridad de la información
  - C) El compromiso de mejora continua del SGSI
  - D) El compromiso de satisfacer los requisitos aplicables

Referencia bibliográfica: Sección 5 de la norma NTP-ISO/IEC 27001

- 17.** Respecto de la NTP-ISO/IEC 27001, ¿qué acción NO debe considerarse al programar una auditoría interna?
- A) Definir los criterios y el alcance de cada auditoría
  - B) Seleccionar a los auditores y conducir auditorías que aseguren objetividad e imparcialidad
  - C) Asegurar que los resultados de las auditorías se reporten a los gerentes
  - D) Implementar un único programa de auditoría, tomando en consideración la importancia de los procesos involucrados\*

Referencia bibliográfica: Sección 9 de la norma NTP-ISO/IEC 27001

- 18.** De acuerdo con la NTP-ISO/IEC 27001, ¿cuál sería la alternativa INCORRECTA al detectar una NO conformidad?
- A) Reaccionar a la NO conformidad, para controlarla y corregirla
  - B) Evaluar la necesidad de la acción necesaria para eliminar sus causas
  - C) Ocuparse de las consecuencias sin modificar el SGSI\*
  - D) Revisar la eficacia de cualquier acción correctiva tomada

Referencia bibliográfica: Sección 10 de la norma NTP-ISO/IEC 27001

- 19.** Respecto de la NTP-ISO/IEC 27001, ¿qué alternativa NO debe tomarse en cuenta por parte de las personas que trabajan bajo el control de la organización?
- A) La política de seguridad de información
  - B) La declaración de aplicabilidad\*
  - C) Su contribución a la eficacia del SGSI
  - D) Las implicancias de no tener conformidad con los requisitos del SGSI



20. Referencia bibliográfica: Sección 7 de la norma NTP-ISO/IEC 27001  
Respecto de la NTP-ISO/IEC 27002, ¿qué término de ciberseguridad se asocia al control Uso aceptable de información y otros activos asociados?
- A) Proteger\*
  - B) Identificar
  - C) Responder
  - D) Recuperar

Referencia bibliográfica: Tabla A.1 de la norma NTP-ISO/IEC 27002