



1. En concordancia con la NTP-ISO/IEC 27002, ¿qué tipo de control corresponde al control denominado roles y responsabilidades de seguridad de la información?

- A) Detectivo
- B) Correctivo
- C) Preventivo *
- D) Paliativo

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

2. Considerando la NTP-ISO/IEC 27002, ¿qué tipo de control corresponde al control denominado seguridad de la información en la gestión de proyectos?

- A) Correctivo
- B) Paliativo
- C) Detectivo
- D) Preventivo *

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

3. De acuerdo con la NTP-ISO/IEC 27002, ¿qué tipo de control corresponde al control denominado planificación y preparación de la gestión de incidentes de seguridad de la información?

- A) Paliativo
- B) Preventivo
- C) Detectivo
- D) Correctivo *

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

4. Considerando la NTP-ISO/IEC 27002, ¿qué tipo de control corresponde al control denominado respuesta a incidentes de seguridad de la información?

- A) Correctivo *
- B) Detectivo
- C) Preventivo
- D) Paliativo

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

5. En consonancia con la NTP-ISO/IEC 27002, ¿qué tipo de control corresponde al control denominado recolección de evidencia?

- A) Preventivo
- B) Correctivo *
- C) Paliativo
- D) Detectivo

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



6. Teniendo en cuenta la NTP-ISO/IEC 27002, ¿qué tipo de control corresponde al control denominado monitoreo de seguridad física?

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

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

7. En concordancia con la NTP-ISO/IEC 27002, ¿qué tipo de control corresponde al control denominado actividades de monitoreo?

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

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

8. De acuerdo con la NTP-ISO/IEC 27002, ¿qué propiedad de seguridad de la información corresponde al control denominado 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. Considerando la NTP-ISO/IEC 27002, ¿qué propiedad de seguridad de la información corresponde al control denominado 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. Con respecto a la NTP-ISO/IEC 27002, ¿qué propiedad de seguridad de la información corresponde al control denominado sincronización de reloj?

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

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



11. En relación con la NTP-ISO/IEC 27002, ¿qué propiedad de seguridad de la información corresponde al control denominado seguridad del cableado?

- A) Disponibilidad y responsabilidad
- B) Confidencialidad y disponibilidad *
- C) Confidencialidad e integridad
- D) Integridad y disponibilidad

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

12. En consonancia con la NTP-ISO/IEC 27002, ¿qué propiedad de seguridad de la información corresponde al control denominado gestión de la capacidad?

- A) Disponibilidad e integridad *
- B) Integridad y confidencialidad
- C) Confidencialidad y disponibilidad
- D) Responsabilidad y disponibilidad

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

13. De acuerdo con la NTP-ISO/IEC 27002, ¿qué propiedad de seguridad de la información corresponde al control denominado 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

14. Teniendo en cuenta la NTP-ISO/IEC 27001, ¿qué elemento NO debe formar parte de la declaración de aplicabilidad?

- A) La necesidad de implementar los controles necesarios
- B) La justificación para la inclusión de los controles necesarios
- C) Las opciones de tratamiento de riesgos de seguridad de la información *
- D) La justificación de excluir controles del Anexo A

Referencia bibliográfica: Sección 6 de la norma NTP-ISO/IEC 27001

15. Con respecto a la NTP-ISO/IEC 27001, ¿qué elemento NO debe formar parte de la política de seguridad de la información?

- A) Los objetivos de seguridad de la información
- B) El compromiso de mejora continua del Sistema de Gestión de Seguridad de la Información
- C) El compromiso de satisfacer los requisitos aplicables
- D) Los controles implementados *

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



- 16.** De acuerdo con la NTP-ISO/IEC 27001, ¿qué acción NO debe considerarse al definir y aplicar un proceso de evaluación del riesgo de seguridad de la información?
- A) Valorar los riesgos para el tratamiento de riesgos, sin priorización *
 - B) Asegurar que las evaluaciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables
 - C) Identificar los riesgos de seguridad de la información, identificando a los responsables de los riesgos
 - D) Analizar los riesgos de seguridad de la información, determinando los niveles de riesgo

Referencia bibliográfica: Sección 6 de la norma NTP-ISO/IEC 27001

- 17.** En concordancia con 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.** Con respecto a la NTP-ISO/IEC 27001, ¿qué acción NO debe considerarse 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 Sistema de Gestión de Seguridad de la Información *
 - D) Revisar la eficacia de cualquier acción correctiva tomada

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

- 19.** Considerando la NTP-ISO/IEC 27001, ¿qué elemento 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 Sistema de Gestión de Seguridad de la Información
 - D) La conformidad de los requisitos del Sistema de Gestión de Seguridad de la Información

Referencia bibliográfica: Sección 7 de la norma NTP-ISO/IEC 27001



- 20.** Con relación a la NTP-ISO/IEC 27002, ¿qué concepto de ciberseguridad se asocia al control denominado 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