Comenzado el	miércoles, 15 de noviembre de 2023, 15:15
Estado	Finalizado
Finalizado en	miércoles, 15 de noviembre de 2023, 15:35
Tiempo empleado	19 minutos 54 segundos
Puntos	40,00/40,00
Calificación	**100,00** de 100,00

Pregunta 1

Correcta

Se puntúa 1,00 sobre 1,00

En la mejora del sistema de gestión cuando ocurra una no conformidad, la organización debe: (elija dos opciones)

- [x] a. si es necesario, hacer cambios al sistema de gestión de la seguridad de la información. ✔
- [ ] b. se entiendan la complejidad de los procesos de la organización
- [ ] c. controlar los cambios de arquitectura de software
- [x] d. revisar la eficacia de las acciones correctivas llevadas a cabo ✔

Las respuestas correctas son: revisar la eficacia de las acciones correctivas llevadas a cabo, si es necesario, hacer cambios al sistema de gestión de la seguridad de la información.

Pregunta 2

Correcta

Se puntúa 1,00 sobre 1,00

Cuando se determina el alcance del sistema de gestión de la seguridad de la información la organización debe considerar:

a. Las cuestiones externas e internas, los requisitos y las interfaces y las dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones. ✔

b. Las referencias del departamento de sistemas y los requisitos para la implementación de un nuevo proyecto software.

c. Algunas veces es necesaria la comprensión de la organización dependiendo el entorno

d. La organización no debe determinar nada

La respuesta correcta es: Las cuestiones externas e internas, los requisitos y las interfaces y las dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones.

Pregunta 3

Correcta

Se puntúa 1,00 sobre 1,00

La organización debe conservar información documentada sobre los objetivos de seguridad de la información. Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar: (elija dos opciones)

- a. Referenciarsen al departamento de sistemas para la implementación de un nuevo proyecto software con estándares internacionales.
- b. Ser coherentes con la política de seguridad de la información ser medibles (si es posible), ser comunicados y ser actualizados ✔
- c. Tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos. ✔
- d. No es necesario determinar los objetivos de seguridad

Las respuestas correctas son: Ser coherentes con la política de seguridad de la información ser medibles (si es posible), ser comunicados y ser actualizados, Tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos.

Pregunta 4

Correcta

Se puntúa 1,00 sobre 1,00

¿Cuál es el nuevo nombre de la norma ISO27001:2022?

a. ISO/IEC 27001Information technology — Security — Information - management systems — Requirements

b. ISO/IEC 27001 Information security, privacy protection — Information security management systems — Requirements

c. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

d. ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements ✔

La respuesta correcta es: ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Pregunta 5

Correcta

Se puntúa 1,00 sobre 1,00

¿Por qué razón fue actualizado el nombre de la norma ISO27001 en el año 2022?

a. Se realiza un cambio en el nombre del comité que desarrolla la norma y como consecuencia se realiza una actualización en el nombre por formalidad. ✔

b. El nombre de la norma ISO no fue actualizado en el año 2022

c. Se realiza un cambio en toda la estructura de la norma y como consecuencia se realiza una actualización en el nombre.

d. Se realiza un cambio en el comité que desarrolla la norma y como consecuencia se genera una nueva estructura.

La respuesta correcta es: Se realiza un cambio en el nombre del comité que desarrolla la norma y como consecuencia se realiza una actualización en el nombre por formalidad.

Pregunta 6

Correcta

Se puntúa 1,00 sobre 1,00

La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información cumple con: (elija dos opciones)

- a. Los requisitos de la norma internacional ISO 27001 ✔
- b. Asegurar la política de reuniones diarias para identificar la razón de posibles retrasos
- c. Reorganizar los procesos de la organización
- d. Los requisitos propios de la organización para su sistema de gestión de la seguridad de la información ✔

Las respuestas correctas son: Los requisitos propios de la organización para su sistema de gestión de la seguridad de la información, Los requisitos de la norma internacional ISO 27001

Pregunta 7

Correcta

Se puntúa 1,00 sobre 1,00

De acuerdo al Anexo A (Normativo) Los objetivos de control y controles de referencia de la Norma ISO/IEC 27002:2022, el "Control" para el control de acceso al código fuente de los programas es:

a. Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión

b. Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.

c. Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

d. Se debe restringir el acceso al código fuente de los programas. ✔

La respuesta correcta es: Se debe restringir el acceso al código fuente de los programas.

Pregunta 8

Correcta

Se puntúa 1,00 sobre 1,00

De acuerdo al Anexo A (Normativo) Los objetivos de control y controles de referencia de la Norma ISO/IEC 27002:2022, el "Control" para los procedimientos seguros de inicio de sesión es:

a. Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.

b. Los derechos de acceso de todos los empleados y terceras partes, la información y los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, el contrato o el acuerdo, el caso de cambio.

c. Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

d. Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión ✔

La respuesta correcta es: Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión

Pregunta 9

Correcta

Se puntúa 1,00 sobre 1,00

La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información. La organización debe realizar: (elija dos opciones)

- a. asegurar la política de reuniones diarias para identificar la razón de posibles retrasos
- b. seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría; ✔
- c. Reorganizar los procesos de la organización
- d. para cada auditoría, definir sus criterios y su alcance; ✔

Las respuestas correctas son: para cada auditoría, definir sus criterios y su alcance;, seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;

Pregunta 10

Correcta

Se puntúa 1,00 sobre 1,00

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.

a. No es necesaria la comprensión de la organización

b. Algunas veces es necesaria la comprensión de la organización dependiendo el entorno

c. Si, es necesaria la comprensión de la organización ✔

d. La organización no debe determinar nada

La respuesta correcta es: Si, es necesaria la comprensión de la organización

Pregunta 11

Correcta

Se puntúa 1,00 sobre 1,00

La información documentada requerida por el sistema de gestión de la seguridad de la información y por la norma internacional ISO 27001 se debe controlar para asegurarse que: (Elija dos opciones)

- a. esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad). ✔
- b. se entiendan la complejidad de los procesos de la organización
- c. esté disponible y preparada para su uso, dónde y cuándo se necesite; ✔
- d. las interacciones y la competencia de las personas.

Las respuestas correctas son: esté disponible y preparada para su uso, dónde y cuándo se necesite;, esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Pregunta 12

Correcta

Se puntúa 1,00 sobre 1,00

El alcance de la información documentada para un sistema de gestión de la seguridad de la información puede ser diferente de una organización a otra, debido a:

- a. la complejidad de los procesos y sus interacciones, y, la competencia de las personas. ✔
- b. No asegurar una política de reuniones diarias para identificar la razón de posibles retrasos
- c. No realizar reuniones semanales con actas de seguimiento
- d. el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios. ✔

Las respuestas correctas son: el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios., la complejidad de los procesos y sus interacciones, y, la competencia de las personas.

Pregunta 13

Correcta

Se puntúa 1,00 sobre 1,00

La alta dirección debe asegurarse que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización. La alta dirección debe asignar la responsabilidad y autoridad para. Elija dos opciones.

- a. informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información. ✔
- b. Garantizar dentro de la política investigación científica.
- c. asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de la norma internacional ISO 27001 ✔
- d. Garantizar que sea firmada por entidades gubernamentales

Las respuestas correctas son: asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de la norma internacional ISO 27001, informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información.

Pregunta 14

Correcta

Se puntúa 1,00 sobre 1,00

La organización debe definir y aplicar un proceso de apreciación de riesgos de seguridad de la información que: (elija dos opciones)

- a. asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables. ✔
- b. Prevenga o reduzca efectos secundarios
- c. Logre la proyección e internacionalización de los procesos de la organización
- d. establezca y mantenga criterios sobre riesgos de seguridad de la información ✔

Las respuestas correctas son: establezca y mantenga criterios sobre riesgos de seguridad de la información, asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables.

Pregunta 15

Correcta

Se puntúa 1,00 sobre 1,00

Es importante que el sistema de gestión de la seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

a. No, porque al implementar el sistema de gestión de la seguridad de la información no se espera en que se ajusten las necesidades de la organización.

b. No, porque al implementar el sistema de gestión de la seguridad de la información no se espera que se ajuste a las necesidades de la organización.

c. Si, porque al implementar el sistema de gestión de la seguridad de la información lo que se espera es que se ajuste a las necesidades de la organización. ✔

d. Ninguna de las opciones

La respuesta correcta es: Si, porque al implementar el sistema de gestión de la seguridad de la información lo que se espera es que se ajuste a las necesidades de la organización.

Pregunta 16

Correcta

Se puntúa 1,00 sobre 1,00

La norma internacional ISO 27001 especifica los requisitos para el establecimiento, la implementación, el mantenimiento y la mejora continua del sistema de gestión de la seguridad de la información en el contexto de la organización

---

La norma internacional ISO 27001 especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información en el contexto de la organización

Seleccione una:

- Verdadero ✔
- Falso

La respuesta correcta es 'Verdadero'

Pregunta 17

Correcta

Se puntúa 1,00 sobre 1,00

En la nueva versión de la norma ISO27001:2022 se introducen nuevas sub-cláusulas

Seleccione una:

- Verdadero ✔
- Falso

La respuesta correcta es 'Verdadero'

Pregunta 18

Correcta

Se puntúa 1,00 sobre 1,00

De acuerdo al Anexo A (Normativo) Los objetivos de control y controles de referencia de la Norma ISO/IEC 27002:2022, el "Control" para la segregación de tareas es:

a. la seguridad de tecnología de la información (TI)

b. Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización. ✔

c. el costo de implementar el sistema de gestión

d. Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas

La respuesta correcta es: Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

Pregunta 19

Correcta

Se puntúa 1,00 sobre 1,00

De acuerdo al Anexo A (Normativo) Los objetivos de control y controles de referencia de la Norma ISO/IEC 27002:2022, el "Control" para las Políticas de seguridad de la información es:

a. El tiempo que toma la implementación de la norma ISO 27001

b. el costo de implementar el sistema de gestión

c. la seguridad de tecnología de la información (TI)

d. Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes ✔

La respuesta correcta es: Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes

Pregunta 20

Correcta

Se puntúa 1,00 sobre 1,00

¿La siguiente afirmación es verdadera?
La nueva versión de la norma ISO27001:2022 es menos restrictiva y está enfocada en proporcionar una guía para la toma de decisiones basadas en riesgos.

Seleccione una:

- Verdadero ✔
- Falso

La respuesta correcta es 'Verdadero'

Pregunta 21

Correcta

Se puntúa 1,00 sobre 1,00

De acuerdo al Anexo A (Normativo) Los objetivos de control y controles de referencia de la Norma ISO/IEC 27002:2022, el "Control" para la restricción del acceso a la información es:

a. Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida. ✔

b. Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.

c. Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

d. Los derechos de acceso de todos los empleados y terceras partes, la información y los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, el contrato o el acuerdo, el caso de cambio.

La respuesta correcta es: Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.

Pregunta 22

Correcta

Se puntúa 1,00 sobre 1,00

Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar como determinar los riesgos y oportunidades que es necesario tratar con el fin de: (Elija dos opciones.)

- a. Prevenir o reducir efectos indeseados ✔
- b. Referenciar al departamento de sistemas los requisitos para la implementación de un nuevo proyecto software.
- c. Lograr la mejora continua ✔
- d. No es necesario determinar los riesgos

Las respuestas correctas son: Prevenir o reducir efectos indeseados, Lograr la mejora continua

Pregunta 23

Correcta

Se puntúa 1,00 sobre 1,00

La organización debe definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información para: (elija dos opciones)

- a. determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información ✔
- b. Seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos ✔
- c. No es necesario determinar los riesgos
- d. Referenciar al departamento de sistemas los requisitos para la implementación de un nuevo proyecto software.

Las respuestas correctas son:
Seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos, determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información

Pregunta 24

Correcta

Se puntúa 1,00 sobre 1,00

Los métodos seleccionados del seguimiento, medición, análisis y evaluación deben producir resultados comparables y reproducibles para ser considerados válidos. (Elija todas las que aplica.)

- a. quién debe hacer el seguimiento y la medición ✔
- b. cuándo se deben llevar a cabo el seguimiento y la medición ✔
- c. cuándo se deben analizar y evaluar los resultados del seguimiento y la medición. ✔
- d. quién debe analizar y evaluar esos resultados. ✔

Las respuestas correctas son: cuándo se deben llevar a cabo el seguimiento y la medición, quién debe hacer el seguimiento y la medición, cuándo se deben analizar y evaluar los resultados del seguimiento y la medición., quién debe analizar y evaluar esos resultados.

Pregunta 25

Correcta

Se puntúa 1,00 sobre 1,00

De acuerdo al Anexo A (Normativo) Los objetivos de control y controles de referencia de la Norma ISO/IEC 27001:2022, el "Control" para la revisión de las políticas para la seguridad de la información es:

a. Planificar la implementación de la norma BS 25999-2

b. Planificar la implementación de la norma ISO 9001 e ISO 22301

c. Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia. ✔

d. El tiempo que toma la implementación de la norma ISO 27001

La respuesta correcta es: Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Pregunta 26

Correcta

Se puntúa 1,00 sobre 1,00

La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas. La revisión por la dirección debe incluir consideraciones sobre: (elija dos opciones)

- a. los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información; ✔
- b. Reorganizar los procesos de la organización
- c. el estado de las acciones desde anteriores revisiones por la dirección; ✔
- d. asegurar la política de reuniones diarias para identificar la razón de posibles retrasos

Las respuestas correctas son: el estado de las acciones desde anteriores revisiones por la dirección;, los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información;

Pregunta 27

Correcta

Se puntúa 1,00 sobre 1,00

De acuerdo al Anexo A (Normativo) Los objetivos de control y controles de referencia de la Norma ISO/IEC 27002:2022, el "Control" para establecer los roles y responsabilidades en seguridad de la información es:

a. la seguridad de tecnología de la información (TI)

b. El tiempo que toma la implementación de la norma ISO 27001

c. Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas ✔

d. el costo de implementar el sistema de gestión

La respuesta correcta es: Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas

Pregunta 28

Correcta

Se puntúa 1,00 sobre 1,00

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información. La organización debe determinar:

a. se entiendan la complejidad de los procesos de la organización

b. los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos; ✔

c. Reorganizar los procesos de la organización

d. a qué es necesario hacer seguimiento y qué es necesario medir, incluyendo procesos y controles de seguridad de la información; ✔

Las respuestas correctas son: a qué es necesario hacer seguimiento y qué es necesario medir, incluyendo procesos y controles de seguridad de la información;, los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos;

Pregunta 29

Correcta

Se puntúa 1,00 sobre 1,00

Las acciones correctivas encontradas en el sistema de gestión deben ser adecuadas a los efectos de las no conformidades encontradas. La organización debe conservar información documentada, como evidencia de: (elija dos opciones)

- a. los resultados de cualquier acción correctiva ✔
- b. el costo de implementar el sistema de gestión
- c. la naturaleza de las no conformidades y cualquier acción posterior llevada a cabo ✔
- d. la seguridad de tecnología de la información (TI)

Las respuestas correctas son: la naturaleza de las no conformidades y cualquier acción posterior llevada a cabo, los resultados de cualquier acción correctiva

Pregunta 30

Correcta

Se puntúa 1,00 sobre 1,00

El sistema de gestión de la seguridad de la información no preserva la confidencialidad, ni la integridad ni la disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos.

Seleccione una:

- Verdadero
- Falso ✔

La respuesta correcta es 'Falso'

Pregunta 31

Correcta

Se puntúa 1,00 sobre 1,00

De acuerdo con los requisitos de la norma internacional ISO 27001, La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información:

a. Nunca
b. No aplica
c. Siempre ✔
d. Algunas veces

La respuesta correcta es: Siempre

Pregunta 32

Correcta

Se puntúa 1,00 sobre 1,00

El sistema de gestión de la seguridad de la información de la organización debe incluir: (elija dos opciones)

- a. Realizar reuniones semanales con actas de seguimiento
- b. la información documentada requerida por la norma internacional ISO 27001 ✔
- c. la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información. ✔
- d. Asegurar una política de reuniones diarias para identificar la razón de posibles retrasos

Las respuestas correctas son: la información documentada requerida por la norma internacional ISO 27001, la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información.

Pregunta 33

Correcta

Se puntúa 1,00 sobre 1,00

De acuerdo al Anexo A (Normativo) Los objetivos de control y controles de referencia de la Norma ISO/IEC 27002:2022, el “Control” para el uso de la información secreta de autenticación es:

a. Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación. ✔

b. Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.

c. Los derechos de acceso de todos los empleados y terceras partes, la información y los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, el contrato o el acuerdo, el caso de cambio.

d. La asignación y el uso de privilegios de acceso debe estar restringida y controlada.

La respuesta correcta es: Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

Pregunta 34

Correcta

Se puntúa 1,00 sobre 1,00

Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable: (elija dos opciones)

- a. se entiendan la complejidad de los procesos de la organización
- b. control de cambios ✔
- c. distribución, acceso, recuperación y uso ✔
- d. Reorganizar los procesos de la organización

Las respuestas correctas son: distribución, acceso, recuperación y uso, control de cambios

Pregunta 35

Correcta

Se puntúa 1,00 sobre 1,00

La adopción de un sistema de gestión de la seguridad de la información es una decisión estratégica para una organización.

- a. Si, siempre y cuando se implemente. ✔
- b. No, existen otros sistemas más estratégicos
- c. No, la norma internacional ISO 27001 se puede adoptar como solo consulta
- d. Si, siempre y cuando la organización pertenezca a la industria

La respuesta correcta es: Si, siempre y cuando se implemente.

Pregunta 36

Correcta

Se puntúa 1,00 sobre 1,00

La organización debe conservar la información sobre los objetivos de seguridad de la información. Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar: (elija dos opciones)

- a. cuándo se finalizará y cómo se evaluarán los resultados. ✔
- b. Como empoderar los equipos de desarrollo de software
- c. Como el implementador del sistema de gestión se centre mas en evitar que la alta Dirección cambie las prioridades
- d. lo que se va a hacer; qué recursos se requerirán y quién será responsable ✔

Las respuestas correctas son: lo que se va a hacer; qué recursos se requerirán y quién será responsable, cuándo se finalizará y cómo se evaluarán los resultados.

Pregunta 37

Correcta

Se puntúa 1,00 sobre 1,00

Cuando se crea y actualiza la información documentada, la organización debe asegurarse, en la manera que corresponda, de lo siguiente: (Elija tres opciones)

- [x] a. review and approval with respect to suitability and adequacy.

  ---

  la revisión y aprobación con respecto a la idoneidad y adecuación.

- [ ] b. el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios.
- [x] c. la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia)
- [ ] d. la complejidad de los procesos y sus interacciones, y, la competencia de las personas.
- [x] e. el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico)

Las respuestas correctas son: la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia), el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico), review and approval with respect to suitability and adequacy.

---

la revisión y aprobación con respecto a la idoneidad y adecuación.

Pregunta 38

Correcta

Se puntúa 1,00 sobre 1,00

Elija dos aspectos que debe garantizar la política de seguridad de la información

- a. Garantizar que sea firmada por entidades gubernamentales
- b. Garantizar dentro de la política investigación científica.
- c. comunicarse dentro de la organización ✔
- d. Estar disponible como información documentada ✔

Las respuestas correctas son: Estar disponible como información documentada , comunicarse dentro de la organización

Pregunta 39

Correcta

Se puntúa 1,00 sobre 1,00

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan:

a. El contenido de la comunicación cuándo comunicar a quién comunicar; quién debe comunicar; los procesos por los que debe efectuarse la comunicación ✔

b. cuándo se finalizará y cómo se evaluarán los resultados.

c. Lo que se va a hacer; qué recursos se requerirán y quién será responsable

d. Como el implementador del sistema de gestión se centre mas en evitar que la alta Dirección cambie las prioridades

La respuesta correcta es: El contenido de la comunicación cuándo comunicar a quién comunicar; quién debe comunicar; los procesos por los que debe efectuarse la comunicación

Pregunta 40

Correcta

Se puntúa 1,00 sobre 1,00

¿Con que periodicidad la organización ISO revisa sus estándares?

a. La vida útil típica de una norma ISO es de seis años.

b. La vida útil típica de una norma ISO es de un año.

c. La vida útil típica de una norma ISO es de cinco años. ✔

d. La vida útil típica de una norma ISO es de dos años.

La respuesta correcta es: La vida útil típica de una norma ISO es de cinco años.