

Comenzado el jueves, 30 de noviembre de 2023, 21:09

Estado Finalizado

Finalizado en jueves, 30 de noviembre de 2023, 21:47

Tiempo empleado 37 minutos 44 segundos

Calificación 57,00 de 57,00 (100%)

Pregunta **1**

Correcta

Se puntúa 3,00 sobre 3,00

En la ISO de 27000 la declaración de aplicabilidad, es una pre-evaluación si es que se puede o no aplicar la ISO en la empresa.

Seleccione una:

- ☐ Verdadero
- ☒ Falso ✓

La declaración de aplicabilidad es la revisión de si se puede implemetar cada uno de los controles de la ISO en el contexto de la organización.


La respuesta correcta es 'Falso'




Pregunta **2**





Correcta

Se puntúa 10,00 sobre 10,00

El nivel de  comunica las prioridades de la misión, los recursos disponibles y la tolerancia general al riesgo al nivel de  .

En esencia, la  es el proceso de desarrollo de un programa de seguridad que satisfaga adecuadamente las necesidades estratégicas de la empresa.

El nivel de  utiliza la información como insumos en el proceso de  que realiza el programa de seguridad. Luego colabora con el nivel de  para comunicar los requisitos de seguridad y crear un perfil de ciberseguridad.

El nivel de  integra este perfil en el ciclo de vida de desarrollo del sistema y supervisa continuamente el rendimiento de la seguridad. Ejecuta o gestiona diariamente los procesos relacionados con la seguridad de la infraestructura actual. El nivel de  utiliza la información de supervisión para evaluar el perfil actual e informa de los resultados de esa evaluación al nivel de  para informar del proceso general de  de la organización.

Respuesta correcta

La respuesta correcta es:

El nivel de [gobernanza de la seguridad de la información] comunica las prioridades de la misión, los recursos disponibles y la tolerancia general al riesgo al nivel de [gestion de la seguridad de la información].

En esencia, la [gobernanza de la seguridad de la información] es el proceso de desarrollo de un programa de seguridad que satisfaga adecuadamente las necesidades estratégicas de la empresa.

El nivel de [gestion de la seguridad de la información] utiliza la información como insumos en el proceso de [gestión de riesgos] que realiza el programa de seguridad. Luego colabora con el nivel de [implementación/operaciones] para comunicar los requisitos de seguridad y crear un perfil de ciberseguridad.

El nivel de [implementación/operaciones] integra este perfil en el ciclo de vida de desarrollo del sistema y supervisa continuamente el rendimiento de la seguridad. Ejecuta o gestiona diariamente los procesos relacionados con la seguridad de la infraestructura actual. El nivel de [gestion de la seguridad de la información] utiliza la información de supervisión para evaluar el perfil actual e informa de los resultados de esa evaluación al nivel de [gobernanza de la seguridad de la información] para informar del proceso general de [gestión de riesgos] de la organización.

Pregunta **3**

Correcta

Se puntúa 5,00 sobre 5,00

Las siguientes son características de solamente un análisis de riesgos cuantitativo (y no cualitativo):

- i. Se asignan números y valores monetarios
- ii. Se pueden llegar a evaluar muchas amenazas sobre los activos identificados
- iii. Permite priorizar las acciones necesarias para mitigar los riesgos mayores.
- iv. Se pueden utilizar diferentes técnicas para obtener datos, entre ellas: tormentas de ideas, reuniones, entrevistas, delphi, entre otras.
- v. Se requieren datos históricos o estadísticos

Seleccione una:

- ☐ a. ii, iii, iv
- ☐ b. i, ii y iii
- ☐ c. i, ii, iii, iv, v
- ☐ d. i, ii, iii, iv
- ☒ e. i y v ✓

Respuesta correcta

La respuesta correcta es: i y v

Pregunta **4**

Correcta

Se puntúa 3,00 sobre 3,00

A la hora de implementar un estándar de seguridad de la información en una organización, lo debo aplicar completamente. Si no lo aplico de esta forma, no podré certificar la organización en el estándar.

Seleccione una:

- ☐ Verdadero
- ☒ Falso ✓

Ninguna organización va a colocar todos los estándares vistos anteriormente en práctica.

Pero estas son buenos toolbox de donde sacar las herramientas adecuadas para nuestra organización.

A medida que el programa de seguridad madura, se van utilizando.

Toda organización es distinta, pero todas están compuestas de gente, procesos, datos y tecnologías y cada una de ellos debe ser protegidos.

La respuesta correcta es 'Falso'

Pregunta **5**

Correcta

Se puntúa 3,00 sobre 3,00

La seguridad a través de la oscuridad se refiere a que mis enemigos no son tan listos como uno, por lo que ocultando el como se hacen las cosas, es suficiente para proteger mis activos de información críticos.

Seleccione una:

- ☒ Verdadero ✓
- ☐ Falso

Seguridad a través de la oscuridad (se asume que mis enemigos no son tan listos como uno).

Ej:

- Un vendedor que diga que sus productos son mejores que uno opensource, ya que los de él son compilados y no se puede ver el código fuente.
- Un algoritmo criptográfico hecho en casa (Lo mejor es utilizar algoritmos ampliamente reconocidos)
- Remapear puertos (fácilmente detectable con herramientas)

La respuesta correcta es 'Verdadero'

Pregunta **6**

Correcta

Se puntúa 5,00 sobre 5,00

Seguridad de la información versus Tecnología

Indique cual de las siguientes afirmaciones es correcta:

- i. El objetivo de una empresa es lucro, por lo tanto, no se puede anteponer la seguridad a tal fin.
- ii. No se debe considerar la seguridad de la información en el caso que esta retrase el lanzamiento de un servicio que traerá muchos dividendos a la empresa.
- iii. En el caso de una empresa que quiera implementar una política BYOD para bajar sus costos, se deberían implementar los controles que se requieran para proteger mis activos de información y no indicar que por seguridad no se puede hacer.
- iv. La seguridad de la información debe ir de la mano con la tecnología y ayudar a la organización a hacer las nuevas formas de hacer dinero de forma segura.
- v. La implementación de tecnologías dentro de las organizaciones no implica la generación de nuevas vulnerabilidad y potenciales amenazas.

Seleccione una:

- ☐ a. i, ii, iv y v
- ☒ b. i, iii y iv ✓
- ☐ c. i, iii y v
- ☐ d. i y iv
- ☐ e. i y iii

La respuesta correcta es: i, iii y iv

Pregunta 7

Correcta

Se puntúa 3,00 sobre 3,00

El programa de seguridad debe estar respaldado totalmente por la alta dirección de la organización. Ya que esto refleja preocupación de esta sobre la protección de sus activos sensibles, entregar los recursos necesarios y que se sigan los lineamientos emanados.

Seleccione una:

- ☒ Verdadero ✓
- ☐ Falso

Un acercamiento Bottom-up es menos efectivo, no abarca todos los riesgos y finalmente falla estrepitosamente.

La respuesta correcta es 'Verdadero'

Pregunta 8

Correcta

Se puntúa 10,00 sobre 10,00

Asocie la definición con el concepto asociado

Conjunto de normas y prácticas que especifican o regulan la forma en que un sistema u organización presta servicios de seguridad para proteger los recursos sensibles y críticos del sistema	✓	Política de seguridad
La supervisión y la toma de decisiones necesarias para alcanzar los objetivos empresariales mediante la protección de los activos de información de la organización.	✓	Gestión de la Seguridad de la Información
Establecimiento de políticas y vigilancia continua de su correcta aplicación por parte de los miembros del órgano rector de una organización	✓	Gobierno de la Seguridad de la Información
Alineación de la gestión y el funcionamiento de la seguridad de la información con la planificación estratégica de la empresa y la tecnología de la información	✓	Planificación estratégica
La implementación, despliegue y operación continua de controles de seguridad definidos dentro de un marco de ciberseguridad.	✓	Operación de la Seguridad de la Información

Respuesta correcta

La respuesta correcta es: Conjunto de normas y prácticas que especifican o regulan la forma en que un sistema u organización presta servicios de seguridad para proteger los recursos sensibles y críticos del sistema → Política de seguridad, La supervisión y la toma de decisiones necesarias para alcanzar los objetivos empresariales mediante la protección de los activos de información de la organización. → Gestión de la Seguridad de la Información, Establecimiento de políticas y vigilancia continua de su correcta aplicación por parte de los miembros del órgano rector de una organización → Gobierno de la Seguridad de la Información, Alineación de la gestión y el funcionamiento de la seguridad de la información con la planificación estratégica de la empresa y la tecnología de la información → Planificación estratégica, La implementación, despliegue y operación continua de controles de seguridad definidos dentro de un marco de ciberseguridad. → Operación de la Seguridad de la Información

Pregunta **9**

Correcta

Se puntúa 5,00 sobre 5,00

¿En qué consiste un Sistema de Gestión de Seguridad de la Información?

- i. Políticas
- ii. Procedimientos
- iii. Pautas y recursos
- iv. Actividades

Seleccione una:

- ☐ a. Ninguna opción es correcta
- ☐ b. ii, iii y iv
- ☒ c. i, ii, iii y iv ✓
- ☐ d. i, iii y iv
- ☐ e. i, ii y iv

Respuesta correcta

La respuesta correcta es: i, ii, iii y iv

Pregunta **10**

Correcta

Se puntúa 5,00 sobre 5,00

Asocie el activo con el dominio adecuado

Contrato firmado a mano alzada	Seguridad de la información	✓
Smartphone personal de un trabajador	Ciberseguridad	✓
Routers y switches	Seguridad de las TI	✓

Respuesta correcta

La respuesta correcta es: Contrato firmado a mano alzada → Seguridad de la información, Smartphone personal de un trabajador → Ciberseguridad, Routers y switches → Seguridad de las TI

Pregunta **11**

Correcta

Se puntúa 5,00 sobre 5,00

¿Qué debe cubrir un plan estratégico de seguridad de la información?

- i. Definición: Misión, visión y objetivos, Prioridades, Criterios de éxito, Integración, Defensa contra amenazas.
- ii. Ejecución: Plan operacional, Plan de monitoreo y Plan de ajustes
- iii. Operación: Indicadores operativos de gestión
- iv. Revisión: Plan de revisión

Seleccione una:

- ☐ a. i, ii, iii y iv
- ☐ b. Solo i
- ☐ c. i y ii
- ☒ d. i, ii y iv ✓
- ☐ e. Ninguna opción es correcta

Respuesta correcta

A nivel estratégico no se definen aún indicadores de operación.

La respuesta correcta es: i, ii y iv

◀ CONTROL N°1: UNIDAD 1

Ir a...

PEP 1 - FUNDAMENTOS DE CIBERSEGURIDAD 2-2022 (PAUTA) ►



Síguenos en:



Prorectoría

✉ E-mail: soporte.uvirtual@usach.cl

En caso de presentar problemas con sus datos institucionales, validar datos en mail.usach.cl, saliendo de su sesión de correo actual.
No ocupe datos guardados.