UNIVERSIDAD DE SANTIAGO DE CHILE

Departamento de Ingeniería Informática

Fundamentos de ciberseguridad

Rut: **PEP 2**

Fecha: 14/12/2022 - **Exigencia:** 60%

Instrucciones:

- Lea atentamente la prueba, se aceptarán preguntas solamente en los 10 primeros minutos.
- Responda con lápiz pasta, sino perderá automáticamente el derecho a re-corrección.
- No se permite el uso de celulares u otros dispositivos electrónicos

I. (40 ptos) Elija la alternativa correcta e indique está en la tabla del final de la sección.

1) (5 ptos) Dentro de las definiciones de gobierno de la seguridad de la información se establece:

   i. Establecer y mantener un marco y estructura y procesos de gestión de apoyo alineado con los objetivos estratégicos.

   ii. Asignar responsabilidades dentro de la organización relacionadas con seguridad de la información.

   iii. Implementar mecanismos la mitigación de riesgos en la organización.

   iv. Dirigir y controlar las actividades relacionadas con la seguridad de la información

   v. Hacer que las estrategias de seguridad de la información sean coherentes con las leyes y reglamentos aplicables.

a) i y ii
b) i, ii y iii
c) i, ii, iii, iv
d) i, ii, iii, iv y v
e) Ninguna de las anteriores

2) (5 ptos) El alcance del Gobierno de la Seguridad de la información abarca:

   i. Activos de información analogos

   ii. Activos de información digital

   iii. Activos que soportan la información digital

   iv. Activos no basados en información vulnerables a amenazas a través de TICs

a) i y ii
b) i, ii y iv
c) ii, iii y iv
d) i, ii, iii y iv
e) Ninguna alternativa es correcta

Rut: **PEP 2**

3) Los siguientes son elementos de un documento de 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. Revisión: Plan de revisión

iv. Ajustes: Revisión de problemas, estadísticas de incidentes y soluciones propuestas.

a) i y ii
b) i, ii y iii
c) i, ii, iii, iv
d) i, ii, iii, iv y v
e) Ninguna de las anteriores

3) (5 ptos) De acuerdo al estándar X.1054 y la ISO 27014, los siguientes son algunos principios que tiene el gobierno de la seguridad de la información::

i. Establecer la seguridad de la información en toda la organización.

ii. Adoptar un enfoque basado en riesgos.

iii. Establecer la dirección de las decisiones de inversión.

iv. Asegurar la conformidad con los requisitos internos y externos.

v. Fomentar un entorno positivo para la seguridad de todos los interesados.

a) i y ii
b) i, ii y iii
c) i, ii, iii, iv
d) i, ii, iii, iv y v
e) Ninguna de las anteriores

4) (5 ptos) En un Programa de seguridad se deben considerar muchas piezas::

i. Mecanismos de protección lógicos, administrativos y físicos.

ii.. Procedimientos y procesos de negocio.

iii. Personas

a) Solo i
b) i y ii
c) i, ii y iii
d) ii y iii
e) Ninguna de las anteriores

5) (5 ptos) En caso de que una organización requiera implementar un nuevo servicio, el encargado de la ciberseguridad de esta debería:

i. Analizar y evaluar los riesgos que este nuevo servicio conlleva.

ii. Proponer controles que permitan implementar el servicio con un nivel de riesgo aceptable.

iii. Identificar que parte de la arquitectura de seguridad de la organización podría ser afectada.

iv. Impedir el funcionamiento de servicio mientras sus riesgos no estén completamente mitigados.

a) i y ii
b) i, ii y iii
c) i, ii, iii, iv
d) i, ii, iii, iv y v
e) Ninguna de las anteriores

6) (5 ptos) Indique las razones de porque la gestión del riesgo es un elemento clave en la evaluación y planeación de la ciberseguridad:

i. Los ambientes completamente seguros no existen.

ii. Cada ambiente tiene sus propias amenazas y vulnerabilidades.

iii. Se requiere de una forma sistemática de priorizar los controles de ciberseguridad dado que se cuenta con un presupuesto acotado.

iv. Es necesario evaluar si los controles por implementar y los implementados son adecuados en costo-beneficio.

v. El valor de los activos de información varía de organización en organización.

a) i y ii
b) i, ii y iii
c) i, ii, iii, iv
d) i, ii, iii, iv y v
e) Ninguna de las anteriores

7) (5 ptos) Entre las diferencias que se tienen entre un análisis cuantitativo y el cualitativo se tiene:

i. En el cuantitativo usa métricas objetivas, mientras que en el cualitativos se requieren un alto número de supuestos.

ii. En el cualitativo se requieren las opiniones de los individuos, mientras que en el cuantitativo se usan métricas verificables y objetivas.

iii. En el cuantitativo se puede usar para el seguimiento de la performance del riesgo, mientras que en el cualitativo proporciona áreas generales e indicaciones de riesgos.

iv. En el cualitativo se recopilan las opiniones de personas que mejor conocen los procesos.

Rut: **PEP 2**

a) i y ii
b) i, y iii
c) i, iii y iv
d) i, ii, y iv
e) i, ii, iii y iv

8) (5 ptos) En la gestión del riesgo, luego de realizar el planeamiento, la recolección de información, la definición de recomendaciones, viene el manejo del riesgo. En esta se debe elegir entre:

i. Transferirlo

ii. Aceptarlo

iii. Cuidarlo

iv. Evitarlo

v. Reducirlo

a) i, ii y iii
b) i, ii, iv y v
c) ii, iii, iv y v
d) i, iv y v
e) i, ii, iii, iv y v

En la siguiente tabla encierre en un circulo sus respuestas (Solamente se corregirá la presente tabla)

N°	Alternativas	N°	Alternativas
1	a - b - c - d - e	5	a - b - c - d - e
2	a - b - c - d - e	6	a - b - c - d - e
3	a - b - c - d - e	7	a - b - c - d - e
4	a - b - c - d - e	8	a - b - c - d - e

Rut: **PEP 2**

II. (30 ptos) Indique el ambito a que pertenece cada proceso (1. Gobierno de la Seguridad, 2. Gestión de la seguridad, 3. Seguridad de las operaciones/implementación).

N°	Ambito (1, 2 o 3)	Proceso
1	2. Gestión de la seguridad	Definición del framework de ciberseguridad
2	1. Gobierno de la Seguridad	Planeamiento estratégico
3	3. Seguridad de las operaciones/implementación	Detección de ataques
4	3. Seguridad de las operaciones/implementación	Mantenimiento
5	1. Gobierno de la Seguridad	Estructura organizacional
6	3. Seguridad de las operaciones/implementación	Detección de ataques
7	1. Gobierno de la Seguridad	Roles y responsabilidades
8	3. Seguridad de las operaciones/implementación	Recuperación ante ataques
9	2. Gestión de la seguridad	Selección de controles
10	1. Gobierno de la Seguridad	Arquitectura empresarial
11	3. Seguridad de las operaciones/implementación	Actualizaciones de software
12	1. Gobierno de la Seguridad	Políticas y guia
13	3. Seguridad de las operaciones/implementación	Medición de la performance
14	2. Gestión de la seguridad	Asignación de recursos
15	3. Seguridad de las operaciones/implementación	Implementar y desplegar

Rut: **PEP 2**

III. (20 ptos) Indique Verdadero o Falso. Justifique las Falsas (1 pto por respuesta correcta, 2 ptos cada justificación de falsa)

1. ___F____ El plan estratégico de la organización debe estar alineado con el de tecnologías de la información.
2. ___F____ La ciberseguridad es más importante que la implementación de cualquier tecnologías, por lo que no se debe instalar ningún sistema 100% seguro.
3. ___V____ La incorporación de nuevas tecnologías en las organizaciones implica la generación de nuevos riesgos.
4. ___F____ En un reporte de la seguridad de la información emanado a la Gobernanza de la organización se deben proveer elementos técnicos detallados sobre lo realizado en el nivel de gestión y operación.
5. ___V____ En la seguridad a través de la oscuridad se asume que mis enemigos no son tan listos como uno.
6. ___F____ En la ISO 27001, la declaración de aplicabilidad es a7quella en que se seleccionan los riesgos que se deben mitigar.
7. ___V____ El objetivo de las empresas es ganar dinero, por lo que no debe interponerse a la seguridad sobre el negocio.
8. ___F____ En el análisis del riesgo este tiene una pérdida potencial y una tardía. Un ejemplo de perdida potencial es daño a la reputación de la compañia y uno de perdida tardía, es reducción en productividad de los empleados.
9. ___V____ Una vez que una organización reduce sus riesgos a nivel aceptable, el riesgo restante se denomína riesgo residual.
10. ___V____ Algunas técnicas para obtener datos para el análisis de riesgo cualitativo son: Story boards, Focus group, Delphi, tormenta de ideas, entre otras..

Justificación

1. Falsa, el plan estratégico de tecnología debe estar alineado con el plan estratégico de la organización.
2. Falsa, la ciberseguridad debe ir de la mano de la tecnología. Además, ningún sistema es 100% seguro.
3. Verdadera.
4. Falsa, la Gobernanza esta compuesta por personas en su mayoría no técnica por lo que se debe informar con un lenguaje de alto nivel.
5. Verdadera.
6. Falsa, en la declaración de aplicabilidad se deben indicar si aplica cada uno de los controles de la ISO 27002 a la organización en donde se esté aplicando.
7. Verdadera.
8. Falsa, están al revez los ejemplos.
9. Verdadera.
10. Verdadera.

Rut: **PEP 2**

IV. (35 ptos) Análisis de riesgos cuantitativo

Hector es el director de seguridad de una empresa que obtiene la mayor parte de sus ingresos de su propiedad intelectual. Hace un año, cuando Hector llevó a cabo un análisis de riesgos cuantitativo, determinó que la empresa corría un riesgo excesivo en cuanto a la posible pérdida de secretos comerciales (con un ratio de ocurrencia de una vez cada diez años). La contramedida que su equipo implementó redujo este riesgo, y Sam determinó que la expectativa de pérdida anualizada del riesgo de que un secreto comercial sea robado una vez en un período de cien años es ahora de 4000 dólares.

a) ¿Cuál es el valor de la expectativa de pérdida única asociada en este escenario? (10 ptos)

SLE = ?

ARO = 1/100 =0.01

ALE = 4000 Dólares

ALE = SLE * ARO

4000 = SLE * 0.01

SLE = 400.000 USD

b) ¿Cuál es el valor del activo si el factor de exposición es del 50%? (5 ptos)

SLE =Valor activo x Factor de exposición

400.000 = Valor activo x 0,5

Valor activo = 800.000 Dólares

c) ¿Cuál era la expectativa de pérdida anualizada en el escenario original (sin controles y considerando un factor de exposicón del 80%)? (10 ptos)

ALE = SLE x ARO
SLE = Valor activo x Factor de exposición
SLE = $800.000 x 80% = $640.000

ARO: 1 vez cada 10 años = 1/10 = 0,1

ALE = $640.000 x 0,1 = $64.000

d) ¿Es conveniente para el negocio la decisión de implementar dichos controles (Con valor de $10.000 USD en total)? Justifiqué con un análisis de costo beneficio (10 ptos).

(ALE antes de implementar el control) –(ALE después de implementar el control) - (valor del control para la compañía)

64.000 - 4.000 - 10.000 = 50.000 de beneficio (es conveniente)

Rut: **PEP 2**