Risk & Security Management

Reactivos

Pregunta 1

Menciona la definición que corresponde al concepto de desarrollo de sistema.

Opciones:

a. Actividades para crear programas, en diferentes etapas y de acuerdo con un plan, que ayuden a optimizar y mejorar un proceso.
b. Procedimiento para crear programas, en diferentes etapas y de acuerdo con un plan, que ayuden a optimizar y mejorar un proceso.
c. Actividades compuestas de diferentes etapas para lograr o no la factibilidad de construir una solución a una problemática ya existente.
d. Proceso compuesto de diferentes etapas para lograr o no la factibilidad de construir una solución a una problemática ya existente.

Pregunta 2

De acuerdo con Pathak (2022), identifica cuál NO es una etapa en el desarrollo de sistemas.

Opciones:

a. Restauración
b. Ideación
c. Diseño
d. Despliegue

Pregunta 3

De acuerdo con Microsoft, menciona la definición de **DevOps**.

Opciones:

a. Esta metodología permite que los roles que antes estaban aislados se coordinen y colaboren para ofrecer un mejor diseño de sistemas.
b. Este proceso permite que los roles que antes estaban aislados se coordinen y colaboren para ofrecer un mejor y más confiable *software*.
c. Este proceso permite que los roles que antes estaban aislados se identifiquen y evalúen para ofrecer un mejor y más confiable software.
d. Esta metodología permite que los roles que antes estaban aislados se identifiquen y evalúen para ofrecer un mejor diseño de sistemas.

Pregunta 4

De los siguientes tipos de pruebas de software, menciona los que pertenecen al tipo funcional:

1. Unitarias.
2. Múltiples.
3. De integración.
4. De rendimiento.

Opciones:

a. 4 y 1
b. 3 y 2
c. 1 y 3
d. 2 y 4

Pregunta 5

Identifica el sistema de gestión de datos en el que la información resguardada puede ser no estructurada.

Opciones:

a. Lagos de datos
b. Depósitos de datos
c. Almacenes de datos
d. Base de datos

Pregunta 6

De acuerdo con lo expuesto por SAP (s.f.) sobre la gobernanza de seguridad de los datos, relaciona cada beneficio con su respectiva acción:

Beneficio	Acción
1. Datos mejores y más confiables.	a) Aminorar los tiempos de las operaciones y de la toma de decisión.
2. Una sola versión de la verdad.	b) Realizar auditorías y revisiones.

3. Cumplimiento de normas regulatorias, legales e industriales.	c) Compartir los datos de la organización.
4. Reducción de costos.	d) Visualizar los datos como materia prima.

Opciones:

a. 1a, 2b, 3d y 4c
b. 1d, 2c, 3b y 4a
c. 1c, 2a, 3b y 4d
d. 1d, 2b, 3a y 4c

Pregunta 7

Menciona el componente del marco de trabajo empleado en la aplicación de la gobernanza, el cual sirve de guía para verificar qué se va a gestionar y controlar, con el objetivo de lograr los resultados esperados por la organización.

Opciones:

a. Estándares y políticas de datos
b. Alcance de los datos
c. Estructura organizativa
d. Supervisión y métricas

Pregunta 8

¿Cuál es la finalidad de considerar la forma en que los objetivos del negocio determinan las decisiones de ciberseguridad?

Opciones:

a. Presentar los objetivos, riesgos y procedimientos de ciberseguridad en todas las áreas del negocio.
b. Incorporar los datos de los activos críticos que sean sensibles a las vulnerabilidades y amenazas del negocio.
c. Determinar qué activos y sistemas son críticos para el negocio.
d. Que el líder de área comprenda las acciones necesarias y prevea cómo afectarán en las operaciones diarias.

Pregunta 9

De las siguientes opciones, identifica ¿cuál NO es un proceso descrito por Arroyo (2020) para emplear un gobierno de ciberseguridad?

Opciones:

a. Aprovisionamiento seguro de los servicios de información
b. Supervisión y métricas
c. Operación y mantenimiento
d. Protección y defensa

Pregunta 10

¿Cuál es la finalidad de la gobernanza de seguridad?

Opciones:

a. Contener un modelo de datos que incluya entradas, salidas y parámetros de almacenamiento.
b. Dar cumplimiento a las normas regulatorias, legales e industriales.
c. Identificar políticas o acciones organizacionales relacionadas con aspectos legales y regulatorios.
d. Garantizar la correcta precisión de los datos, así como su acceso desde distintos puntos de la organización.

Pregunta 11

Menciona la definición completa de política de seguridad, según IBM:

Conjunto de ______ que se aplican a las ______ del sistema y a los recursos de comunicación de una organización.

Opciones:

a. Guías – funciones
b. Estándares – operaciones
c. Reglas – actividades
d. Procedimientos – amenazas

Pregunta 12

De la siguiente lista, cuál NO puede ser un objetivo de seguridad.

Opciones:

a. Confidencialidad
b. Integridad de los datos
c. Desarrollo de sistemas
d. Protección de activos

Pregunta 13

Si te contratan por tus habilidades para desarrollar políticas de seguridad, ¿qué estándares utilizarás para dicha actividad?

1. SOC 2
2. ISO
3. IEC
4. NIST
5. SGSI

Opciones:

a. 4 y 2
b. 1 y 4
c. 3 y 1
d. 2 y 5

Pregunta 14

Una PyME se acerca a la empresa en la que laboras y solicita tu asesoría para desarrollar tres procedimientos de seguridad de la información. Identifica cuáles puedes recomendarle de la siguiente lista:

1. Gestión de continuidad del negocio.
2. Reglas para la instalación de software.
3. Políticas de contraseñas y de acceso a los dispositivos de TI de la organización.
4. Controles de acceso.
5. Seguridad del entorno físico.

Opciones:

a. 1, 4 y 5
b. 3, 5 y 4
c. 4, 2 y 1
d. 2, 3 y 4

Pregunta 15

Ordena los pasos que integran la metodología PASTA para el modelado de amenazas:

1. Análisis de las amenazas.
2. Análisis de riesgo e impacto.
3. Análisis de vulnerabilidades y debilidades.
4. Definir el alcance técnico.
5. Definir los objetivos.
6. Descomposición de la aplicación.
7. Modelado de ataque.

Opciones:

a. 2, 6, 1, 7, 3, 5 y 4
b. 6, 5, 7, 4, 2, 1 y 3
c. 4, 7, 5, 2, 1, 3 y 6
d. 5, 4, 6, 1, 3, 7 y 2

Pregunta 16

¿Cuál es la unidad mínima de información que puedes tener a tu disposición y que, además, sirve para representar alguna información?

Opciones:

a. Activo
b. Dato
c. Control
d. Usuario

Pregunta 17

Menciona algunos ejemplos de datos sensibles en las organizaciones.

1. Procesos de manufactura.
2. Orientación sexual.
3. Creencias religiosas.
4. Estados financieros.

Opciones:

a. 3 y 2
b. 1 y 4
c. 2 y 1
d. 4 y 3

Pregunta 18

De acuerdo con la norma ISO 27001, ordena los pasos para clasificar la información:

1. Hacer un manejo y tratamiento seguro de la información.
2. Proceder a la clasificación de la información.
3. Incluir la información en el inventario de activos.

4. Asignar una etiqueta a la información.

Opciones:

a. 3, 2, 4 y 1
b. 3, 1, 4 y 2
c. 4, 2, 1 y 3
d. 1, 4, 3 y 2

Pregunta 19

Identifica los siguientes controles de seguridad para relacionarlos con su descripción correcta:

Control	Descripción
1. Seguridad física y ambiental	a) Inventario, clasificación y almacenamiento de los datos.
2. Gestión de recursos	b) Credenciales y medios de acceso a la información
3. Seguridad operacional	c) Protección contra la vulnerabilidad
4. Control de acceso	d) Garantizar la seguridad a través de los factores externos del sistema.

Opciones:

a. 1d, 2a, 3c y 4b
b. 1c, 2d, 3b y 4a
c. 1d, 2a, 3b y 4c
d. 1a, 2d, 3c y 4b

Pregunta 20

En el proceso de determinar la propiedad de los datos y activos, identifica la parte designada de una entidad, ubicación, proceso o grupo de trabajo responsable de verificar el cumplimiento de las restricciones de acceso y clasificación.

Opciones:

a. Arrendador
b. Usuario
c. Propietario
d. Custodio

Pregunta 21

Toda debilidad del sistema que puede ser explotada por algún atacante es:

Opciones:

a. Una susceptibilidad
b. Una amenaza
c. Un riesgo
d. Una vulnerabilidad

Pregunta 22

Identifica cuál de las siguientes opciones es una amenaza **No intencional**

Opciones:

a. Inundaciones por deficiencia en sistema hidráulico
b. Eventos atmosféricos
c. Erupciones
d. Accidentes de vehículos

Pregunta 23

Ordena las fases para el análisis de riesgos

1. Definir el alcance
2. Evaluar el riesgo
3. Identificar amenazas
4. Identificar los activos
5. Identificar vulnerabilidades y salvaguardas
6. Tratar el riesgo

Opciones:

a. 2, 4, 5, 1, 3, 6
b. 3, 1, 5, 2, 6, 4
c. 6, 3, 5, 1, 2, 4
d. 1, 4, 3, 5, 2, 6

Pregunta 24

La duplicación es un tipo de control de riesgo que:

Opciones:

a. Implica diversificar el negocio a través de diferentes líneas de este.
b. Implica la dispersión de activos críticos en diversas áreas.
c. Busca la elaboración de un plan de respaldo que apoye a las operaciones críticas del negocio.
d. Busca evitar el riesgo por completo, a través de la implementación de diferentes herramientas.

Pregunta 25

Las siguientes actividades forman parte de ______, de acuerdo con la norma ISO 27000:

1. Estimar el impacto
2. Estima probabilidad de ocurrencia
3. Determinar riesgos
4. Identificar controles
5. Evaluar controles

Opciones:

a. Valores del riesgo
b. Analizar los riesgos
c. Identificar el contexto
d. Tratamiento de los riesgos

Pregunta 26

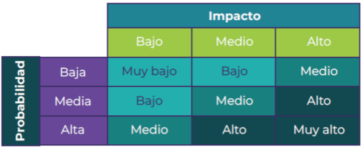
Son herramientas para realizar análisis de riesgo cuantitativo, **EXCEPTO**:

Opciones:

a. Modelado y simulación
b. Análisis del valor monetario esperado (EMV)
c. Juicio de expertos.
d. Análisis de sensibilidad

Pregunta 27

La siguiente imagen es _________ y se utiliza para realizar _________.



		Impacto		
		Bajo	Medio	Alto
Probabilidad	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Opciones:

a. Una tabla de impacto – un umbral de riesgos
b. Una matriz de riesgo – un análisis cualitativo
c. Una tabla de impacto – un análisis cuantitativo
d. Una matriz de riesgo – mitigación de riesgos

Pregunta 28

Relaciona el beneficio con su acción de acuerdo a lo expuesto por SAP (s.f.) sobre la gobernanza de seguridad de los datos:

Estrategia	Características
1. Evitar o eliminar el riesgo	a) El problema puede ser atendido por alguien más capacitado.
2. Reducir o mitigar	b) Cuando no se tiene una opción vieble, se deberá aprender a convivir con el riesgo.
3. Transferir o compartir	c) Implementar las acciones necesarias para desaparecer los factores que propicien los riesgos.
4. Aceptar el riesgo	d) Se realiza cuando el anular un riesgo tiene un mayor gasto de recursos que las consecuencias de este.

Opciones:

a. 1c, 2d, 3b, 4a
b. 1c, 2d, 3a, 4b
c. 1b, 2c, 3d, 4a

d. 1b, 2d, 3c, 4a

Pregunta 29

Este factor de priorizar la respuesta al riesgo es la más sencilla ya que hace uso del sentido común (a mayor probabilidad e impacto, mayor la prioridad).

Opciones:

a. Por tiempo de respuesta.
b. Por capacidad de gestión.
c. Por nivel de riesgo.
d. Por actitud

Pregunta 30

De acuerdo con los Planes de acción correctiva, ordena las etapas de un plan de acción.

1. Plazos del Plan
2. Asignación de roles
3. Definir el objetivo
4. Acciones del Plan

Opciones:

a. 4, 2, 3, 1
b. 3, 2, 4, 1
c. 3, 4, 2, 1
d. 2, 3, 4, 1

Pregunta 31

¿Cómo define María Teresa Moreno (2022) el término "incidente" en el contexto de la seguridad de la información de una empresa?

Opciones:

a. Compromiso de un sistema en el que el atacante puede haber adquirido una cuenta con privilegios.
b. Intento de compromiso de un sistema mediante la explotación de vulnerabilidades conocidas.
c. Ataque que afecta a la disponibilidad de los sistemas de una empresa.
d. Suceso que afecta a la confidencialidad, integridad y disponibilidad de los activos de información.

Pregunta 32

Según la clasificación taxonomía de los incidentes, ¿en qué clasificación está el incidente “Suplantación de identidad”?

Opciones:

a. Fraude
b. Disponibilidad
c. Intrusión
d. Intento de intrusión

Pregunta 33

Perteneces a una empresa líder en ciberseguridad y una organización sin fines de lucro te contrata pues se ha comprometido su información. Después de un análisis que se realizó determinan los conceptos mostrados en la tabla siguiente:

Concepto	Nivel de criticidad
1. Amenazas persistentes avanzadas	a) Alto
2. Intrusión de cuentas con privilegios	b) Medio
3. Contenido abusivo (spam)	c) Crítico
4. Disponibilidad (mala configuración)	d)Bajo

Opciones:

a. 1c, 2a, 3d, 4b
b. 1c, 2a, 3b, 4d
c. 1a, 2c, 3b, 4d
d. 1a, 2d, 3b, 4c

Pregunta 34

De la lista siguiente señala cuáles son fases de planificación y preparación para hacer frente a un incidente de seguridad

1. Contención del incidente.
2. Detección y análisis.
3. Lecciones aprendidas.
4. Erradicación y recuperación.
5. Recuperación tras el incidente.

Opciones:

a. 4, 2
b. 2, 3
c. 5, 4
d. 1, 5

Pregunta 35

Las siguientes acciones forman parte de una de las subetapas del análisis posterior a un incidente:

1. Cambios en los dispositivos de red, como desconectar equipos de la red o aislar segmentos de red específicos.
2. Aislar unidades organizativas en el directorio activo.
3. Suspender servicios específicos, como la salida de correo o la navegación web.
4. Considerar técnicas como el DNS *sinkholing* para controlar el tráfico malicioso.

Opciones:

a. Identificación del incidente
b. Erradicación del incidente
c. Contención del incidente
d. Recuperación tras el incidente

Pregunta 36

¿Cuáles son los procesos clave que debe incluir un plan de continuidad del negocio, según IBM (2020)?

Opciones:

a. 1. Operaciones continuas.
   2. Recopilar la información necesaria.
   3. Planificación de cómo realizar el BIA.

b. 1. Planificación de cómo realizar el BIA.
   2. Reunir información.
   3. Analiza los datos.

c. 1. Identificar actividades y recursos empresariales clave
   2. Analizar el impacto financiero de las interrupciones comerciales.
   3. Recopilar la información necesaria.

d. 1. Alta disponibilidad.
   2. Operaciones continuas.
   3. Recuperación de desastres.

Pregunta 37

Método para analizar la manera en que un evento afecta a la empresa dentro de sus procesos.

Opciones:

a. Plan de recuperación de desastres
b. Plan de continuidad del negocio
c. Estrategia de recuperación
d. Valoración de Impacto al Negocio

Pregunta 38

Selecciona los 3 elementos que se deben considerar en el BIA (Valoración de Impacto al Negocio).

1. Alcance
2. Organigrama
3. Objetivo
4. Partes interesadas
5. Presupuesto

Opciones:

a. 1, 3, 5
b. 2, 4, 5
c. 1, 3, 4
d. 1, 2, 4

Pregunta 39

El ___ es el tiempo en que una interrupción es tolerable, mientras que el ___ es la máxima cantidad de pérdidas tolerable.

Opciones:

a. BIA – RPO
b. RTO – RPO
c. BIA – BCP
d. RTO – BCP

Pregunta 40

Relaciona el concepto con su principal característica

Concepto	Características
1. Plan de continuidad del negocio.	a) Sirve para recopilar los datos necesarios para enfrentar los desafíos que se presentan.
2. Valoración de Impacto al Negocio	b) Describe qué es lo que se puede esperar cuando el negocio presenta alguna interrupción en sus operaciones.
3. Estrategia de recuperación	c) Documento que describe cómo una empresa seguirá funcionando durante una interrupción no planificada del servicio.

Opciones:

a. 1c, 2b, 3a
b. 1c, 2a, 3b
c. 1b, 2c, 3a
d. 1a, 2c, 3b