

Nombre:

Cantidad de hojas entregadas:

OBSERVACIONES GENERALES:

- Lea todo el ejercicio antes de comenzar a desarrollarlo
- Enumere y ponga su nombre a todas las hojas. Indique cuántas hojas entrega.
- Durante el examen no se contesten preguntas. Si encuentra ambigüedades en el enunciado, tome una decisión, documéntela y continúe resolviendo el ejercicio respectivo.

1) Sistema de pago electrónico: en un sistema de pago de servicios electrónicos se debe identificar al usuario fehacientemente mediante la introducción de un usuario y PIN (Personal Identification Number) de seis dígitos. Como primer paso del circuito el cliente de la entidad financiera propietaria del sistema de pagos recibe en su domicilio un PIN generado por la entidad con las instrucciones que, de acuerdo a la opinión de la entidad, permitirán un funcionamiento seguro. Como protección la primera vez que se ingresa al sistema se cambiará por única vez el PIN por uno a elección del cliente. Junto con estas instrucciones recibe una tarjeta denominada de coordenadas donde se especifica una serie de contraseñas en forma de grilla. Estas contraseñas son solicitadas por subconjuntos y aleatoriamente al momento de realizar cada transferencia electrónica.

Como auditor, se le solicita:

- a. Identificar los controles internos implementados, clasificarlos de acuerdo al objetivo de su aplicación y justificar esta clasificación
- b. Identificar debilidades de control y establecer el riesgo asociado. De ser necesario proponer nuevos controles.

2) Un consultor externo de esta entidad financiera consiguió realizar una transferencia fraudulenta utilizando una clave de acceso de un empleado de la entidad, es decir suplantando su identidad. El sistema funcionó de acuerdo a lo esperado y realizó tal transferencia por un monto superior a \$ 100.000.000.

de contraseñas en forma de g...
aleatoriamente al momento de realizar cada transacción

Como auditor, se le solicita:

- a. Identificar los controles internos implementados, clasificarlos de acuerdo al objetivo de su aplicación y justificar esta clasificación
- b. Identificar debilidades de control y establecer el riesgo asociado. De ser necesario proponer nuevos controles.

2) Un consultor externo de esta entidad financiera consiguió realizar una transferencia fraudulenta utilizando una clave de acceso de un empleado de la entidad, es decir suplantando su identidad. El sistema funcionó de acuerdo a lo esperado y realizó tal transferencia por un monto superior a \$ 100.000-. La operación fue realizada a última hora del día y aún después de un mes de sucedida no ha sido detectada.

- a. ¿Qué controles debería realizar la entidad para detectar tal anomalía?
- b. ¿Se podría prevenir tal situación? Justifique adecuadamente su respuesta.

3) Una empresa que desarrolla sus actividades comerciales en la Pcia de Río Negro desde hace 20 años. Cuenta con 30 empleados en total cubriendo las áreas de Comercialización, Compras, Administración. Los sistemas utilizados no son propios sino que se compran a un conocido proveedor o los desarrollos menores son llevados a cabo por los propios usuarios. Debido a que se está planificando duplicar la capacidad de comercialización la decisión de la empresa es formar un departamento nuevo de sistemas para desarrollar las aplicaciones internamente. Como auditor se le pide evaluar la situación y opinar respecto a:

- a. dependencia funcional del área de sistemas, especificar a quien reporta.
 - b. estructura a cubrir por el área de sistemas
 - c. planificación necesaria del área de sistemas, de acuerdo a los modelos estudiados
 - d. procedimientos que recomendaría seguir para el desarrollo de aplicaciones.
- 4) "Si la estrategia de backups se basa en tener disponibles en un proveedor los equipos necesarios para recuperar los sistemas estamos ante una estrategia de HOT SITE" ¿Es esto correcto? Justifique.
- 5) Dados los siguientes pasos en un programa de seguridad, ¿cuál es la secuencia más lógica para llevarlos a cabo y por qué?
- a. Identificación de controles
 - b. Análisis de exposición.
 - c. Valuación de bienes
 - d. Identificación de escenarios.
- 6) ¿Cuál de las siguientes es la mejor medida preventiva para reducir los riesgos de un sistema con respecto a los posibles desastres naturales? Justifique.
- a. Identificar las amenazas naturales.
 - b. Elegir un lugar seguro para la ubicación de las facilidades de sistemas.
 - c. Mantener los sistemas críticos separados de los sistemas generales.

b. Análisis de exposición.

c. Valuación de bienes

d. Identificación de escenarios.

6) ¿Cuál de las siguientes es la mejor medida preventiva para reducir los riesgos de un sistema con respecto a los posibles desastres naturales? Justifique.

a. Identificar las amenazas naturales.

b. Elegir un lugar seguro para la ubicación de las facilidades de sistemas.

c. Mantener los sistemas críticos separados de los sistemas generales.

d. Actualizar y guardar los backups fuera del lugar de operaciones habituales.

7) Suponga que la empresa descrita en el punto 3 ha decidido tercerizar el desarrollo de un sistema web para realizar ventas online.

a. ¿Qué recomendaría Ud. como auditor que se debe tener en cuenta al redactar el contrato de servicios? Tenga en cuenta especialmente que se desea lograr la continuidad del sistema a lo largo del tiempo, ¿cómo lo aseguraría? En caso de que este sistema tenga una licencia open source, explique de qué tipo de cláusulas se podría prescindir, que serían clave en un sistema cerrado.

b. ¿Qué sería conveniente incluir en el service level agreement (SLA) asociado?