UNIVERSIDAD DE SANTIAGO DE CHILE
Departamento de Ingeniería Informática
Fundamentos de ciberseguridad

Rut: **PEP 1**

Fecha: 12/05/2023 - 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

Primera parte: Preguntas con alternativas

Escenario

Eres el responsable de ciberseguridad en una pequeña empresa de comercio electrónico. Recientemente, has notado un aumento en los intentos de phishing dirigidos a tus compañeros de trabajo. Los correos electrónicos de phishing parecen provenir de una entidad que se hace pasar por el soporte técnico del servicio de correo electrónico que utiliza la empresa. Los correos electrónicos solicitan a los empleados que proporcionen sus credenciales de inicio de sesión para resolver problemas técnicos inexistentes. Esto sugiere que un grupo de ciberdelincuentes está tratando de obtener acceso no autorizado a las cuentas de correo electrónico de los empleados para lanzar ataques más amplios y acceder a información sensible.

Preguntas sobre el escenario.

Pregunta 1: ¿Cuál de las siguientes vulnerabilidades están explotando los agentes de amenaza en este escenario?

A) Vulnerabilidades en el software de la empresa
B) Fallos en la configuración de la red
C) Falta de concienciación y formación en ciberseguridad de los empleados
D) Malas prácticas de contraseñas
E) Inadecuada segmentación de la red

Respuesta correcta: C) Falta de concienciación y formación en ciberseguridad de los empleados.
Justificación: Los ciberdelincuentes están aprovechando la falta de conocimientos de los empleados sobre phishing y seguridad, lo que los hace susceptibles a entregar sus credenciales de inicio de sesión.

Pregunta 2: ¿Qué tipo de agente de amenaza está involucrado en este escenario?

A) Hacktivistas
B) Grupos terroristas
C) Ciberdelincuentes
D) Espías industriales
E) Insiders maliciosos

Respuesta correcta: C) Ciberdelincuentes.
Justificación: El escenario sugiere que el grupo detrás de los ataques de phishing tiene motivaciones financieras y busca acceso no autorizado para obtener información sensible, lo que encaja con el perfil de ciberdelincuentes.

Rut: **PEP 1**

Pregunta 3: ¿Cuál de los siguientes objetivos de ciberseguridad está directamente amenazado en este escenario?
A) Disponibilidad
B) Confidencialidad
C) Integridad
D) No repudio
E) Autenticidad

Respuesta correcta: B) Confidencialidad.
Justificación: Al obtener acceso a las cuentas de correo electrónico de los empleados, los ciberdelincuentes podrían acceder a información confidencial, lo que pone en riesgo la confidencialidad de los datos de la empresa.

Pregunta 4: ¿Cuál de las siguientes medidas podría ayudar a prevenir futuros ataques de phishing?
A) Implementar un firewall de red
B) Realizar copias de seguridad de datos periódicas
C) Establecer políticas de contraseñas seguras
D) Capacitar a los empleados en concienciación sobre phishing y ciberseguridad
E) Utilizar software antivirus actualizado

Respuesta correcta: D) Capacitar a los empleados en concienciación sobre phishing y ciberseguridad.
Justificación: La formación en concienciación sobre phishing y ciberseguridad ayudará a los empleados a reconocer y evitar ataques de phishing, reduciendo así el riesgo de que proporcionen sus credenciales a los ciberdelincuentes.

Pregunta 5: Si un ataque de phishing tiene éxito, ¿qué consecuencia directa podría tener en la empresa?
A) Interrupción del servicio de correo electrónico
B) Pérdida de la integridad de los datos
C) Dificultades en la autenticación de los usuarios
D) Acceso no autorizado a información confidencial
E) Compromiso de la disponibilidad de la red

Respuesta correcta: D) Acceso no autorizado a información confidencial.

Rut: **PEP 1**

Justificación: Si un empleado proporciona sus credenciales en respuesta a un correo electrónico de phishing, los atacantes tendrían acceso a su cuenta de correo electrónico y a cualquier información confidencial contenida en ella.

Preguntas sobre conceptos

Pregunta 6: ¿Qué es el cibercrimen y cuál es su relación con las amenazas en el ámbito de la ciberseguridad?

A) El cibercrimen se refiere a la explotación de vulnerabilidades en sistemas informáticos para obtener acceso no autorizado, mientras que las amenazas son eventos o acciones que pueden explotar esas vulnerabilidades.
B) El cibercrimen es el acto de crear software malicioso, mientras que las amenazas son los diferentes tipos de software malicioso que existen.
C) El cibercrimen es una disciplina de la informática que estudia cómo proteger sistemas y redes, mientras que las amenazas son eventos que pueden poner en riesgo la seguridad de dichos sistemas y redes.
D) El cibercrimen se refiere a la realización de actividades delictivas utilizando tecnologías de la información y la comunicación, mientras que las amenazas son eventos o acciones que pueden causar daños o pérdidas en el ámbito de la ciberseguridad.
E) Ninguna de las anteriores.

Respuesta correcta: D) El cibercrimen se refiere a la realización de actividades delictivas utilizando tecnologías de la información y la comunicación, mientras que las amenazas son eventos o acciones que pueden causar daños o pérdidas en el ámbito de la ciberseguridad.

Pregunta 7: ¿Cuál es la diferencia entre autenticidad y autenticación en el contexto de la ciberseguridad?

A) La autenticidad se refiere a la verificación de la identidad de un usuario, mientras que la autenticación es la capacidad de demostrar que un evento o transacción ha tenido lugar.
B) La autenticidad se refiere a la capacidad de demostrar que un evento o transacción ha tenido lugar, mientras que la autenticación es la verificación de la identidad de un usuario.
C) La autenticidad y la autenticación son sinónimos y se utilizan indistintamente en el ámbito de la ciberseguridad.
D) La autenticidad se refiere al proceso de cifrado de datos, mientras que la autenticación es el proceso de descifrado de datos.
E) Ninguna de las anteriores

Respuesta correcta: B) La autenticidad se refiere a la capacidad de demostrar que un evento o transacción ha tenido lugar, mientras que la autenticación es la verificación de la identidad de un usuario.

Rut: **PEP 1**

Pregunta 8: ¿Qué es un vector de ataque en el contexto de la ciberseguridad?

A) Un vector de ataque es un método utilizado por los ciberdelincuentes para explotar vulnerabilidades y comprometer la seguridad de un sistema o red.
B) Un vector de ataque es una medida preventiva implementada para proteger los sistemas y redes de la explotación de vulnerabilidades.
C) Un vector de ataque es un evento inesperado que puede causar daños o pérdidas en un sistema o red.
D) Un vector de ataque es un tipo específico de software malicioso diseñado para atacar y comprometer la seguridad de un sistema o red.
E) Ninguna de las anteriores

Pregunta 9: ¿Quién es el dueño del riesgo en el contexto de la ciberseguridad y cuál es su función?
A) El dueño del riesgo es el individuo que realiza un ataque cibernético, y su función es explotar las vulnerabilidades en los sistemas de seguridad.
B) El dueño del riesgo es el individuo o entidad que acepta la responsabilidad de gestionar un riesgo, incluyendo su identificación, evaluación y mitigación.
C) El dueño del riesgo es el individuo o entidad que se ve directamente afectado por un riesgo, y su función es soportar las consecuencias si el riesgo se materializa.
D) El dueño del riesgo es el individuo que desarrolla las políticas de seguridad de una organización, y su función es garantizar que estas políticas se cumplan.
E) Ninguna de las anteriores

Respuesta correcta: B) El dueño del riesgo es el individuo o entidad que acepta la responsabilidad de gestionar un riesgo, incluyendo su identificación, evaluación y mitigación.

Pregunta 10: ¿Qué es el no repudio en el contexto de la ciberseguridad?

A) El no repudio es la capacidad de demostrar que un evento o acción específica ha tenido lugar, de manera que esta no pueda ser negada posteriormente.
B) El no repudio es la capacidad de un sistema para resistir ataques cibernéticos sin interrupción o pérdida de funcionalidad.
C) El no repudio es la garantía de que la información transmitida a través de una red llegue a su destino sin ser interceptada o alterada.
D) El no repudio es la capacidad de un sistema para recuperarse rápidamente de un ataque cibernético y restaurar su funcionalidad normal.
E) Ninguna de las anteriores

Respuesta correcta: A) El no repudio es la capacidad de demostrar que un evento o acción específica ha tenido lugar, de manera que esta no pueda ser negada posteriormente.

Rut: **PEP 1**

Pregunta 11: ¿Cómo impactaría en una empresa el acceso no autorizado a información confidencial?
A) No tendría impacto significativo en la empresa.
B) Podría tener un impacto financiero significativo, incluyendo posibles multas y pérdida de negocio debido a la pérdida de confianza de los clientes.
C) Podría aumentar la eficiencia de los procesos de negocio, ya que los empleados tendrían acceso a más información.
D) Podría mejorar la seguridad de la empresa, ya que se identificarían y corregirían las vulnerabilidades.

Respuesta correcta: B) Podría tener un impacto financiero significativo, incluyendo posibles multas y pérdida de negocio debido a la pérdida de confianza de los clientes.

Preguntas sobre buenas prácticas, estándares y metodologías
Pregunta 12: ¿Qué estándar o marco de control deberías considerar si tu organización procesa, almacena o transmite información de tarjetas de crédito?
A) CIS Controls
B) ISO 27000
C) NIST CSF
D) PCI DSS
E) COBIT

Respuesta correcta: D) PCI DSS
Justificación: PCI DSS es el estándar de seguridad de datos de la industria de tarjetas de pago y es específicamente para organizaciones que manejan información de tarjetas de crédito.

Pregunta 13: ¿Cuál de los siguientes marcos de ciberseguridad es más apropiado para una organización que busca un enfoque de gestión de riesgos de ciberseguridad que sea consistente con las recomendaciones del gobierno de los Estados Unidos?

A) CIS Controls
B) ISO 27000
C) NIST CSF
D) PCI DSS
E) COBIT

Respuesta correcta: C) NIST CSF

Rut: **PEP 1**

Justificación: NIST CSF es un marco de ciberseguridad creado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, y está ampliamente reconocido y recomendado por el gobierno de los EE.UU.

Pregunta 14: Si tu organización está interesada en un marco de ciberseguridad que no sólo se centre en la tecnología, sino también en los aspectos de gestión y gobierno de la tecnología de la información, ¿cuál de los siguientes sería la mejor opción?

A) CIS Controls
B) ISO 27000
C) NIST CSF
D) PCI DSS
E) COBIT
Respuesta correcta: E) COBIT

Justificación: COBIT es un marco de gobernanza de TI que incluye principios y prácticas para la gestión y gobierno de la ciberseguridad, no solo se centra en los aspectos técnicos.

Pregunta 15: ¿Cuál de los siguientes marcos sería más adecuado para una organización que busca un conjunto de controles de ciberseguridad pragmáticos y centrados en la práctica?

A) CIS Controls
B) ISO 27000
C) NIST CSF
D) PCI DSS
E) COBIT

Respuesta correcta: A) CIS Controls
Justificación: CIS Controls es un conjunto de prácticas recomendadas que se centran en un conjunto de controles de ciberseguridad prácticos y efectivos.

Pregunta 16: Si tu organización está interesada en un marco de ciberseguridad que sea compatible con las normas internacionales y que se centre en un enfoque de gestión de la seguridad de la información, ¿cuál de los siguientes sería la mejor opción?

A) CIS Controls
B) ISO 27000
C) NIST CSF
D) PCI DSS
E) COBIT

Rut: **PEP 1**

Respuesta correcta: B) ISO 27000
Justificación: La serie ISO 27000 es un conjunto de estándares internacionales para la gestión de la seguridad de la información.

Tercera Parte: Caso de estudio (50 ptos)

TechnoBank, un prominente banco digital, sufrió una significativa violación de datos en 2023. A pesar de las diversas medidas y protocolos de seguridad establecidos, como el cifrado de datos, la autenticación de dos factores, el uso de una red segura privada virtual (VPN), el firewall, y la implementación de programas antivirus, la información de más de un millón de clientes fue comprometida. Un correo electrónico de phishing meticulosamente diseñado logró infiltrarse en el sistema, engañando a un empleado para que revelara sus credenciales de inicio de sesión.
A pesar de la detección del incidente por parte del sistema de detección de intrusiones, la intervención fue tardía. Los atacantes lograron exfiltrar los datos antes de que se activara el sistema de respuesta a incidentes y se cerraran las conexiones no seguras. Además, una vez que los atacantes obtuvieron las credenciales de un empleado, se autenticaron en el sistema. Con este nivel de acceso, habrían tenido la capacidad de manipular los datos en varias formas. Esto podría incluir la creación de transacciones bancarias fraudulentas, la modificación de los detalles de la cuenta del cliente o incluso la alteración de los registros de transacciones para ocultar su actividad. Posteriormente, TechnoBank movilizó su equipo de respuesta a incidentes, que trabajó junto con la gestión de cambios y la gestión de incidentes para controlar la situación.
Después del incidente, para tranquilizar a los clientes afectados y minimizar el daño a su reputación, TechnoBank implementó un programa de crédito gratuito, además de mejorar sus protocolos de seguridad con la introducción de la formación en seguridad cibernética para el personal y la revisión de su política de seguridad de la información.
Los almacenes de datos comprometidos durante este incidente incluían la base de datos principal de clientes y una carpeta de documentos financieros importantes. Los procesos que estaban en marcha durante el incidente implicaban el sistema de inicio de sesión del cliente y el sistema de transacciones bancarias.

Rut: **PEP 1**

1. ¿Cuáles y de qué tipo son los controles presentes en el caso, funcionalidad y objetivo de ciberseguridad (puede ser mas de uno en cada caso)? (Indique al menos 8 controles)

Control (1 pto)	**Tipo de Control (1 pto, técnico, administrativo, físico)**	**Funcionalidad del Control (1 pto, puede ser mas de uno: Preventivo, Detectivo, Correctivo, Recuperativo)**	**Objetivo de Ciberseguridad (1 pto, puede ser mas de uno: Integridad, disponibilidad, confidencialidad, no repudio, accountability)**
Cifrado de datos	Técnico	Preventivo	Confidencialidad
Autenticación de dos factores	Técnico	Preventivo	Autenticidad, No Repudio
Red Privada Virtual (VPN)	Técnico	Preventivo	Confidencialidad, Integridad
Firewall	Técnico	Preventivo	Disponibilidad, Integridad
Programas antivirus	Técnico	Preventivo, Detectivo	Integridad, Disponibilidad
Detección de intrusiones	Técnico	Detectivo	Integridad, Disponibilidad
Sistema de respuesta a incidentes	Técnico, Administrativo	Correctivo, Recuperativo	Todos los objetivos
Cierre de conexiones no seguras	Técnico	Correctivo	Disponibilidad, Integridad
Formación en seguridad cibernética	Administrativo	Preventivo	Todos los objetivos
Política de seguridad de la información	Administrativo	Preventivo	Todos los objetivos

Rut: **PEP 1**

Rut: **PEP 1**

2. Modelado de amenazas de acuerdo al caso de estudio.

a) (5 ptos) Identifique los procesos relevantes del sistema afectados por el incidente:

Procesos:

- Sistema de inicio de sesión del cliente: Este proceso maneja las credenciales del cliente y autentica a los usuarios antes de permitirles el acceso al sistema bancario. Fue comprometido cuando los atacantes obtuvieron las credenciales de inicio de sesión.
- Sistema de transacciones bancarias: Este proceso maneja todas las transacciones realizadas por los clientes, incluyendo depósitos, retiros y transferencias. Aunque no se especifica directamente en el caso de estudio, es probable que este proceso también se viera afectado si los atacantes obtuvieron acceso a la cuenta de un cliente.

b) (5 ptos) Identifique los almacenes de datos:

Almacenes de datos:

- Base de datos principal de clientes
- Carpeta de documentos financieros importantes

c) (5 ptos) Identifica los flujos de datos entre los procesos y entidades identificadas y nombra sus contenido.

Flujos de datos:

- Datos de Autenticación de Clientes: Estos datos fluyen desde el cliente hasta el sistema de inicio de sesión. Este flujo de datos fue comprometido cuando las credenciales del empleado fueron robadas y utilizadas por los atacantes.
- Solicitudes de Transacciones Bancarias: Estos datos fluyen desde el cliente hasta el sistema de transacciones bancarias. Aunque no se especifica en el caso de estudio, es posible que este flujo de datos haya sido comprometido si los atacantes obtuvieron acceso a las cuentas de los clientes.

d) (5 ptos) Identifica y justifique las entidades que pueden interactuar con los procesos identificados y que podrían ser culpables del incidente.

Entidades

- Clientes: Interactúan con el sistema de inicio de sesión y el sistema de transacciones bancarias. Son el origen de los datos de inicio de sesión y las solicitudes de transacciones.
- Empleados: Los empleados, especialmente aquellos en roles de TI y de servicio al cliente, pueden interactuar con estos sistemas para mantener la operatividad y seguridad.
- Atacantes: En este caso, los atacantes son una entidad externa no deseada. Interactuaron con el sistema de inicio de sesión al proporcionar credenciales robadas y posiblemente con otros sistemas durante el incidente de seguridad.

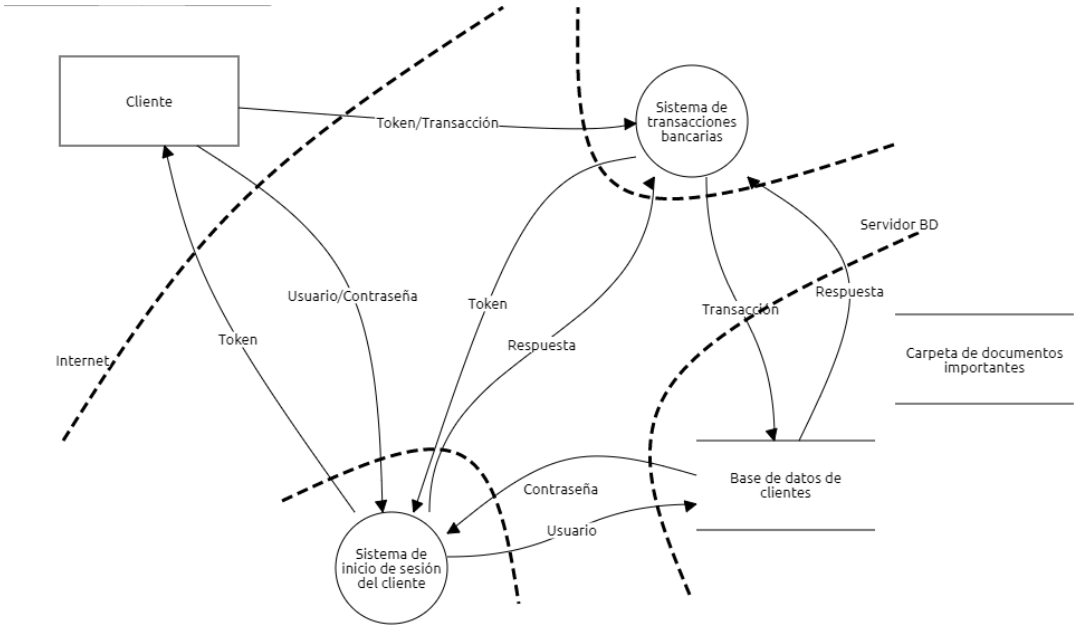
e) (5 ptos) Indica los limites de confianza.

Límites de confianza:

- Entre el usuario y el sistema de inicio de sesión: este límite se rompió cuando los atacantes obtuvieron las credenciales de un empleado.
- Entre el sistema de inicio de sesión y la base de datos de clientes: este límite se rompió cuando los atacantes pudieron acceder a la base de datos de clientes.

Rut: **PEP 1**

f) Diagrame el modelo de amenazas desde el punto de vista del cliente y considerando lo anterior.



Entidades relacionadas: 2 ptos
Flujos de datos: 4 ptos
Procesos: 4 ptos
Límites de confianza y almacenesca: 5 ptos.

Rut: **PEP 1**

3. De acuerdo a la taxonomia STRIDE y al diagrama anterior, indique tres amenazas que se materializaron durante el incidente, considerando el agente de amenaza “atacante”.

Categoria de la amenaza STRIDE	**Objetivo de seguridad afectado**	**Descripción amenaza específica del escenario**
Spoofing	Autenticidad	Suplantación de identidad (Spoofing): Es una táctica que se utiliza para ocultar la identidad o hacerse pasar por otra persona o entidad. En el contexto de la ciberseguridad, la suplantación de identidad puede involucrar el uso de credenciales robadas para acceder a un sistema como si se fuera un usuario legítimo, la manipulación de direcciones IP para ocultar la ubicación de un atacante o hacerse pasar por un servidor de confianza, o el envío de correos electrónicos que parecen ser de una fuente confiable en un intento de engañar al destinatario para que revele información sensible (phishing).
Tampering	Integridad	Manipulación de Datos: Esto se refiere al acto de alterar o distorsionar la información dentro de un sistema de manera maliciosa o fraudulenta. En el caso de un banco, esto podría incluir la alteración de los registros de transacciones para ocultar la actividad ilegal, el cambio de los detalles de la cuenta para dirigir los fondos a una cuenta controlada por un atacante, o la modificación de los parámetros del sistema para permitir acciones que normalmente estarían restringidas.
Information disclousure	Confidencialidad	Exfiltración de Datos: Este es el proceso de transferir datos desde su ubicación original a otra sin autorización. Los atacantes pueden exfiltrar datos para una variedad de propósitos, como el robo de información confidencial o sensible para su propio uso, la venta de datos a terceros, o el uso de los datos robados para extorsionar a la víctima. La exfiltración de datos puede llevarse a cabo de muchas maneras, incluyendo la transferencia de datos a través de la red a un servidor controlado por el atacante, el uso de dispositivos físicos para copiar datos, o incluso el envío de datos a través de canales encubiertos como el DNS o el tráfico de red aparentemente benigno.

Rut: **PEP 1**

4. Desarrolle un análisis de riesgo cualitativo que refleje el escenario anterior.Considere la siguiente matriz de análisis cualitativo con 5 niveles de impacto y 5 niveles de probabilidad.

Probabilidad	Consecuencias				
	Insignificante	Menor	Moderado	Mayor	Severo
Casí seguro	M	A	A	E	E
Probable	M	M	A	A	E
Posible	B	M	M	A	E
Improbable	B	M	M	M	A
Raro	B	B	M	M	A

E	Extremadamente alta
A	Alta
M	Media
B	Baja

a. Analice la amenaza “Suplantación de identidad” y agente de amenaza “atacante” en la siguiente tabla (sea consistente con la tabla anterior).

b. Proponga controles para conseguir un riesgo medio.

c. Justifique la elección de impacto y probabilidad de acuerdo al control escogido.

Amenaza	**Vulnerabilidad**	**Activo involucrado**	**Impacto**	**Probablidad**	**Riesgo inherente**
Suplantación de identidad	Autenticación de un factor	Datos de cliente	Mayor	Probable	Alta

Controles mitigantes	**Impacto**	**Probabilidad**	**Riesgo residual**
Autenticación de doble factor	Mayor	Improbable	Media

El impacto se mantiene por que si se materializa la amenaza, el control propuesto no tiene ningún efecto. El control tiene efecto sobre la probabilidad que la disminuye, ya que sería mas dificil suplantar a la persona.

d. Se requiere un control que baje la probabilidad o el impacto de la suplantación de identidad. Por ejemplo:
    - Para bajar el impacto se podría considerar control de acceso.
    - Para bajar la probabilidad un sistema de prevención de intrusiones, que al detectar la intrusión