UNIVERSIDAD DE SANTIAGO DE CHILE

Departamento de Ingeniería Informática

Fundamentos de ciberseguridad

Rut: **PEP 1** **25/10/2023**

Fecha: 12/05/2023 - Exigencia: 60%

Instrucciones:

- Responda con lápiz pasta, sino perderá automáticamente el derecho a re-corrección.
- No se permite el uso de celulares u otros dispositivos electrónicos.
- Escriba su rut en cada hoja.

Primera parte: Preguntas con alternativas (3 ptos la alternativa correcta)

Se corregirá solamente la siguiente tabla. Encierre en esta tabla la alternativa correcta.

1	**A - B - C - D - E**		**15**	**A - B - C - D - E**
2	**A - B - C - D - E**		**16**	**A - B - C - D - E**
3	**A - B - C - D - E**		**17**	**A - B - C - D - E**
4	**A - B - C - D - E**		**18**	**A - B - C - D - E**
5	**A - B - C - D - E**		**19**	**A - B - C - D - E**
6	**A - B - C - D - E**		**20**	**A - B - C - D - E**
7	**A - B - C - D - E**		**21**	**A - B - C - D - E**
8	**A - B - C - D - E**		**22**	**A - B - C - D - E**
9	**A - B - C - D - E**		**23**	**A - B - C - D - E**
10	**A - B - C - D - E**		**24**	**A - B - C - D - E**
11	**A - B - C - D - E**		**25**	**A - B - C - D - E**
12	**A - B - C - D - E**		**26**	**A - B - C - D - E**
13	**A - B - C - D - E**		**27**	**A - B - C - D - E**
14	**A - B - C - D - E**		**28**	**A - B - C - D - E**

Rut: **PEP 1** **25/10/2023**

Escenario

Una empresa de comercio electrónico, que ha alcanzado un éxito significativo en su mercado local, se encuentra en el proceso de expandirse a mercados internacionales. Esta firma, además de ofrecer productos propios, facilita transacciones entre usuarios en un estilo similar a un mercado en línea. En el marco de esta expansión, planea integrar una diversidad de sistemas de pago, establecer alianzas con proveedores de diferentes partes del mundo y adoptar tecnologías avanzadas para la logística y administración del inventario.

Con la expansión global en mente, la empresa reconoce la necesidad de alojar su plataforma en servidores ubicados estratégicamente alrededor del mundo, asegurando así una rápida respuesta y constante disponibilidad. Además, la integración de múltiples sistemas de pago y alianzas con proveedores internacionales añade una capa adicional de complejidad a su infraestructura tecnológica. Por otro lado, al considerar la implementación del Internet de las Cosas (IoT) para la gestión de inventarios y logística, surgen desafíos relacionados tanto con la conectividad como con la seguridad. A todo esto, se suma el hecho de que, al servir a una clientela global, la plataforma deberá ser accesible desde una amplia variedad de dispositivos y sistemas operativos, cada uno con sus propias particularidades y requerimientos de seguridad.

Sin embargo, al entrar en nuevos territorios, la empresa no solo se enfrenta a retos tecnológicos, sino también a una amplia gama de problemas. Estos incluyen la exposición a actores maliciosos regionales, variaciones en las legislaciones de protección de datos y la posibilidad de que competidores busquen obtener información estratégica. Cada región presenta sus propios riesgos y la empresa debe estar preparada para enfrentar amenazas tanto legales como tecnológicas.

Uno de los desafíos más complejos radica en equilibrar las necesidades y expectativas de los usuarios con las demandas de una implementación de seguridad robusta. Mientras que las medidas de seguridad sólidas, como la autenticación multifactor, pueden ofrecer una capa adicional de protección, también pueden ser percibidas por los nuevos usuarios como barreras que complican la experiencia de usuario. Además, las expectativas en cuanto a usabilidad y características varían entre regiones, y lo que es estándar en un mercado puede ser nuevo o desconocido en otro.

Por último, otro desafío crucial es la dificultad inherente a estimar los costos y beneficios de las inversiones en ciberseguridad. La exposición a posibles ataques aumenta con la expansión, pero determinar cuánto invertir en prevención es una tarea compleja. Los costos asociados a la prevención y respuesta ante amenazas pueden ser elevados, y una brecha de seguridad en un nuevo mercado puede tener repercusiones en la reputación de la empresa que duren mucho más que el incidente en sí.

Rut: **PEP 1** **25/10/2023**

1. ¿Cuál de los siguientes se considera un activo crítico para la empresa de comercio electrónico en expansión internacional?

a) Los comentarios en las redes sociales.
b) La diversidad de sistemas de pago.
c) La plataforma en línea.
d) El software de administración de inventario.
e) Los vehículos de entrega.

Respuesta: c. La plataforma en línea.
Justificación: La plataforma en línea es el núcleo del negocio, facilitando todas las transacciones y la interacción con los clientes. Si esta se ve comprometida, todo el negocio corre riesgo.

2. ¿Qué aspecto representa una vulnerabilidad en el contexto de la diversidad de sistemas de pago?

a) Diversas monedas.
b) Diferentes proveedores de sistemas de pago.
c) Diferentes tipos de sistemas de autenticación y tecnologías.
d) Altas comisiones.
e) Compatibilidad con distintos sistemas operativos.

Respuesta: c. Diferentes tipos de sistemas de autenticación y tecnologías.
Justificación: La diversidad en los métodos de autenticación entre diferentes sistemas de pago puede crear puntos débiles que los atacantes podrían explotar.

3. ¿Cuál de las siguientes es una amenaza a considerar debido a la expansión a mercados internacionales?

a) Actores maliciosos regionales.
b) Incremento de tráfico en la plataforma.
c) Fallos de hardware.
d) Fluctuaciones de la moneda.
e) Opiniones de clientes insatisfechos.

Respuesta: a. Actores maliciosos regionales.
Justificación: Al expandirse internacionalmente, la empresa se expone a actores maliciosos que son específicos de diferentes regiones y que podrían no haber sido una preocupación en su mercado local.

4. En el contexto de implementación de IoT para la gestión de inventarios, ¿qué factor incrementa la exposición a riesgos?

a) Mayor eficiencia en el seguimiento del inventario.
b) Uso de tecnología de vanguardia.
c) Mayor cantidad de puntos de acceso.
d) Reducción en los costos operativos.
e) Facilita la adaptación a mercados internacionales.

Respuesta: c. Mayor cantidad de puntos de acceso.

Justificación: Al implementar IoT, el número de dispositivos conectados y, por lo tanto, los puntos de acceso a la red aumentan, lo que amplía la superficie de ataque.

5. Ante el desafío de equilibrar seguridad y experiencia de usuario, ¿qué control podría implementarse?

a) Aumentar la complejidad de las contraseñas.
b) Autenticación multifactorial sin contraseñas.
c) Verificación de identidad por video.
d) Encriptación de datos de usuarios.
e) Reconocimiento facial.

Respuesta: b. Autenticación multifactorial.
Justificación: La autenticación multifactorial proporciona una capa adicional de seguridad sin sacrificar significativamente la experiencia del usuario, ya que suele ser rápida y, en muchos casos, ya es conocida por los usuarios.

6. En el contexto del ciberespacio, ¿qué representa el hecho de que la empresa de e-commerce esté expandiéndose a mercados internacionales?

a) Limitación de riesgos.
b) Reducción del cibercrimen.
c) Aumento de la exposición.
d) Autenticidad garantizada.
e) Incremento de la disponibilidad.

Respuesta: c) Aumento de la exposición.
Justificación: Al expandirse a mercados internacionales, la empresa está extendiendo su presencia en el ciberespacio, lo que inevitablemente aumenta su exposición a potenciales amenazas.

7. Considerando la integridad de los datos, ¿qué amenaza podría comprometer las transacciones entre usuarios en el mercado en línea?

a) Fallos en la autenticación multifactorial.
b) Manipulación de datos de transacciones.
c) Control físico inadecuado.
d) Controles disuasivos insuficientes.
e) Expansión internacional.

Respuesta: b) Manipulación de datos de transacciones.
Justificación: La integridad se refiere a asegurar que los datos no sean alterados sin autorización. La manipulación de datos de transacción comprometería directamente esta integridad.

8. Dada la naturaleza global de la empresa de e-commerce, ¿qué representa una mayor preocupación en términos de accountability?

a) Diversos sistemas de pago.
b) Diferentes legislaciones de protección de datos.
c) Variedad de productos ofertados.
d) La utilización del Internet de las Cosas (IoT).

e) Autenticación unifactorial.

Respuesta: b) Diferentes legislaciones de protección de datos.
Justificación: La accountability se refiere a la responsabilidad de las acciones y decisiones. Diferentes legislaciones pueden tener diferentes requisitos y consecuencias legales, lo que complica la responsabilidad.

9. ¿Cuál de las siguientes opciones es un control técnico?
   a) Políticas de seguridad.
   b) Vigilancia en las instalaciones.
   c) Firewalls.
   d) Capacitación sobre seguridad.
   e) Señalizaciones de seguridad.

Respuesta: c) Firewalls.
Justificación: Los firewalls son herramientas técnicas diseñadas para filtrar tráfico y proteger sistemas contra amenazas.

10. Considerando la expansión a mercados internacionales, ¿qué tipo de control sería más efectivo para mitigar riesgos asociados al cibercrimen?
   a) Controles disuasivos.
   b) Controles recuperativos.
   c) Controles compensatorios.
   d) Controles preventivos.
   e) Controles correctivos.

Respuesta: d) Controles preventivos.
Justificación: Dada la ampliación y exposición a nuevas amenazas, es fundamental implementar controles que prevengan el cibercrimen antes de que ocurra.

11. En relación con el principio de defensa en profundidad, ¿qué acción es más coherente?
   a) Implementar un solo control robusto.
   b) Depender únicamente de controles físicos.
   c) Establecer múltiples capas de seguridad.
   d) Concentrarse solo en la autenticidad.
   e) Ignorar los controles recuperativos.

Respuesta: C) Establecer múltiples capas de seguridad.
Justificación: La defensa en profundidad se refiere a la implementación de múltiples capas de seguridad para protegerse contra amenazas.

12. ¿Qué elemento garantiza la autenticidad de una transacción?
   a) La disponibilidad constante.
   b) Un certificado digital.
   c) Una política de privacidad sólida.
   d) La expansión a nuevos mercados.
   e) Controles disuasivos.

Respuesta: b) Un certificado digital.

Justificación: Los certificados digitales validan la identidad de una entidad y garantizan la autenticidad de la comunicación o transacción.

13. Ante un incidente de seguridad, ¿qué control se activaría para corregir el problema?
    a) Control disuasivo.
    b) Control compensativo.
    c) Control preventivo.
    d) Control recuperativo.
    e) Control correctivo.

Respuesta: e) Control correctivo.
Justificación: Los controles correctivos se implementan para corregir problemas una vez que han sido identificados.

14. ¿Qué representa el no repudio en una transacción de comercio electrónico?
    a) Garantiza la disponibilidad de la transacción.
    b) Asegura la confidencialidad de los datos.
    c) Verifica la autenticidad de la transacción.
    d) Asegura que ninguna de las partes puede negar su participación.
    e) Evalúa la vulnerabilidad de la transacción.

Respuesta: d) Asegura que ninguna de las partes pueda negar su participación.
Justificación: El no repudio se refiere a la garantía de que ninguna de las partes involucradas en una transacción pueda negar posteriormente su participación en ella.

15. Ante una brecha de seguridad en la que se filtraron datos sensibles de usuarios, ¿qué principio se ha comprometido primordialmente?

    a) Disponibilidad
    b) Autenticidad
    c) No repudio
    d) Integridad
    e) Confidencialidad

Respuesta: e) Confidencialidad
Justificación: La confidencialidad se refiere a la protección de la información contra la divulgación no autorizada.

16. ¿Qué tipo de control es primordialmente un sistema de videovigilancia en las instalaciones de un centro de datos?

    a) Técnico
    b) Físico
    c) Administrativo
    d) Disuasivo
    e) Recuperativo

Respuesta: b) Físico
Justificación: Los controles físicos están destinados a proteger activos reales o tangibles, como las instalaciones o hardware.

17. Al establecer políticas de acceso a datos y definir roles dentro de la plataforma, la empresa está implementando principalmente controles:

a) Técnicos
b) Físicos
c) Administrativos
d) Correctivos
e) Compensativos

Respuesta: c) Administrativos
Justificación: Los controles administrativos son políticas y procedimientos diseñados para gestionar y monitorear el acceso y uso de procesos, sistemas y datos.

18. Un empleado recibe un correo electrónico de un atacante haciéndose pasar por un proveedor. ¿Qué tipo de cibercrimen es esto?

a) Ataque DDoS
b) Phishing
c) Ransomware
d) Virus
e) Worm
Respuesta: b) Phishing
Justificación: El phishing implica engañar a las víctimas para que compartan información confidencial, a menudo haciéndose pasar por una entidad confiable.

19. De acuerdo con la ley chilena actual sobre delitos informáticos, ¿qué delito está asociado con la introducción, alteración, daño o supresión de datos informáticos con la intención de que estos se consideren auténticos?
a) Ataque a la integridad de un sistema informático.
b) Interceptación ilícita.
c) Falsificación informática.
d) Fraude informático.
e) Abuso de dispositivos.

Respuesta: c) Falsificación informática.

Justificación: El Artículo 5° señala que aquel que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos será sancionado bajo el delito de "Falsificación informática".

20. Según la ley proporcionada, ¿cuál de las siguientes opciones NO es considerada una circunstancia agravante para los delitos tratados en este Título?
a) Cometer el delito abusando de una posición de confianza en la administración del sistema informático.
b) Cometer el delito mientras se interrumpe la prestación de servicios de utilidad pública como transporte.
c) Cometer el delito con la intención de obtener un beneficio económico.
d) Cometer el delito abusando de la vulnerabilidad de niños, niñas, adolescentes o adultos mayores.

e) Cometer el delito utilizando dispositivos creados principalmente para la perpetración de dichos delitos.

Respuesta: c) Cometer el delito con la intención de obtener un beneficio económico.

Justificación: Mientras que las opciones a, b, y d están mencionadas como circunstancias agravantes en el Artículo 10, la opción c es una característica del fraude informático según el Artículo 7°, pero no se menciona como una circunstancia agravante específica en el Artículo 10. La opción está relacionada con el contenido del Artículo 8° pero tampoco se menciona como una circunstancia agravante en el Artículo 10.

21. Según el Código de Ética de EC-Council, ¿cuál de las siguientes afirmaciones es correcta en relación con la propiedad intelectual?

a) Está permitido utilizar la propiedad intelectual de otros siempre que no se obtenga beneficio económico de ello.
b) Se puede usar la propiedad intelectual de otros siempre y cuando no se infrinjan las leyes del país.
c) La propiedad intelectual de otros se debe proteger y confiar en la propia innovación y esfuerzo.
d) Se puede usar la propiedad intelectual de otros si se tiene el consentimiento del propietario.
e) La propiedad intelectual no es relevante en el Código de Ética de EC-Council.

Respuesta: c) La propiedad intelectual de otros se debe proteger y confiar en la propia innovación y esfuerzo.

Justificación: Según el Código de Ética, se debe "Proteger la propiedad intelectual de otros confiando en tu propia innovación y esfuerzos, garantizando que todos los beneficios recaigan en su creador".

22: De acuerdo con el Código de Ética de EC-Council, ¿cuál es la postura correcta respecto a la participación en comunidades de hacking underground que promueven actividades de sombrero negro?

a) Es aceptable si el profesional no participa activamente en actividades de sombrero negro.
b) Se puede participar solo para recopilar información y mejorar la seguridad de los sistemas.
c) Es aceptable siempre y cuando no se violen las leyes del país.
d) Está estrictamente prohibido participar en dichas comunidades.
e) Solo es aceptable si se tiene el consentimiento de EC-Council.

Respuesta: d) Está estrictamente prohibido participar en dichas comunidades.

Justificación: El Código de Ética señala que uno no debe "formar parte de ninguna comunidad de hacking underground con el propósito de predicar y expandir actividades de sombrero negro".

23. Según el Código de Ética Profesional de ISACA, ¿cuál de las siguientes afirmaciones es correcta con respecto a la privacidad y confidencialidad de la información?

a) La información confidencial obtenida puede ser utilizada para beneficio personal si se estima conveniente.
b) La información confidencial debe divulgarse siempre para transparencia.

c) La información confidencial puede ser divulgada únicamente cuando sea requerido por una autoridad legal.
d) La información confidencial puede ser compartida con cualquier parte interesada.
e) La divulgación de información es a discreción del miembro de ISACA.

Respuesta correcta: C) La información confidencial puede ser divulgada únicamente cuando sea requerido por una autoridad legal.

Justificación: El código especifica que los miembros deben "mantener la privacidad y confidencialidad de la información obtenida en el curso de sus deberes a menos que la divulgación sea requerida por una autoridad legal."

24. Según el Código de Ética de ISC2, ¿cuál de las siguientes afirmaciones es correcta respecto a la relación entre los miembros de ISC2 y el Código?

Alternativas:

a) Todos los miembros de ISC2 tienen la opción de seguir o no el Código de Ética.
b) Sólo aquellos miembros de ISC2 que deseen mantener su certificación deben seguir el Código.
c) Aquellos miembros de ISC2 que violen cualquier disposición del Código no enfrentarán ninguna acción disciplinaria.
d) Se obliga a los miembros de ISC2 a seguir el procedimiento de queja ética al observar cualquier acción por parte de un miembro de ISC2 que viole el Código.
e) El Código de Ética de ISC2 tiene como principal objetivo ser un sustituto del juicio ético del profesional.

Respuesta: d) Se obliga a los miembros de ISC2 a seguir el procedimiento de queja ética al observar cualquier acción por parte de un miembro de ISC2 que viole el Código.

Justificación: El Código establece claramente que los miembros de ISC2 están obligados a seguir el procedimiento de queja ética cuando observan una violación del Código por parte de otro miembro.

25. De acuerdo con los cánones del Código de Ética de ISC2, ¿cuál es uno de los deberes fundamentales que los profesionales certificados por ISC2 deben cumplir?

a) Brindar servicios solo cuando se obtenga un beneficio personal.
b) Actuar de manera deshonesta si es necesario para proteger la información.
c) Proporcionar un servicio diligente y competente a los principios.
d) Abstenerse de proteger la infraestructura si va en contra de los intereses de la organización.
e) No adherirse a estándares éticos de comportamiento.

Respuesta: c) Proporcionar un servicio diligente y competente a los principios.

Justificación: Uno de los Cánones del Código de Ética establece explícitamente que los profesionales deben "Proporcionar un servicio diligente y competente a los principios".

26: Para garantizar una expansión efectiva en mercados internacionales, ¿qué metodología puede ayudar mejor a la empresa a alinear su tecnología de la información con las metas empresariales?

a) PCI DSS
b) ISO 27000
c) COBIT
d) CIS Controls
e) Ninguna de las anteriores

Respuesta Correcta: c) COBIT
Justificación: COBIT (Control Objectives for Information and Related Technologies) se enfoca en la gobernanza de TI y cómo alinear los recursos tecnológicos con los objetivos y estrategias empresariales. Sería la opción más adecuada para la empresa que está buscando expandirse internacionalmente y enfrenta desafíos complejos de TI.

27. Para garantizar la seguridad en las transacciones de pago, ¿qué estándar debería seguir la empresa?

a) COBIT
b) CIS Controls
c) PCI DSS
d) ISO 27000
e) Ninguna de las anteriores

Respuesta Correcta: c) PCI DSS
Justificación: PCI DSS (Payment Card Industry Data Security Standard) está específicamente diseñado para proteger las transacciones con tarjetas de crédito y débito y la manipulación de datos sensibles asociados a ellas.

28. ¿Qué conjunto de prácticas se centra más en la implementación y monitoreo de configuraciones de seguridad en dispositivos y sistemas?

a) PCI DSS
b) ISO 27000
c) COBIT
d) CIS Controls
e) Ninguna de las anteriores

Respuesta Correcta: d) CIS Controls
Justificación: CIS Controls (Center for Internet Security Controls) ofrece un conjunto de acciones para la ciberdefensa que proporcionan una defensa específica y efectiva contra amenazas cibernéticas. Estas acciones incluyen la implementación y el monitoreo de configuraciones de seguridad.

Rut: **PEP 1** **25/10/2023**

Segunda Parte: Caso de estudio (50 ptos)

SoftWave Solutions: Violación de Datos en un Proveedor de Desarrollo de Software
SoftWave Solutions, una empresa de desarrollo de software que provee soluciones de gestión empresarial, sufrió un incidente de seguridad crítico en septiembre de 2023. La empresa había implementado múltiples medidas de seguridad como un sistema de detección de intrusiones (IDS), firewalls avanzados, y prácticas de escaneo estático y dinámico de código fuente. Además, contaba con un protocolo de respuesta a incidentes y autenticación de dos factores para acceder a sistemas críticos.

Sin embargo, un grupo de ciberdelincuentes pudo explotar una vulnerabilidad zero-day en una de las bibliotecas de terceros utilizadas en su producto de administración de proyectos. Este acceso inicial les permitió moverse lateralmente a través de la red, eludiendo el firewall y aprovechando brechas en el sistema de autenticación de dos factores.

A pesar de que el sistema de detección de intrusiones (IDS) y el monitoreo de red en tiempo real detectaron comportamientos anómalos, la intervención fue tardía. Para cuando se activó el protocolo de respuesta a incidentes para implementar medidas correctivas y recuperativas, los atacantes ya habían comprometido repositorios de código fuente y bases de datos que contenían información sensible de clientes y empleados.

Inmediatamente después del incidente, SoftWave Solutions movilizó su equipo de respuesta a incidentes y aplicó parches de seguridad para remediar la vulnerabilidad explotada. Se realizaron copias de seguridad de emergencia para garantizar la disponibilidad de los datos y se reforzó la educación en ciberseguridad para todos los empleados. También se revisó y ajustó el firewall para mejorar su funcionalidad preventiva y detectiva. Adicionalmente, la empresa ofreció a sus clientes y empleados afectados un servicio de monitoreo de identidad gratuito como parte de sus medidas correctivas y recuperativas.

Para fortalecer la seguridad en el futuro, SoftWave Solutions implementó cambios en su protocolo de respuesta a incidentes y fortaleció sus controles técnicos y administrativos. Se añadió una capa adicional de autenticación de dos factores, y se intensificaron los esfuerzos en escaneo de código y monitoreo de red en tiempo real para prevenir futuros ataques.

Rut: **PEP 1** **25/10/2023**

1. ¿Cuáles y de qué tipo son los controles presentes en el caso, funcionalidad y objetivo de ciberseguridad (puede ser más 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)
Sistema de Detección de Intrusiones (IDS)	Técnico	Detectivo	Integridad, Confidencialidad, Disponibilidad
Firewall	Técnico	Preventivo, Detectivo	Integridad, Confidencialidad
Escaneo de Código	Técnico	Preventivo	Integridad, Confidencialidad
Educación en Ciberseguridad para Empleados	Administrativo	Preventivo	Integridad, Confidencialidad, Accountability
Monitoreo de Red en Tiempo Real	Técnico	Detectivo, Correctivo	Integridad, Disponibilidad
Protocolo de Respuesta a Incidentes	Administrativo	Correctivo, Recuperativo	Integridad, Confidencialidad, Disponibilidad, Accountability
Autenticación de Dos Factores	Técnico	Preventivo	Confidencialidad, No repudio
Copias de Seguridad	Físico	Recuperativo	Disponibilidad

Rut: **PEP 1** **25/10/2023**

2. Usted es parte del equipo de respuesta a incidentes de "SoftWave Solutions". Se ha decidido que es crucial reevaluar la criticidad de los activos de la empresa para fortalecer las estrategias de mitigación y respuesta. Su tarea es evaluar al menos tres activos críticos de la empresa utilizando los siguientes parámetros:

- Clasificación de Activos (e.g., hardware, software, datos, personal, procesos)
- Valor para el Negocio (en una escala de 1-10)
- Promedio de los principios de Confidencialidad, Integridad, y Disponibilidad (CIA) (en una escala de 1-10)
- Probabilidad de Amenaza (en una escala de 1-10)
- Impacto en Caso de Compromiso (en una escala de 1-10)

Índice de Criticidad = (Valor para el Negocio×Promedio de CIA)+(Probabilidad de Amenaza×Impacto en Caso de Compromiso)

Instrucciones:

Complete la tabla que incluya cada uno de los parámetros y el cálculo del Índice de Criticidad. Priorice los activos según su Índice de Criticidad.

Activos Críticos	Clasificación de Activos	Valor para el Negocio (1-10)	Promedio de CIA (1-10)	Probabilidad de Amenaza (1-10)	Impacto en Caso de Compromiso (1-10)	Índice de Criticidad	Prioridad
Sistema de Detección de Intrusos (IDS)	Software	9	8	8	9	144	2
Bases de Datos de Clientes	Datos	10	9	7	10	170	1
Repositorios de Código Fuente	Datos	8	8	6	8	112	3

Rut: **PEP 1** **25/10/2023**

3. Después del reciente incidente de seguridad, la alta dirección ha decidido reevaluar la eficacia de los controles de seguridad en torno a sus activos más críticos. Se le solicita:

a) Si la amenaza más peligrosa es “Divulgación de Información (Information Disclosure)” sobre el activo más crítico identificado siguiendo el modelo STRIDE. Justifique su elección utilizando el modelo DREAD.

	Justificación
D	● Daño Potencial: Alta exposición de datos personales y financieros de los clientes.
R	● Reproducibilidad: Fácil si no se aplican los controles apropiados.
E	● Explotabilidad: Alta, ya que los atacantes suelen buscar este tipo de información.
A	● Alcance de la Amenaza: Global, podría afectar a todos los clientes.
D	● Descubrimiento: Moderado, podría requerir cierta habilidad técnica para descubrir la vulnerabilidad.

b) Evaluar la efectividad de un control de seguridad actual para mitigar esta amenaza y proponga un nuevo control de seguridad que podría implementarse para mejorar la protección de la base de datos.

Tabla de Análisis

Campo	Detalle	Justificación
Activo	Base de Datos de Clientes	Es el activo más crítico identificado en la etapa anterior.
Vulnerabilidad	Exposición de datos sensibles	Se hace el supuesto que el software de base de datos es legado (por lo que no se puede actualizar).
Amenaza	Divulgación de Información (Information Disclosure)	Justificado anteriormente
Agente de Amenaza	Ciberdelincuentes	Podrían ser empleados descontentos o maliciosos.
Exposición	Alta	Dado que contiene información financiera y personal de todos los clientes.

Rut: **PEP 1** **25/10/2023**

Control Actual (ca)	Autenticación de dos factores para el acceso	Para autenticar a los clientes y empleados.
Impacto (ca)	Alto	pérdida de confianza, consecuencias legales
Probabilidad (ca)	Alta	Dados los ataques previos y el valor de los datos
Riesgo (ca)	Relevante	Dada la tabla provista
Control Propuesto	Encriptación de Datos en Reposo y en Tránsito	Dado que buscamos que incluso si se filtran los datos no podamos obtenerlos.
Impacto (cp)	Bajo	Ya que si se filtra estará encriptado.
Probabilidad (cp)	Alta	Este control no afecta la probabilidad de ocurrencia. Quizás como control disuasorio podría bajar su probabilidad
Riesgo (cp)	Aceptable	Dada la tabla provista.

Instrucciones:

- Asegúrese de completar la tabla.
- Proporcione una explicación detallada para cada uno de los campos de la tabla.
- Asegúrese de justificar todas sus elecciones y resultados.
- Haga los supuestos que sean necesarios (Indíquelos a continuación).
- Utilice la siguiente tabla de impacto-probabilidad.

Prob\Impacto	Muy bajo	Bajo	Medio	Alto	Muy alto
Altisima	Aceptable	Relevante	Crítico	Crítico	Crítico
Alta	Aceptable	Aceptable	Relevante	Relevante	Crítico
Media	Irrelevante	Aceptable	Aceptable	Relevante	Relevante
Baja	Irrelevante	Irrelevante	Aceptable	Aceptable	Relevante
Insignificante	Irrelevante	Irrelevante	Irrelevante	Aceptable	Aceptable