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

Rut: **PEP 1**

Fecha: 02/11/2022 - **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) Buenas prácticas, estándares y metodologías. Escoja la alternativa correcta y encierrela en un circulo en la tabla del final de la sección.

1. (5 pts) Marco de trabajo que permite el reconocimiento de tácticas y técnicas utilizadas por un atacante sobre un sistema. Alguna de sus 14 tácticas son el reconocimiento, desarrollo de ruecrsos y acceso inicial, filtración e impacto.
    a. STRIDE
    b. Cyber Kill Chain
    c. CAPEC
    d. Mitre Att&ck Framework
    e. Ninguna de las anteriores

2. (5 ptos) Las siguientes son características de los controles CIS:
    i. Ayuda a los defensores a identificar los puntos más críticos que deben hacer para detener los ataques más importantes .
    ii. Sus primeros controles apuntan a identificar y controlar activos.
    iii. Se definen con el principio de “ofensiva informa a la defensiva”.
    iv. Todas sus recomendaciones individuales son específicas y prácticas de implementar.
    v. Establece las prácticas más fundamentales y valiosas que toda empresa debería considerar.

    a. i,ii
    b. i,ii,iii
    c. i,ii,iii,iv
    d. i, ii, iii, iv, v
    e. i, ii, iii, v

3. (5ptos) A la hora defender la necesidad de invertir en nuevos controles de ciberseguridad, la estimación de costos y beneficios es un desafío ¿Por qué?
    a. Es dificil estimar los beneficios de las políticas y mecanismos de seguridad.
    b. La seguridad a través de la oscuridad es una práctica habitual en las organizaciones.
    c. Los activos de la organización en el ciberespacio están bajo amenaza constante.
    d. Todas las anteriores
    e. Ninguna de las anteriores

4. (5 pts) Buena práctica, estándar o metodología que identifica controles de seguridad en cada etapa del ciclo de vida del software.

Rut: **PEP 1**

a. CWE Top 25
b. OWASP SAMM
c. Microsoft SDL.
d. NIST SP 800-53
e. LINDDUN

5. (5 pts) A cual de los siguientes estándares, metodologías o buenas prácticas corresponde el siguiente objetivo:

"Enfoque priorizado, flexible, repetible, basado en el desempeño y costo efectivo, que incluya medidas de seguridad de la información y controles que los propietarios y operadores de infraestructura crítica puedan adoptar voluntariamente para ayudarlos a identificar, evaluar y gestionar los riesgos cibernéticos"

a. ISO 27000
b. NIST Cybersecurity Framework
c. CIS Controls
d. COBIT
e. Ninguna de las anteriores

6. (5 pts) Entre los objetivos del PCI DSS se tienen:

i. Construir y mantener una red y sistemas seguros
ii. Reglas de comportamiento (uso aceptable)
iii. Proteger los datos del titular de la tarjeta de crédito
iv. Mantener una política de seguridad de la información.
v. Monitorear y probar redes regularmente

Son verdaderas:

a. ii, iii, iv y v
b. i, ii, iii y iv
c. i, iii y iv
d. i, iii, iv y v
e. Todas son verdaderas

7. (5 pts) Entre las caterogorias del SGP se tiene la gestión de la función de la ciberseguridad, esta consta de 12 funciones, entre las cuales se tiene:

i. Gestión de personas
ii. Gestión de la información
iii. Gestión de la cadena de suministro
iv. Continuidad del negocio
v. Acceso a sistemas

Son verdaderas:

a. i, ii, iii y v
b. i, ii, iv y i
c. i, iii y iv
d. ii, iii, iv y v
e. Todas son verdaderas

8. (5 pts) Para crear un programa de ciberseguridad con el NIST CSF uno de los pasos es crear el perfil actual de la organización. Para ello es escencial contar con:

i. Objetivos de la organización

Rut: **PEP 1**

ii. Ambiente de amenazas en que se desenvuelve

iii. Requerimientos y controles actuales

iv. Análisis de riesgos

Son verdaderas:

a. i, ii y iii
b. i y ii
c. i, iii y iv
d. ii, iii, iv
e. Todas son verdaderas

Encierre en un circulo la alternativa escogida.

Pregunta	**Alternativa**		**Pregunta**	**Alternativa**
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 1**

II. (20 ptos) Conceptos

1. Rellene el cuadro con el concepto o la definición correspondiente:

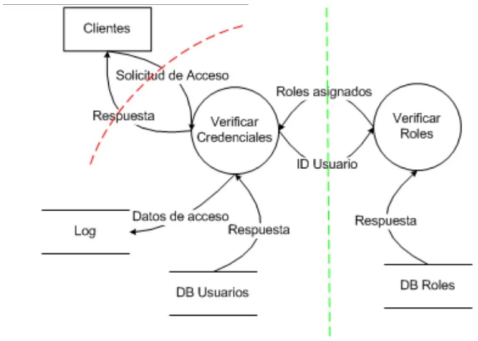
Concepto	**Definición**
Confidencialidad	La propiedad de que los datos no se divulgan a las entidades del sistema a menos que hayan sido autorizados para conocer los datos.
Nivel de riesgo	Magnitud de un riesgo o combinación de riesgos, expresados en términos de la combinación de las consecuencias y su probabilidad.
Disponibilidad	La propiedad de un sistema o un recurso del sistema que es accesible o utilizable u operacional bajo demanda, por una entidad autorizada del sistema, de acuerdo con las especificaciones de rendimiento del sistema; es decir, un sistema está disponible si proporciona servicios de acuerdo con el diseño del sistema cuando los usuarios lo soliciten.
Vulnerabilidad	Debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
Integridad	La propiedad de que los datos no se han cambiado, destruido o perdido de manera no autorizada o accidental.
Autenticidad	La propiedad de ser genuino y poder ser verificado y confiable
Vector de ataque	Camino o medios por los cuales un atacante puede obtener acceso a un equipo para entregar un resultado malicioso.
Política	Intenciones y dirección de una organización, como las expresa formalmente su alta dirección.
Control	Que elimina una vulnerabilidad o que reduce la probabilidad de que un agente de amenaza sea capaz de explotar una vulnerabilidad
Defensa en profundida	Coordinación de multiples controles utilizando una aproximación en capas tal que el atacante deba sortear varias dificultades antes de poder acceder a algún activo crítico de la organización.

Rut: **PEP 1**

III. Caso de estudio (60 ptos)

La empresa DRAGON S.A. ha puesto en producción un nuevo sitio de web de atención clientes. Estos clientes se encuentran clasificados por diferentes roles, de acuerdo a los cuales estos pueden acceder a diferentes servicios de la empresa. Para ello, el sistema se encuentra expuesto a internet, para que los clientes puedan acceder directamente a través de la web.

La gerencia de ACME S.A. se encuentra preocupada por sus medidas de seguridad, dado los últimos ciberataques que han aparecido en la prensa. Por lo anterior, el encargado de seguridad implementa algunos controles sobre los servidores de la organización en donde se tienen los servicios, ej: Firewalls, sistema anti-DoS, configuraciones restrictivas sobre los servidores web (hardening), separación de ambientes, política de desarrollo seguro, procedimientos de recuperación ante desastre (DRP), sistema de respaldo, entre otras. Además, ha realizado una revisión en detalle del sistema objetivo realizando modelos de amenaza por cada módulo. En particular, el siguiente modelo es sobre el módulo de autenticación.



Este modelo se separa en dos limites de confianza, el primero que limita con Internet y el segundo que separa el servicio de verificación de credenciales con el servicio de verificar roles. Esta última conexión se realiza a través de APIs. El servicio de verificación de credenciales se le entrega nombre de usuario y contraseña del cliente y se contrasta contra la DB de usuarios, si estos son correctos se le entrega el id de usuario al servicio de verificación de roles y este entrega el rol del usuario en la plataforma.

1. (24 ptos) ¿Cuáles y de qué tipo son los controles presentes en el caso y funcionalidad? (Indique 8)

Control **1 ptos/cu**	**Tipo de control (administrativo, técnico, físico) 1pto/cu**	**Funcionalidad o principal razón de ser del control (Preventivo, Detectivo, Correctivo, Recuperativo) 1 pto/cu**
Logs	Técnico	Detectivo
Control de acceso basado en roles	Técnico	Preventivo
Separación de ambientes	Técnico	Preventivo
Firewall	Técnico	Preventivo
Sistema anti-DoS	Técnico	Preventivo
Hardening	Técnico	Preventivo
Política de desarrollo seguro	Administrativo	Preventivo
Sistema de respaldo	Técnico	Recuperativo
DRP	Técnico	Recuperativo

Rut: **PEP 1**

UdeSantiago de Chile

Rut: **PEP 1**

2. (18 pts) De acuerdo a la taxonomia STRIDE y al diagrama anterior, indique el objetivo de seguridad asociado, una amenaza y su agente de amenaza para cada categoria.

Categoria de la amenaza	**Objetivo de seguridad deseado (1 pto)**	**Agente de amenaza (1 pto)**	**Descripción Amenaza (1 pto)**
Spoofing (Suplantacion)	Autenticidad	Hacker	Alguien externo obtiene las credenciales del cliente y realiza solicitudes de servicios.
Tampering (Manipulación)	Integridad	Hacker	Inyección de SQL sobre las bases de datos de la organización
Repudiation (Repudiación)	No repudio	Cliente	Cliente solicita servicio de la organización y este no se hace responsable de su solicitud.
Information Disclouse (Revelación de información)	Confidencialidad	Empleado	Un empleado podría extraer desde los logs los id de los usuario y consultar sus roles desde el servicio de verificación de roles.
Denial of service (Denegación de servicio)	Disponibilidad	Hacker	Ataque de denegación de servicio al intentar una autenticación masiva en el servidor.
Elevation of privilege (Elevación de privilegio)	Autorización	Cliente	Un cliente autenticado podría intentar acceder a secciones de otros servicios web dentro del aplicativo.

Rut: **PEP 1**

3. Desarrolle un análisis de riesgo cualitativo que refleje el escenario anterior.

   a. (6 ptos) Plantee una matriz de análisis cualitativo con 3 niveles de impacto y 3 niveles de probabilidad (Considere riesgo: extremo, alto, medio, bajo).

Probabilidad / Impacto	Alta	Medio	Bajo
Alto	Extremo	Alto	Medio
Medio	Alto	Medio	Bajo
Bajo	Medio	Bajo	Bajo

   b. (10 ptos) Realice el análisis de riesgos sobre una de las amenazas identificadas (STRIDE), considerando lo anterior.

Amenaza	**Vulnerabilidad**	**Activo involucrado**	**Impacto**	**Probabilidad**	**Riesgo inherente**
Debe ser acorde al problema y a la definición de amenaza	Debe ser acorde al problema y a la definición de vulnerabilidad	Debe ser acorde al problema	Debe ser acorde a la tabla	Debe ser acorde a la tabla	Debe ser acorde a la tabla

Controles mitigantes	**Impacto**	**Probabilidad**	**Riesgo residual**
Debe mitigar la amenaza	Debe ser acorde a la tabla y al control	Debe ser acorde a la tabla y al control	Debe ser acorde a la tabla

   c. (6 ptos) Justifique los niveles de impacto y probabilidad escogidos

Debe justificar los niveles escogidos de acuerdo al control

Rut: **PEP 1**

d. (6 ptos) Proponga al menos 1 control para conseguir un riesgo medio. Justifique la elección del control, el nuevo impacto y probabilidad.

Debe justificar el control de acuerdo al problema.
Debe justificar el impacto y la probabilidad de acuerdo a la tabla y al control escogido.