Universidad Nacional Mayor de San Marcos

Facultad de Ingeniería de Sistemas e Informática
Unidad de POSTGRADO
Maestría de Ingeniería de Sistemas e Informática
Mención en Ingeniería de Software

Examen: EXAMEN FINAL

Curso: Ciberseguridad en la Ingeniería de Software
Docente: JORGE ERNESTO PISCOYA PRÍNCIPE
Fecha: 02.08.24
Alumno: _____
Código de alumno: _____

Instrucciones Generales:

1. Lea cuidadosamente cada pregunta antes de responder.
2. Responda de forma clara y precisa.
3. Justifique sus respuestas cuando se indique.
4. Este examen tiene un total de **20 puntos**.
5. El examen debe ser enviado a **jorge.piscoya1@unmsm.edu.pe** con el asunto "EXAMEN FINAL – *CÓDIGO_DE_ALUMNO – NOMBRE_COMPLETO*"

Universidad Nacional Mayor de San Marcos

CASO 1: Fortalecimiento de la Ciberseguridad en el Hospital SaludVida (7 puntos)

El hospital SaludVida es una institución médica de alta complejidad, dedicada a proporcionar atención médica integral a más de 500 pacientes diarios. En los últimos años, el hospital ha adoptado una infraestructura tecnológica avanzada para optimizar tanto la atención de los pacientes como la gestión administrativa. Entre sus sistemas más importantes se encuentran:

- Historia Clínica Electrónica (HCE): Un sistema digitalizado que almacena y gestiona los registros médicos de los pacientes, accesible tanto por médicos como por personal administrativo.
- Sistema de Gestión Hospitalaria (HIS): Un software utilizado para gestionar la programación de citas, asignación de camas y control de insumos médicos, accesible para el personal administrativo y clínico.
- Portal Web para Pacientes: Una plataforma en línea que permite a los pacientes agendar citas, consultar resultados de laboratorio y acceder a información médica general.

A lo largo de los últimos años, SaludVida ha incrementado su dependencia de tecnologías interconectadas, entre las que destacan los dispositivos médicos conectados a la red, como monitores de signos vitales, bombas de infusión y ventiladores mecánicos. Estos dispositivos, clasificados como Internet de las Cosas (IoT), recopilan y transmiten datos sensibles sobre la salud de los pacientes en tiempo real. Sin embargo, la falta de políticas estrictas en ciberseguridad para este tipo de dispositivos ha generado preocupaciones sobre su vulnerabilidad a ciberataques.

El hospital también tiene una red interna de trabajo que conecta a su personal administrativo, clínico y de apoyo. Además, ha implementado una red Wi-Fi abierta para los pacientes, lo que, si bien facilita la conectividad, también incrementa el riesgo de intrusión. Aunque se han realizado esfuerzos para actualizar sus sistemas, no existe una estrategia formal de gestión de la seguridad cibernética.

En los últimos meses, SaludVida ha experimentado varios incidentes de seguridad:

- Phishing: El personal administrativo ha sido víctima de un ataque de phishing que comprometió varias credenciales de acceso, afectando la seguridad de los sistemas internos.
- Malware: En un incidente reciente, dos estaciones de trabajo fueron infectadas por malware debido a un clic en un enlace malicioso en un correo electrónico. Aunque el ataque fue contenido rápidamente, dejó al descubierto la falta de un sistema adecuado de detección y respuesta.
- Ransomware en hospitales cercanos: La reciente infección de ransomware en un hospital vecino ha puesto en alerta a SaludVida, ya que este tipo de ataques podrían paralizar completamente las operaciones del hospital, poniendo en riesgo la atención médica y la seguridad de los pacientes.

Dada la creciente preocupación sobre la seguridad cibernética y los incidentes que han ocurrido en hospitales cercanos, la gerencia de SaludVida ha decidido tomar medidas inmediatas para mejorar la postura de seguridad del hospital y prevenir futuros incidentes.

La dirección ha optado por implementar el Marco de Ciberseguridad NIST 2.0 como base para este esfuerzo, con el fin de garantizar la confidencialidad, integridad y disponibilidad de sus sistemas y datos sensibles.

SaludVida enfrenta un desafío importante, ya que su personal de TI está compuesto por solo cinco personas y los recursos financieros para implementar una estrategia de ciberseguridad son limitados. No obstante, el hospital cuenta con el respaldo de su junta directiva para realizar las inversiones necesarias en seguridad, con el objetivo de proteger tanto la infraestructura digital como la información sensible de los pacientes.

En este contexto, los consultores contratados deberán aplicar el Marco NIST 2.0 para diseñar un plan de ciberseguridad integral.

Pueden utilizar las siguientes plantillas que se encuentran en la siguiente carpeta: https://drive.google.com/drive/folders/1miUrhgYVpDVILIAV1NLAutLti8q1ivGC?usp=sharing en caso crean conveniente.

ACTIVIDAD

1. Identificar

Realizar un análisis para entender el entorno tecnológico del hospital y sus riesgos asociados.

Actividades:

1. **Identificar activos críticos:**
    - Crear un inventario de sus activos críticos del hospital, como HCE, HIS, dispositivos IoT, y redes internas.
    - Incluir datos sensibles que requieren protección, como información médica de pacientes y credenciales de acceso.
2. **Evaluar riesgos:**
    - Identificar amenazas específicas, como ataques de phishing, malware, y vulnerabilidades en dispositivos IoT.
    - Priorizar los riesgos según su impacto potencial en la operación del hospital.

---

2. Proteger

Proponer medidas para reducir los riesgos identificados en la fase anterior.

Actividades:

1. **Medidas de control de acceso:**
    - Diseñar una estrategia para implementar autenticación multifactor (MFA) en sistemas como HCE y HIS.

- Crear la política “Control de Accesos Seguros”.

2. **Protección de dispositivos IoT:**
   - Proponer un plan para segmentar la red y aislar dispositivos IoT.
3. **Educación y concienciación:**
   - Crear un calendario de concienciación para evitar ataques de phishing y fomentar buenas prácticas entre el personal del hospital. El calendario y las capacitaciones deben estar orientadas al rol y a sus funciones.
4. **Respaldo de datos:**
   - Definir un procedimiento para realizar copias de seguridad automáticas de los sistemas críticos.

---

3. Detectar

La detección temprana de incidentes es clave para mitigar daños.

Actividades:

1. **Sistemas de monitoreo:**
   - Establecer los puntos clave de monitoreo clave para la organización.
2. **Alertas y notificaciones:**
   - Establecer el tipo de alertas y notificaciones para salvaguardar los aspectos claves del sistema.
3. **Auditorías de seguridad:**
   - Establecer un calendario de auditorías regulares para evaluar la efectividad de las medidas de detección. Además de establecer los responsables de las auditorías.

---

4. Responder

Crear un plan de respuesta para minimizar los daños en caso de un incidente.

Actividades:

1. **Protocolo de respuesta:**
   - Diseñar un procedimiento paso a paso para responder a ataques de phishing y malware.
2. **Comunicación en caso de incidentes:**
   - Crear un plan de comunicación interno y externo que detalle cómo notificar al personal, autoridades y pacientes en caso de un incidente.
3. **Equipo de respuesta a incidentes:**

- Definir roles y responsabilidades dentro del equipo de respuesta.

---

5. Recuperar

En esta fase, se deben proponer medidas para restaurar las operaciones del hospital tras un incidente.

Actividades:

1. **Plan de recuperación:**
   - Diseñar un plan para restaurar las funciones críticas del hospital en menos de 24 horas, priorizando sistemas como HCE y HIS.
2. **Simulacros de recuperación:**
   - Proponer ejercicios prácticos para identificar la efectividad del plan de recuperación.
   - Calendarizar los simulacros de recuperación y establecer qué roles participarán de cada simulacro.
3. **Lecciones aprendidas:**
   - Establecer un proceso para documentar y analizar los incidentes, a fin de mejorar la seguridad a largo plazo.

Universidad Nacional Mayor de San Marcos

CASO 2: Fortalecimiento de la Ciberseguridad en el distrito de Miraflores (4 puntos)

La municipalidad de Miraflores ha impulsado la transformación digital para ofrecer servicios más eficientes a sus ciudadanos. En los últimos años, han implementado sistemas tecnológicos avanzados que incluyen:

- Plataforma de Gobierno Digital (PGD): Un portal para trámites municipales en línea.
- Infraestructura IoT: Sensores para monitorear tráfico, alumbrado público y calidad del aire.
- Red de Videovigilancia Inteligente (RVI): Cámaras con análisis de video en tiempo real para seguridad ciudadana.
- Sistema de Gestión de Emergencias (SGE): Una plataforma para coordinar respuestas ante desastres naturales.
- Aplicación Móvil SmartApp: Permite a los ciudadanos reportar incidencias en tiempo real y consultar servicios municipales.

A pesar de los avances, Miraflores enfrenta crecientes amenazas de ciberseguridad, que incluyen intentos de acceso no autorizado, ataques de ransomware, y vulnerabilidades en su infraestructura IoT. Recientemente, un incidente comprometió temporalmente el acceso a la PGD, generando desconfianza en la ciudadanía.

La municipalidad ha decidido implementar el Marco NIST 2.0 para mejorar su postura de ciberseguridad. Los estudiantes deberán identificar funciones, categorías y subcategorías específicas del marco, basándose en el caso.

ACTIVIDAD

Los estudiantes trabajarán en las siguientes fases:

Fase 1: Identificación de Funciones

Instrucción: Identifica las funciones del marco NIST 2.0 (Identificar, Proteger, Detectar, Responder y Recuperar) aplicables a las necesidades del caso.

Ejemplo: de resolución

- Función: Identificar: Identificar activos críticos como sensores IoT, servidores de la PGD y el SGE, y bases de datos sensibles.

Fase 2: Análisis por Categorías

Instrucción: Para cada función, identifica las categorías relacionadas.

Ejemplo de resolución:

- Función: Proteger
    - Categoría: Protección de Identidad y Accesos (PR.AC): Implementar autenticación multifactor en la PGD y segmentación de red para sensores IoT.

Fase 3: Asignación de Subcategorías

Basándote en las categorías identificadas, selecciona subcategorías específicas que Miraflores debería implementar. Justifica tu elección con ejemplos concretos del caso.

Ejemplo de resolución:

- Función: Detectar
  - Categoría: Actividades de Monitoreo (DE.CM)
    - Subcategoría: DE.CM-1: La red de la municipalidad debe ser monitoreada para detectar actividades no autorizadas.
    - Subcategoría: DE.CM-8: Integrar alertas automatizadas en la Red de Videovigilancia Inteligente para detectar anomalías.

Fase 4: Estrategias de Implementación

Instrucción: Proponer estrategias prácticas para implementar todas las subcategorías seleccionadas. Explica cómo estas estrategias contribuyen a reducir riesgos y aumentar la seguridad.

Ejemplo:

- Función: Responder
  - Subcategoría: RS.RP-1: Crear un plan de respuesta a incidentes para ataques de ransomware en la PGD.
  - Estrategia: Diseñar simulacros trimestrales de respuesta a incidentes con participación del personal técnico y administrativo.

Universidad Nacional Mayor de San Marcos

CASO 3: Análisis de Seguridad en el Portal Académico Universitario (4 puntos)

Contexto General

La **Universidad Metropolitana** es una institución educativa con más de 15,000 estudiantes y 2,000 docentes. Recientemente, la universidad ha lanzado su **Portal Académico Universitario (PAU)**, un sistema integral diseñado para mejorar la interacción entre estudiantes, docentes y administrativos. A través de este portal, se gestionan funciones críticas como la inscripción a cursos, la visualización de calificaciones, la descarga de documentos personales, y la comunicación interna entre estudiantes y profesores.

Sin embargo, después de un par de meses de uso, varios usuarios han reportado incidentes de seguridad y privacidad en el portal, lo que ha generado preocupaciones tanto en la administración universitaria como en los estudiantes y docentes. El objetivo de este caso es que los estudiantes analicen estos incidentes de seguridad y apliquen las categorías del **OWASP Top 10 (2021)** para identificar y mitigar las vulnerabilidades presentes en el sistema.

Detalles Técnicos del Sistema

1. **Usuarios del Portal:**
    - **Estudiantes:** Acceden a su perfil, visualizan y descargan sus calificaciones y documentos personales, y gestionan la inscripción a cursos.
    - **Docentes:** Acceden a sus cursos, pueden ver las calificaciones de los estudiantes, gestionar asignaciones y subir material de lectura.
    - **Administrativos:** Administran procesos internos como la inscripción a cursos, modificación de horarios y carga de información académica en la plataforma.
2. **Autenticación:**
    - El portal utiliza autenticación basada en **correo electrónico institucional** y **contraseña**. Además, algunos usuarios (principalmente administrativos) tienen **autenticación multifactor (MFA)** habilitada por medidas de seguridad adicionales.
    - Existe un **módulo de recuperación de contraseñas** que envía un enlace al correo electrónico institucional del usuario para restablecer la contraseña.
3. **Funciones Críticas del Sistema:**
    - **Inscripción a cursos:** Los estudiantes se inscriben en los cursos de cada semestre a través de un formulario en línea.

- **Generación de calificaciones y reportes:** Los docentes cargan las calificaciones de los estudiantes a través de formularios en el portal.
- **Documentos personales:** Los estudiantes pueden descargar documentos como boletas de pago, constancias de estudios, y horarios de clase.
- **Comunicaciones internas:** Los estudiantes y docentes pueden enviar y recibir mensajes dentro del sistema de mensajería del portal.

4. **Base de Datos:**
   El sistema almacena datos sensibles de los usuarios, como nombres completos, documentos de identidad, direcciones, correos electrónicos y registros académicos. También se guardan registros de la actividad de los usuarios para auditoría interna.

Problemas Detectados en el Portal

1. **Accesos indebidos a información personal de otros usuarios:**
   - Un estudiante reportó que, al acceder a su perfil, pudo visualizar las calificaciones de otros estudiantes que no pertenecen a su curso. Tras investigar, se descubrió que los identificadores de los perfiles no eran lo suficientemente robustos y no existían restricciones en las URL, lo que permitía modificar el parámetro de la URL y acceder a datos de otros usuarios.
2. **Subida de archivos inseguros:**
   - Docentes informaron que al cargar archivos para las evaluaciones de los estudiantes (en formato PDF), algunos de esos archivos contenían **código malicioso** que afectaba el funcionamiento del sistema. No se estaba realizando un análisis adecuado del contenido de los archivos cargados, ni se verificaban los tipos de archivo permitidos.
3. **Alteración no autorizada de datos académicos:**
   - Un estudiante logró alterar su horario de clases a través de una vulnerabilidad en el formulario de inscripción en línea. El estudiante manipuló los parámetros en la URL, permitiéndole inscribirse en asignaturas que no le correspondían.
4. **Manejo deficiente de contraseñas:**
   - Se descubrió que el sistema de recuperación de contraseñas era vulnerable a ataques de **phishing**. En lugar de confirmar la identidad del usuario a través de múltiples capas de seguridad, el sistema solo validaba el correo electrónico, lo que permitía a un atacante acceder a una cuenta simplemente conociendo el correo de un usuario.

Universidad Nacional Mayor de San Marcos

ACTIVIDAD

Los estudiantes deberán analizar cada uno de los problemas mencionados y relacionarlos con las vulnerabilidades del **OWASP Top 10 (2021)**.

Actividades del Caso

1. **Identificación de Vulnerabilidades:**
    - Relacionar cada uno de los problemas descritos con una categoría del OWASP Top 10. Justificar la elección con ejemplos específicos del caso.
    - Para cada vulnerabilidad, describir cómo se podría haber explotado para afectar la seguridad del sistema.
2. **Impacto de las Vulnerabilidades:**
    - Analizar el impacto de cada vulnerabilidad en la **confidencialidad, integridad y disponibilidad** del sistema.
    - Evaluar el daño potencial tanto a nivel **técnico** como **reputacional** para la universidad, sus estudiantes y docentes.
3. **Recomendaciones y Mitigaciones:**
    - Proponer medidas específicas y **factibles** para mitigar cada vulnerabilidad, incluyendo cambios en la configuración del sistema, desarrollo de nuevas funcionalidades o mejoras en los procesos de autenticación y validación.
    - Sugerir **mejores prácticas** para prevenir estos problemas en el futuro y mejorar la seguridad del portal en su conjunto.

Universidad Nacional Mayor de San Marcos

CASO 4: Implementación de una Plataforma de Aprendizaje en Línea para la Universidad Global de Tecnología (UGT) (5 puntos)

La Universidad Global de Tecnología (UGT) es una institución educativa internacional con más de 50,000 estudiantes distribuidos en diversos países de América Latina, Europa, y Asia. Debido a su carácter global, la universidad ha decidido implementar una nueva plataforma de aprendizaje en línea para ofrecer cursos y programas académicos de forma remota, facilitando el acceso a la educación superior a estudiantes de diversas partes del mundo.

La plataforma permitirá la gestión de los contenidos académicos, la realización de exámenes en línea, la comunicación entre estudiantes y profesores, la administración de notas y la gestión de pagos de matrícula. Además, deberá garantizar una experiencia personalizada según las necesidades de cada estudiante y las particularidades de cada país, considerando las regulaciones locales, los distintos dispositivos y sistemas operativos que utilizan los estudiantes y la infraestructura tecnológica variada de cada región.

A través de esta plataforma, los estudiantes podrán acceder a materiales de cursos como videos, lecturas, tareas y foros, pero también interactuar con otros usuarios en tiempo real a través de videoconferencias o chats. El sistema de pagos permitirá a los estudiantes pagar la matrícula y otras tarifas, y contará con diferentes métodos de pago dependiendo de la región en la que se encuentren. Además, la universidad desea garantizar la privacidad de los datos de los estudiantes, cumpliendo con las normativas internacionales como el Reglamento General de Protección de Datos (GDPR) para sus usuarios en Europa, y las leyes locales de privacidad en América Latina y Asia.

La universidad también busca asegurar que su plataforma sea inclusiva, de fácil acceso y que se adapte a las condiciones cambiantes del entorno y del usuario. La plataforma debe ser accesible desde diferentes dispositivos (computadoras de escritorio, portátiles y dispositivos móviles) y funcionar correctamente incluso en áreas con infraestructuras de red limitadas.

La universidad planea integrar funcionalidades adicionales en el futuro, tales como un sistema avanzado de recomendación de cursos, herramientas de gamificación para mejorar la interacción de los estudiantes, y un sistema de seguimiento de progreso académico. La plataforma también debe ofrecer soporte para distintos idiomas y cumplir con las normativas locales en cada país sobre educación y privacidad.

Universidad Nacional Mayor de San Marcos

ACTIVIDAD I

Analizar cómo se presentan las dimensiones de variabilidad dentro de la implementación de la plataforma de aprendizaje en línea. Para ello, debe identificar 3 ejemplos específicos de cada una de las siguientes dimensiones y su relación con el contexto planteado. (El ejemplo 1 ya lo tienen establecido, les faltaría 2 ejemplos más)

Dimensiones de variabilidad:

1. Variabilidad Funcional: La variabilidad funcional se refiere a los cambios o adaptaciones en las funcionalidades del sistema según las necesidades del usuario o las características del entorno de implementación.

Ejemplo 1:

- **Funciones de evaluación en línea:** La universidad permite a los profesores crear y administrar exámenes en línea. Sin embargo, en algunos países, los exámenes deben cumplir con ciertos **requisitos de anonimato**, como no mostrar el nombre del estudiante a los profesores durante el proceso de evaluación.

2. Variabilidad Técnica

La variabilidad técnica se refiere a las diferencias en la infraestructura tecnológica, sistemas operativos, plataformas y dispositivos que deben ser soportados por el software.

Ejemplos:

- **Compatibilidad con diferentes dispositivos:** La plataforma debe ser accesible tanto en **computadoras de escritorio** como en **dispositivos móviles** (smartphones y tablets), independientemente del sistema operativo (Windows, MacOS, Android, iOS).

3. Variabilidad Organizacional

La variabilidad organizacional se refiere a los cambios necesarios en el sistema basados en las políticas internas de la universidad o las regulaciones locales que deben cumplirse.

Ejemplos:

- **Políticas de privacidad y acceso:** La universidad tiene **políticas internas** sobre la gestión de los datos personales de los estudiantes. Por ejemplo, en Europa, la plataforma debe cumplir con el **GDPR** y garantizar que los datos personales sean manejados de forma segura. En otros países, las políticas locales sobre privacidad pueden ser más o menos estrictas.

4. Variabilidad Contextual

La variabilidad contextual se refiere a los ajustes del sistema basados en el entorno o las condiciones externas del usuario.

Ejemplos:

- **Adaptación a las condiciones de red:** En algunos países con infraestructuras de red limitadas, la plataforma debe ofrecer una versión **ligera** de los contenidos (como materiales en **bajas resoluciones** o versiones sin videos), para que los estudiantes puedan acceder sin problemas de carga.

ACTIVIDAD II

Además, responder las siguientes preguntas

1. ¿Qué cambios o adaptaciones serían necesarios en la plataforma para cada tipo de variabilidad? (Contemplar las 8 variabilidades establecidas por el alumno)
2. ¿Cómo impactaría cada tipo de variabilidad en el diseño y seguridad del sistema? (Contemplar las 8 variabilidades establecidas por el alumno)
3. ¿Qué medidas de seguridad serían necesarias para mitigar los riesgos asociados a cada tipo de variabilidad? (Contemplar las 8 variabilidades establecidas por el alumno)
4. ¿Cuáles serían los desafíos más importantes para garantizar una implementación exitosa de la plataforma en todas las regiones involucradas?