UNIVERSIDAD DE SANTIAGO DE CHILE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE INGENIERÍA INFORMÁTICA

FUNDAMENTOS DE CIBERSEGURIDAD
Prof. Juan Ignacio Iturbe

ACTIVIDAD GRUPAL 1:
INTRODUCCIÓN
BUENAS PRÁCTICAS, ESTÁNDARES, METODOLOGÍAS Y NORMATIVAS

Exigencia: 70%

1. CONTEXTO

El avance acelerado de la tecnología y la creciente digitalización de los servicios financieros han dado lugar a un entorno donde la ciberseguridad no es solo un aspecto técnico, sino también una cuestión crítica de negocio. En este contexto, el presente trabajo se centra en evaluar la estrategia de ciberseguridad de "BankSecure", una aplicación de banca digital desarrollada por la compañía FinTech InverSecure. La app se diseñó utilizando una arquitectura de microservicios y microfrontends para ofrecer a los usuarios una experiencia segura y personalizada en la gestión de sus finanzas.

Los objetivos de este trabajo son dobles. Primero, buscamos aplicar los conceptos teóricos de ciberseguridad para identificar vulnerabilidades, riesgos y posibles controles en el caso práctico de BankSecure. Segundo, pretendemos integrar las mejores prácticas, estándares y legislaciones relevantes en la planificación y evaluación de su estrategia de ciberseguridad.

Para lograr estos resultados de aprendizaje, se realizará un análisis detallado que incluirá la identificación de activos críticos, modelado de amenazas, análisis de riesgos cualitativo y propuestas para mejorar la postura de seguridad de la aplicación. Este enfoque nos permitirá no solo entender las debilidades y fortalezas de BankSecure sino también proponer soluciones prácticas y fundamentadas teóricamente para mejorar su seguridad.

Este trabajo contribuye a la comprensión más amplia de cómo aplicar de forma efectiva los principios de ciberseguridad en el mundo real, combinando el rigor teórico con la aplicación práctica.

2. ESCENARIO

La compañía FinTech "InverSecure" ha desarrollado una nueva aplicación móvil para banca digital llamada "BankSecure". Esta aplicación tiene como objetivo ofrecer a sus usuarios servicios bancarios seguros y fiables desde la comodidad de sus dispositivos móviles. Con BankSecure, los usuarios pueden realizar transacciones bancarias, como transferencias de dinero, pagos de facturas, consultas de saldo y mucho más. Además, la aplicación cuenta con funciones de inversión que permiten a los usuarios comprar y vender acciones, bonos y otros instrumentos financieros con facilidad.

BankSecure fue diseñada utilizando una arquitectura de microservicios para permitir la escalabilidad y la eficiencia. Cada microservicio se encarga de una funcionalidad específica, como la gestión de cuentas, las transacciones o los servicios de inversión. Asimismo, para mejorar la experiencia del usuario, se ha utilizado una arquitectura de microfrontends que permite personalizar y adaptar la interfaz de usuario según las necesidades de cada usuario.

Las bases de datos de los clientes, que contienen información personal y financiera, son uno de los activos más valiosos de la empresa. Además, los sistemas de procesamiento de transacciones son cruciales para mantener la operatividad y la reputación de la empresa. Por último, el sistema de autenticación, que garantiza que sólo los usuarios autorizados pueden acceder a sus cuentas, es otro activo valioso.

Dada la naturaleza de la aplicación, BankSecure es un objetivo atractivo para los ciberdelincuentes. Un agente de amenazas podría ser un hacker que busca robar información financiera para llevar a cabo fraudes o vender la información en el mercado negro. Otro posible agente de amenazas son los empleados descontentos o malintencionados que pueden tener acceso a información privilegiada o sistemas críticos.

Considerando el impacto potencial de un ataque exitoso, es crucial que InverSecure tome medidas adecuadas para proteger su aplicación y su infraestructura. El equipo de seguridad de la empresa ha decidido realizar un modelado de amenazas para identificar y priorizar las amenazas potenciales. Deberán tener en cuenta la posibilidad de que un agente de amenazas pueda explotar vulnerabilidades en el sistema para robar datos, interrumpir los servicios o realizar actividades fraudulentas.

La aplicación BankSecure de InverSecure interactúa con una serie de entidades externas. Por ejemplo, se comunica con las pasarelas de pago para procesar las transacciones bancarias y con las bolsas de valores para gestionar las operaciones de inversión. Además, interactúa con las agencias de informes crediticios para verificar la solvencia de los usuarios antes de aprobar ciertos servicios financieros.

Los principales procesos que se llevan a cabo en la aplicación son el inicio de sesión del usuario, las operaciones bancarias (como transferencias y pagos de facturas), las operaciones de inversión y las consultas de saldo. Cada uno de estos procesos requiere interacciones con distintos microservicios y la transferencia de datos entre ellos.

El flujo de datos en BankSecure es fundamental para su funcionamiento. Por ejemplo, cuando un usuario inicia sesión, su nombre de usuario y contraseña se envían desde su dispositivo a través del microservicio de autenticación. Si las credenciales son correctas, se le otorga al usuario un token de acceso que se utiliza para autenticar las solicitudes posteriores. Cuando se realiza una transacción, los detalles de la transacción se envían desde el dispositivo del usuario al microservicio correspondiente, que luego interactúa con la pasarela de pago para completar la transacción.

En cuanto a los almacenes de datos, BankSecure cuenta con varias bases de datos que almacenan información de los clientes, detalles de transacciones, historial de inversiones y otros datos relacionados. Estas bases de datos son mantenidas por InverSecure y se accede a ellas a través de microservicios específicos.

InverSecure ha implementado varias medidas de seguridad en su aplicación BankSecure. Por ejemplo, para proteger contra ataques de fuerza bruta, ha implementado límites en el número de intentos de inicio de sesión y un sistema CAPTCHA. También se utiliza la autenticación de dos factores para proteger las cuentas de los usuarios. Sin embargo, a pesar de estas medidas, un atacante determinado todavía podría ser capaz de superar estas defensas.

Las interacciones con entidades externas se llevan a cabo a través de interfaces API seguras. Por ejemplo, para procesar una transacción, el microservicio de transacciones envía los detalles de la transacción a la pasarela de pago a través de una API segura. Los datos transmitidos están encriptados para proteger contra el espionaje. Sin embargo, si un atacante logra comprometer una de estas API, podría ser capaz de interceptar o alterar los datos transmitidos.

Los flujos de datos en BankSecure son complejos. Por ejemplo, cuando se realiza una transacción, los detalles de la transacción se envían desde el dispositivo del usuario al microservicio de transacciones. Este microservicio luego interactúa con varios otros microservicios y bases de datos para procesar la transacción. Este flujo de datos puede presentar varias oportunidades para un atacante que logra infiltrarse en el sistema.

Las bases de datos de BankSecure están protegidas por múltiples capas de seguridad. Están alojadas en servidores seguros y el acceso a ellas está restringido a microservicios específicos que requieren los datos para su funcionamiento. A pesar de estas medidas, un atacante que logra comprometer un microservicio podría ser capaz de acceder a los datos que éste puede acceder.

3. ENTREGAS Y PRESENTACIÓN

3.1 ANTE-PROYECTO

Se debe cumplir y considerar lo siguiente:

- Objetivo General y Específicos: Establecer claramente el objetivo principal del proyecto y desglosarlo en objetivos específicos, que en conjunto contribuyan al logro del objetivo general.
- Actividades por Objetivo Específico: Listado detallado de las actividades que se deben realizar para alcanzar cada uno de los objetivos específicos.
- Roles de cada Integrante: Descripción de las responsabilidades y funciones de cada miembro del equipo.
- Matriz RACI: Un cuadro que identifica quién es Responsable, Quién Aprueba, Quién es Consultado, y Quién es Informado para cada actividad.
- Hitos de Entrega: Fechas clave para la entrega de partes del informe y de la presentación.
- Esfuerzo Requerido (HH): Estimación del tiempo que se espera invertir en cada tarea, que debe ser repartido equitativamente entre los miembros del equipo.
- Carta Gantt: Un gráfico que visualice el cronograma del proyecto, incluyendo las actividades, hitos y responsables.
- Mecanismo interno de solución a problemáticas grupales: definir un mecanismo que les permita solucionar los problema que se generen al interior del grupo.

3.2 INFORME

El informe debe tener la siguiente estructura. El tamaño máximo del informe son 30 páginas, sin incluir los anexos.

Portada

- Título del Proyecto
- Nombres de los integrantes del equipo
- Fecha

Índice

- Enumeración de las secciones y subsecciones

Capítulo 1: Introducción y Planificación

- Contexto: Breve descripción del entorno y la necesidad que motiva el proyecto.
- Objetivo General: Descripción del objetivo principal.
- Objetivos Específicos y Actividades: Detallados y actualizados para alcanzar el objetivo general.
- Matriz RACI Actualizada: Descripción de la matriz RACI con roles y responsabilidades.
- Planificación y Comparación con el Anteproyecto: Carta Gantt actual y comparativa con la del anteproyecto, identificación de las principales dificultades y cómo se solucionaron.

Capítulo 2: Desarrollo

- Desafíos de Ciberseguridad: Identifiquen los principales desafíos de ciberseguridad que enfrenta "BankSecure".
- Modelado de Amenazas: Desarrollen un modelo de amenazas que contemple los posibles agentes de amenazas y cómo podrían explotar las vulnerabilidades existentes en "BankSecure".
- Activos Críticos y Análisis de Riesgo: Elijan los tres activos más críticos de "BankSecure" y realicen un análisis de riesgo cualitativo sobre ellos.
- Estándares y Legislación: Investiguen y seleccionen al menos un estándar y tres artículos de legislación relevantes para "BankSecure".
- Análisis Autónomo: De manera autónoma, apliquen una metodología, estándar o buena práctica en ciberseguridad para proponer controles que mitiguen los riesgos identificados.
- Aspectos Éticos: Comenten sobre los aspectos éticos relacionados con la protección de datos financieros y personales de los usuarios.
- Estrategia de Ciberseguridad: Sinteticen sus hallazgos y propuestas que incluya una estrategia preliminar para abordar los desafíos identificados.

Capítulo 3: Conclusiones

- Reflexiones finales, logros alcanzados y futuros pasos.

Anexos

- Material adicional, capturas de pantalla, etc.

Referencias Bibliográficas

- Citación de fuentes, documentación, etc.

3.3 PRESENTACIÓN

El orden de la presentación se sorteará la clase antes de la presentación. En la presentación solamente estará el grupo en cuestión. La presentación contará con una duración máxima de 15 minutos y deberá estructurarse de la siguiente manera:

Introducción (2 minutos)

- Breve contextualización del proyecto y los objetivos que se buscan alcanzar en esta primera entrega.

Desarrollo (12 minutos)

- (1 minutos) Desafíos de Ciberseguridad: Identifiquen los principales desafíos de ciberseguridad que enfrenta "BankSecure".
- (2 minutos) Modelado de Amenazas: Desarrollen un modelo de amenazas que contemple los posibles agentes de amenazas y cómo podrían explotar las vulnerabilidades existentes en "BankSecure".
- (2 minutos) Activos Críticos y Análisis de Riesgo: Elijan los tres activos más críticos de "BankSecure" y realicen un análisis de riesgo cualitativo sobre ellos.
- (2 minutos) Estándares y Legislación: Investiguen y seleccionen al menos un estándar y tres artículos de legislación relevantes para "BankSecure".
- (2 minutos) Análisis Autónomo: De manera autónoma, apliquen una metodología, estándar o buena práctica en ciberseguridad para proponer controles que mitiguen los riesgos identificados.
- (1 minutos) Aspectos Éticos: Comenten sobre los aspectos éticos relacionados con la protección de datos financieros y personales de los usuarios.
- (2 minutos) Estrategia de Ciberseguridad: Sinteticen sus hallazgos y propuestas que incluya una estrategia preliminar para abordar los desafíos identificados.

Conclusiones (1 minuto)

- Resumen de los hallazgos más significativos y su relevancia para el entendimiento de las redes de computadoras.

Preguntas y Respuestas (Abrir al público, tiempo restante)

- Espacio para que el público haga preguntas y los presentadores proporcionen respuestas.

Se espera que cada equipo siga este esquema con rigor para asegurar que todos los aspectos críticos de la primera entrega sean cubiertos de manera efectiva y dentro del tiempo estipulado. Incluya el ensayo de la presentación en su planificación.

4. AUTOEVALUACIÓN GRUPAL

En caso de que el profesor lo considere necesario. Se activará el procedimiento de autoevaluación grupal (AG):

- Este consiste en una autoevaluación anónima en donde cada uno de los integrantes del grupo evaluará la contribución del resto (AG: 0% a 100%).
- Se evaluarán aspectos como participación en la actividad grupal, responsabilidad, organización, cumplimiento con los comprometido, entre otros.
- La anterior evaluación se ponderará con la evaluación final del grupo (EFG). Quedando la Nota Final del estudiante (NFE) como NFE = EFG * AG.

5. NOTAS

Tener en cuenta las siguientes consideraciones.

- La entrega del ante-proyecto es para el 21 de Septiembre 2023.
- El formato del ante-proyecto y el informe es el mismo que el de propuesta de memoria.

- 1 punto de descuento en la nota final por hora de atraso de cualquiera de los documentos solicitados.
- Todos los grupos deben estar preparados para presentar en la fecha de entrega.
- Todos los estudiantes deben demostrar conocimientos en todos los aspectos de lo solicitado. En la presentación se sortearán preguntas a los integrantes sobre cualquiera de los temas.
- Puede establecer los supuestos que estime conveniente, siempre y cuando los explicite tanto en el informe como en la presentación.
- Todos los documentos deben ser entregados a través de un link de google drive en el foro social en formato PDF.

6. RÚBRICA

La nota de la actividad se evaluará de acuerdo a los puntajes de la siguiente tabla con una exigencia del 70%.

- RA1: Aplicar conceptos de ciberseguridad a situaciones reales, trabajando de forma autónoma y en equipo.
- RA2: Identificar metodologías, normativas y estándares adecuados para proteger los activos digitales, considerando el contexto de la organización y aplicando una postura ética y profesionalismo.

Criterio	**0 puntos (No se aprecia)**	**1 punto (Insuficiente)**	**2 puntos (Aceptable)**	**3 puntos (Bueno)**	**4 puntos (Óptimo)**
Ante-proyecto	No se entrega anteproyecto o el entregado no contiene información relevante.	El anteproyecto se entrega, pero carece de elementos clave como objetivos, matriz RACI o Carta Gantt.	El anteproyecto incluye la mayoría de los elementos requeridos, pero muestra poca profundidad o detalle en la planificación.	El anteproyecto es completo, incluye todos los elementos requeridos y muestra un nivel adecuado de detalle y planificación.	El anteproyecto es excepcionalmente bien elaborado, con claridad en objetivos, asignación de roles y planificación. Muestra un entendimiento profundo de la tarea a realizar y cómo se llevará a cabo.
Informe: Claridad y Organización del Informe	Desorganizado , incompleto	Falta de estructura	Alguna organización	Bien organizado	Coherente, lógico
Informe: Calidad de Análisis Técnico	Ausente	Superficial	Adecuado	Detallado	Exhaustivo, perspicaz
Informe: Planificación y Gestión del Proyecto	Ausentes o incompletos	Parciales	Casi completos	Completos	Meticulosos, efectivos
Presentación: Uso eficiente del tiempo	Se pasa del tiempo o no utiliza el tiempo	Utiliza mal el tiempo, saltándose secciones clave	Buen uso del tiempo pero con algunos retrasos	Utiliza el tiempo de manera efectiva para cubrir la mayoría de los puntos clave	Utiliza el tiempo de manera óptima, cubriendo todos los puntos clave sin apresurarse

Aplicación de Conceptos Teóricos	No aplica conceptos	Aplica incorrectamente los conceptos	Aplica básicamente algunos conceptos	Aplica la mayoría de los conceptos bien	Aplica todos los conceptos de forma excelente
Identificación de Vulnerabilidades y Riesgos	No identifica nada	Identifica muy pocas vulnerabilidades	Identifica algunas vulnerabilidades	Identifica la mayoría de vulnerabilidades	Identifica todas las vulnerabilidades con detalle
Propuesta de Controles	No propone controles	Propuestas irrelevantes o incorrectas	Propuestas genéricas o poco justificadas	Propuestas mayormente eficaces	Propuestas completamente eficaces y bien justificadas
Integración de Estándares y Legislación	No menciona nada	Menciona pero no integra	Integra de forma básica o incompleta	Integra de forma coherente pero limitada	Integra de forma completa y bien justificada
Análisis Autónomo	No realiza análisis	Análisis superficial o irrelevante	Análisis básico y/o poco relevante	Análisis autónomo y parcialmente relevante	Análisis autónomo, relevante y robusto
Aspectos Éticos	No menciona ética	Menciona pero no discute	Discute superficialmente	Discute de forma limitada pero adecuada	Discute de forma completa y reflexiva