CIBERSEGURIDAD
Prof. Juan Ignacio Iturbe

ACTIVIDAD GRUPAL - parte 1:
Levantamiento de la situación actual y análisis de riesgos cualitativo en el proceso de desarrollo de software

Exigencia: 70%

1. INTRODUCCIÓN

1.1 Contexto

La Universidad de Santiago de Chile cuenta con una plataforma pública donde se documentan diversos procesos, incluidos los relacionados con el desarrollo de software. El acceso público a esta documentación y la falta de controles de seguridad en ciertas áreas pueden exponer a la universidad a riesgos significativos. Esta actividad tiene como objetivo que los estudiantes realicen un levantamiento de la situación actual, identifiquen los activos digitales involucrados en el proceso de desarrollo de software y lleven a cabo un análisis de riesgos cualitativo. A partir de este análisis, los estudiantes deberán identificar normativas, legislación, metodologías y estándares adecuados para proteger dichos activos, aplicando una postura ética y profesional.

2. OBJETIVOS

2.1 Objetivo General

Realizar un levantamiento detallado del proceso de desarrollo de software en la Universidad, identificando los activos digitales y los riesgos de ciberseguridad mediante un modelado de amenazas complementado por STRIDE. Finalmente, realizar un análisis de riesgos cualitativo y proponer controles adecuados, identificando normativas, legislación y estándares aplicables, considerando el contexto organizacional y aplicando una postura ética y profesional.

2.2 Objetivos Específicos

1. Elaborar un anteproyecto que defina el enfoque y la planificación del trabajo grupal.
2. Levantar la situación actual del proceso de desarrollo de software en la Universidad, identificando los activos digitales involucrados.
3. Realizar entrevistas con funcionarios clave como CITIAPS, Facultad de Ingeniería (FING), y el Departamento de Ingeniería Informática (DEI), complementando la información documental con la obtenida de estas entrevistas.
4. Modelar amenazas utilizando la metodología STRIDE para identificar y analizar los riesgos asociados a los activos digitales identificados.

5. Realizar un análisis de riesgos cualitativo que priorice las vulnerabilidades, proponiendo controles de seguridad adecuados.
6. Identificar normativas, metodologías, legislación (nacional e internacional) y estándares aplicables para la protección de los activos digitales en base al análisis de riesgos, considerando el contexto organizacional y aplicando una postura ética y profesional.

3. ENTREGAS Y PRESENTACIÓN

3.1 Anteproyecto

Cada equipo deberá preparar un anteproyecto que incluya lo siguiente:

- Objetivo General y Específicos: Establecer claramente el propósito principal y desglosarlo en objetivos específicos.
- Actividades por Objetivo Específico: Describir detalladamente las actividades que se deben realizar para cumplir cada objetivo.
- Roles de cada Integrante: Asignación clara de responsabilidades para cada miembro del equipo.
- Matriz RACI: Identificar quién es Responsable (R), quién Aprueba (A), quién es Consultado (C) y quién es Informado (I) para cada actividad.
- Hitos de Entrega: Fechas clave para la entrega de avances y del trabajo final.
- Esfuerzo Requerido (HH): Estimación de las horas de trabajo necesarias para cada tarea, distribuidas equitativamente entre los integrantes.
- Carta Gantt: Cronograma visual que muestre las actividades, hitos y responsables.

3.2 Levantamiento de la situación actual

Cada equipo deberá realizar un levantamiento detallado del proceso de desarrollo de software en la Universidad, considerando la información obtenida tanto de documentos como de entrevistas con funcionarios relacionados con el desarrollo de software, tales como CITIAPS, Facultad de Ingeniería (FING), Departamento de Ingeniería Informática (DEI), entre otros. Es importante que cada grupo complemente la información documental con entrevistas a estos actores clave, quienes proporcionarán información relevante que no siempre estará completamente documentada. Los equipos que logren realizar entrevistas adicionales con fuentes distintas al profesor de la asignatura recibirán una mejor evaluación.

El levantamiento debe considerar tres componentes clave:

- **Procesos:** Diagrama del proceso en BPMN, detallando las etapas del desarrollo de software.
- **Personas:** Identificar roles y responsabilidades dentro del proceso de desarrollo.

- **Tecnologías:** Descripción de las herramientas y tecnologías utilizadas en el desarrollo de software.
- **Identificación de activos digitales**: Determinar los activos digitales involucrados en el proceso de desarrollo de software.

Entregables:

1. **Informe del levantamiento de la situación actual:** Incluir el diagrama BPMN de los procesos identificados, roles de las personas involucradas, las tecnologías utilizadas y activos identificados.
2. **Entrevistas:** Resumen de las entrevistas realizadas, incluyendo las fuentes consultadas y los principales hallazgos obtenidos de dichas entrevistas.

3.3 Modelado de amenazas, análisis de riesgos e identificación de normativas y estándares

Una vez finalizado el levantamiento, cada equipo deberá realizar un modelado de amenazas utilizando la metodología STRIDE. Este modelado permitirá identificar posibles amenazas y vulnerabilidades en el proceso de desarrollo de software. Los resultados del modelado de amenazas deberán ser utilizados para alimentar el análisis de riesgos cualitativo.

Con base en el análisis de riesgos cualitativo, cada equipo debe identificar las normativas, metodologías y estándares aplicables a la protección de los activos digitales, considerando el contexto organizacional. Se espera que los estudiantes analicen la postura ética y profesional que debe guiar la protección de estos activos y los riesgos asociados.

- Matriz de amenazas STRIDE, que identifique las amenazas para cada activo digital.
- Análisis de riesgos cualitativo, que incluya una matriz que evalúe la probabilidad e impacto de los riesgos, así como una propuesta preliminar de controles de seguridad (desde estándares y buenas prácticas) para mitigar los riesgos más significativos.
- Informe sobre legislación, normativas y estándares, que detalle las normativas, metodologías y legislación aplicables (ej. ISO 27001, NIST, Ley 19.628), justificando su pertinencia y aplicabilidad a los riesgos identificados.
- Análisis ético y profesional, reflexionando sobre el impacto de las vulnerabilidades y la importancia de la ética en la ciberseguridad.

Entregables:

1. Matriz de amenazas según STRIDE, que identifica las amenazas para cada activo digital.
2. Análisis de riesgos cualitativo, que incluya una matriz que evalúe la probabilidad e impacto de los riesgos, así como una propuesta preliminar de controles de seguridad para mitigar los riesgos más significativos.

3.4 INFORME FINAL

El informe final deberá consolidar todo el trabajo realizado, incluyendo el levantamiento de la situación actual, el modelado de amenazas y el análisis de riesgos cualitativo. La estructura será la siguiente:

- Introducción y contexto del proyecto
- Levantamiento de la situación actual (con diagrama BPMN y activos digitales)
- Resultados de las entrevistas con actores clave
- Modelado de amenazas STRIDE
- Análisis de riesgos cualitativo (con matriz de riesgos)
- Normativas, legislación y estándares aplicables
- Análisis ético y profesional
- Conclusiones
- Reflexiones: Indicar sus apreciaciones sobre el presente trabajo y que sugerencias realizan para la siguiente parte.

Cómo parte de la introducción y contexto del proyecto contrastar lo definido en el anteproyecto con lo finalmente realizado. Identificar brechas y aportes de cada integrante del grupo. Indicar problemáticas internas y cómo se solucionaron.

3.5 PRESENTACIÓN

Cada equipo realizará una presentación de 15 minutos que incluya:

- Descripción del levantamiento de la situación actual, destacando los activos digitales y los principales hallazgos de las entrevistas.
- Explicación del modelado de amenazas STRIDE y el análisis de riesgos cualitativo.
- Propuesta de controles de seguridad, identificando las normativas, legislación y estándares aplicables, con una reflexión ética sobre la seguridad en el contexto organizacional.

4. AUTOEVALUACIÓN GRUPAL

Se realizará una autoevaluación grupal (%AG):

- Este consiste en una evaluación anónima en donde cada uno de los integrantes del grupo evaluará la contribución del resto (%AG: 0% a 120%).
- Se evaluarán aspectos como participación en la actividad grupal, responsabilidad, organización, cumplimiento de los compromisos, entre otros.

- La anterior evaluación se ponderará con la nota final del grupo (NFG). Dejando la nota final del estudiante (NFE) cómo: NFE = NFG * %AG
- Si un/a estudiante se ve perjudicado por la presente medida, puede apelar a esta decisión enviando un correo al profesor entregando evidencia de lo realizado en el transcurso del trabajo. La evaluación final en este caso quedará a criterio del profesor.

5. NOTAS

- El formato del informe será el mismo que el utilizado en la presentación de propuestas de memoria.
- 1 punto de descuento por hora de atraso en la entrega de los documentos solicitados.
- Todos los miembros del grupo deben estar preparados para la presentación y ser capaces de responder preguntas sobre cualquier aspecto del trabajo realizado.
- Si utiliza para el desarrollo del trabajo herramientas cómo chat gpt, debe indicar en un anexo del informe asociado los prompts utilizados. Esto no afectará la nota, pero sí es importante, no dejar el análisis crítico a la herramienta. Usted es la/el responsable de lo que se entrega en el informe y presentación.
- Todos los documentos deben ser entregados a través de un link de google drive en el foro grupal en formato PDF (grupoX_entregaY.pdf), formatos de excel y Bizagi BPMN (NO SE ACEPTARÁN DOCUMENTOS CON FECHAS POSTERIORES AL FECHA DE ENTREGA).

6. RÚBRICA

- 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.

Rúbrica de Evaluación: Actividad Grupal - Parte 1

Criterios	**Indicadores**	**Insuficiente (1)**	**Aceptable (2)**	**Bueno (3)**	**Óptimo (4)**	**Factor**
Aplicación de conceptos de ciberseguridad (Unidad 1)	Grado de aplicación de los conceptos de amenazas, vulnerabilidades, controles y análisis de riesgos en el contexto del proceso de desarrollo de software.	Los conceptos de ciberseguridad no se aplican correctamente o no se identifican amenazas relevantes.	Se identifican algunas amenazas y vulnerabilidades, pero la aplicación de conceptos es superficial o incompleta.	La mayoría de las amenazas, vulnerabilidades y controles se identifican correctamente, aunque falta más profundidad en el análisis de riesgos.	Aplicación precisa de los conceptos de amenazas, vulnerabilidades y controles, con un análisis de riesgos detallado, bien justificado y completo.	4
Levantamiento de información y procesos (Unidad 1 y 2)	Uso de fuentes de información y construcción de un diagrama BPMN, considerando procesos, personas y tecnologías.	El levantamiento de información es incompleto y el diagrama BPMN no refleja correctamente	Se recopila información adecuada, pero el diagrama BPMN es básico y faltan detalles en algunos procesos o roles.	El levantamiento incluye entrevistas relevantes y el diagrama BPMN cubre la mayoría de los procesos, roles y	Levantamiento exhaustivo con múltiples fuentes. El diagrama BPMN refleja con precisión todos los procesos, personas y	4

		los procesos clave.		tecnologías con buen detalle.	tecnologías identificadas.	
Identificación de normativas, metodologías, legislación y estándares (Unidad 2)	Identificación y análisis de normativas, metodologías, legislación y estándares para proteger los activos digitales, en base al análisis de riesgos realizado, considerando el contexto organizacional y aplicando postura ética y profesionalismo.	No se identifican normativas, metodologías o estándares relevantes, o no se aplica una postura ética en el análisis.	Se identifican algunos estándares, pero su análisis o aplicación en el contexto organizacional es limitado o superficial.	Se identifican normativas, metodologías, legislación y estándares adecuados, aplicados correctamente al contexto de la organización, con postura ética general.	Identificación y análisis exhaustivo de normativas, metodologías, legislación y estándares, alineados con el contexto de la organización, con postura ética clara y profesional.	4
Modelado de amenazas (Unidad 1 y 2)	Uso de la metodología STRIDE para identificar amenazas en el proceso de desarrollo de software.	No se utiliza STRIDE correctamente o no se identifican amenazas significativas.	Se aplica STRIDE de manera básica, pero faltan amenazas relevantes o el análisis no es profundo.	Se aplica STRIDE correctamente, identificando las amenazas más importantes, pero con espacio para profundizar.	Aplicación exhaustiva de STRIDE, identificando todas las amenazas importantes, con un análisis bien estructurado y profundo.	3
Análisis de riesgos cualitativo (Unidad 1)	Evaluación de los riesgos en base a probabilidad e impacto, y propuesta de controles para mitigarlos.	El análisis de riesgos es incompleto o carece de justificación clara.	Se realiza un análisis básico, pero faltan detalles sobre la justificación de la probabilidad o impacto de los riesgos.	Análisis de riesgos adecuado, con buena justificación de la probabilidad e impacto, aunque algunos controles podrían ser más específicos.	Análisis de riesgos completo y justificado en detalle, con controles claros, viables y bien alineados con los riesgos más críticos.	4
Análisis del contexto ético y profesional (Unidad 2)	Reflexión sobre la ética y el profesionalismo al analizar el impacto de las vulnerabilidades en el contexto de la organización.	No se aborda la dimensión ética o profesional en el análisis de riesgos y las propuestas de mitigación.	Se menciona de manera superficial la importancia de la ética y el profesionalismo, pero sin relación con las propuestas de mitigación.	Se considera adecuadamente la ética y el profesionalismo en la justificación de los controles de seguridad propuestos, con recomendaciones generales.	Análisis profundo sobre la postura ética y profesional en el contexto organizacional, con justificación clara y detallada de las propuestas de mitigación.	3
Calidad del informe final	Claridad, organización y profundidad del informe final, incluyendo el uso adecuado de citas, fuentes de información y entrega de los objetivos propuestos.	El informe es desorganizado, incompleto o no aborda los puntos clave del análisis de seguridad.	El informe cubre los puntos principales, pero presenta errores de organización, falta de profundidad o un uso inadecuado de las fuentes.	El informe es claro, bien organizado y cubre los aspectos clave del análisis, aunque con algunos detalles	El informe es excelente, bien estructurado, claro y profundo, con un análisis exhaustivo de todos los puntos solicitados, respaldado por	5

				que podrían mejorarse.	fuentes adecuadas.	
Calidad de la presentación	Estructura, claridad y calidad visual de la presentación, así como el manejo del tiempo y la capacidad para responder preguntas del público.	La presentación es desorganizada, no cubre los puntos clave, o el equipo no respeta el tiempo asignado.	La presentación cubre la mayoría de los puntos, pero es desorganizada o se excede en el tiempo límite.	La presentación es clara y bien organizada, aunque puede tener pequeños desajustes en el tiempo o en la cobertura de algunos temas.	La presentación es excelente, bien organizada, cubre todos los puntos clave y respeta el tiempo asignado, con un manejo adecuado de preguntas del público.	5
Trabajo en equipo y colaboración (Unidad 1 y 2)	Grado de colaboración entre los integrantes del equipo, asignación de roles claros y equitativos, y manejo de responsabilidades.	Poca colaboración, asignación poco clara de roles o participación desigual entre los integrantes.	Colaboración adecuada, pero algunos roles no se distribuyen equitativamente o falta claridad en la asignación de tareas.	Buena colaboración, con roles claramente distribuidos y participación activa de la mayoría de los miembros.	Excelente colaboración, roles bien definidos, participación activa y equitativa de todos los miembros del equipo.	3