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

FUNDAMENTOS DE CIBERSEGURIDAD
Prof. Juan Ignacio Iturbe

ACTIVIDAD GRUPAL 1: INTRODUCCIÓN

Exigencia: 70%

1. CONTEXTO

En la presente actividad usted y su grupo deberán desarrollar una serie de tareas relacionadas con la materia dictada en la cátedra.

2. ESCENARIO

La gestión de la organización ACME históricamente se ha realizado a través de documentos en papel. Estos documentos son de tipo memorandums, contratos, proyectos, facturas, entre otros. Lo cual produce una gran cantidad de problemas, entre los que se encuentran la pérdida de documentos, desconocimiento sobre en qué etapa se encuentran los trámites, largos tiempos de procesamiento, entre otros.

Durante el último tiempo se han realizado una serie de iniciativas que han permitido avanzar en la solución de estos problemas. Se desarrolló un sistema de trazabilidad documental, se están desarrollando los proyectos de actualización de la plataforma ERP, se ha desarrollado la plataforma para el seguimiento estratégico institucional, entre otros.

En el último tiempo ACME generó su plan estratégico donde uno de sus principales lineamientos es el “Cero Papel”. Uno de los proyectos más importantes en este sentido, es el Sistema de Riesgo de Perdida de Clientes (SRPC). El objetivo de este proyecto es el seguimiento de la cartera de clientes, evaluando el riesgo de irse del cliente a la competencia o que por algún motivo dejarán de ser clientes. A los clientes que cumplen cierto umbral, se les ofrecen ofertas y descuentos.

El proyecto se encuentra actualmente con módulos en desarrollo. Por esta razón, el proyecto se encuentra bajo varios riesgos de ciberseguridad, los cuales son necesarios evaluar y tratar.

Para ello, su grupo realizará dicha evaluación y propondrá controles para mitigar los riesgos que encuentre. El profesor de la asignatura será quien actúe como cliente y podrá entregarles más detalles sobre el proyecto (a solicitud del grupo). Por lo tanto, su grupo debe preparar una serie de preguntas para hacerle al cliente para levantar la problemática.

3. ACTIVIDAD

3.1 INTRODUCCIÓN

i. Identifique los desafíos de la ciberseguridad que está afrontando la empresa.
ii. ¿Existe ciberseguridad en los proyectos que se están desarrollando? Justifique.
iii. De acuerdo al escenario propuesto:

- Identifique todos los activos de información digital relacionados del proyecto SRPC.
- Indique cuales son los 3 activos más importantes del proyecto. Justifique.
- Desarrolle un modelo de amenazas sobre estos 3 activos y sus soportes tecnológicos.
- Identifique la legislación que debe ser tener en cuenta para el desarrollo del proyecto. Indique al menos 3 artículos que estén estrechamente relacionados con el proyecto. Justifique.
- Para lo anterior, desarrolle un análisis de riesgos cualitativo considerando los siguientes conceptos. Justifique cada elección.
    - Activo de información digital.
    - Vulnerabilidad.
    - Amenazas.
    - Agente de amenaza.
    - Objetivo(s) de ciberseguridad comprometido.
    - Controles actuales.
    - Probabilidad. Justifique.
    - Impacto. Justifique.
    - Riesgo actual.
    - Exposición.

Id	Activo de información digital	Vulnerabilidad	Amenaza	Agente de amenaza	Objetivo comprometido	Controles actuales	Probabilidad	Impacto	Riesgo actual	Exposición
1										

v. Proponga una tabla de impacto vs probabilidades. Por ejemplo:

		Probabilidad		
		Baja	Media	Alta
	Alto			
	Medio			
Impacto	Bajo			

vi. Establezca un criterio de aceptación del riesgo.
vii. Mitigar aquellos riesgos que superan el apetito definido (al menos 3). Agregue a la tabla anterior:

- Controles propuestos (Utilice un estándar o buena práctica de la Unidad II). Justifique.
- Probabilidad actualizada. Justifique.
- Impacto actualizado. Justifique.
- Riesgo residual.

viii. Identifique el tipo y función de los controles aplicados.

ix. De acuerdo a los controles seleccionados, ilustre en una figura una estrategia de defensa en profundidad (sobre uno de los activos) de acuerdo a las funcionalidades de los controles seleccionados.

3.2 BUENAS PRÁCTICAS, ESTÁNDARES Y METODOLOGÍAS

De acuerdo a la buena práctica, estándar o metodología asignada en la Tabla 1:
i. Describa a través de un mapa conceptual el documento asignado.
ii. ¿Cual es la diferencia entre buena práctica, estándar y metodología? ¿El documento asignado de qué tipo es?
iii. Indique cuál es el objetivo general y los específicos del documento.
iv. Muestre con un ejemplo cómo se compone un control/item dentro del documento.
v. Aplique el documento en un caso de uso.

Tabla 1. Asignación de buenas prácticas, estándares, metodologías, normativa, legislación

Grupo	**Buena práctica, estándar o metodología**
A	Cloud Security Alliance - Security, Trust, Assurance and Risk (STAR)
B	European Cybersecurity Skills Framework (ECSF)
C	General Data Protection Regulation (GDRP)
D	Nueva ley chilena sobre delitos informáticos (Ley 21459)
E	Cyber Essentials (National Cyber Security Centre, UK)
F	OWASP Application Security Verification Standard

4. ENTREGA

Se debe cumplir y considerar lo siguiente:

4.1 Primera parte:

- La primera parte de la entrega corresponde a una presentación resumen (PPT) de lo desarrollado en el punto 3.1 la cual debe ser entregada a través del foro social antes de la fecha y hora de la presentación.
- Es importante que la presentación tenga un hilo conductor y se vaya desarrollando coherentemente a medida que se incorporan nuevos elementos.
- La presentación debe exponerse frente al curso. Esta no debe sobrepasar los 20 minutos + 5 minutos de preguntas.

4.2 Segunda parte:

- Para esta parte es necesaria la elaboración de una cápsula en video de 4 a 5 minutos que resuma el contenido del punto 3.2.
- Este video debe quedar disponible en Google Drive para su descarga durante todo el semestre.
- La presentación base final debe ser aprobada por el profesor. Para ello, se debe enviar la ppt (incluyendo el guión colocado en la sección de notas de la presentación) al correo del profesor hasta una semana antes de la fecha límite. El profesor puede a) Aprobar o b) Reformular:
    - En caso de Aprobar, se debe proceder a grabar el video y publicar.
    - En caso de Reformular, el grupo tendrá tres días para hacer los cambios solicitados y enviar nuevamente al profesor.
    - En caso de no entregar esta parte se descontará un punto en la nota final de la Actividad Grupal.
- El link al video se debe publicar en el foro social.
- Este material entrará en la PEP 1.

5. AUTOEVALUACIÓN GRUPAL

Autoevaluación grupal:

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

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

- OA1: Comprender los conceptos y sus relaciones sobre ciberseguridad.
- OA2: Conocer y aplicar metodologías, normativas y/o estándares para proteger los activos digitales en las organizaciones.

Indicadores	O	S	B	I	n/o
Se realiza un buen levantamiento por parte del grupo respecto al caso de estudio					
Se comprenden y aplican los conceptos sobre ciberseguridad durante el desarrollo del trabajo.					
Se conocen y aplican correctamente las metodologías, normativas, estándares y legislación relacionada con el trabajo.					
Todos los integrantes del grupo saben responder todas las preguntas, independiente si presenta o no dicha parte.					
Entrega la presentación en los plazos correspondientes y no hace modificaciones posteriores.					
Resume correctamente todos los contenidos que deben ir en la presentación de 20 minutos.					
El video de la segunda parte del trabajo se entrega de acuerdo a lo solicitado.					
Se entrega un archivo excel como respaldo del análisis de riesgos realizado y este se realiza correctamente.					
La forma de los documentos presentados y entregados es correcta (Incluye introducción, desarrollo, conclusión, bibliografía, referencias y sigue los formatos)					

Resuelve internamente las problemáticas que surjan a nivel de grupo culminando el proyecto exitosamente.					
Puntaje total					
Nota					

Óptimo	4ptos
Satisfactorio	3ptos
Básico	2ptos
Insuficiente	1pto
N/O No Observado	0ptos