

FUNDAMENTOS DE CIBERSEGURIDAD

Prof. Juan Ignacio Iturbe

ACTIVIDAD GRUPAL 2

Exigencia 70%

1. INTRODUCCIÓN

En la presente actividad usted y su grupo deberán desarrollar una serie de tareas relacionadas con la materia dictada en la cátedra. Es importante que mientras avance la materia, cada grupo resuelva las tareas asociadas y sus dudas con el profesor. El objetivo de la presente actividad es que cada estudiante “Desarrolle habilidades para planificar la ciberseguridad en las organizaciones proponiendo soluciones de seguridad para los activos digitales de acuerdo con el perfil de la organización”.

2. ACTIVIDAD

En la presente actividad se estudiará la creación de un programa de ciberseguridad sobre una organización. Para ello su profesor actuará como encargado de tecnologías que desconoce de estos temas, por lo que cada grupo actuará como una empresa consultora especializada en estas temáticas.

2.1 Escenario

2.1.1 Contexto

La Universidad de Santiago de Chile está en el proceso de pasar su infraestructura crítica a la nube y está consciente de los riesgos que enfrenta. Antes de proceder con proyectos de gran escala, la universidad implementará un programa piloto en proyectos menos críticos para asegurar que la estrategia de ciberseguridad sea sólida y eficaz. Como parte de este programa piloto, la Universidad ha abierto una licitación en la que las empresas están invitadas a proponer la implementación de un proceso de DevOps en la nube acompañado por el Framework de Ciberseguridad de NIST (NIST CSF). Para ello, se deberán considerar las normas ISO 27002, CIS Controls y otras específicas como referencias informativas.

Cada grupo representará una empresa de ciberseguridad, las cuales deberán presentar una propuesta que aborde los siguientes puntos:

1. Proponer en BPMN el proceso específico que se va a abordar.
2. Identificar las tecnologías a utilizar sobre el proceso propuesto.
3. Identificar los requisitos legales y normativos de la implementación.
4. Realizar un modelado de amenaza del proceso anterior de acuerdo a STRIDE y priorizar las amenazas de acuerdo a DREAD.
5. Identificar los riesgos cibernéticos y activos digitales asociados con este proceso.

6. Propuesta para la aplicación del NIST CSF a este proceso, incluyendo cómo se abordarán los cinco pilares del NIST CSF (Identificar, Proteger, Detectar, Responder, Recuperar) identificando perfil actual y propuesto.
7. Un plan de acción de 3 años para implementar las medidas de seguridad propuestas, incluyendo los recursos necesarios, cronograma y presupuesto detallado.
8. Un método para evaluar la eficacia de la implementación del NIST CSF en este proceso, basado en la metodología de gestión de riesgos ISO 31000.

3. ENTREGA

La entrega corresponde a la presentación de lo desarrollado anteriormente. Es importante que:

- La presentación tenga un hilo conductor y se vaya desarrollando coherentemente a medida que se incorporan nuevos elementos.
- En total, la presentación no debe sobrepasar los 30 minutos.
- En caso de querer agregar más antecedentes, déjelos en un apéndice. Estos últimos solamente serán revisados en caso de que en estos exista algún antecedente importante a considerar para alguna pregunta.
- Se debe generar una carpeta compartida con toda la documentación generada (pdf, doc, excel). La cual se debe compartir con todos los integrantes del curso.
- La fecha de creación de dichos archivos no debe sobrepasar la fecha de entrega, sino se considerará como atrasada.
- Explícite todos los supuestos realizados en la ppt.
- La entrega de la documentación es a través del foro social

4. DESARROLLO Y ORIENTACIÓN DE LA ACTIVIDAD

Para el desarrollo de la presente actividad se tendrán reuniones semanales en las cuales el profesor guiará el desarrollo de la actividad. Sin embargo, es importante que cada grupo vaya avanzando de forma autónoma (inclusive en los contenidos no vistos, demostrando capacidad de autoaprendizaje) para ir haciendo consultas al profesor sobre los resultados obtenidos.

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 $NFE = EFG * AG$.

6. RÚBRICA

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

Tabla 6.1 Criterios de evaluación

Criterios de Evaluación	Insuficiente (1-2 puntos)	Aceptable (3-4 puntos)	Sobresaliente (5 puntos)
Propuesta del proceso en BPMN y tecnologías a utilizar	La propuesta del proceso y las tecnologías seleccionadas no son apropiadas o no están claramente explicadas.	La propuesta del proceso y las tecnologías son adecuadas y se describen de manera clara.	La propuesta del proceso y las tecnologías son muy adecuadas y se describen con detalles, mostrando un alto nivel de entendimiento.
Identificación de los requisitos legales y normativos	Los requisitos legales y normativos no están bien identificados o faltan elementos importantes.	Los requisitos legales y normativos están identificados y son apropiados para el proyecto.	Los requisitos legales y normativos están completamente identificados, bien explicados y son altamente pertinentes para el proyecto.
Modelado y priorización de amenazas (STRIDE y DREAD)	El modelado de amenazas es insuficiente y la priorización no es coherente.	El modelado de amenazas es correcto y la priorización es coherente.	El modelado de amenazas es exhaustivo y la priorización es altamente coherente, con justificaciones claras.
Identificación de riesgos y activos digitales	Los riesgos y los activos digitales no están bien identificados o faltan elementos importantes.	Los riesgos y los activos digitales están identificados y son apropiados para el proyecto.	Los riesgos y los activos digitales están completamente identificados, bien explicados y son altamente pertinentes para el proyecto.
Propuesta de aplicación del NIST CSF	La propuesta para la aplicación del NIST CSF es insuficiente o no está bien fundamentada.	La propuesta para la aplicación del NIST CSF es adecuada y se describe de manera clara.	La propuesta para la aplicación del NIST CSF es excelente, bien fundamentada y demuestra un alto nivel de entendimiento del framework.
Plan de acción de 3 años	El plan de acción es insuficiente, falta claridad en los recursos, cronograma o presupuesto.	El plan de acción es adecuado con detalles de recursos, cronograma y presupuesto.	El plan de acción es muy detallado, realista y con justificaciones claras para los recursos, cronograma y presupuesto.
Método para evaluar la eficacia de la implementación	El método propuesto es insuficiente o no está bien fundamentado.	El método propuesto es adecuado y se describe de manera clara.	El método propuesto es excelente, bien fundamentado y demuestra un alto nivel de entendimiento de la gestión de riesgos.
Avance de reunión en reunión	No se muestra progreso o el progreso es mínimo de reunión en reunión.	Se muestra progreso de reunión en reunión, pero podría ser más significativo o consistente.	Se muestra un progreso significativo y consistente de reunión en reunión.
Trabajo en equipo y aprendizaje autónomo	El trabajo en equipo es ineficaz: mala comunicación, poca	El trabajo en equipo es aceptable, con una comunicación,	El trabajo en equipo es excelente: comunicación eficaz, colaboración activa, distribución

	colaboración o mala distribución de tareas. Dependencia excesiva del profesor y falta de iniciativa para aprender de forma autónoma.	colaboración y distribución de tareas adecuada, pero podría mejorar. Algún grado de iniciativa y aprendizaje autónomo, aunque todavía se depende en gran medida de la orientación del profesor.	equitativa de tareas y una fuerte iniciativa y habilidades de autodirección, buscando activamente soluciones y aprendiendo de forma autónoma.
Adaptabilidad	Tienen dificultades para adaptarse a los cambios o desafíos que surgen durante el proyecto.	Se adaptan a los cambios o desafíos que surgen durante el proyecto, pero podrían demostrar una mayor resiliencia o flexibilidad.	Demuestran una fuerte capacidad de adaptación, manejando con eficacia los cambios o desafíos que surgen durante el proyecto.