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

FUNDAMENTOS DE CIBERSEGURIDAD
Prof. Juan Ignacio Iturbe

ACTIVIDAD GRUPAL 3

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. Es importante que mientras avance la materia, cada grupo resuelva las tareas asociadas y sus dudas con el profesor.

2. ACTIVIDAD

En la presente actividad se estudiará la aplicación de Gobierno y Gestión en la misma organización de la actividad anterior. 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 temáticas específicas.

2.1 Escenario

La organización de acuerdo a sus lineamientos estratégicos se ha embarcado hacia una política de cero papel en todos sus procesos de negocio. Por lo tanto, se han definido una serie de iniciativas de acuerdo a un marco de Gobierno TI para lograr dicho objetivo. Varias de estas iniciativas tienen que ver con el desarrollo de proyectos informáticos para sustentar dichos procesos. Sin embargo, la información que se maneja es altamente sensible, por lo que se debe proteger en todas sus formas. De este modo se aprecia necesario el desarrollo de una política general de seguridad de la información y una serie de políticas complementarias que permita proteger la información en los lugares que se realiza su tratamiento.
Actualmente se cuenta con una política aprobada de seguridad de la información. Esta se encuentra a su disposición en el entorno virtual.

3. DESARROLLO

3.1 Gobierno de la ciberseguridad

- Cada grupo consultor debe revisar la política de seguridad y evaluarla de acuerdo a lo que indica la UNE-EN ISO 27002:2017 en el punto 5 y en el Framework NIST en:
    - La Subcategoría ID.GV-1. ¿Se cumple lo propuesto en la presente subcategoría? Sino ¿Que propone y de acuerdo a que estándar, normativa o buena práctica?

    - La Subcategoría ID.GV-2 ¿Los roles y las responsabilidades de la ciberseguridad están coordinados y alineados con roles internos y socios externos? ¿Qué faltaría?
    - La Subcategoría ID.GV-3 ¿Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética? ¿Se cumple lo propuesto en la presente subcategoría? Sino ¿Que propone y de acuerdo a que estándar, normativa o buena práctica?
    - La Subcategoría ID-GV-4 ¿Los procesos de gobernanza y gestión de riesgos abordan los riesgos de ciberseguridad? Sino ¿Que propone y de acuerdo a que estándar, normativa o buena práctica?
    - Como grupo consultor ¿se requiere alguna política o procedimiento adicional?
    - Para consolidar la presente revisión desarrolle un checklist en un archivo excel y defina niveles de cumplimiento.
- Cada grupo debe proponer a la Gobernanza de la organización una política de acuerdo a la Tabla 3.1 y tomando en cuenta lo siguiente:
    - Todas las políticas deben estar alineadas con lo establecido en la política general de seguridad de la información.
    - Se debe seguir el mismo formato y estructura de la política general de seguridad de la información (Se deja un ejemplo que se puede usar como base en el entorno virtual).
    - Esta política debe presentarse como un documento word y pdf adjunto al video.
    - Utilice la ISO 27002 para el desarrollo de la política propuesta.
    - Identifique en el Framework NIST, Categorías y Subcategorías que le permitan enriquecer su propuesta.
    - De acuerdo a lo anterior, desarrolla propuestas que enriquezcan la política desde las referencias informativas asociadas. Destaque lo propuesto desde COBIT 5 en amarillo, ISO 27002 en verde y NIST SP 800-53 en celeste, CIS CSC en naranjo y otro estándar en magenta. Debe utilizar al menos dos referencias informativas.

Tabla 3.1. Asignación de políticas por grupo

Grupo	**Nombre de la política**
A	Política de mantención, desarrollo y adquisición de sistemas
B	Política de gestión de incidentes de seguridad de la información
C	Política de gestión de continuidad

3.2 Gestión de riesgos de ciberseguridad

- Proponga una política de gestión de riesgos (con enfoque cuantitativo) alineada con las políticas anteriores (utilice la UNE-ISO 31000:2018).
- Simule la aplicación de dicha política para realizar la gestión de riesgos del activo "Información sensible y personal de un usuario de sistema". Proponga:
    - Valor monetario asignado al activo.
    - Al menos 3 amenazas significativas.
    - Probabilidad del ratio de ocurrencia de cada amenaza (Justifique).
    - Pérdida potencial que la compañía puede soportar por amenaza en una ventana de tiempo de 12 meses.
    - Controles recomendados (Recomiende al menos un control relacionado con software y alineado con de la política asignada en la Tabla 3.1)
    - ¿En qué amenaza se focalizará primero?
    - ¿Cuánto dinero gastaría en protegerse de dicha amenaza?

3.3 Gestión

Es hora de planear la implementación de dichos controles. Para ello se debe planificar su implementación:

- Para uno de los controles seleccionados (que requiera software) compare la opción comercial, open source o libre, y desarrollo ad hoc (Construya una tabla comparativa). Debe considerar aspectos como:
    - Costo del producto
    - Costo del diseño, planificación e implementación
    - Modificaciones del entorno
    - Compatibilidad con otros controles
    - Requerimientos de mantenimiento
    - Requerimientos de prueba
    - Costos de reparación, reemplazo o actualización
    - Costos de operación y soporte
    - Efectos en la productividad
    - Costos de suscripción
    - Horas Humanas (HH) extras para monitoreo y respuesta a alertas
- Realice un análisis costo/beneficio para seleccionar la mejor alternativa.

4. ENTREGA

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

- La presentación tenga un hilo conductor y se vaya desarrollando coherentemente a medida que se incorporan nuevos elementos.
- En total, el video no debe sobrepasar los 20 minutos.
- En caso de querer agregar más antecedentes, déjelos en un apéndice de video a parte. Estos últimos solamente serán revisados en caso de que en estos exista algún antecedente importante a considerar en una potencial re-corrección.
- Se debe generar una carpeta compartida con toda la documentación (pdf, doc, excel) y videos asociados. 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.
- La entrega final es a través del foro social hasta las 23:59 del día definido en la programación del curso.

Se sugiere la utilización de herramientas de edición de video para mejorar la presentación del video. Estas herramientas le permitirán eliminar tiempos muertos en el video, repartir la grabación entre los integrantes del grupo, agregar elementos gráficos y de texto al video entre otros.

4. RÚBRICA

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

Descripción	**Puntaje**
Presenta introducción acorde al trabajo	20
Los conceptos se explican de forma correcta	40
Realiza la actividad de acuerdo a las instrucciones indicadas	20
Indica todos los supuestos requeridos.	30
Resuelve en su totalidad y correctamente el apartado 3.1	150
Resuelve en su totalidad y correctamente el apartado 3.2	150
Resuelve en su totalidad y correctamente el apartado 3.3	150
Desarrolla conclusión de acuerdo a los resultados obtenidos	20
Incluye referencias en la presentación (formato APA o IEEE) y además incluye bibliografía desde fuentes confiables (Esto último se debe mostrar en el video, no presentar)	20
Se respeta el tiempo de la presentación (15 a 20 minutos máximo, entre la introducción, desarrollo y conclusión).	20
Se indica el integrante del grupo que está hablando en cada momento.	10
El video presenta esquemas y figuras de acuerdo al contenido.	10
El audio del video es claro.	10
Forma: Hace un buen balance entre el texto, imágenes y videos presentados	30