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

FUNDAMENTOS DE CIBERSEGURIDAD
Prof. Juan Ignacio Iturbe

ACTIVIDAD GRUPAL 2

Exigencia 70%

1. INTRODUCCIÓN

En esta actividad, los equipos de estudiantes simularán la creación de empresas de desarrollo de software, las cuales competirán por obtener una licitación. La Universidad de Santiago de Chile servirá como cliente que busca una solución integral de Software como Servicio (SaaS) en el área de Recursos Humanos (RR.HH.) con un enfoque sólido en la ciberseguridad. El reto para los estudiantes será desarrollar una propuesta que satisfaga los estándares de seguridad y funcionalidad exigidos.

2. LICITACIÓN

La Universidad desea externalizar su sistema de RR.HH. mediante una solución SaaS segura y eficiente. Se invita a las empresas de desarrollo de software a presentar propuestas para un sistema que mejore la gestión de RR.HH. y asegure la protección de datos sensibles.

2.1 Escenario

2.1.1 Contexto

Las empresas participantes deben presentar un paquete integral que se encuentre alineado y que incluya:

1. Inventario de procesos de RRHH y selección de proceso crítico.
2. Diseño del proceso de RR.HH. en BPMN.
3. Mostrar mockups de ejemplos del software.
4. Selección de tecnologías para el SaaS de RR.HH para soportar lo anterior.
5. Cumplimiento con leyes de protección de datos y normativas de seguridad (nacionales e internacionales).
6. Identificación de riesgos cibernéticos y protección de activos digitales.
7. Aplicación del Framework de Ciberseguridad de NIST (NIST CSF) al diseño propuesto y otros estándares y buenas prácticas relacionadas.
8. Plan de implementación de seguridad a dos años, con recursos y presupuesto detallado.
9. Simulación del software con la tecnología seleccionada, demostrando controles tecnológicos, físicos y administrativos.

Las prácticas de ciberseguridad deben alinearse con las áreas de Gobierno, Gestión y Operación/Implementación, según la especialización de cada grupo indicada en la Tabla 1.1.

Tabla 1.11: Enfoques de cada grupo

Grupo	**Enfoque**
Grupo A	Desarrollo de software seguro
Grupo B	Continuidad del negocio y recuperación ante desastres
Grupo C	Seguridad de las redes y comunicaciones
Grupo D	Gestión de la identidad y control de acceso
Grupo E	Respuesta a incidentes de ciberseguridad
Grupo F	Seguridad de los activos

2.1.2 Requisitos

Además de integrar las funcionalidades que soporten el proceso crítico de RRHH escogido. El software deberá contar con los siguientes requisitos mínimos. Cada empresa deberá proponer otros de acuerdo a sus enfoques.

Requisitos Funcionales:

- Gestión de Usuarios: El sistema debe permitir la creación y gestión de cuentas de usuario con diferentes niveles de privilegios.
- Autenticación Segura: Integración de autenticación de dos factores para mejorar la seguridad de las cuentas de usuario.
- Auditoría y Seguimiento: Capacidad de monitorear y registrar actividades de desarrollo, incluyendo cambios en el código y la configuración del sistema.
- Detección de Vulnerabilidades: Funcionalidad para identificar y alertar sobre vulnerabilidades de seguridad en tiempo real.
- Respaldo y Recuperación: Mecanismos automáticos para realizar y restaurar copias de seguridad de datos, y pruebas de recuperación de desastres.
- Seguridad de la Red: Implementación de firewall avanzado y cifrado de datos para proteger contra amenazas externas e internas.
- Acceso Remoto Seguro: Facilitar conexiones VPN seguras para el acceso remoto al sistema.
- Control de Acceso: Soporte para integración con sistemas de identidad y gestión de políticas de acceso basadas en roles.
- Alertas y Respuesta: Configuración de alertas de seguridad personalizadas y un panel para visualizar incidentes y amenazas.

- Gestión de Activos: Inventario automatizado y gestión de la seguridad de activos digitales, con generación de informes de cumplimiento.

Requisitos No Funcionales:

- Estándares de Seguridad: Desarrollo en línea con el estándar OWASP Top 10 y los últimos estándares de seguridad de red.
- Rendimiento y Escalabilidad: Capacidad para manejar transacciones rápidas, soportar un gran número de usuarios simultáneos y escalar según sea necesario.
- Disponibilidad y Resiliencia: Alta disponibilidad del sistema, objetivos de recuperación claros y compatibilidad con infraestructuras de nube para redundancia.
- Eficiencia y Mantenibilidad: Bajos tiempos de respuesta, facilidad de mantenimiento y actualizaciones sin interrupciones.
- Interoperabilidad: Capacidad para integrarse con diversas plataformas y herramientas de terceros.
- Seguridad de Datos: Garantizar la integridad y confidencialidad de los datos almacenados y en tránsito.

3. ENTREGA

3.1 Anteproyecto

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. Considerar un hito de reunión semanal en donde se debe preparar una minuta con lo realizado en la semana, los problemas y dudas que han tenido y lo que se desarrollará la siguiente semana.
- 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 visualiza 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 Presentación e informe

La entrega corresponde a un informe que evidencia el desarrollo completo de lo anterior y una presentación de lo desarrollado. Es importante que:

- El informe y la presentación tengan un hilo conductor y se vaya desarrollando coherentemente a medida que se incorporan nuevos elementos.
- En total, la presentación no debe sobrepasar los 15 minutos.
- El informe no deberá exceder las 30 páginas.
- En caso de querer agregar más antecedentes (a las 30 páginas o 15 minutos de presentación), déjelos en un apéndice.
- 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 fuera de bases (nota mínima).
- Explicite todos los supuestos realizados en el informe y en la presentación (hacer una sección o ppt asociada).
- 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 cada empresa deberá realizar preguntas al licitante (representado por el profesor). 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 evaluación 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 compromisos, 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. NOTAS

Tener en cuenta las siguientes consideraciones.

- La entrega del anteproyecto es el (19 de Noviembre 2023). Esta se debe entregar a través del link provisto.

- El formato del anteproyecto y el informe es el mismo que el de propuesta de memoria.
- 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.
- En la entrega final, 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%.

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.
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 2 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.
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 colaboración o mala distribución de tareas. Dependencia excesiva del profesor y falta de iniciativa para aprender de forma autónoma.	El trabajo en equipo es aceptable, con una comunicación, colaboración y distribución de tareas adecuada, pero podría mejorar. Algún grado de iniciativa y aprendizaje autónomo, aunque todavía depende en gran medida de la orientación del profesor.	El trabajo en equipo es excelente: comunicación eficaz, colaboración activa, distribución 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.