Sistema ‘Seguridad Web’

Ingrid Margarita Lefiguala Banda

i.lefiguala01@ufromail.cl

***Abstract***

*In 2012, the Universidad Católica de Temuco decided to implement a new computer system integrated in a web environment called KELLUN, which in Mapudungun means "To provide support".*

*The institutional management system integrates the fundamental processes of the different areas of the university; therefore, KELLUN is made up of different modules that support this management, configured by the 'Web Security' system.*

*The objective of this project is to improve the 'Web Security' system, in order to have a better record of the KELLUN configurations.*

***UNIVERSIDAD DE LA FRONTERA***

[**ANTECEDENTES DEL PROYECTO** 1](#_Toc533085729)

[**MOTIVACION** 1](#_Toc533085730)

[**SISTEMAS HEREDADOS Y SGSI** 1](#_Toc533085731)

[**JUSTIFICACION DEL PROBLEMA A RESOLVER** 4](#_Toc533085732)

[**ALCANCE** 5](#_Toc533085733)

[**OBJETIVO GENERAL** 5](#_Toc533085734)

[**OBJETIVOS ESPECÍFICOS** 5](#_Toc533085735)

[**REQUERIMIENTOS** 5](#_Toc533085736)

[**DIAGRAMA DE CASOS DE USO** 6](#_Toc533085737)

[**PLANTILLAS CASOS DE USO** 6](#_Toc533085738)

[**DIAGRAMAS DE ACTIVIDADES** 10](#_Toc533085739)

[**CALCULO DE ESFUERZO** 11](#_Toc533085740)

**ANTECEDENTES DEL PROYECTO**

En el año 2012 la Universidad Católica de Temuco resolvió implementar un nuevo sistema informático integrado en ambiente web llamado KELLUN, que en mapudungun significa “Prestar Apoyo”.

KELLUN es un sistema de elaboración propia, desarrollado e implementado por Desarrollo de Sistemas, adecuado a las necesidades de los usuarios y unidades de la Universidad, que permite la gestión, comunicación e integración de los procesos entre las distintas áreas de la Institución.

El sistema de gestión Institucional integra los procesos fundamentales de las áreas Académicas y de Administración y Finanzas, por tanto, KELLUN está conformado por distintos módulos que apoyan a la gestión de las áreas antes mencionadas.

Anterior al sistema KELLUN y con la finalidad de gestionar pequeños sistemas, se creó el sistema de ‘Seguridad Web’, que luego se siguió utilizando para gestionar KELLUN, el objetivo actual del sistema de ‘Seguridad Web’ es:

* Dar la estructura a los nuevos módulos que se agregan a KELLUN, es decir por medio de este sistema se ingresan los nuevos módulos y sus respectivos menús y submenús, y se direccionan las rutas de las páginas que los componen.
* Ingresar nuevos usuarios al KELLUN.
* Ingresar los perfiles de usuarios de alguno de los módulos.
* Ingresar los roles de usuario a los módulos que lo requieran.
* Asignar 1 o más módulos a los usuarios

El sistema de ‘Seguridad Web’ (SWeb), gestiona los permisos a cualquiera de los módulos que integran KELLUN, y es utilizado, exclusivamente, por solo algunos de los miembros del equipo de desarrollo de sistemas.

**MOTIVACION**

Este proyecto se encuentra en la frontera del conocimiento, tenemos un sistema heredado que es precisamente el sistema de gestión de seguridad, tal combinación es un desafío interesante y motivante.

**SISTEMAS HEREDADOS Y SGSI**

***Implementación de un SGSI***

Un sistema de gestión de la seguridad de la información (SGSI) (en inglés: *information security management system*, ISMS) es un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

Un SGSI es para una organización el diseño, implementación y mantenimiento de un conjunto de procesos para gestionar eficientemente la información, buscando asegurar su confidencialidad, integridad y disponibilidad, minimizando a la vez los riesgos de seguridad.

Toda empresa necesita un [plan para sus SGSI](https://www.gb-advisors.com/es/gestion-servicios-ti/), este plan debe regirse por protocolos y normas aceptadas internacionalmente. Entre dichos protocolos y normas, una de las mayormente aceptadas es la Norma ISO 27001.

Si bien existen muchas normas internacionales para evaluar los riesgos informáticos y aplicar controles para mitigarlos o eliminarlos, la norma ISO 27001 cuenta con amplia aceptación para asegurar la integridad de los datos. Sus principales características son:

* **Confidencialidad.**Garantiza acceso seguro a la información
* **Integridad.** Estrechamente relacionado al punto anterior, ISO 27001 asegura que tanto los procesos como la información relacionada con los sistemas de seguridad sean completos y precisos.
* **Disponibilidad.**  las personas autorizadas podrán acceder a la información pertinente cuando lo necesiten.

Los pasos para implementar un SGSI bajo esta norma, son:

1. **Fase de evaluación**, Este diagnóstico indicará la etapa y las medidas correctivas a tomar para corregir y darle paso a la implementación del SGSI bajo estándares ISO 27001.
2. **Planificación,** recoger tareas y actividades que van desde la elección del personal técnico encargado; hasta la puesta en marcha de la implementación.
3. **Documentación + Gantt,** reunir toda la documentación pertinente y agruparla por actividades y tareas lógicas en un tiempo determinado.
4. **Organización,** organizar la documentación por fases de ejecución y organización del proyecto. En esta etapa también se compilan los manuales para ser utilizados al momento de lanzar las campañas de concientización respecto a la implementación del SGSI bajo norma ISO 27001.
5. **Presentación,** integrar todo lo recogido en los pasos anteriores, se presenta el proyecto factible a la alta gerencia y a los involucrados en su ejecución.
6. **La presentación,** incluye alcances de la norma ISO 27001; exposición de motivos y políticas; recoge los resultados de la fase de evaluación; define el tratamiento de los riesgos detectados; los motivos que apoyan la decisión y la forma de aplicación.
7. **Despliegue y puesta en marcha,** comienza con la aprobación de la directiva. Una vez es aprobado, inician las campañas de concientización en forma de programas cortos  para el despliegue y puesta en marcha del proyecto.

Esto supone implementar de la misma manera los controles; procedimientos exigidos; los programas de capacitación unidos a los de concientización. Con ello; comenzará la emisión de registros que mantendrán informados a los auditores y agentes autorizados sobre el verdadero rendimiento de la empresa, sus empleados, y el éxito de la implementación de la Norma ISO 27001 para tus SGSI.

Hasta aquí tenemos un enfoque general de un SGSI, en este proyecto nos enfocaremos en una parte importante de la seguridad de la información, de la Universidad Católica de Temuco, que es el sistema de seguridad informática SWeb, encargado de administrar los permisos de acceso al sistema integrado KELLUN y que forma parte del plan del SGSI de la universidad.

***Mantención de un sistema heredado***

La problemática del mantenimiento de un software es muy amplia y lo es cada vez más con el paso del tiempo. Las circunstancias por las que se deba enfrentar la tarea de tomar el control de un sistema heredado, son generalmente porque no existen mejores alternativas a corto plazo y simplemente se debe hacer.

Algunas características frecuentes de estos proyectos incluyen, tecnologías obsoletas, limitaciones de escalabilidad, escasez o nula documentación técnica y funcional, arquitectura de caja negra, ausencia de referentes con conocimientos prácticos del diseño técnico, una larga lista de mejoras pendientes de implementación, etc. Por otro lado es probable que se cuente con un aspecto positivo no menor: el sistema suele ser estable, si lleva tiempo en producción es porque funciona en forma aceptable, al menos una buena parte de él.

Cada proyecto de reingeniería tiene una combinación particular de estas características y conforman una problemática muy específica que debe ser analizada de acuerdo a los objetivos del cliente en cuanto a ese sistema (mejorar, corregir, adaptar, rediseñar, migrar, agregar funcionalidad, etc.). A continuación, se describe un proceso de alto nivel que debería guiar cualquier proyecto de reingeniería:

1. **Asegurar una apropiada gestión de configuración,** con el objetivo de completar una evaluación del estado actual es necesario establecer una línea base sobre él o los repositorios que se posean. Si no hay repositorio o éste no es adecuado, es altamente recomendable regularizar esta situación antes de continuar con cualquier tipo de modificación. Suele ser una buena ocasión para generar una rama en el repositorio de manera de contener los cambios aislados de la versión productiva
2. **Realizar una auditoría inicial,** la auditoría tendrá un tinte diferente según el nivel de responsabilidad y las condiciones contractuales con que se asuma el proyecto. No obstante, lo anterior, el propósito práctico de la auditoría es conocer el estado actual del sistema y determinar la brecha con respecto al sistema deseado.

La auditoría debe cubrir el menos las siguientes actividades:

* Identificar las fronteras tecnológicas
* Relevar la arquitectura y el stack tecnológico
* Analizar el código estático
* Relevar documentación existente

1. **Documentar y comentar (el código)**, en este punto es necesario completar la documentación inexistente tanto funcional como técnica según sea necesario, incluyendo el propio código en la medida que favorezca la entendibilidad del trabajo a realizar próximamente.
2. **Implementar pruebas unitarias**, esta actividad incluye la elaboración de un plan de pruebas apropiado. La estrategia de pruebas habrá ido modelándose durante la auditoría inicial y tendrá el foco puesto en los objetivos del proyecto. Suele ser muy valiosa la participación de  usuarios, técnicos y referentes de los  sistemas que  interactúan con el software a modificar para lograr un set de pruebas completo y efectivo.
3. **Planificar y comunicar la reingeniería**, dentro de las  tareas de gestión también se debe contemplar un plan de comunicación adecuado que involucre a todos los stakeholders incluyendo a los referentes de los sistemas que interoperan y que podrían verse afectado aún si en la reinigeniería no se prevé cambios en el protocolo, o comportamiento de las interfaces ya que es probable que éstas requieran ser testeadas oportunamente.
4. **Realizar la reingeniería**, las tareas de reingeniería constituyen un escenario ideal para un desarrollo guiado por pruebas o test-driven development (TDD). En caso de no ser posible suele ser conveniente comenzar por  el modelo de datos, luego por  las interfaces y finalmente por el modelo de negocios  y  los servicios, permitiendo una  definición temprana  de lo que serían  las fronteras del sistema.
5. **Ejecutar el plan de pruebas**, si las pruebas unitarias son suficientemente consistentes sólo habrá que realizar las pruebas de integración y de aceptación. La cantidad de pruebas depende de la envergadura del proyecto, sin embargo no se debe subestimar el esfuerzo de las pruebas y las tareas de bug fixing y estabilización sencillamente porque se ha alterado un código que ha logrado un equilibrio operacional luego de mucho tiempo.
6. **Auditoría final**, este paso busca mostrar los resultados obtenidos de acuerdo a los objetivos iniciales y a las observaciones y  no conformidades identificadas en la auditoría inicial.
7. **Puesta en producción**, basados en ese conocimiento la auditoría final podría haber expuesto nuevos riesgos sobre potenciales problemas en la liberación de un upgrade de un sistema que estaba estable y fue alterado, por lo que es imperioso contar con un plan de "vuelta a atrás" lo más eficiente posible.  
   Luego de ello habrá naturalmente un período de observación y mantenimiento correctivo que se evaluará en cada caso.

Si la reingeniería fue exitosa, el sistema habrá sido sometido a una reinversión con múltiples beneficios, tanto por la inclusión de mejoras o adaptaciones como por el control y conocimientos recuperados sobre el código, y si el proceso fue prolijo se habrán prevenido desvíos y anticipado todos los problemas evitables.

**JUSTIFICACION DEL PROBLEMA A RESOLVER**

Los módulos, que se gestionan en el SWeb, son críticos para el funcionamiento de la universidad. Cada nuevo módulo se está montando sobre esta arquitectura de seguridad y, por lo tanto, de alguna forma, existe una conexión entre ellos, lo que significa que el error ocasionado en la gestión de alguno de los módulos puede repercutir en los demás, por ejemplo; en todos los módulos se usan los perfiles de usuario ‘Administrador’ y ‘Asistente’, entre otros, con diferentes permisos de acceso a la información de la universidad, y distintos accesos a los menús de algún modulo, un error en la configuración de estos perfiles puede provocar graves problemas al dar acceso o quitar el acceso a determinados datos.

En este proyecto me enfrento a la problemática de tomar un producto heredado, este es un caso particular, ya que el sistema heredado es el sistema que gestiona la seguridad de KELLUN. Además, no es uno de los sistemas que ve un usuario normal de la universidad, sino que es administrado por los funcionarios de soporte de la dirección de desarrollo de sistemas.

Una decisión complicada es determinar si es necesario hacerlo de nuevo o buscar una alternativa menos invasiva. En el caso de tener que hacerlo de nuevo, la ingeniería de software es diferente a un proyecto que inicia desde cero, porque involucra datos históricos que no deben perder su integridad y trazabilidad, por lo cual se ve un escenario complicado.

Los problemas más importantes que presenta hoy el SWeb son:

* No hay registro histórico de los movimientos realizados en el sistema de seguridad, esto deja sin evidencia cuando se ingresan o quitan permisos, cuando se crean nuevos sistemas, menús o usuarios. Este es el principal problema, ya que, al no existir esta información, muchas veces tenemos movimiento de permisos que no se logra saber quién los hizo.
* No permite generar reportes de ningún tipo desde el sistema
* No existe una sesión de usuario para los funcionarios de la universidad, en donde puedan tener acceso a información restringida?? para sus análisis.

Una opción viable podría ser, mejorar el sistema ya existente, las razones por las que no se ha considerado esta opción son:

* No existe documentación del sistema actual
* No existe soporte en la dirección de sistemas, para la tecnología utilizada, por lo tanto, esta se convierte en una barrera para hacer progresos en el sistema. El sistema fue desarrollado en .NET.
* Las personas que lo hicieron ya no trabajan en la dirección de sistemas y tampoco es posible que se puedan reincorporar, porque trabajan en otras empresas o en otras ciudades.

Otra opción es hacer de nuevo el sistema de seguridad, algunas de las complicaciones para ello son:

* Las autoridades buscan nuevas funcionalidades adicionales al sistema actual, no pretenden rehacerlo en estos momentos, por lo tanto, no es prioridad y no hay apoyo para ello.
* No se sabe cuánto conocimiento se va perder si lo hacemos de nuevo y nada asegura que los problemas que presenta actualmente el sistema de seguridad no se presentarán en una nueva versión.

Como no tenemos, a corto plazo, opción de migrarlo o mejorar el actual sistema de seguridad tenemos otra alternativa, usar Wraps, es decir darle un envoltorio con alguna tecnología manejable en la dirección de sistemas, sin intervenir el sistema, pero ofreciendo las funcionalidades que hoy no posee.

Hacer el sistema de seguridad de nuevo no es un proyecto fácil, ni abordable en este documento, por lo que nos enfocaremos en un problema específico el cual pueda ser una contribución real orientada a resolver problemas puntales que lo? afectan actualmente.

**ALCANCE**

El alcance que se quiere obtener con este proyecto corresponde a una porción del problema que se abordara:

* Gestionar la trazabilidad de los datos, en este caso la información relacionada a la asignación de módulos y permisos.
* Gestionar la seguridad de los datos bajo la misma plataforma, pero mejorada.

**OBJETIVO GENERAL**

Existen 2 niveles de objetivos, el primero aborda el proyecto general del sistema SWeb, y el otro es el proyecto de la asignatura de Ingeniería de software que es en el que trabajaremos. Este objetivo apunta a realizar una intervención precisa al actual sistema, que permita obtener la trazabilidad de los datos, que registran los movimientos de los permisos asignados a los usuarios del KELLUN en sus diversos módulos.

**OBJETIVOS ESPECÍFICOS**

* Generar documentación inicial de la arquitectura del sistema Sweb que permita orientar los cambios hacia una extensión trazable del sistema, aclarando la disponibilidad de datos de trazabilidad en el sistema actual, como también la eventual existencia de perfiles.
* Generar un sistema web que permita obtener el historial de movimientos, de los gestores de seguridad, en la concesión de permisos para usuarios del KELLUN.
* Permitir asegurar que la jerarquía de seguridad se respete, tanto en la asignación de permisos de los gestores de seguridad como en el acceso a los datos de trazabilidad.
* Analizar la factibilidad técnica de que datos de trazabilidad sean agregados dentro del wrap, es decir, como parte de Sweb y no como parte del envoltorio.
* Evaluar la conveniencia y/o factibilidad de mantener en paralelo los conceptos de perfiles y roles o si es necesario realizar re-ingeniería a estos conceptos.

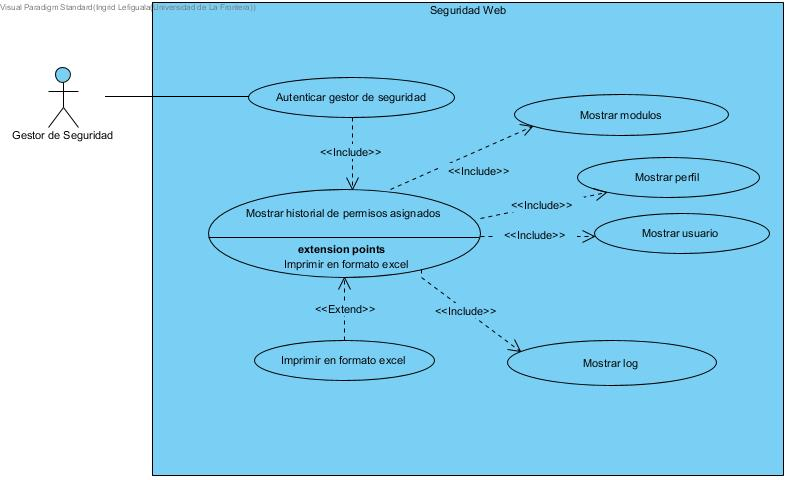
**REQUERIMIENTOS**

Para mejorar el sistema SWeb, en esta primera etapa, se abordaran los siguientes requerimientos:

* Desarrollar una extensión web que permita la autentificación del gestor de seguridad para revisar los historiales.
* Desarrollar un apartado de informes, exportables a Excel, que muestre la información de asignaciones de módulos y perfiles. El cual debe permitir realizar búsquedas por; usuario que registro el cambio (alguno de los gestores de seguridad), por fecha, por usuario al que se le asignó un módulo o perfil, por modulo o por perfil.

**DIAGRAMA DE CASOS DE USO**

A continuación se grafican los casos de uso de la nueva extensión web.



***Fig. 01, casos de uso del gestor de seguridad***

**PLANTILLAS CASOS DE USO**

A continuación se detallan las plantillas de los casos de uso.

|  |  |  |
| --- | --- | --- |
| **SW- 01** | **Autenticar gestor de seguridad** | |
| **Objetivos asociados** | Gestión de permisos | |
| **Requisitos asociados** | ninguno | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando el gestor de seguridad se autentifique en la nueva extensión web. | |
| **Precondición** | ninguna | |
| **Secuencia Normal** | **Paso** | **Acción** |
| 1 | El gestor de seguridad solicita autentificarse |
| 2 | La nueva extensión solicita los datos de autentificación |
| 3 | El gestor de seguridad ingresa los datos solicitados |
| 4 | La nueva extensión permite el ingreso del gestor de seguridad |
| **Postcondición** | El gestor de seguridad ingresa a la nueva extensión web | |
| **Excepciones** | **Paso** | **Acción** |
|  | 3 | El gestor de seguridad cancela la acción, termina el caso de uso |
| **Rendimiento** | **Paso** | **Cota de Tiempo (en segundos)** |
|  | 4 | 2 |
| **Frecuencia esperada** | 5 veces al mes | |
| **Comentarios** | ninguno | |

***Tabla 01,*** *Agregar nuevo usuario*

|  |  |  |
| --- | --- | --- |
| **SW- 02** | **Historial de permisos y asignaciones** | |
| **Objetivos asociados** | Gestión de permisos | |
| **Requisitos asociados** | ninguno | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando el gestor de seguridad lo considere oportuno, para ver el historial de permisos y módulos asignados en un periodo de tiempo | |
| **Precondición** | ninguno | |
| **Secuencia Normal** | **Paso** | **Acción** |
| 1 | El gestor de seguridad solicita al sistema mostrar el historial de permisos |
| 2 | El sistema solicita datos de filtro para la  búsqueda |
| 3 | El gestor ingresa los datos de filtro para  la búsqueda |
| 4 | El sistema muestra la información  solicitada y ofrece la impresión de  documentos en excel con la información |
| **Postcondición** | Se muestra la información histórica de los permisos y asignaciones | |
| **Excepciones** | **Paso** | **Acción** |
|  | 3 | El gestor de seguridad cancela la acción, termina el caso de uso |
| **Rendimiento** | **Paso** | **Cota de Tiempo (en segundos)** |
|  | 4 | 1 |
| **Frecuencia esperada** | 15 veces al mes | |
| **Comentarios** | ninguno | |

***Tabla 02,*** *Historial de permisos y asignaciones*

|  |  |  |
| --- | --- | --- |
| **SW- 03** | **Mostrar Usuario** | |
| **Objetivos asociados** | Gestión de permisos | |
| **Requisitos asociados** | ninguno | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando se solicite información sobre un usuario | |
| **Precondición** | Debe estar identificado el usuario por el que se  consulta | |
| **Secuencia Normal** | **Paso** | **Acción** |
| 1 | El actor solicita información sobre un usuario |
| 2 | El sistema solicita datos para buscar el usuario |
| 3 | El actor envía los datos solicitados |
| 4 | El sistema entrega los datos del usuario |
| **Postcondición** | Se obtiene los datos del usuario | |
| **Excepciones** | **Paso** | **Acción** |
|  | 4 | No se encuentra el usuario, termina el caso de uso |
| **Rendimiento** | **Paso** | **Cota de Tiempo (en segundos)** |
|  | 4 | 2 |
| **Frecuencia esperada** | 100 veces al día | |
| **Comentarios** | ninguno | |

***Tabla 03,*** *Mostrar Usuario*

|  |  |  |
| --- | --- | --- |
| **SW- 04** | **Mostrar perfil** | |
| **Objetivos asociados** | Gestión de permisos | |
| **Requisitos asociados** | ninguno | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando se solicite información sobre un perfil | |
| **Precondición** | Debe estar identificado el perfil por el que se consulta | |
| **Secuencia Normal** | **Paso** | **Acción** |
| 1 | El actor solicita información sobre un perfil |
| 2 | El sistema solicita datos para buscar el perfil |
| 3 | El actor envía los datos solicitados |
| 4 | El sistema entrega los datos del perfil |
| **Postcondición** | Se obtiene los datos del perfil | |
| **Excepciones** | **Paso** | **Acción** |
|  | 4 | No se encuentra el perfil, termina el caso de uso |
| **Rendimiento** | **Paso** | **Cota de Tiempo (en segundos)** |
|  | 4 | 2 |
| **Frecuencia esperada** | 100 veces al día | |
| **Comentarios** | ninguno | |

***Tabla 04,*** *Mostrar perfil*

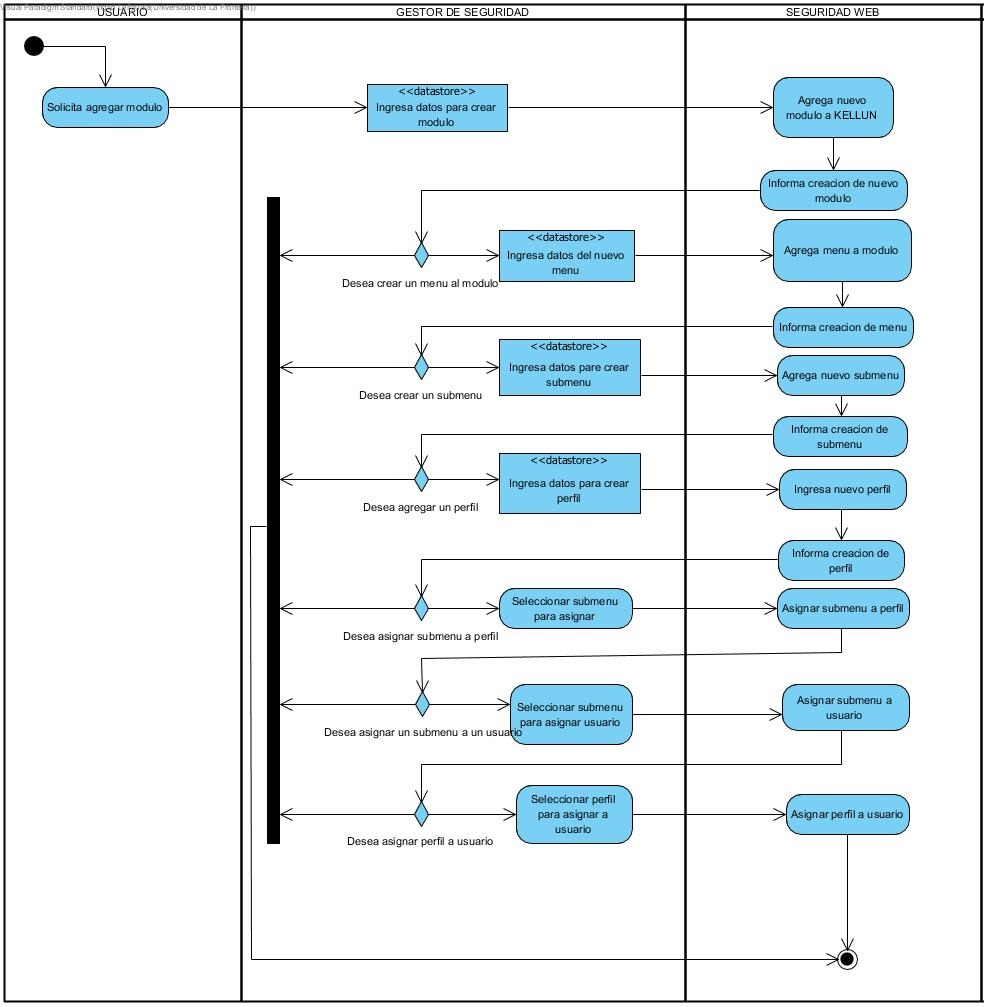
|  |  |  |
| --- | --- | --- |
| **SW- 05** | **Mostrar módulo** | |
| **Objetivos asociados** | Gestión de permisos | |
| **Requisitos asociados** | ninguno | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando se solicite información sobre algún modulo | |
| **Precondición** | Debe estar identificado el modulo por el que se  consulta | |
| **Secuencia Normal** | **Paso** | **Acción** |
| 1 | El actor solicita información sobre un modulo |
| 2 | El sistema solicita datos para buscar el modulo |
| 3 | El actor envía los datos solicitados |
| 4 | El sistema entrega los datos del modulo |
| **Postcondición** | Se obtiene los datos del modulo | |
| **Excepciones** | **Paso** | **Acción** |
|  | 4 | No se encuentra el modulo, termina el caso de uso |
| **Rendimiento** | **Paso** | **Cota de Tiempo (en segundos)** |
|  | 4 | 2 |
| **Frecuencia esperada** | 100 veces al día | |
| **Comentarios** | ninguno | |

***Tabla 05,*** *Mostrar modulo*

|  |  |  |
| --- | --- | --- |
| **SW- 06** | **Mostrar log** | |
| **Objetivos asociados** | Gestión de permisos | |
| **Requisitos asociados** | ninguno | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando se solicite información sobre el historial | |
| **Precondición** | ninguna | |
| **Secuencia Normal** | **Paso** | **Acción** |
| 1 | El actor solicita información sobre el historial |
| 2 | El sistema solicita datos para buscar en el historial |
| 3 | El actor ingresa los datos solicitados |
| 4 | El sistema muestra los datos solicitados |
| **Postcondición** | Se obtiene un informe con el historial | |
| **Excepciones** | **Paso** | **Acción** |
|  | 3 | El gestor de seguridad cancela la acción, termina el caso de uso |
| **Rendimiento** | **Paso** | **Cota de Tiempo (en segundos)** |
|  | 4 | 2 |
| **Frecuencia esperada** | 1 veces al día | |
| **Comentarios** | ninguno | |

***Tabla 06,*** *Mostrar log*

**DIAGRAMAS DE ACTIVIDADES**



**CALCULO DE ESFUERZO**

Basándonos en los casos de uso diseñados, se calcula el esfuerzo con el método de estimación CEIS UFRO, obteniendo los siguientes resultados (este cálculo está basado en la realización del proyecto completo)

