

Tipo de artículo: Artículo original
Temática: seleccionar la temática a partir de las líneas editoriales de la revista
Recibido: 22/09/16 | Aceptado: 24/11/16 | Publicado: 20/12/2018

Sistema para el diagnóstico y seguimiento de riesgo en el centro DATEC

System for the diagnosis and monitoring of risk in the DATEC center

Barbara Bron Fonseca¹, Maiker Rodríguez Troche², Pedro M. Puig Díaz³

¹ Facultad de Ciencias y Tecnologías Computacionales, Universidad de las Ciencias Informáticas, bbron@uci.cu

² Facultad de Ciencias y Tecnologías Computacionales, Universidad de las Ciencias Informáticas, maiker@uci.cu

³ Facultad de Ciencias y Tecnologías Computacionales, Universidad de las Ciencias Informáticas, pmpuig@uci.cu

* Autor para correspondencia: bbron@uci.cu

Resumen

En la Universidad de las Ciencias Informáticas, específicamente el Centro de Tecnologías de Gestión de Datos "DATEC", se especializa en el desarrollo de aplicaciones informáticas entre las que se pueden contar: el sistema Elecciones, el sistema Generador dinámico de reportes y el proyecto Fiscalía, entre otros. A pesar de la experiencia en cuanto al desarrollo de sistemas y la calidad de los productos presentados por el centro, existen deficiencias en cuanto a la gestión y seguimiento de riesgos de los proyectos. Actualmente en el centro DATEC la gestión de riesgos se realiza de forma manual, pues a pesar de que existe una herramienta para la gestión de los mismos, no está regida por las directivas establecidas en la Resolución No. 60/11. El hecho de que el proceso de gestión captura y seguimiento de riesgos se realice de forma manual, dificulta y demora el trabajo debido a que se necesita más tiempo para aplicar las acciones correctivas, pues las personas involucradas no son notificadas a tiempo y por tanto las decisiones no se toman oportunamente. Con el objetivo de dar solución a las deficiencias antes mencionadas, se propone el desarrollo de una herramienta que contribuya a erradicar las deficiencias y mejorar el proceso de gestión, diagnóstico y seguimiento de los riesgos en el centro DATEC de la Universidad de las Ciencias Informáticas.

Palabras clave: Riesgo, Gestión de riesgos, Gestión de datos.

Abstract

At the University of Computer Sciences, specifically the Center for Data Management Technologies "DATEC", specializes in the development of computer applications among which can be counted: the Elections system, the dynamic report generator system and the Fiscalía project, among others. Despite the experience in the development of systems and the quality of the products presented by the center, there are deficiencies in the management and monitoring of project risks. Currently in the DATEC center risk management is done manually, because although

there is a tool for managing them, it is not governed by the directives established in Resolution No. 60/11. The fact that the management process captures and follows up on risks is done manually, hinders and delays the work due to the fact that more time is needed to apply the corrective actions, because the people involved are not notified in time and therefore the decisions are not made in a timely manner. In order to solve the aforementioned shortcomings, it is proposed to develop a tool that contributes to eradicating the deficiencies and improve the process of management, diagnosis and monitoring of risks in the DATEC center of the University of Computer Sciences.

Keywords: *Risk, Risk management, Data management.*

Introducción

En la actualidad, la informática ocupa un rol importante, no solo en la vida diaria de las personas, sino también en el desarrollo de las empresas. El significativo avance de las Tecnologías de la Información y la Comunicación (TIC) ha brindado grandes progresos en diferentes sectores de la actividad humana como: la medicina, la biología, la ingeniería, la industria, la investigación científica, la gestión empresarial, entre otros.

No es extraño que hoy día, la mayoría de las tareas de oficina, en las empresas o incluso en lugares como bancos, hospitales, centros educacionales y agencias de viajes, sean ejecutadas y controladas por sistemas de información con el objetivo de recolectar, procesar, almacenar y distribuir datos en apoyo al control y la toma de decisiones.

El desarrollo alcanzado en cuanto a la conectividad entre las computadoras, las posibilidades de transmisión de datos entre ellas, así como el uso de Internet e Intranet, han aportado numerosas ventajas contribuyendo a facilitar la gestión de la información, pero también trayendo consigo riesgos y amenazas por lo que la Seguridad Informática y sus estándares cobran una importancia vital en el uso de sistemas informáticos conectados a pequeñas o grandes redes.

Para el caso de las entidades estatales cubanas, el 1ro de agosto de 2009, fue aprobada por la Asamblea Nacional del Poder Popular (ANPP) la Ley No. 107 “De la Contraloría General de la República”, como resultado de un proceso de fortalecimiento de la Entidad Fiscalizadora Superior. La creación de la Contraloría General de la República (en lo adelante CGR) forma parte del proceso de institucionalización del país, así como el fomento de la gestión gubernamental. Gracias a la creación de este Órgano del Estado una vez más se eleva el rango de las funciones de control del Estado al tiempo que se eliminan dualidades innecesarias en las funciones de control (CONTRALORÍA 2009), (HERNÁNDEZ-DÍAZ *et al.* 2013).

En la sección segunda de la resolución antes mencionada, titulada Gestión y prevención de riesgos, el Artículo 11 plantea: “El componente Gestión y Prevención de Riesgos establece las bases para la identificación y análisis de los

riesgos que enfrentan los órganos, organismos, organizaciones y demás entidades para alcanzar sus objetivos. Una vez clasificados los riesgos en internos y externos, por procesos, actividades y operaciones, y evaluadas las principales vulnerabilidades, se determinan los objetivos de control y se conforma el Plan de Prevención de Riesgos para definir el modo en que habrán de gestionarse. Existen riesgos que están regulados por disposiciones legales de los organismos rectores, los que se gestionan según los modelos de administración previstos”(CONTRALORÍA 2011), (BLANCO 2012).

La Universidad de las Ciencias Informáticas (UCI) ha sido desde sus inicios la mayor protagonista de los logros informáticos del país. Debido a que en Cuba existen pocas empresas que se dediquen al desarrollo de software, la UCI ocupa un lugar importante en la producción de software a nivel nacional.

En la UCI existen diversos Centros de Desarrollo de Software, los cuales están integrados por diferentes Proyectos Productivos. Tal es el caso del Centro de Tecnologías de Gestión de Datos “DATEC”, el cual se especializa en la gestión de datos y el desarrollo de sistemas que manejan bases de datos.

En el centro se han realizado varios proyectos de gran relevancia entre los que se pueden mencionar: el sistema Elecciones y el sistema Generador dinámico de reportes entre otros. Pero a pesar de la experiencia en cuanto a desarrollo de sistemas y la calidad de los productos presentados por el centro, existen deficiencias en cuanto a la gestión y seguimiento de riesgos de los proyectos. Actualmente la gestión de riesgos en dicho centro se realiza de forma manual, pues a pesar de que existe una herramienta para la gestión de los mismos, esta no posee todas las funcionalidades requeridas, permitiendo solo realizar acciones correctivas trayendo como resultado que el proceso de gestión del diagnóstico y seguimiento de riesgos no se realice de manera eficiente. El hecho de que el proceso de gestión captura y seguimiento de riesgos se realice de forma manual, dificulta y demora el trabajo debido a que se necesita más tiempo para aplicar las acciones correctivas, pues las personas involucradas no son notificadas a tiempo y por tanto las decisiones no se toman oportunamente (CALZADA and LEÓN 2010), (MAR, O. *et al.* 2017), (MAR CORNELIO *et al.* 2016).

La situación descrita anteriormente acarrea otros problemas entre los que se pueden mencionar:

El aumento del margen de errores humanos debido a la mala manipulación de la información derivada del proceso de diagnóstico y seguimiento de riesgos.

Incertidumbre en la gestión de riesgos del centro afectándose el proceso de toma de decisiones.

Inexistencia de registros que posibiliten identificar deficiencias para su corrección oportuna.

Inexistencia de planes de mitigación y contingencia.

Inexistencia de acciones de mitigación y contingencia.

Materiales y métodos

La presente sesión está dedicado a las características del sistema. Se abordan temas relacionados con la propuesta de solución para responder a la situación problemática en cuestión, además quedarán definidos los requisitos no funcionales así como las principales funcionalidades del sistema. Las funcionalidades se describen mediante los casos de uso del sistema (MUÑOZ and RIVAS 2015), (HERNÁNDEZ *et al.* 2015). (CORNELIO *et al.* 2016).

Se lleva a cabo la realización del plan de entrega, donde se indican las historias de usuario que se crearán para cada versión de la aplicación propuesta, así como las fechas en las que se publicarán dichas versiones.

Descripción del Sistema Propuesto

El presente trabajo tiene como finalidad, implementar de manera ordenada y sistemática los procesos que dan solución a todo tipo de riesgo detectado, asociado a los diferentes proyectos que existen en el centro DATEC. La herramienta propuesta consiste en un sistema de gestión orientado a la web, el cual permite el diagnóstico y seguimiento de los riesgos. El sistema cuenta con varios módulos, los cuales desempeñan diferentes funciones (CHÁVEZ ORELLANA 2013), (MAR CORNELIO *et al.* 2012).

El sistema propuesto emplea el principio de seguridad informática control de acceso basado en roles (RBAC), además cuenta con un registro de los diferentes riesgos detectados en cada proyecto del centro, así como las diferentes acciones para la mitigación de los mismos. Mediante la realización de los planes de mitigación y contingencia, los integrantes de cada proyecto, cuentan con las herramientas necesarias para actuar de forma inmediata ante la detección de riesgos que puedan afectar al proyecto en curso. Por otra parte y con el objetivo de prevenir la ocurrencia de riesgos se lleva a cabo el monitoreo de los riesgos lo cual consiste en la revisión del correcto funcionamiento de los componentes que integran la administración de riesgos del centro mediante actividades de supervisión permanentes. A continuación se listan las principales funcionalidades brindadas por el sistema las cuales se detallan posteriormente en el presente documento (SERRANO *et al.* 2011).

Principales funcionalidades del sistema:

- Autenticar usuario.
- Gestionar usuario.
- Gestionar proyecto.
- Gestionar riesgo.

- Determinar exposición al riesgo.
- Gestionar plan de mitigación.
- Gestionar plan de contingencia
- Gestionar acciones de mitigación.
- Gestionar acciones de contingencia.

Modelo del Dominio

En un modelo de dominio se capturan los tipos más importantes de objetos que existen o los eventos que suceden en el entorno donde estará el sistema, trayendo consigo la ventaja de ayudar a usuarios, clientes y desarrolladores a utilizar un vocabulario común para entender el contexto en que se desarrollará el sistema.

La gestión de riesgos se encarga de definir los procesos que se manipulan en un negocio. Es necesario tener en cuenta que al no tener un cliente definido, no es posible establecer un patrón o similitud en cuanto a las características que se desarrollan en el entorno de los proyectos productivos del centro, para de esta forma manipular y controlar los riesgos asociados a cada uno de estos proyectos (*MAR-CORNELIO and CAEDENTEY-MORENO 2016*), (*MAR, OMAR et al. 2015*).

Con el objetivo de definir el flujo de eventos que se realiza, teniendo como punto de partida la detección de un riesgo en cada proyecto del centro DATEC y llegando hasta la elaboración de los planes de contingencia y mitigación asociados a dicho riesgo, se realiza la concepción del diagrama de dominio. Este modelo permite identificar las funcionalidades necesarias para que el sistema propuesto realice la gestión de riesgos definida por los proyectos de dicho centro. El modelo de dominio permitirá identificar los principales conceptos asociados al problema en cuestión y la relación existente entre ellos.

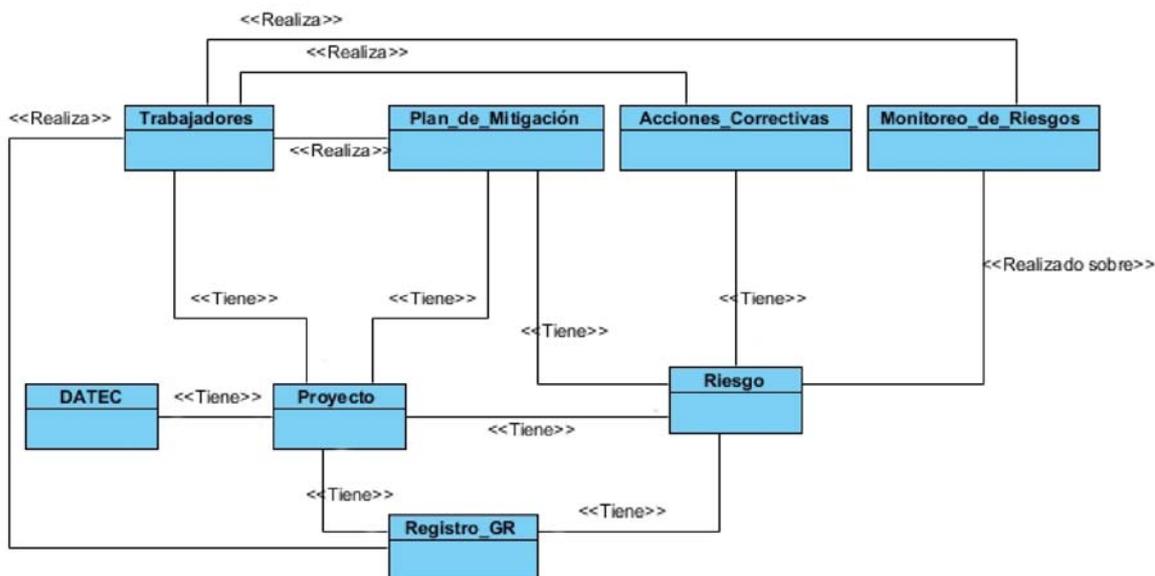


Figura 1: Diagrama del Modelo de Dominio creado a partir del problema planteado.

Descripción de los Objetos

A continuación se muestra la Tabla 1 con la definición de las entidades que interactúan en el negocio y los principales conceptos que se tratan en el problema que se analiza.

Tabla 1: Descripción de las entidades que interactúan en el negocio.

Entidad	Descripción
DATEC	Es el centro de desarrollo al cual se asocian diferentes proyectos productivos.
Proyecto	Representa a cada proyecto del centro DATEC. A cada proyecto se asocian uno o varios riesgos y a su vez representa el entorno en el que se va a aplicar la gestión de los riesgos.
Trabajadores	Representa la generalización de los trabajadores del centro DATEC, asociados a los diferentes proyectos.
Riesgo	Representa la probabilidad de que una amenaza que tendrá un impacto en los objetivos del proyecto se materialice.
Registro GR	Representa el registro de gestión de riesgos llevado en cada proyecto, consiste en un documento en el cual son registradas todas las características de cada uno de los riesgos detectados.
Acciones correctivas	Representa cada acción realizada encaminada a corregir los problemas

	causados por un riesgo.
Plan de mitigación	Representa el conjunto de acciones a realizar encaminadas a reducir la ocurrencia de un riesgo.
Monitoreo de Riesgos	Representa la revisión del funcionamiento de los componentes que integran la administración de riesgos del centro mediante actividades de supervisión permanentes, las cuales permiten calcular la exposición a los riesgos detectados, así como la calidad real de su control interno.

Especificación de los Requisitos del Sistema

Para que un esfuerzo de desarrollo de software tenga éxito, es esencial comprender perfectamente los requisitos del software. Independientemente de lo bien diseñado o codificado que esté un programa, si se ha analizado y especificado pobremente, decepcionará al usuario y desprestigiará al que lo ha desarrollado. La parte más difícil en la construcción de sistemas software es decidir precisamente qué construir. Ninguna otra parte del trabajo conceptual es tan ardua como establecer los requisitos técnicos detallados, incluyendo todas las interfaces con humanos, máquinas y otros sistemas.

La calidad con que se realice la captura de los requisitos va a influenciar en todo el proceso de desarrollo del software repercutiendo en el resto de las fases del mismo. Una definición eficiente de los requisitos permite mostrar un nivel de disciplina en el proceso de desarrollo, dar un mejor soporte a la Gestión de Cambios y ganar una mayor eficiencia en las pruebas reduciendo el riesgo, mejorando la calidad y permitiendo la automatización. Además contribuye a tomar mejores decisiones de diseño y de arquitectura. También le permite al equipo de desarrollo reducir los problemas de mantenimiento.

Requisitos Funcionales

Los requisitos funcionales enuncian la definición de los servicios que un sistema debe proveer o su comportamiento ante las diferentes entradas y situaciones que le sean presentadas (PRESSMAN 1998). A continuación se muestran los requisitos funcionales del sistema.

Requisitos Funcionales

1. Autenticar usuario.
 - 1.1. Iniciar sesión.
 - 1.2. Cerrar sesión.
2. Gestionar usuario.
 - 2.1. Insertar usuario.
 - 2.2. Asignar permisos.
 - 2.3. Actualizar usuario

- 2.4. Eliminar usuario.
- 3. Gestionar Departamento
 - 3.1. Insertar departamento.
 - 3.2. Modificar departamento.
 - 3.3. Obtener lista de departamentos.
 - 3.4. Eliminar departamentos.
- 4. Gestionar proyecto.
 - 4.1. Insertar proyecto.
 - 4.2. Modificar un proyecto.
 - 4.3. Obtener lista de proyectos.
 - 4.4. Eliminar proyecto.
- 5. Gestionar riesgo.
 - 5.1. Insertar riesgo.
 - 5.2. Actualizar riesgo.
 - 5.3. Obtener lista de riesgos.
 - 5.4. Eliminar riesgo.
- 6. Determinar exposición al riesgo.
- 7 Gestionar plan de mitigación de riesgos.
 - 7.1. Insertar plan de mitigación de riesgos.
 - 7.2. Modificar plan de mitigación de riesgos.
 - 7.3. Actualizar plan de mitigación de riesgos.
 - 7.4. Eliminar plan de mitigación de riesgos.
- 8. Gestionar plan de contingencia.
 - 8.1. Insertar plan de mitigación de riesgos.
 - 8.2. Modificar plan de mitigación de riesgos.
 - 8.3. Actualizar plan de mitigación de riesgos.
 - 8.4. Eliminar plan de mitigación de riesgos.
- 9. Gestionar acciones de mitigación.
 - 9.1. Insertar acción de mitigación.
 - 9.2. Actualizar acción de mitigación.
 - 9.3. Obtener listado de acciones de mitigación.
 - 9.4. Eliminar acción de mitigación.
- 10. Gestionar acciones de contingencia.

- 10.1. Insertar acción de contingencia.
- 10.2. Actualizar acción de contingencia.
- 10.3. Obtener listado de acciones de contingencia.
- 10.4. Eliminar acción de contingencia.

2.5.2 Requisitos no Funcionales

Los RNF especifican propiedades del sistema que el sistema debe cumplir, como restricciones del entorno o de la implementación, rendimiento, dependencia de la plataforma, facilidad de mantenimiento, extensibilidad, fiabilidad. Tienen que ver con las características del sistema, que incluye también interfaces de usuario (PÉREZ QUINTERO 2008).

Para un correcto funcionamiento el sistema debe tener como características principales para su funcionamiento los siguientes requisitos no funcionales:

Usabilidad: El sistema puede ser utilizado por cualquier persona que tenga al menos conocimientos básicos en el manejo de la computadora, navegación y exploración de los sitios Web en sentido general, las operaciones se realizan con bajo nivel de complejidad.

Disponibilidad: El sistema garantiza sus servicios los 5 días hábiles de la semana, mientras la infraestructura (servicio eléctrico, de redes, etc.) del centro lo permita.

Seguridad: Se establecen niveles de acceso, de esta forma se garantiza que la aplicación será utilizada correctamente por cada usuario según sus respectivos niveles de acceso.

Integridad: Se debe tratar el manejo de la información de forma tal, que la información no sea modificada por personal ajeno. Esto evitará alteraciones en los resultados planteados en la documentación.

Interfaz: El diseño de la interfaz visual debe ser amigable e intuitiva para los usuarios que interactúan con la aplicación, de forma tal que permita el fácil entendimiento de las funcionalidades que brinda, además de poseer colores amigables y refrescantes para una mejor interacción entre el usuario y la aplicación.

El diseño de la interfaz permitirá mostrar mensajes para la guía de usuarios en caso de errores en entradas inválidas de los datos o de confirmación de realización de actividades.

Cliente:

Hardware:

Se necesita como requerimiento mínimo una Computadora Personal (*Personal Computer*) que posea una tarjeta de red de 10 MB o superior.

Software:

Necesita un sistema operativo y un navegador Web.

Servidor:

Hardware:

Se necesita como requerimiento mínimo una Computadora Personal (*Personal Computer*)

Memoria RAM de 1GB o superior.

HDD de 80 GB o superior.

Tarjeta de red de 100 MB o superior.

Software:

Necesita un Sistema Operativo.

Servidor Web Apache 2.2.4 o superior.

Servidor de Bases de Datos PostgreSQL 9.1 o superior.

PHP 5.2.3.

Rendimiento: La disponibilidad de trabajo en red contra el servidor es constante. Se garantiza que la respuesta a solicitudes de los usuarios, sea en un período de tiempo breve para evitar la acumulación de trabajo por parte de los responsables. El sistema deberá ser lo más estable y confiable posible.

Restricciones en el diseño y la implementación: Es un sistema Web desarrollada con la tecnología Groovyy base de datos en *PostgreSQL*.

Resultados y discusión

Patrón de Casos de Uso (CRUD)

Los patrones de casos de uso son comportamientos que deben existir en el sistema, ayuda a describir qué es lo que el sistema debe hacer, es decir, describe el uso del sistema y cómo este interactúa con los usuarios. Estos son utilizados generalmente como plantillas que especifican como deberían ser estructurados y organizados los casos de uso y capturan mejores prácticas para modelar casos de uso.

Los patrones de casos de uso brindan los siguientes beneficios:

- Aumentar la productividad.
- Reutilizar elementos existentes.
- Evitar el re trabajo por errores.
- No invertir tiempo en resolver problemas ya resueltos.
- Aplicarla teoría al trabajo práctico.
- Habilitar las herramientas de soporte para modelar el desarrollo.
- Durante el diseño de los casos de uso del sistema se utilizó el patrón CRUD (acrónimo de Crear, Obtener, Actualizar y Borrar del original en inglés: *Create, Read, Update and Delete*).

Diagrama de Casos de Uso del Sistema

Gracias a las facilidades que ofrece el UML, se procede a capturar los requisitos funcionales del sistema y a representar a los mismos mediante un diagrama de casos de uso (DCU).

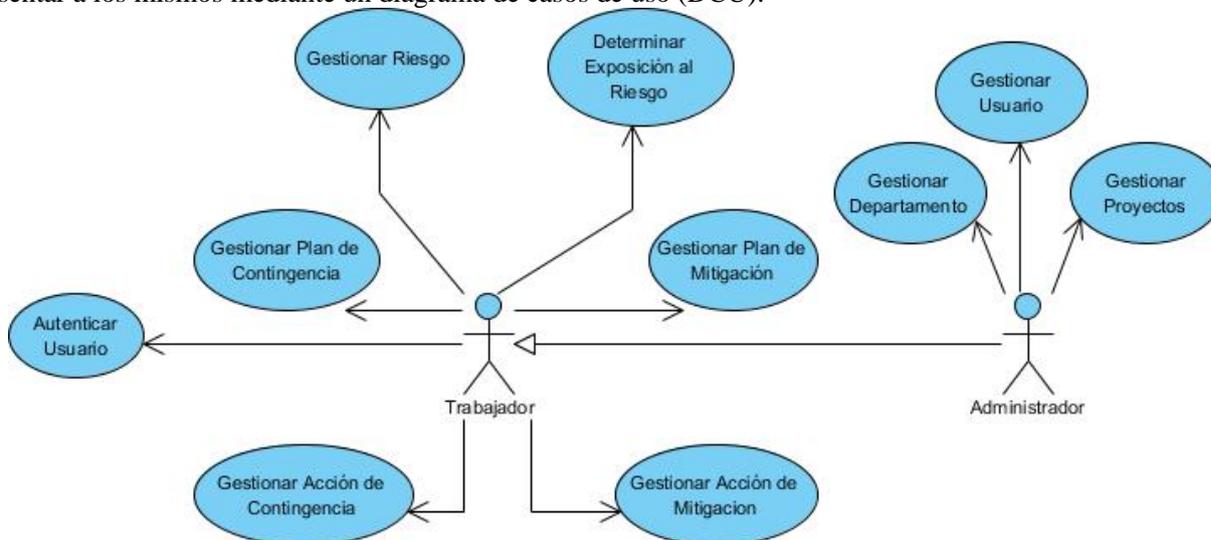


Figura 2: Diagrama de Casos de Uso del Sistema.

Descripciones de los Casos de Uso del Sistema

A continuación se muestra la descripción de los casos de uso del sistema (CUS) Autenticar Usuario y Gestionar Usuario.

Tabla 2. CU Autenticar Usuario.

Caso de Uso	Autenticar Usuario	
Actores	Usuario	
Resumen	Se inicia cuando el usuario ingresa sus credenciales para acceder al sistema. Los datos serán verificados a través del servicio Web de autenticación de la UCI; de ser correctos, el acceso se habilita al sistema en dependencia de los permisos que tenga habilitado su rol. El caso de uso termina cuando el usuario accede al sistema.	
Precondiciones		
Referencias	RF 1	
Prioridad	Alto	
Flujo Normal de Eventos		
Acción del Actor	Respuesta del Sistema	

<p>1. El caso de uso inicia cuando los usuarios acceden al sistema.</p> <p>3. El usuario introduce sus credenciales.</p>	<p>2. El sistema brinda la posibilidad de introducir usuario y contraseña.</p> <p>4. El sistema verifica que los campos del formulario no estén vacíos.</p> <p>5. Se verifica que el usuario exista en la BD y que la contraseña especificada sea correcta.</p> <p>6. Si los datos son correctos, la aplicación muestra la interfaz principal, donde aparecen las funcionalidades según el rol que tenga.</p>
Flujos Alternos	
Acción del Actor	Respuesta del Sistema
	<p>4.1. De existir un campo vacío el sistema muestra un mensaje de error y regresa a la actividad 1 del flujo normal de los eventos.</p> <p>5.1. Si los datos no son correctos, la aplicación muestra un mensaje de error, y le permite al usuario volver a introducir las credenciales.</p>
Pos condiciones	El usuario queda autenticado.

Tabla 1. CU Gestionar Usuario.

Caso de Uso	Gestionar Usuario
Actores	Administrador
Resumen	El caso de uso inicia cuando el administrador selecciona en el menú la opción Gestionar Usuario. El sistema muestra las opciones de agregar, buscar, modificar y eliminar usuario. El administrador realiza las operaciones que desee y de esta forma se gestionan los usuarios. El caso de uso termina.
Precondiciones	El administrador tiene que estar autenticado.
Referencias	RF 2
Prioridad	Alto
Flujo Normal de Eventos	
Acción del Actor	Respuesta del Sistema

1. El administrador selecciona la opción gestionar usuario	2. El sistema muestra el listado de usuarios existentes brinda la posibilidad de Agregar, Buscar, Modificar o Eliminar usuario.
Sección “Agregar Usuario”	
3.El administrador Selecciona la opción agregar usuario.	4.El sistema muestra los datos correspondientes: <ul style="list-style-type: none"> • nombre de usuario • rol • proyecto productivo al que pertenece. Y brinda la opción:“ guardar usuario “para guardar los datos del nuevo usuario o Cancelar: ver Alternativa 1: “Cancelar Operación ”
5. El administrador introduce los datos y selecciona la opción guardar.	6. Valida los datos, si hay campos incompletos: ver Alternativa 2: “Hay campos vacíos”, si hay campos incorrectos: ver Alternativa 3: “Hay campos incorrectos”. 7. El caso de uso termina.
Flujos Alternos “Cancelar Operación”	
Acción del Actor	Respuesta del Sistema
1. Selecciona la opción de Cancelar operación.	2. Regresa a la vista anterior. 3. El caso de uso termina.
Flujos Alternos “Hay campos vacíos”	
Acción del Actor	Respuesta del Sistema
	1. Muestra un indicador al lado de los campos vacíos.
Flujos Alternos “Hay campos incorrectos”	
Acción del Actor	Respuesta del Sistema
	1.Muestra el mensaje de error “Existen campos incorrectos” 2. Muestra un indicador sobre los campos incorrectos.
Sección “Buscar Usuario”	
Acción del Actor	Respuesta del Sistema
1. El Administrador selecciona la opción Buscar Usuario.	2. El sistema muestra los datos correspondientes: <ul style="list-style-type: none"> • nombre de usuario • rol

3. El administrador introduce los criterios de búsquedas.	<ul style="list-style-type: none"> • proyecto productivo al que pertenece. 4. El sistema muestra el resultado de acuerdo con los criterios de búsquedas. 5. El caso de uso termina.
Sección “Modificar Usuario”	
Acción del Actor	Respuesta del Sistema
1. El Administrador selecciona el campo que desea modificar haciendo doble clic sobre él.	2. Muestra un cuadro de texto para introducir el nuevo valor que tendrá el usuario en ese campo. 3. El sistema envía el nuevo valor para ser procesado. 4. El caso de uso termina.
Sección “Eliminar Usuario”	
Acción del Actor	Respuesta del Sistema
1. El Administrador selecciona un usuario de la lista y luego la opción Eliminar Usuario. 3. En el mensaje Presiona el botón Sí.	2. Muestra un mensaje de confirmación de eliminación. 4. Envía la información del usuario y se elimina. 5. El caso de uso termina.
Flujos Alternos: “Cancelar operación”	
Acción del Actor	Respuesta del Sistema
1. En el mensaje Presiona el botón No.	2. Regresa a la vista anterior. 3. El caso de uso termina.
Pos condiciones	Se gestionaron los datos de los usuarios de manera correcta.

Conclusiones

- Como resultado del estudio realizado, queda definida *OpenUp* como la metodología a utilizar, se modelaron los artefactos que genera la misma entre los que se encuentran: modelo de dominio, actores y casos de uso del sistema, descripciones de los mismos, así como el levantamiento de los requisitos funcionales y no funcionales.
- Se identificaron los casos de uso del sistema en correspondencia con las funcionalidades recogidas en los requisitos funcionales.

- Se utilizó el patrón CRUD para estructurar y organizar los casos de uso, lo que definió el diagrama de casos de uso del sistema y la descripción detallada de cada uno.
- Luego de quedar definido el diseño del sistema y las relaciones entre sus elementos, es posible dar comienzo el proceso de implementación del sistema propuesto en la presente investigación.

Referencias

- BLANCO, B. EVALUACIÓN DE RIESGOS DE OPERACIÓN CON MATEMÁTICAS BORROSAS *Revista Caribena de Ciencias Sociales*, 2012, 10.
- CALZADA, R. and J. LEÓN Características de la gestión de riesgos en las empresas cubanas *RCCI*, 2010, Vol.4(No3).
- CONTRALORÍA. *Ley de la Contraloría General de la República*. Habana, 2009. Ley_No.107/09.
- . *Normas del Sistema de Control Interno*. Habana, 2011. Resolución No. 60/11.
- CORNELIO, O. M.; I. S. CHING, *et al.* *Herramienta para la simulación de sistemas dinámicos integrado al sistema de laboratorios virtuales ya distancia*. Anais do Encontro Virtual de Documentação em Software Livre e Congresso Internacional de Linguagem e Tecnologia Online, 2016. p.
- CHÁVEZ ORELLANA, E. E. A. M. R., WILLIAMS FREDY Propuesta de un sistema de control interno que contribuya a la maximización de los recursos y a la toma de decisiones financieras y tributarias en la Estación de Servicio Jefe dedicada a la compra y venta de combustibles y lubricantes en la ciudad de San Miguel para el año 2013. *Tesis Bachelor, Universidad de El Salvador*, 2013.
- HERNÁNDEZ-DÍAZ, N.; M. YELANDY-LEYVA, *et al.* Modelos causales para la Gestión de Riesgos *Revista Cubana de Ciencias Informáticas*, 2013, 7(4): 58-74.
- HERNÁNDEZ, L.; S. KHARUF, *et al.* *Sistema de fotogrametría de bajo costo para el Mapeado de agro-ecosistemas, basadas en Vehículos Aéreos No Tripulado (UAV)*, [En línea]. 2015. [III Congreso de Percepción Remota y Sistemas de Información Espacial]. Disponible en: <http://www.researchgate.net/publication/282249626>
- MAR-CORNELIO, O. and N. CAEDENTEY-MORENO Monitoreo energético en los laboratorios de la Universidad de las Ciencias Informáticas *Ingeniería Industrial*, 2016, 37(2): 190-199.
- MAR CORNELIO, O.; N. CARDENTEY MORENO, *et al.* Aplicación informática para el control energético de la tecnología utilizando herramienta de monitoreo de red Nmap *Revista Cubana de Ciencias Informáticas*, 2012, 6(2).
- MAR CORNELIO, O.; J. GULÍN GONZÁLEZ, *et al.* Sistema de Laboratorios a Distancia para la práctica de Control Automático *Revista Cubana de Ciencias Informáticas*, 2016, 10(4): 171-183.
- MAR, O.; I. SANTANA, *et al.* Competency assessment model for a virtual laboratory system and distance using fuzzy cognitive map *Revista Investigación Operacional*, 2017, 38(2): 170-178.
- MAR, O.; Y. Z. VÉLIZ, *et al.* Motor de inferencia decisional en sistema informático para la evaluación del desempeño *Revista Cubana de Ciencias Informáticas*, 2015, 9(4): 16-29.
- MUÑOZ, M. and L. RIVAS Estado actual de equipos de respuesta a incidentes de seguridad informática *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, 2015: 1-15.
- PÉREZ QUINTERO, L. Y. V. G., CARLOS MANUEL. *Estrategia para el desarrollo de requisitos no funcionales de software en proyectos productivos de la Universidad de las Ciencias Informáticas*. La Habana, 2008. p.
- PRESSMAN, R. S. *Ingeniería de Software*. New York, EEUU: Mc Grow-hil, 1998. p. ISBN: 9786071503145
- SERRANO, R.; G. C. JESÚS, *et al.* Una visión desde Sistemas Complejos para la evaluación Multicriterio- Multiobjetivo. *Gestión Turística*, 2011, N° 16. ISSN 0717 - 1811