

Tipo de artículo: Artículo original  
Temática: Desarrollo de aplicaciones informáticas  
Recibido: 10/05/16 | Aceptado: 14/06/16

## Sistema para el diagnóstico y seguimiento de riesgos en centros de producción de software

### *System for the diagnosis and monitoring of risks in software production centers*

Bárbara Bron Fonseca<sup>1\*</sup>, Maiker Rodríguez Troche<sup>2</sup>

<sup>1</sup> Empresa de Tecnologías de la Información para la Defensa. [bbron@xetid.cu](mailto:bbron@xetid.cu)

<sup>2</sup> Universidad de las Ciencias Informáticas. [maiker@uci.cu](mailto:maiker@uci.cu)

\* Autor para correspondencia: [bbron@xetid.cu](mailto:bbron@xetid.cu)

---

#### Resumen

El diagnóstico y seguimiento de riesgo juega un papel importante en la forma organizativa de las instituciones cubanas. Por tal motivo, para garantizar una correcta implementación de este proceso, la Contraloría General de la República de Cuba, ha definido las pautas para la gestión de riesgos. En la Universidad de las Ciencias Informáticas se gestiona mediante documentos en los que se reflejan los elementos definidos. Sin embargo, la gestión de la información resulta compleja cuando se quiere comparar su implementación en diferentes momentos y no es posible tomar decisiones en tiempo real sobre determinado comportamiento. La presente investigación propone una herramienta informática para la gestión y prevención de riesgos, regida por las directivas establecidas en la Resolución No. 60/11 de la Contraloría. El sistema propuesto implementa un conjunto de funcionalidades que permite crear, editar y eliminar las estructuras, el diagnóstico de riesgos, los planes de prevención y el control del cambio. El sistema brinda además un conjunto de reportes que permite la toma de decisiones en tiempo real a los principales directivos sobre los comportamientos y tendencias identificadas.

**Palabras clave:** *Gestión y diagnóstico de riesgos; contingencia; mitigación; sistema informático*

#### Abstract

*The diagnosis and monitoring of risk plays an important role in the organizational form of the Cuban institutions. For that reason, to ensure proper implementation of this process, the Comptroller General of the Republic of Cuba has*

*defined the guidelines for risk management. At the University of Informatics Science, it is managed by documents that reflect the defined elements. However, the information management is complex when you want to compare their implementation at different times and it cannot make decisions in real time, on a particular behavior. This research proposes a software tool for management and risk prevention governed by the guidelines established in Resolution No. 60/11 of the Comptroller. The proposed system implements a set of features that allows you to create, edit and delete structures, diagnosis of risks, prevention plans and change control. The system also provides a set of reports that allows decision making in real time to top management on behaviors and trends identified time.*

**Keywords:** *Risk management and diagnosis; contingency; mitigation; computer system*

---

## **Introducción**

Las Tecnologías de la Información y las Comunicaciones (TICs), se han introducido de forma masiva en los procesos de la sociedad, redefiniendo los paradigmas tradicionales de gestionar y priorizar información. En medio del desarrollo tecnológico, el estado cubano realiza numerosos esfuerzos sentando las bases necesarias para garantizar la informatización de la sociedad cubana, ejemplo de esto lo representa la Universidad de las Ciencias Informáticas (UCI), creada con fines docentes – productivos.

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, 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 (CALZADA and LEÓN 2010).

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. La vigencia 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 2009b), (CONTRALORÍA 2009a).

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” (BLANCO 2012).

La Universidad de las Ciencias Informáticas 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.

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.

Según la práctica cotidiana del autor y la utilización de métodos empíricos como encuestas a directivos y guía de observaciones se pudo determinar las siguientes insatisfacciones:

- 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.

- Con la herramienta actual el proceso es lento y engorroso para el usuario.
- Los riesgos detectados solo pueden publicarlos los especialistas.

Del análisis sobre la situación anterior se plantea como objetivo a Desarrollar una herramienta que contribuya a la gestión del diagnóstico y seguimiento de riesgo en el centro DATEC de la Universidad de las Ciencias Informáticas.

## **Materiales y métodos**

En la presente sesión se describe el proceso de gestión y diagnóstico de riesgos, se describen las características del sistema y los principales elementos que facilitan la comprensión de la propuesta. 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. 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.

El Sistema para el diagnóstico y seguimiento de riesgo en su versión 1.0, está orientado a soportar la gestión sobre el proceso de gestión de riesgos en los centros productores de software. Realiza tres actividades básicas: entrada, almacenamiento y salida de información como se describe a continuación:

- **Entrada de información:** Proceso mediante el cual el sistema informático toma los datos que requiere para procesar la información (LEMONS and CASTELLANO 2012). En la propuesta, existen datos gestionados manualmente que son aquellas que se proporcionan de forma directa por el usuario como es la estructura organizativa del centro, los riesgos identificados, el plan de mitigación y el plan de contingencia, etc.; mientras que otros datos de forma automáticas son informaciones que provienen o son tomados de otros sistemas o módulos como datos de personas, áreas, etc.
- **Almacenamiento de información:** El almacenamiento es una de las actividades o capacidades más importantes que garantizan los sistemas informáticos, ya que a través de esta propiedad pueden recordar la información guardada en la sección o proceso anterior. Para el sistema propuesto las informaciones derivadas del proceso de entrada de información son almacenadas en una base de datos (ABURAWI 2015).
- **Salida de información:** La salida es la capacidad de un sistema informático para visualizar la información almacenada. Las unidades típicas de salida son las impresoras, interfaces, cintas magnéticas entre otros (GARAY 2015), (GONZÁLEZ and MAR 2015). Para el sistema propuesto, existe un módulo destinado a la

gestión de reportes, mediante dicha interfaz es posible visualizar las informaciones procesadas por el sistema y brindar los elementos necesarios para la toma de decisiones así como la exportación de dichos reportes en el formato de almacenamiento deseado. La Fig. 1 representa un esquema general de la propuesta donde intervienen las actividades antes expuestas.



Figura 1: Esquema general de la propuesta.

En el sistema pueden interactuar tres actores “Trabajadores”, ”Usuario”, ”Administrador”, que representan los roles que pueden cumplir los usuarios, posibilitándose los nivel de interacción con las funcionalidades implementadas como se muestra en la Tabla 1:

Tabla 1. Actores del sistema.

Actores	Descripción
Administrador	Encargado de la gestión de usuarios, de activos fijos, áreas, centros de costo y organizaciones.
Trabajadores	Tienen permisos especiales en el sistema, poseen el rol de “usuario avanzado”.
Usuario	Solamente puede visualizar los datos publicados en el sistema.

La Fig. 2 muestra un Diagrama de Casos de Uso donde son representados los actores con las funcionalidades o requisitos que ofrece el sistema de gestión de riesgos (BAQUERO *et al.* 2016):

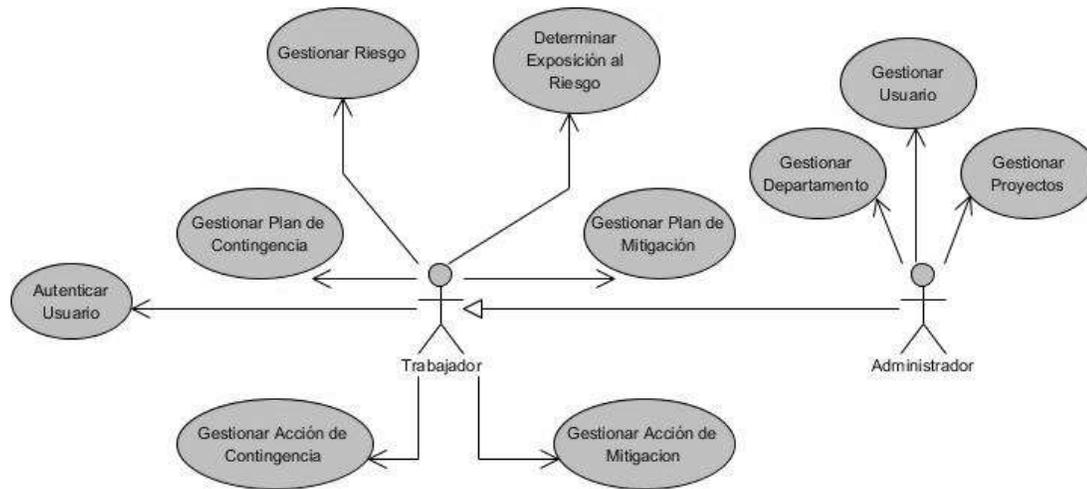


Figura 2: Diagrama de Casos de Uso del Sistema.

## Tecnologías y herramientas a utilizar

Para el desarrollo del sistema se utilizaron las siguientes tecnologías y herramientas cumpliendo con el criterio de selección de tributar a la soberanía tecnológica sobre plataforma libre:

Servidor web Apache 2.0: Además de las ventajas de ser OpenSource, gratis y de fácil adquisición, Apache es el servidor web más empleado en los centro de desarrollo de la UCI por los que los trabajadores están familiarizados con su uso (SCRIBID 2014).

Lenguaje de programación Groovy 2.0.7: Con el objetivo de aprovechar todas las ventajas de la tecnología Java y se agregan otras como: el tipado dinámico y estático, el soporte nativo a listas, mapas, expresiones regulares. Además, Groovy es un lenguaje dinámico, que disminuye la cantidad de líneas de código respecto al lenguaje Java e incluye muchas nuevas funcionalidades en su GDK (Análogo al JDK de Java) (MUMBAI 2009).

Gestor de Base de Datos PostgreSQL 8.3: Es un sistema multiplataforma, lo que posibilita el constante perfeccionamiento de sus funcionalidades y está publicado al amparo de una licencia BSD la cual pertenece a las licencias de software libre (GARZÓN 2010).

Framework Grails: Mediante la integración de dicho framework con el lenguaje de programación Groovy, permite a los desarrolladores Web la construcción de sistemas robustos, desarrollados en un entorno coherente y fiable. Además posibilita el empleo de la reutilización de código y la obtención de sistemas modulares desarrollados bajo el patrón Modelo Vista Controlador (MVC).

IDE de desarrollo IntelliJ IDEA: Posee gran compatibilidad con el framework de desarrollo y el lenguaje de programación seleccionados (CHARTE 2009), (MAR *et al.* 2013).

La Fig.3 muestra a través del diagrama de despliegue una representación de los nodos unidos por conexiones de comunicación que evidencian las relaciones físicas entre los componentes del sistema propuesto.

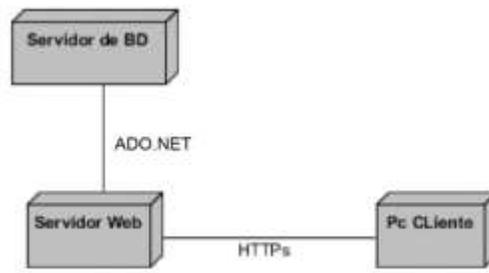


Figura 3: Diagrama de Despliegue.

Descripción de los nodos físicos del sistema

- PC Cliente: El nodo representa una PC cliente desde la cual se podrá acceder al sistema por medio de un navegador Web e interactuar con todas las funcionalidades que este brinda.
- Servidor Web: El nodo representa el servidor Web donde estará alojado el sistema así como los componentes almacenados en el mismo.
- Servidor de Base de Datos: El nodo representa el servidor de Base de Datos PostgreSQL en el que estará alojada la base de datos del sistema.

## Resultados y discusión

### Sistema informático

Las pantallas de sistema son imágenes tomadas durante su funcionamiento (MAR *et al.* 2016). Estas imágenes muestran parte de los resultados obtenidos con el desarrollo de esta investigación y permite comprobar el funcionamiento del sistema propuesto por el autor.

Sistema de gestión de riesgos, vista Autenticación de usuario:

La Fig. 4 muestra la vista Autenticación de usuario, la autenticación esta implementada a partir de la clase LDAP de Java que permite la autenticación con el LDAP de la UCI. Las cuentas pueden ser creadas sobre la marcha cuando un usuario se encuentra en el directorio de esta institución.



Figura 4: Autenticación de usuario.

Sistema de gestión de riesgos, vista Plan de Contingencia:

En la Fig. 5 se muestran los Planes de Contingencia de un proyecto de prueba. El sistema permite editar el plan existente, eliminarlo y exportar el documento en formato pdf.

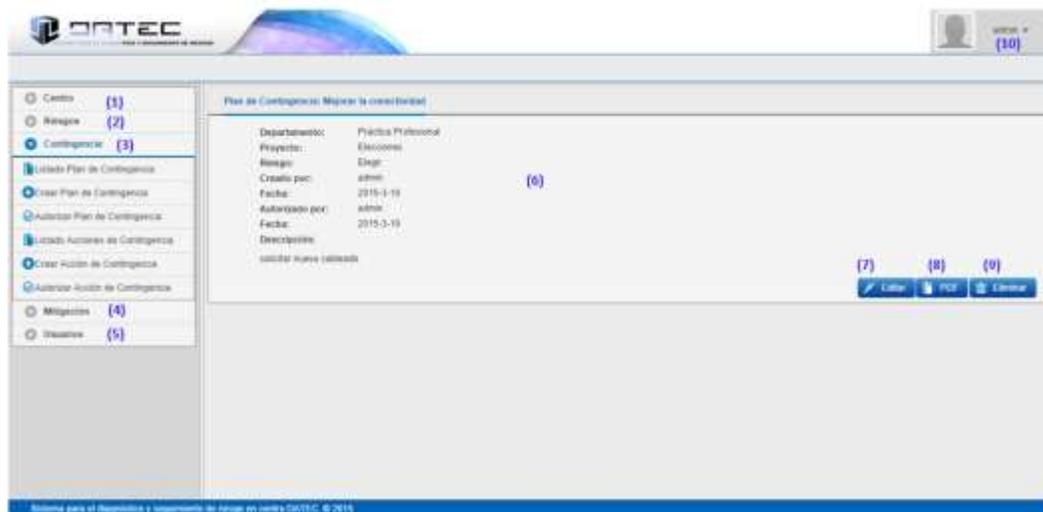


Figura 5: Sistema de gestión de riesgos, vista Plan de Contingencia.

A continuación se realiza una descripción de las principales funcionalidades presentadas en la Figura 5.

- (1) Centro: Permite gestionar la estructura organizativa del Centro Productivo así como la creación de los proyectos en ejecución de dicho centro.
- (2) Riesgos: Permite Crear, Editar y Eliminar los riesgos que son identificados, estos riesgos solo se crean una vez en el sistema, en lo adelante se le da seguimiento a partir del impacto y la criticidad que hayan tenido en el proyecto en que fueron identificados y registrados.

- (3) Contingencia: Permite Crear un Plan de Contingencia, Editarlo, eliminarlo autorizarlo y exportarlo como PDF para su almacenamiento. Permite además crear una Acción de contingencia y autorizar dicha acción.
- (4) Mitigación: Permite Crear un Plan de Mitigación, Editarlo, eliminarlo autorizarlo y exportarlo como PDF para su almacenamiento.
- (5) Usuarios: Permite la gestión de usuarios del sistema así como la asignación del rol que tendrán dentro del mismo.
- (6) Panel de visualización: Área donde se muestran los detalles de las configuraciones realizadas y donde se permite la edición de las mismas. Se describe en que consiste el plan.
- (7) Editar: Permite editar la configuración previamente realizada. Esta puede ser la creación de un usuario del sistema, de un plan de contingencia y mitigación etc.
- (8) PDF: Permite exportar en formato PDF las configuraciones realizadas previamente para su posterior consulta y almacenamiento.
- (9) Eliminar: Permite eliminar las configuraciones realizadas previamente.
- (10) Sesión de usuario: Muestra el usuario registrado en el sistema y permite cerrar la sesión para salir.

### Pruebas de seguridad realizadas

Las pruebas de seguridad tienen como objetivo hacer un análisis con el fin de encontrar vulnerabilidades en el sistema, o sea fallos de seguridad tanto en el diseño como en la implementación de la aplicación. Además buscan medir la confidencialidad, integridad y disponibilidad de los datos. Las pruebas de seguridad del sistema se realizaron con la herramienta Acunetix en su versión 8.0. A continuación se muestran los resultados de las 3 iteraciones de pruebas realizadas, las imágenes mostradas fueron tomadas de la propia herramienta utilizada.



Figura 6: Primera iteración de pruebas.

Después de realizar la primera iteración se encuentran un total de 50 alertas como muestra la figura 6. Luego de corregidas, se realiza la segunda iteración cuyos resultados se muestran en la Figura7.



Figura 7: Segunda iteración de pruebas.

Luego de realizada la segunda iteración la herramienta arroja 8 no conformidades como muestra la figura 7, las cuales son corregidas para posteriormente realizar una tercera iteración la cual arroja los resultados mostrados en la Figura 8.



Figura 8: Tercera iteración de pruebas.

## Conclusiones

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.

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.

Después de la realización de las pruebas se comprobó que el sistema posee una adecuada seguridad para ser desplegado en un ambiente real.

## Referencias

- ABURAWI, A. Emergency Communication *Bachelor Programme in Computer and Telecom Engineering: Technology and Management and Service Science*, 2015.
- BAQUERO, L.; D. MENDOZA, *et al.* Extensión de la herramienta Visual Paradigm for UML para la evaluación y corrección de Diagramas de Casos de Uso *Publicaciones*, 2016, Vol.9(N0.4): 1-14.
- 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. *Bases para la constitución de la contraloría general*, [En línea]. 2009a. [Disponible en: <http://www.contraloria.cu/>]
- . *Contraloría General de la República de Cuba*, [En línea]. 2009b. [Disponible en: [http://www.contraloria.cu/index.php?option=com\\_content&view=article&id=84&Itemid=22](http://www.contraloria.cu/index.php?option=com_content&view=article&id=84&Itemid=22)]
- CHARTE, F. *Ensamblador para Dos, Linux y Windows*. 2009. 701 p. ISBN 9788441514829. 2009
- GARAY, M. Interfaces Inteligentes en el aprendizaje de la Modelación *Ingeniería Industrial*, 2015, Vol. XXXVI(No. 2): 187-201.
- GARZÓN, T. SISTEMAS GESTORES DE BASES DE DATOS *Innovación y Experiencia Educativa*, 2010, Vol.30.
- GONZÁLEZ, J. and O. MAR Algoritmo de clasificación genética para la generación de reglas de clasificación *Publicaciones*, 2015, Vol.8(No.1): 1-14.
- LE MOS, J. and G. CASTELLANO Integrated Management of Health Services in the Areas of Magdalene College *Union V Scientia et Technica*, 2012, Año XVII(No. 50).

MAR, O.; L. ARGOTA, *et al.* Módulo para la evaluación de competencias a través de un Sistema de Laboratorios a Distancias *RCCI*, 2016, Vol.10(No.2): 132-147.

MAR, O.; Y. PÉREZ, *et al.* Entorno Integral de desarrollo para lenguaje en ensamblador basado en los servicios de Linux *Sociedad de la Información*, 2013, 40.

MUMBAI, B.-. Grails 1.1 Web Application Development *Packt*, 2009.

SCRIBID. *Manual del usuario de PostgreSQL*, 2014. [Disponible en: <http://es.scribd.com/doc/5703210/Manual-del-usuario-de-PostgreSQL>].