GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA NORMA ISO/IEC 27005 DE 2011, PROPONIENDO UNA ADAPTACIÓN DE LA METODOLOGÍA OCTAVE-S. CASO DE ESTUDIO: PROCESO DE INSCRIPCIONES Y ADMISIONES EN LA DIVISIÓN DE ADMISIÓN REGISTRO Y CONTROL ACADÉMICO (DARCA) DE LA UNIVERSIDAD DEL CAUCA.

Diego Espinosa T.
Universidad del Cauca
despinosa@unicauca.edu.co

Juan Martínez P.
Universidad del Cauca
juanpmartinez@unicauca.edu.co

Siler Amador D.
Universidad del Cauca
samador@unicauca.edu.co

(Tipo de Artículo: Revisión. Recibido el 13/11/2014. Aprobado el 02/12/2014)

RESUMEN
Este documento presenta la aplicación de la metodología OCTAVE-s para el análisis y gestión del riesgo en la seguridad de la información, adaptada al proceso Inscripciones y Admisiones, en la División de Admisión, Registro y Control Académico (DARCA) de la Universidad del Cauca; siguiendo las directrices de la norma ISO/IEC 27005:2011. Además se incluye la estructura del proceso, y el procedimiento escogido como caso de estudio para aplicar el tratamiento del riesgo. Finalmente, se muestran los resultados obtenidos y las conclusiones de la gestión del riesgo con la metodología adaptada.

Palabras Clave. Activo, amenaza, impacto, ISO/IEC 27005, Metodología de las Elipses, Metodología Octave-s, riesgo, seguridad de la información.

MANAGING RISK IN INFORMATION SECURITY BASED ON ISO / IEC STANDARD 27005, 2011, PROPOSING AN ADAPTATION OF OCTAVE-S METHODOLOGY. CASE STUDY: INSCRIPTION AND ADMISSION PROCESS AT THE DIVISION OF ADMISSION, REGISTERING AND ACADEMIC CONTROL (DARCA) AT THE UNIVERSITY OF CAUCA

ABSTRACT
This paper presents the application of OCTAVE-s methodology for the analysis and risk management in information security adapted to Inscription and Admission Process at the Division of Admission, Registering and Academic Control (DARCA) at the University of Cauca; following the guidelines of ISO / IEC 27005: 2011 standard. Additionally the structure of the process is included, and the method chosen as a case study for implementing risk treatment. Finally, the obtained results and conclusions of risk management with the adapted methodology are presented.

Keywords. *Asset, Threat, Effect, ISO / IEC 27005, Ellipse Method, Octave-s Methodology, Risk, Information Security.*

Gestion des risques pour la sécurité de l'information d'après le standard ISO/IEC 27005 de 2011, en proposant une adaptation de la méthodologie OCTAVE-S. Cas d'étude : Processus d'inscriptions et admissions dans la Division d'Admissions, Registre et Contrôle Académique (DARCA) de l'Université du Cauca

Résumé
Cet article présent l'application de la méthodologie OCTAVE-s pour l'analyse et gestion des risques pour la sécurité de l'information, adapté au processus de inscriptions et admissions dans la Division d'Admissions, Registre et Contrôle Académique (DARCA) de l'Université du Cauca (Colombie) , d'après les directives du standard ISO/IEC 27005 :2011. Par ailleurs on inclut la structure du processus choisi comme cas d'étude pour appliquer traitement des risques. Finalement on présente les résultats obtenus et les conclusions de la gestion des risques avec la méthodologie adaptée.

Mots-clés. *Actif, Menace, Effet, ISO/IEC 27005, Méthode de l'ellipse, Méthodologie Octave-s, Risques, Sécurité de l'information.*

1. INTRODUCCIÓN

En la actualidad, las empresas manejan la información referente a sus procesos de negocio de forma física y digital. Dicha información, independiente de su medio de almacenamiento y transmisión, es un recurso vital para el éxito y la continuidad del servicio en cualquier organización, ya que de ella depende la toma de decisiones y el conocimiento interno de la empresa.

Debe tenerse en cuenta que un sistema de información no necesariamente está asociado a un sistema informático. Un sistema de información pueden ser personas, materiales, objetivos, actividades, etc., aunque también tecnologías de la información y de comunicación. Es por esto que la gestión del riesgo en la seguridad de la información debe considerar aspectos tanto físicos como lógicos para lograr un adecuado tratamiento del riesgo.

La gestión del riesgo en la seguridad de la información implica inversión de tiempo, esfuerzo y otros recursos con los que una pequeña organización no suele disponer, siendo esta una de las razones por las que no suelen ejecutar a gestión del riesgo como una prioridad.

Las organizaciones que conocen el valor de sus activos de información y desean invertir en gestionar su riesgo, suelen acogerse a las normas de la familia ISO 27000, en especial la norma ISO 27005. La norma ISO 27005 [1] es el estándar internacional encargada de la gestión de riesgos de seguridad de información. Dicha norma contiene las directrices que se deben realizar para llevar a cabo el proceso de gestión del riesgo, y es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que amenacen la seguridad de la información de su organización. No recomienda una metodología concreta, lo cual dependerá de la organización escoger la metodología que mejor se acople a sus objetivos de negocio. Es por esto que se hace necesario definir y seguir una metodología que se adapte al entorno o contexto a abarcar; es aquí donde una organización toma lo que puede ser la decisión más importante en el proceso de gestión del riesgo, ya que elegir el camino menos adecuado traerá como resultado menos eficiencia, y por lo tanto mayor costo y esfuerzo para lograr el objetivo, que consiste en manejar el riesgo de una manera más económica de lo que costaría recuperarse de un incidente de seguridad. Una metodología recomendada por muchos para la gestión del riesgo es la llamada OCTAVE-s. Esta es una técnica de evaluación y planificación estratégica basada en el riesgo para la seguridad, la cual aprovecha los conocimientos de los empleados, de las prácticas y los procesos relacionados con la seguridad de la organización para capturar el estado actual de las prácticas de la seguridad dentro de la misma. Su enfoque consiste en tomar decisiones de protección de la información basadas en los riesgos para la confidencialidad, integridad y disponibilidad de los activos. Al momento de tomar dichas decisiones, se deben tener en cuenta todos los aspectos de riesgo (activos, amenazas, vulnerabilidades y el impacto en la organización).

Teniendo en cuenta las consideraciones mencionadas anteriormente, el presente artículo aborda una propuesta del cómo llevar a cabo la gestión del riesgo en la seguridad de la información, proponiendo una adaptación de la metodología OCTAVE-s que cumpla con las directrices de la norma ISO/IEC 27005, para ser aplicada al proceso de Inscripciones y Admisiones, correspondiente a la División de Admisiones Registro y control académico (DARCA) de la Universidad del Cauca, con el fin de minimizar el riesgo actual de dicho proceso.

2. PROCESO INSCRIPCIONES Y ADMISIONES Y DEFINICIÓN DEL ALCANCE DEL CASO DE ESTUDIO

La norma ISO 27005 se fue acoplando con la metodología OCTAVE-s a medida que se gestionaba el riesgo a la seguridad de la información al proceso Inscripciones y Admisiones. La norma ISO 27005 cuenta con 7 pasos los cuales son:

1. Establecimiento del contexto
2. Identificación del riesgo
3. Estimación del riesgo
4. Evaluación del riesgo
5. Tratamiento del riesgo
6. Aceptación del riesgo
7. Comunicación del riesgo

La norma OCTAVE-s cuenta con 3 fases las cuales son:

1. Construcción de perfiles de amenazas basados en los activos.
2. Identificación de las vulnerabilidades de la infraestructura.
3. Desarrollo de estrategia y planes de seguridad.

Cada fase de Octave-s se fue adaptando a los pasos de la norma ISO 27005. Pero antes de usar la metodología Octave-s, se empezó por establecer el contexto (Establecimiento del contexto – Norma ISO 27005), es decir por definir el alcance del proceso Inscripciones y Admisiones.

El proceso de Inscripciones y Admisiones cuenta con los siguientes siete procedimientos:

1. Definición del calendario de admisión
2. Justificación del servicio de aplicación de la prueba
3. Inscripciones
4. Alistamiento para la aplicación de la prueba

5. Aplicación de la prueba
6. Evaluación de la prueba
7. Admisiones

Cada procedimiento cuenta con una serie de actividades las cuales se deben seguir en estricto orden para cumplir con sus objetivos. El alcance del procedimiento se elaboró a través la Metodología de las Elipses propuesta en [2] como herramienta de identificación de los componentes de cada proceso y las interacciones con otros procesos en la organización y con entidades externas a la empresa.

3. CONSTRUCCIÓN DE PERFILES DE AMENAZAS BASADOS EN LOS ACTIVOS (FASE 1. OCTAVE-S)

En esta fase se definen los criterios de evaluación de impacto que se utilizan posteriormente en la evaluación de riesgos. Luego se identifican los activos organizacionales y se evalúan las prácticas actuales de la seguridad en DARCA para proteger dichos activos. Posteriormente, se seleccionan activos críticos para analizar en profundidad basado en su importancia relativa a la organización. Finalmente, se definen los requisitos de seguridad y un perfil de amenaza para cada activo crítico.

A continuación se indica de manera detallada las actividades realizadas en esta fase (entre paréntesis se detalla la fase de Octave-s en la cual se realiza dicha actividad y el paso de la norma ISO 27001 con el cual está asociada dicha fase):

a. Establecimiento de Criterios de Evaluación de Impacto. (Fase 1-Octave-s. Identificación del riesgo- ISO 27005).

Se definieron un conjunto cualitativo y cuantitativo de medidas (criterios de evaluación de impacto) con las cuales se puede evaluar el efecto de un riesgo para los objetivos del proceso de Inscripciones y Admisiones. Para lo anterior se consideraron las siguientes variables de impacto a evaluar:

- Reputación / confianza.
- La vida / salud de los usuarios y funcionarios.
- Financiero.
- Productividad.

Los criterios de evaluación considerados son

- Alto Impacto (valor de impacto = 3)
- Medio Impacto (valor de impacto =2)
- Bajo Impacto (valor de impacto = 1)

b. Identificación de Activos de Información. (Fase 1-Octave-s. Identificación del riesgo- ISO 27005).

Los activos del Proceso Inscripciones y Admisiones se clasificaron según las categorías propuestas en ISO/IEC 27002 de la siguiente manera: Activos de Información, Activos Físicos, Activos de Aplicaciones (activos de software), Activos de Servicios, y Personas Involucradas en el proceso Inscripciones y Admisiones.

En total se identificaron 68 activos, que hacen parte del proceso de Inscripciones y Admisiones.

c. Evaluación de Procedimientos de Seguridad de DARCA. (Fase 1-Octave-s. Identificación del riesgo- ISO 27005).

En esta parte se procede a evaluar las diferentes áreas de seguridad respecto al proceso Inscripciones y Admisiones. Se tomaron como referencia dos tipos de áreas propuestas en OCTAVE-s [3], que son: áreas de práctica estratégica y áreas de práctica operacionales.

Las áreas de práctica estratégica trata sobre todo lo que concierne a políticas de seguridad. Estas áreas son:

1. *Conciencia y Formación de Seguridad.*
2. *Estrategia de Seguridad*
3. *Gestión de la Seguridad*
4. *Políticas y Reglamentos de Seguridad*
5. *Gestión de la Seguridad Colaborativa*
6. *Planes de Contingencia / Recuperación de Desastres.*

Las áreas de práctica operacionales trata sobre todo lo que concierne a procesos tecnológicos y físicos así como su uso diario. Estas áreas son:

1. *Control de Acceso Físico*
2. *Monitoreo y Auditoría de Seguridad Física*
3. *Gestión de Sistema y Red*
4. *Seguimiento y auditoría de Seguridad de TI*
5. *Autenticación y autorización*
6. *Gestión de Vulnerabilidades*
7. *Cifrado*
8. *Arquitectura y Diseño de Seguridad*
9. *Gestión de Incidentes*

Cada área de práctica de seguridad se evaluó de acuerdo a una cantidad de actividades que la metodología OCTAVE-s proporciona; Estas actividades se evalúan respecto a tres criterios:

- Mucho- la organización está haciendo totalmente la actividad para el área determinada.
- Algo – la organización está haciendo a medias dicha actividad para el área determinada.
- Nada - la organización no está haciendo dicha actividad para el área determinada.

Cuando esta evaluación se realizó para todas las áreas de práctica se seguridad, se procede a colocar un color para cada área evaluada. Dicho color representa lo bien o mal que esta dicha área. Los criterios de evaluación respecto al color es el siguiente:

- Verde – el área está haciendo todo bien. No se necesita ninguna mejora.

- Amarillo – el área está haciendo algunas actividades bien. Hay espacio para la mejora.
- Rojo – el área no está haciendo las actividades bien. Se debe mejorar muchas actividades.

Octave-s sugiere colocar el color intuitivamente, pero en este caso se adaptó una forma de colocar el color por medio de valores. Estos valores salen de lo siguiente: primero se le agrego a los criterios *mucho, algo, nada* los valores 1, 2, y 3 respectivamente. Luego, suponiendo que un área de práctica de seguridad tiene 3 actividades, en donde la primera actividad dio Mucho (1), la segunda actividad dio Nada (3), y la tercera actividad dio Algo (2), la suma de estos valores da 1+3+2=6. Para conocer un rango para ver en qué color se posiciona el valor 6, se basó tanto en el valor máximo (9) como el valor mínimo (3) que podría dar en dicha área. Entonces el rango seria: [3,4,5,6,7,8,9], en donde equitativamente se asignó el color verde para los valores 3 y 4, el color amarillo para los valores 5, 6, y 7, y el color rojo para los valores 8 y 9. Como la evaluación del área dio 6, el color que se le asigna es amarillo. Este cálculo se utilizó para las 15 áreas de práctica se seguridad.

d. Selección de Activos Críticos. (Fase 1-Octave-s. Identificación del riesgo- ISO 27005).

Para considerar un activo como crítico, se tomó como referencia el impacto que podría ocasionar al proceso Inscripciones y Admisiones en cuanto a su continuidad de negocio si dicho activo fuera modificado, revelado, destruido, o el acceso a este fuera interrumpido. Como resultado de lo anterior, se identificaron quince activos críticos; para luego proceder a documentar información específica de cada uno de ellos, especificando el fundamento para ser seleccionado, junto con una descripción de dicho activo.

e. Identificación de los requisitos de seguridad para los activos críticos. (Fase 1-Octave-s. Identificación del riesgo- ISO 27005).

En este punto se procede a obtener los requisitos de seguridad para cada activo crítico. Para ello, se centra en los requisitos que debería tener, más no los que tiene actualmente. Posteriormente se procede a registrar el requisito de seguridad más importante para el activo crítico.
Los requisitos de seguridad para los activos críticos son confidencialidad, integridad y disponibilidad.

f. Identificación de las amenazas a los activos críticos. (Fase 1-Octave-s. Identificación del riesgo- ISO 27005).

Es esta paso se procede a encontrar los actores tanto internos como externos que podrían amenazar dichos activos críticos. Para ello se toman como referencia dos categorías:

- Los actores utilizando acceso a la red.
- Los actores usando el acceso físico.

Tanto para los actores que acceden al activo crítico por medio de la red como los actores que acceden al activo crítico por medio físico, se seleccionan actores internos (que colaboran en DARCA) y externos (UDEA, estudiantes, aspirantes,…etc.) que puedan amenazar de forma accidental o de forma deliberada los activos críticos. Luego se estima el motivo del actor para amenazar dichos activos. La estimación se realiza de acuerdo a lo siguiente escala:

- Alta - El actor se centra en atacar al proceso, tiene metas muy definidas, está dirigido específicamente a los activos críticos, aplicarán medidas extraordinarias para atacar el activo crítico y tomara medidas extraordinarias para asegurar el éxito.
- Medio - El actor se centra en atacar al proceso, tiene metas generales, se dirige a una amplia gama de activos del proceso, tiene límites en los medios que se aplicarán para atacar el activo crítico, y tiene una explícita o implícita estrategia de salida que define cuando abandonar el ataque.
- Bajo - El actor está enfocado en atacar al proceso, no tiene objetivos específicos, se dirige a cualquier activo que pueda ser atacado fácilmente, aplicará medios limitados para el ataque, y abandonará rápidamente el ataque si el éxito no llega fácilmente.

A partir de ello, se procede a identificar la frecuencia con la que ha ocurrido esta amenaza en el pasado, revisando cualquier dato objetivo que se pudiera tener (por ejemplo, los registros, los datos de incidentes), así como datos subjetivos con el fin de calcular cuantas veces y en cuantos años sucedió dicha amenaza.

4. IDENTIFICAR LAS VULNERABILIDADES DE LA INFRAESTRUCTURA (FASE 2. OCTAVE-S)

a. Análisis de vías de acceso. (Fase 2-Octave-s. Identificación del riesgo- ISO 27005).

En primer lugar, se estableció el sistema (s) que está más estrechamente ligado a un activo crítico. Se empieza por verificar en donde los activos residen, a qué lugar se tendría que ir para obtener una copia "oficial" del activo, cual es el sistema que ofrece a los usuarios legítimos tener acceso a un activo crítico y cuáles son los sistemas que un actor de amenaza apuntaría para acceder a una activo crítico.

Se identificaron múltiples sistemas de interés para un activo crítico, pero se depuró la lista considerando sólo los sistemas más relevantes por cada activo crítico.

Al examinar las vías de acceso, primero se establece qué componentes son parte del sistema de interés. Se tomó como referencia las siguientes clases de componentes del sistema de interés:

- Servidores
- Redes internas
- Estaciones de trabajo en las instalaciones
- Otros

Luego, se determinó cómo se transmite la información y las aplicaciones del sistema de interés para las personas que tienen acceso a ese sistema. Los tipos de componentes de acceso intermedio que se tomaron como referencia son los siguientes:

- Redes internas
- Redes externas
- Otros

Se examinó qué componentes utilizan las personas (por ejemplo, los usuarios, los atacantes) para acceder al sistema de interés. Para esto, se tomaron en cuenta los puntos de acceso tanto internos como externos a las redes de DARCA. Los componentes de acceso que las personas podrían usar son:

- Estaciones de trabajo en las instalaciones
- Computadoras portátiles
- PDAs / componentes inalámbricos
- Desde casa / estaciones de trabajo externas
- Otros

Se determinó en qué clase de componentes de almacenamiento se encuentra la información del sistema de interés almacenada como copia de seguridad. Como opciones se tomaron:

- Dispositivos de almacenamiento
- Otros

b. Análisis de los procesos tecnológicos relacionados. (Fase 2-Octave-s. Identificación del riesgo- ISO 27005).

En esta parte, las actividades de análisis no se realizan desde la perspectiva de los activos, sino que se asume el punto de vista de la infraestructura.

Durante esta actividad, se analizaron los procesos relacionados con la tecnología utilizadas durante la configuración y el mantenimiento de la infraestructura informática. Luego, se compiló la información para cada clase de componente que se ha identificado durante la actividad anterior. La información de cada clase incluye:

- Los activos críticos que están relacionados con cada clase.
- La parte (o partes) responsable de mantener y asegurar cada clase de componentes.
- La medida en que la seguridad se considera a la hora de configurar y mantener cada clase de componentes (mucho, poco, nada, no se sabe)
- El cómo se determinó el grado en el que la seguridad se considera al momento de configurar y mantener cada clase de componentes (técnicas formales, medios informales, otros)
- Cualquier información adicional.

Antes de empezar esta actividad, se revisó los tipos de componentes que se identificaron para cada activo crítico durante la actividad anterior (Análisis de vías de acceso). Ahora los activos críticos están relacionados con cada clase de componentes. En este paso se documentó esa información, se consultó las rutas de acceso a la red para cada activo crítico y se revisó la información registrada anteriormente. Para cada clase de componente registrada anteriormente, se registraron los activos críticos que estuvieran relacionados con esa clase.

A continuación, se identificó la parte (o partes) responsable de mantener y asegurar cada clase (y subclases) de componentes; se anotó el nombre de la parte o partes responsables de mantener y asegurar cada clase (o subclase en su caso) del componente. También se determinó qué tan bien está protegida actualmente cada clase (y subclases) de componentes. Luego, se planteó una escala de referencia con los siguientes valores para indicar el grado de seguridad que se considera durante la configuración y mantenimiento de cada clase de componentes:

- Mucho - Se tiene una cantidad considerable de datos objetivos relacionados con la estimación. Cualquier persona razonable que revise los datos objetivos llegaría a la misma conclusión.
- Algo - Se tiene una cantidad limitada de datos objetivos relacionados con su estimación. Una persona razonable tendría que hacer inferencias y suposiciones para llegar a la misma conclusión. Sin embargo, es probable que una persona razonable llegara a la misma conclusión.
- No, en absoluto Se tiene datos objetivos poco o nada relacionados con su estimación. Una persona razonable podría llegar a una conclusión diferente, porque hay poco o nada de datos objetivos sobre los que basar la estimación.
- No sabe - No se tiene suficiente experiencia y conocimientos para hacer una conjetura plausible.

También se tuvo en cuenta específicamente las fuentes de los datos que se utilizó para determinar el grado en el que la seguridad es considerada a la hora de configurar y mantener cada clase de componentes. Se consideró tres formas de obtener la información:

- Técnicas Formales - Se emplean técnicas rigurosas de recopilación y análisis de datos para llegar a la conclusión. Esto puede incluir una

evaluación de la vulnerabilidad específica de la infraestructura informática por personal experimentado, una auditoría formal de los componentes por personal cualificado, o cualquier otra técnica de evaluación / análisis formal.

- Medios informales - Se ha realizado una evaluación somera de la situación para llegar a la conclusión. Esto puede incluir una evaluación muy limitada de la vulnerabilidad de la infraestructura de computación, una revisión o auditoría limitada de los componentes, o cualquier otra técnica o anuncio incompleta. Esto también puede incluir cualquiera de las técnicas de recolección de datos y análisis rigurosos realizados por personal sin experiencia.
- Otros - Se utilizó esta categoría para identificar cualquier otro medio que se utilizó para llegar a la conclusión de que no corresponde a ninguna de las categorías anteriores.

Después de esto se realizó un Análisis Gap, en donde se refino la información de la Fase 1 basado en el análisis de las vías de acceso y procesos relacionados con la tecnología. Para ello se llevaron a cabo las siguientes tareas:

- Se documentó información que describa donde reside cada activo crítico.
- Se documentó información que describa donde residen las prácticas de seguridad. También se buscó los casos en los que se puede revisar las prácticas de seguridad existentes y las vulnerabilidades de la organización mediante la adición de detalles, o donde se pudiera identificar nuevas prácticas de seguridad y vulnerabilidades de la organización. Por último, se revisó la información para cada área de práctica de seguridad en donde se hubiera hecho adiciones o cambios, y se revisó el estado de luz (verde-amarilla-roja) en esa zona cuando fue apropiado.

A continuación se mostrara la gráfica donde se ilustra los diferentes pasos a seguir en esta actividad (Fig.1)**.**

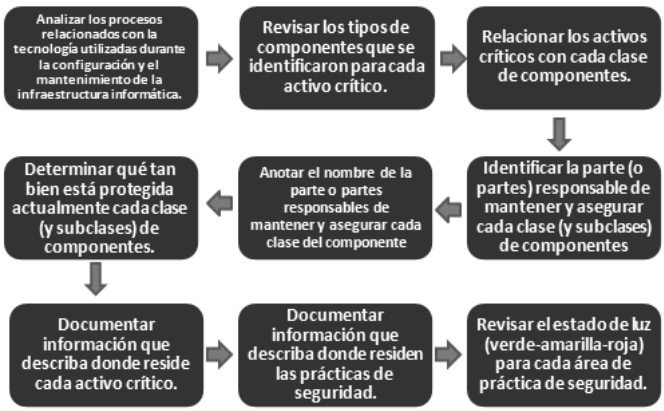

Fig. 1. Análisis de los procesos tecnológicos relacionados.

5. DESARROLLO DE ESTRATEGIA Y PLANES DE SEGURIDAD (FASE 3. OCTAVE-S)

a. Evaluación de los impactos de las amenazas. (Fase 2-Octave-s. Estimación del riesgo- ISO 27005).

Antes de evaluar los posibles impactos en la organización como resultado de las amenazas a los activos críticos, se revisó la información de activos críticos y la amenaza que se habían documentado previamente durante la evaluación; se revisó la información sobre la amenaza registrada para cada activo crítico. Para ello, se centró en los siguientes puntos:

- Amenazas a los activos críticos
- Contexto de la amenaza (actores de amenaza, el motivo, la historia)
- Contexto adicional de la amenaza

También, se revisó la información registrada sobre los activos críticos. Para ello, se centró en los siguientes puntos:

- Justificación de la selección de activos relacionados.
- Requisitos de seguridad.
- Requisitos de seguridad más importantes.

Luego se revisó los criterios de evaluación de impacto. Se enfocó en cómo se definió alto, medio y bajo impacto para el proceso de Inscripciones y Admisiones. Se utilizó los criterios de evaluación de impacto para evaluar el impacto de cada amenaza sobre los objetivos del proceso de Inscripciones y Admisiones en Darca, donde se revisó los criterios registrados para las siguientes áreas:

- Reputación / confianza de los estudiantes
- La vida / salud de los estudiantes
- Financiera
- Productividad

Para cada activo crítico, así como para cada amenaza del activo, se consideraron las siguientes preguntas:
¿Cuál es el impacto potencial a la reputación de DARCA?
¿Cuál es el impacto potencial sobre la confianza de los estudiantes?
¿Cuál es el impacto potencial para la salud o la seguridad de DARCA y/o los estudiantes?
¿Cuál es el potencial de impacto financiero para DARCA?
¿Cuál es el impacto potencial de la productividad de DARCA?

A medida que se revisaron y se fueron respondiendo las preguntas, se analizó el impacto potencial sobre DARCA debido a cada amenaza activa (Cada una de las preguntas anteriores está vinculada a un área de impacto).

Después de responder y analizar las preguntas anteriores, se compararon los impactos potenciales que se discutieron para cada área de impacto frente a los criterios de evaluación de impacto para esa área.
Usando los criterios de evaluación de impacto como una guía, se asignó una medida de impacto (alta, media o baja) así como un valor respectivo (3, 2, 1) para cada amenaza activa:

- " A" para cada alto impacto (valor 3)
- " M " para cada medio impacto (valor 2)
- " B " para cada bajo impacto (valor 1)

b. Establecimiento de criterios de evaluación de probabilidad. (Fase 2-Octave-s. Estimación del riesgo- ISO 27005).

En esta actividad se definieron medidas de probabilidad basados en la frecuencia de qué tan probable es que ocurran amenazas. Para ello se revisó la siguiente información:

- Los tipos de amenazas a los activos críticos
- Con qué frecuencia ha ocurrido cada amenaza en el pasado (la historia)

También se consideraron, se respondieron y se analizaron las siguientes cuestiones:
¿Qué define a una "alta" probabilidad de ocurrencia? ¿Con qué frecuencia debe producirse una amenaza para ser considerado una amenaza de alta probabilidad?
¿Qué define una probabilidad "media" de que se produzca? ¿Con qué frecuencia debe producirse una amenaza para ser considerada una amenaza de media probabilidad?
¿Qué define una probabilidad "baja" de que se produzca? ¿Con qué frecuencia debe producirse una amenaza para ser considerado una amenaza de baja probabilidad?
Luego para cada probabilidad Alta, Media, Baja se le asignaron los valores 3, 2, 1 respectivamente.

c. Evaluación de probabilidades de amenazas. (Fase 2-Octave-s. Estimación del riesgo- ISO 27005).

La siguiente información de cada amenaza activa se ha ido registrando para cada activo crítico:

- La información contextual acerca de los actores de amenaza
- El motivo de acciones deliberadas por parte de actores humanos
- La historia de cada amenaza activa
- Las áreas de preocupación

Cabe resaltar que para estimar la probabilidad se utilizó como base la historia de las amenazas, y así de esta forma analizar qué tan probable es que la amenaza se produzca en el futuro. Para ello se revisó la historia de la amenaza y se asignó a esa amenaza un valor de probabilidad cualitativa (alta, media o baja) y cuantitativa (3, 2, 1) respectivamente en base a los criterios de evaluación de probabilidad que se creó en la actividad pasada, y la historia de esa amenaza. También se analizó si los otros datos que se ha registrado para la amenaza cambian la estimación basada en la historia.

Para ello se retomó la siguiente información:

- Motivo de acciones deliberadas por parte de actores humanos
- Resumen de vulnerabilidades de la infraestructura informática para amenazas de red y código malicioso
- Resumen de vulnerabilidades de la infraestructura física para amenazas físicas
- Información contextual sobre factores de amenaza
- Ejemplos concretos de amenazas

Luego se ajustó la estimación de cualquier probabilidad de amenaza cada vez que la información lo ameritaba.

Para ello se consultaron los criterios de probabilidad al ajustar las estimaciones de probabilidad. Luego se documentó cada probabilidad de acuerdo a los siguientes criterios:

- "A" para cada alta probabilidad y el valor de 3.
- "M" para cada probabilidad media y el valor de 2.
- "B" para cada baja probabilidad y el valor de 1.

También se consideró la siguiente información:

- Exactitud de los datos del historial.
- Exhaustividad de la evaluación de las vulnerabilidades de la infraestructura informática.
- Exhaustividad de la evaluación de las vulnerabilidades de la infraestructura física.

d. Calculo del Valor del Riesgo. (Fase 2-Octave-s. Evaluación del riesgo- ISO 27005).

Luego de calcular el valor de impacto de amenaza para cada variable (reputación, productividad, financiera, salud) en un activo crítico, se procede a sumar dichos valores de cada variable. Al resultado se multiplica por la probabilidad de ocurrencia de dicha amenaza. El resultado de dicho cálculo es el valor del riesgo (para solo un activo crítico). Este cálculo se realizó para todos los 15 activos críticos.

Como resultado de haber identificado todos los posibles valores del riesgo para cada activo crítico, se obtuvo la siguiente escala de valores: (Fig.2).

ACTOR	INTERNO								EXTERNO								
MOTIVO	ACCIDENTAL				DELIBERADO				ACCIDENTAL				DELIBERADO				
AMENAZA	REVELACION	MODIFICACION	PERDIDA - DESTRUCCION	INTERRUPCION	REVELACION	MODIFICACION	PERDIDA - DESTRUCCION	INTERRUPCION	REVELACION	MODIFICACION	PERDIDA - DESTRUCCION	INTERRUPCION	REVELACION	MODIFICACION	PERDIDA - DESTRUCCION	INTERRUPCION	VALOR TOTAL DEL RIESGO
VALORES DE RIESGO	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	64
	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	80
	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	96
	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	112
	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	128
	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	144
	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	160
	11	11	11	11	11	11	11	11	11	11	11	11	11	11	11	11	176
	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	192
	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	224
	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	240
	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	256
	18	18	18	18	18	18	18	18	18	18	18	18	18	18	18	18	288
	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	320
	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	336
	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	352
	24	24	24	24	24	24	24	24	24	24	24	24	24	24	24	24	384
	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	432
	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	480
	33	33	33	33	33	33	33	33	33	33	33	33	33	33	33	33	528
	36	36	36	36	36	36	36	36	36	36	36	36	36	36	36	36	576

Fig. 2. Valores del riesgo.

El valor del riesgo máximo que podría hallarse es de 576, mientras que el valor mínimo es de 64. Fue decisión de la dirección de DARCA aceptar el riesgo del activo crítico si su valor estaba entre 64 y 192, mitigar el riesgo si su valor estaba entre 224 y 384, y eliminar el riesgo si su valor estaba entre 432 y 576.

Luego de esto, se analizaron todos los activos que tuviera un gran impacto de amenaza, es decir, se analizaron tanto sus valores cualitativos como sus cuantitativos, y luego de esto se revisó a que procedimiento afectaban en gran cantidad dichos activos. Al mirar esto, se observó que el procedimiento que más era afectado por dichos activos era el procedimiento Evaluación de la Prueba.

e. Selección planteamiento de mitigación. (Fase 3-Octave-s. Tratamiento del riesgo- ISO 27005).

El objetivo final en este proceso es seleccionar áreas de práctica de seguridad como áreas de mitigación. Sobre la base de los riesgos de seguridad de DARCA, así como la financiación y las restricciones de personal, influyo en la decisión del número de áreas para mitigar. Por lo tanto se revisó la siguiente información:

- Perfil de riesgo (para cada activo crítico)
- Activos Críticos (para cada activo crítico)
- Prácticas de Seguridad
- Revisión de Infraestructura
- Criterios de Evaluación de Impacto
- Criterios de Evaluación Probabilidad

Luego se consideraron, se respondieron y se analizaron las siguientes preguntas:
¿Qué está impulsando la selección de las áreas de mitigación?
¿Cuáles áreas de impacto son las más importantes para DARCA?
¿Cómo se va a factorizar la probabilidad en las decisiones?
¿Qué requisitos de seguridad son los más importantes para cada activo crítico?
¿Qué áreas específicas de preocupación se necesitan abordar?
¿Qué áreas específicas de práctica de seguridad necesitan la mayoría de las mejoras?
¿Qué vulnerabilidades organizacionales específicas es necesario abordar?
¿Qué otros factores pueden influir en la selección de las áreas de mitigación?

Se analizó la forma de abordar cada riesgo, así como pensar acerca de qué riesgos se tiene la intención de mitigar, aceptar, transferir y eliminar. Para esta decisión, se tomó como referencia los valores del riesgo mostrados en la Fig.3, en donde los activos críticos que tuviesen un valor del riesgo entre 64 y 192, el enfoque es de aceptar el riesgo. Si el valor del riesgo tuviese un valor del riesgo entre 193 y 384, el enfoque es de mitigar el riesgo. Pero si el valor del riesgo tuviese un valor del riesgo mayor a 384, el enfoque es de eliminar el riesgo. Luego se determinó el impacto con respecto a cada riesgo. Finalmente se determinó qué impactos son tan bajos que no habría la necesidad de tomar alguna acción proactiva para prevenirlos.

A este punto, se ha seleccionado los riesgos que se han de mitigar, eliminar o aceptar.

Luego de haber asignado un enfoque de mitigación para cada riesgo, a continuación, se seleccionan las áreas de mitigación. Se debe aclarar que todas las áreas de práctica de seguridad y todos los procedimientos del proceso *Inscripciones y Admisiones* tienen asociados los activos críticos correspondientes.

Para ello, se estudiaron las áreas de práctica de seguridad y se analizó cómo podrían estas áreas afectar los riesgos que deben ser mitigados. También se estudió y se analizó lo siguiente:

¿Cuáles áreas de práctica de seguridad, si se selecciona para la mitigación, podrían mitigar muchos riesgos a más de un activo crítico?
¿Existen todas las normas o políticas que deben tenerse en cuenta al seleccionar las áreas de mitigación? Si es así, ¿qué áreas se llevará a seleccionar?

Por lo tanto, se seleccionaron dos (2) áreas de práctica de seguridad como áreas de mitigación las cuales son

Estrategia de Seguridad y *Planes de Contingencia / Recuperación de Desastres*, con la seguridad de considerar todas las limitaciones (por ejemplo, fondos y personal) al hacer las selecciones. Una vez que se decidió implementar mejoras en un área de práctica de seguridad para mitigar los riesgos de seguridad del proceso de Inscripciones y Admisiones en DARCA, esas áreas de práctica se designaron como áreas de mitigación.

f. Desarrollo de planes de mitigación de riesgo. (Fase 3-Octave-s. Tratamiento del riesgo- ISO 27005).

En este punto se revisó la siguiente información:

- Perfil de riesgo (para cada activo crítico)
- Procedimientos de seguridad
- Información de activos críticos (para cada activo crítico).
- Criterios de Evaluación de Impacto
- Criterios de Evaluación de Probabilidad.

Lo anterior se hizo debido a que constituyen el conjunto mínimo de información que se necesitará durante esta actividad.

En este paso, se crearon planes de mitigación para cada área de práctica de seguridad que se seleccionaron durante la actividad anterior (área *Estrategia de Seguridad* y área *Planes de Contingencia / Recuperación de Desastres*).

Por lo anterior se analizó qué actividades de mitigación reducirían el riesgo, así como la justificación de la selección de cada actividad y quién debía participar en la ejecución de cada actividad. Luego de esto, se desarrolló un plan de mitigación para las 2 áreas seleccionadas, es decir se implanto un control para el área *Estrategia de Seguridad* y un control para el área *Planes de Contingencia / Recuperación de Desastres*.

El control implantado para el área *Estrategia de Seguridad* se describe: "Documentar las estrategias de seguridad, metas y objetivos del Proceso de Inscripciones y Admisiones". El control implantado para el área *Planes de Contingencia / Recuperación de Desastres* es: "Identificar los eventos que puedan causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información del Proceso de Inscripciones y admisiones".

Luego de haberse implantado los controles en estas dos áreas, los valores de riesgo de los activos críticos asociados a dichas áreas, fueron reducidos. Por ende los procedimientos que tienen asociados dichos activos críticos, también fueron afectados con la reducción del riesgo.

6. RESULTADOS

Se definió el alcance del caso de estudio aplicando la metodología de las Elipses al proceso *Inscripciones y Admisiones*. En la siguiente figura, se visualizan tres elipses: la primera elipse (de adentro hacia afuera) encierra los 7 procedimientos que hacen parte del proceso, la segunda elipse encierra todos los procesos internos a DARCA que intervienen en los procedimientos, y la tercera elipse encierra las organizaciones externas al proceso *Inscripciones y Admisiones*. (Fig. 3.)

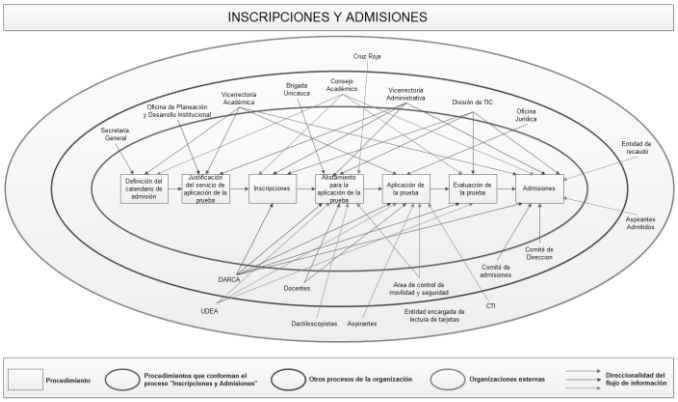

Fig. 3. Alcance del caso de estudio aplicando la metodología de las Elipses.

Se determinaron los valores del riesgo para cada activo crítico:

Tabla 1. Valor del riesgo en los activos criticos del proceso

Activo	Valor del riesgo
Archivo cifrado del documento que almacena los puntajes	139
Claves de respuesta	64
Material Empacado y Sellado en bolsas de Seguridad	**204**
Tarjetas de respuesta diligenciadas	136
Servidores que contienen la plataforma para la publicación de las listas	**279**
Maquina lectora	134
Personal DARCA	134
Personal TICS	134
Archivos de Inscripción	159
Convenio de cooperación interadministrativo	88
Credenciales de Citación	164
Formularios	148
Base de datos de personas inscritas	168
Plataforma de inscripciones	152

Activo	Valor del riesgo
Sistema integrado de recaudo (SQUID)	64
TOTAL	**2167**

El Valor del riesgo se calcula a partir de la suma del valor del Impacto de las amenazas de cada activo, multiplicado por la probabilidad de que se materialice cada amenaza.

Los activos críticos 'Material Empacado', y 'los servidores que contienen la plataforma para la publicación de las listas' tienen los niveles más altos de riesgo. Según la escala mostrada en la (Fig.2)**,** se recomendó realizar mitigación a través de la implantación de controles que beneficien principalmente a dichos activos. El resultado de la implantación de dos controles se visualiza a continuación (Tabla2).

Tabla 2. Segunda medición del valor del riesgo en los activos criticos del proceso (después de implantar controles)

Activo	Valor del riesgo
Archivo cifrado del documento que almacena los puntajes	139
Claves de respuesta	64
Material Empacado y Sellado en bolsas de Seguridad	170
Tarjetas de respuesta diligenciadas	136
Servidores que contienen la plataforma para la publicación de las listas	279
Maquina lectora	134
Personal DARCA	90
Personal TICS	90
Archivos de Inscripción	159
Convenio de cooperación interadministrativo	88
Credenciales de Citación	164
Formularios	148
Base de datos de personas inscritas	168
Plataforma de inscripciones	152
Sistema integrado de recaudo (SQUID)	64
TOTAL	**2045**

Luego de implantar los controles, el riesgo se redujo en 122 unidades, que representa una reducción del 5.63 por ciento de riesgo total de todos los activos involucrados en el Proceso de Inscripciones y Admisiones.

Procedimiento	Valor de riesgo inicial	Valor Total del Riesgo con los controles implantados	Porcentaje de reducción de riesgo (%)
Evaluación de la prueba	1224	1102	9.97
Inscripciones	747	659	11,78
Alistamiento para la aplicación de la prueba	520	432	16,92
Aplicación de la prueba	620	498	19,67
Admisiones	332	244	26,50
TOTAL	**3443**	**2935**	**14,75**

Para la medición del valor del riesgo de cada procedimiento, se tuvo en cuenta los activos que hacen parte de cada uno de ellos, en algunos casos hay activos que aparecen en más de un procedimiento a la vez.

7. CONCLUSIONES

- La metodología OCTAVE-S se alinea con las directrices de la norma ISO 27005 de 2011, brindando una guía para identificar amenazas y estimar su impacto y probabilidad de manera cualitativa, sin embargo se consideró conveniente adaptarla a un método cuantitativo que permitiera medir el riesgo y visualizar la reducción de éste a medida que se ejecuta la estrategia de tratamiento del riesgo.
- No es suficiente gestionar el riesgo de la seguridad de la información solo con la norma ISO 27005. Es necesario apoyarse de una metodología para el análisis y gestión del riesgo, como por ejemplo OCTAVE-s, ya que la norma ISO 27005 solo describe los pasos que se deben seguir para la gestión del riesgo, pero no explica las actividades que se deben llevar a cabo específicamente, lo que OCTAVE-s si determina.
- Al realizar el análisis del riesgo en la seguridad de la información en DARCA con ayuda de la metodología OCTAVE-s se pudo definir a estrategia de protección y el plan de mitigación de riesgo, incluyendo los controles a implantar para realizar el tratamiento del riesgo y así ejecutar el proceso de Inscripciones y Admisiones con un nivel bajo de riesgo.
- Con la implantación de solo dos de los controles sugeridos para el tratamiento del riesgo, se redujo éste último un promedio de 3.2% por procedimiento y un total de reducción de 1.46% en todo el Proceso.
- OCTAVE-S a pesar de ser una versión pequeña de la metodología OCTAVE, permite realizar un proceso de análisis y gestión de riesgo completo, cumpliendo con lo propuesto en la norma internacional ISO 27005:2011.
- La versión adaptada de la metodología OCTAVE-S producto del presente trabajo, no queda

estrictamente cerrada al Proceso de Inscripciones y admisiones de la Universidad del Cauca y puede usarse como base para realizar análisis de riesgos de seguridad de la información en otros procesos de la División de admisiones Registro y control Académico, u otras Divisiones de la Universidad.

- Se deben continuar implantando controles conforme a la Declaración de aplicabilidad para continuar con el tratamiento del riesgo hasta lograr el nivel de riesgo más bajo posible.

8. RECONOCIMIENTO

Los autores le damos agradecimientos a la División de admisiones, registro, y control académico DARCA, de la Universidad del Cauca, por permitirnos realizar el análisis y gestión de riesgo al proceso de Inscripciones y Admisiones.

9. REFERENCIAS

[1] ICONTEC, "Estándar Internacional ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition)," ed, 2011.
[2] A. A. G, Diseño de un Sistema de Gestión de Seguridad de Información: Alfaomega, 2007.
[3] CERT, “The OCTAVE-S method,” Software Engineering Institute.

10. BIBLIOGRAFIA

[4] ICONTEC, "Estándar Internacional ISO/IEC 27001:2005 Information Technology -- Securitytechniques --Specification for an Information Security Management System," ed, 2005.
[5] ICONTEC, "Estándar Internacional ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition)," ed, 2011.
[6] C. Serrano, Modelo Integral para el Profesional en Ingeniería, 2 ed. Popayán, Colombia, 2005.
[7] T. Tower, "FAIR – ISO/IEC 27005 Cookbook," ed. United Kingdom: The Open Group.
[8] P. A. Silberfich, "Análisis y Gestión de riesgos en TI ISO 27005 – Aplicación Práctica," A. O. Cruz, Ed., ed. Buenos Aires, Argentina: Segurinfo 2009 – Quinto Congreso Argentino de Seguridad de la Información, 2009.
[9] D. A. d. l. F. P. (DAFP), "Guía para la administración del riesgo," D. d. C. I. y. R. d. Trámites, Ed., 4 ed. Bogotá, D.C., 2011.
[10] M. d. C. C. Rin, "El Análisis de Riesgos dentro de una Auditoría Informática: pasos y posibles metodologías," Departamento de Informática, Universidad Carlos III de Madrid, 2013.
[11] I. N. d. T. d. l. Comunicación, "Guía Avanzada de Gestión de Riesgos," INTECO, Ed., ed, 2008.
[12] M. P. Konzen, "Gestão de Riscos de Segurança da Informação Baseada na Norma ISO/IEC 27005 Usando Padrões de Segurança," R. C. N. Lisandra Manzoni Fontoura, Ed., ed, 2012.
[13] P. D. P. Naranjo, "Análisis de los Riesgos y Vulnerabilidades de la Red de Datos de Escuela Politécina Nacional," Escuela de Ingeniería, Escuela Politécnica Nacional, Quito, 2007.
[14] P. O. J. C. Maria Cristina Gallardo Piedra, "Análisis de Riesgos Informáticos y Elaboración de un Plan de Contingencia T.I para la Empresa Eléctrica Quito S.A.," Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, 2011.
[15] L. A. B. Torres, "Plan de Seguridad de la Información Compañía XYZ Soluciones," Universidad Autónoma de Barcelona, 2013.
[16] G. P. Mega, "Metodología de Implantación de un SGSI en un grupo empresarial jerárquico," Instituto de Computación – Facultad de Ingeniería, Universidad de la República, Montevideo, Uruguay, 2009.
[17] I. N. d. T. d. l. Comunicación, "Implantación de un SGSI en la empresa," INTECO, Ed., ed, 2009.
[18] C. A. G. Guevara, "Establecimiento del Sistema de Seguridad de Informacion en SFG bajo los Estándares de la Norma ISO 27001: 2005," Facultad de Postgrados, Universidad EAN, 2012.
[19] A. A. G, Diseño de un Sistema de Gestión de Seguridad de Información: Alfaomega, 2007.
[20] M. T. R. Y. S., "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UN SISTEMA DE INFORMACIÓN (Caso de estudio: Sistema Administrativo Integrado SAI en la Red de datos de la UNEXPO- Puerto Ordaz)," Ciencia y Tecnología, Universidad Centrooccidental Lisandro Alvarado, Barquisimeto, 2008.
[21] P. D. A. A. G., "Análisis y Evaluacion del Riesgo de Información: Un Caso en la Banca," 2006.
[22] D. H. P. Ricardo Gómeza, Yezid Donoso, Andrea Herrera, "Metodología y gobierno de la gestión de riesgos de tecnologías de la información," Agosto, 2010 2010.
[23] Z. O. B. Alexandra Ramírez Castro, "Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios," vol. 16, pp. 56-66, 2011.
[24] J. M. M. Veiga, "Análisis de Riesgos de Seguridad de la Información," Facultad de Informática, Universidad Politécnica de Madrid, 2009.
[25] L. E. S. Antonio Santos-Olmo, Eduardo Fernández-Medina, Mario Piattini, "Revisión Sistemática de Metodologías y Modelos para el Análisis y Gestión de Riesgos Asociativos y Jerárquicos para PYMES," 2012.
[26] P. H. Ohtoshi, "Análise Comparativa de Metodologias de Gestão e de Análise de Riscos sob a Ótica da Norma NBR-ISO/IEC 27005," Departamento de Ciência da Computação, Universidad de Brasilia, Brasilia, 2008.
[27] P. P. Páez, "Aplicación de la Norma OCTAVE-S en la Empresa Pirámide Digital CIA. LTDA," ed. Quito, Ecuador, 2013.
[28] F. Soldan, "L'utilizzo di OCTAVE," in XXII Convegno Nazionale di Information Systems Auditing, ed. Parma, 2008.