ENCUENTROS
Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico
ISSN: 2343-6131 / ISSN-e: 2610-8046
Universidad Nacional Experimental Rafael María Baralt
Maracaibo, Venezuela
EXTRA N°1 (2022)

SOFTWARE PARA LA GESTIÓN DE RIESGOS EN LAS PRÁCTICAS FORENSES DE DERECHO BASADO EN LOS PRINCIPIOS DE LA NORMA ISO 31000 E ISO 27005

SOFTWARE FOR RISK MANAGEMENT IN FORENSIC LAW PRACTICES BASED ON THE PRINCIPLES OF THE ISO 31000 AND ISO 27005 STANDARDS.

pp:243-257

Mauricio Mejía Lobo
Universidad Católica Luis Amigó
Medellín, Colombia
mauricio.mejialo@amigo.edu.co

Este trabajo está depositado en Zenodo:
DOI: http://doi.org/10.5281/zenodo.6551136

RESUMEN

El objetivo principal es proponer un software para la gestión de riesgos en las practicas forenses basado en los principios de la norma ISO 31000 e ISO 27005, debido a que estas no cuentan con una metodología explicita que permita gestionar las amenazas de riesgo, por tal razón y tomando en cuenta que en el desarrollo de un proyecto suelen presentarse riesgos que afectan directa e indirectamente los procesos y sistemas produciendo pérdidas, se debe considerar alternativas que permitan la gestión oportuna de los riesgos. Para dicha propuesta se hará un análisis de estándares, técnicas, metodologías, y buenas prácticas en la gestión de riesgos en las practicas forenses, los resultados servirán de soporte para plantear la gestión de riesgos basada en las normas ISO 3100 e ISO 27005, una vez que se tenga definida la propuesta, conocer si esta ofrece aportes significativos sobre su implementación en la gestión del riesgo en las practicas forenses de derecho.

Palabras claves: Software, normas ISO, gestión del riesgo, prácticas forense, ciclo PHVA

ABSTRACT

The main objective is to propose a software for risk management in forensic practices based on the principles of ISO 31000 and ISO 27005, because they do not have an explicit methodology that allows managing risk threats, for this reason and taking into account that in the development of a project there are usually risks that directly and indirectly affect the processes and systems producing losses, alternatives should be considered that allow the timely management of risks. For this proposal, an analysis of standards, techniques, methodologies, and good practices in risk management in forensic practices will be made, the results will serve as support to propose risk management based on ISO 3100 and ISO 27005 standards, once the proposal has been defined, find out if it offers significant contributions on its implementation in risk management in forensic law practices.

Keywords: Software, ISO standards, Risk management, forensic practices, PHVA cycle

RECIBIDO: 05/12/21

ACEPTADO: 01/03/22

INTRODUCCIÓN

El ejercicio forense del derecho, al igual que en toda actividad profesional conlleva a lidiar con una serie de riesgos. Los sistemas para gestionar los riesgos que se hacen presentes en las prácticas forenses del derecho deben ser desarrollados con la finalidad de minimizar o mitigar los distintos tipos de riesgos que se hacen presentes en ellas. Para llevar a cabo una excelente gestión del riesgo es necesario invertir todos los recursos humanos, económicos y materiales posibles con el propósito de minimizar las amenazas de riesgo que se hacen presente en las prácticas forenses de derecho.

Actualmente, es muy común que las organizaciones, gobiernos y sociedad en general hagan frente a retos económicos, sociales y ambientales entre otros, lo que implica que la gestión del riesgo debe contar con una visión, liderazgo y herramientas tecnológicas adecuadas para ello. Si bien es cierto, el progreso para la minimización de los riesgos a teniendo grandes avances, puesto que la normativa vinculada con los sistemas de gestión del riesgo coadyuvan a las organizaciones a que estas logren sus objetivos. Los sistemas de riesgo y seguridad de las organizaciones están basados en un amplio abanico de normas ISO, por lo que el objetivo principal de este artículo es proponer un software fusionando dos tipos de elementos, la ingeniería de software y el derecho, los cuales van a estar sustentados en las normas ISO 31000:2018 e ISO 27005:2008, con los cuales se pretende crear valor a los procesos y mejorar constantemente las practicas forenses durante la gestión del riesgo.

El software que se pretende desarrollar permitirá implementar mejoras de eficiencia operativa dentro de la estructura organizacional, de manera proactiva y constante. Así, como mejorar el rendimiento y la sostenibilidad de otros Sistemas de Gestión. De esta forma el ISO 31000 permitirá mantener la calidad del proceso para minimizar el impacto negativo de los riesgos, y por otro lado, el ISO 27005 servirá de apoyo y ofrecerá la norma que suministra las directrices para la gestión de riesgos, generando una lista completa de los riesgos basados en eventos que tienen la capacidad de crear, aumentar, evitar, reducir, acelerar o retrasar el logro de sus objetivos. El software tiene las siguientes características, lenguaje de programación PHP VER. 7.5, con un servidor Apache 3.5, con sistema operativo Chrome, entre otras cosas.

El software propuesto, será programado con el lenguaje UML, con lo que se programará con diagrama de clases. El diagrama de clases recrea la estructura estática de un sistema. Las cosas que existen y que nos rodean se agrupan naturalmente en categorías. Una clase es una categoría o grupo de cosas que tienen atributos (propiedades) y acciones similares. La asignación de las tareas del software será realizada a través del método RUP, el cual se basa en cuatro fases: Inicio (alcance del proyecto), elaboración (análisis, definición y diseño del proyecto), construcción (implementación del proyecto), y transición

(cierre del proyecto y producción). El software tendrá las siguientes características: En primer lugar, el software creará y protegerá el valor de la información, en segundo lugar, los procesos del software deberán estar integrados a la red de procesos de la organización; en tercer lugar, deberá controlar la incertidumbre y mejorar la toma de decisiones, en cuarto lugar, será sistemático, estructurado y adecuado, en quinto lugar, la gestión del riesgo está alineada con el contexto externo e interno de la organización, en sexto lugar, será dinámica, interactiva y sensible al cambio, y en séptimo lugar, facilitará la mejora continua de la organización. El software será alojado en una página web, de lenguaje HTML, con página de inicio y de menú. Asimismo, se explicará el como se procesarán los riesgos a través del software, el cual pasa por la filtración de la información a través de categorías, como riesgo, delito, proceso, contingencia, reincidencia entre otras. El software será utilizado por los abogados, secretarias, clientes y administradores lo que permitirá mitigar por lo menos las amenazas de riesgo.

1. METODOLOGÍA

Para el desarrollo de la propuesta, la metodología de este artículo es documental y se basa en la recopilación de información de páginas web, para estructurar el artículo, el discurso de la literatura a usar estará sustentado en las normas ISO 31000; ISO 27005; PHVA; UML; diagrama de clases; RUP; características de software, sitio web; riesgos de la práctica forense del derecho; procesamiento del riesgo, y procesos. Por lo que se usara una sistematización metodológica basada en una hermenéutica para el desarrollo de los aspectos señalados a continuación:

A. Búsqueda bibliográfica

B. Criterios de selección

C. Evaluación de la calidad de la bibliografía seleccionada

D. Uso de documentos oficiales

E. Análisis de la viabilidad, fiabilidad y valides de la bibliografía

Para el criterio de selección de la información, serán consideradas las literaturas con pertinencia en el tema central para el desarrollo del artículo. De allí que, toda la información será seleccionada de cuerdo a la estructura del texto y el diseño metodológico. Es decir, la información concerniente a la creación de un software basado en los ISO 31000 e ISO 27005, con lenguaje de programación UML y desarrollo de arquitectura RUP. Las fuentes revisadas han sido seleccionadas, de universidades y páginas web reconocidas, como Scopus, Web of Science, ISOTOOLS.

Evolución tecnológica del derecho

El mundo de las nuevas Tecnologías de la Información y Comunicación (TIC) es un mundo global, conceptual y funcionalmente nuevo. Desde el punto de vista funcional la plataforma usada para acceder a las relaciones sociales, y jurídicas ha tenido cambios significativos. Todo se desarrolla a través de una plataforma tecnológica, la cual permite el acceso

a la información e interactuar través de las redes. La nueva realidad creada por las Tecnologías de la Información y Comunicación (TIC) requiere de cobertura por parte del ordenamiento jurídico para que queden protegidos los derechos de los ciudadanos. El derecho necesita adaptarse a las nuevas tecnologías para poder cumplir con la función social reguladora de la comunidad que le es propia. Ello implica, la actualización del software usado por el derecho en toda su extensión, lo que permitiría la unificación legislativa y el control del sistema en caso de irregularidades o riesgos de amenazas. Es decir, que los sistemas del derecho forense deberán considerar en sus sistemas la inclusión de un software basado en las normas ISO dentro de sus prácticas. Desde una perspectiva conceptual el derecho sustantivo va adaptándose a las nuevas necesidades jurídicas pero necesita dar cobertura en muchos nuevos ámbitos donde no cuenta con una regulación específica, o bien la existente no está unificada, aplicándose, en ocasiones, normativa que fue en su día diseñada para objetos y relaciones jurídicas diferentes.

La informática como tecnología forense

La Informática forense fue definida por McKemmish en 1999 como la identificación, conservación, análisis y presentación de pruebas electrónicas o digitales. Tradicionalmente se clasifica atendiendo a su ámbito de actuación en computación forense, forensia en redes, y forensia digital. La «computación forense» (computer forensics) se entiende como aquella disciplina de las ciencias forenses que considerando las tareas propias asociadas con la evidencia procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o como disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

La «forensia en redes» (network forensics) actúa en un escenario más complejo, pues, es necesario comprender la manera en que los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento en particular. Se trata de un profesional que entendiendo las operaciones que las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer rastros, movimientos y acciones que un intruso ha desarrollado para concluir una acción. A diferencia de la definición de computación forense este contexto exige capacidad de correlación de eventos muchas veces disyunta y aleatoria, que en equipos particulares es poco frecuente. Se trata de capturar, almacenar y analizar eventos de una red para descubrir el origen de un ataque o un posible incidente.

Y finalmente por «forensia digital» (digital forensics) se entiende aquella forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios

informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿Quién?, ¿Cómo?, ¿Dónde?, ¿Cuándo?, y ¿Por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la seguridad informática La Ciencia informático-forense desde un punto de vista técnico-científico comprende cualquier principio o técnica que pueda ser aplicada para individualizar, identificar, recuperar, reconstruir o analizar un hecho electrónico. Se trata de una actividad científica de indudable importancia en el proceso, pero que, sin embargo, no es suficientemente conocida y apreciada en el sistema de impartición de justicia. El principal problema que encuentra dicha disciplina y que afecta, como consecuencia, a la valoración que puedan efectuar los tribunales de la prueba pericial informático-forense, probablemente consista en la falta uniformidad y consenso de la comunidad científica tanto sobre el proceso como sobre la validación no solo de los resultados obtenidos sino también de las herramientas y las técnicas utilizadas para obtener la evidencia electrónica69. Efectivamente, puede constatarse en la actualidad la existencia de una gran diversidad de herramientas en uso por parte de los expertos en informática forense70 . Por otro lado, la falta de homogeneización de protocolos de investigación y análisis del hecho electrónico suponen que no siempre la prueba cumpla con plena garantía tanto en su obtención como en su custodia.

Investigación informático-forense:

Fases La investigación informático-forense tendrá por objeto el análisis de distintos hechos que tienen por base hechos electrónicos. Una conducta humana como el envío o recepción de un correo electrónico puede suponer una serie de hechos de naturaleza electrónica que pueden ser objeto de análisis por los expertos informático-forenses en una investigación de tal naturaleza. Dichos expertos concluirán verificando ese primer hecho a través del análisis de los demás. Es decir, a través del análisis efectuado por los expertos en informática forense de los metadatos, logs, copias de seguridad etc. podrá constatarse la

2. CONSIDERACIONES SOBRE LA NORMA ISO 31000:2018 E ISO 27005:2008

La ISO 31000, es una norma de gestión de riesgos cuya finalidad es beneficiar a las diversas instituciones, públicas o privadas, a través de buenas prácticas y herramientas para mejorar la eficiencia operativa, la confianza entre las partes, fomenta el liderazgo entre otros beneficios. La aplicación de la norma ISO 31000 se basa en la utilización de herramientas como la planificación, la gestión, o la comunicación. ISOTOOLS EXCELLENCE (2017) menciona que implementar la norma 31000 aporta a la organización mejoras de eficiencia operativa

organizacional, de manera proactiva y constante y, fomenta el liderazgo de la Alta Dirección. Implementar el ISO 31000 construye confianza entre las partes involucradas en el proceso, cuales quiera que sea, que se ven beneficiadas con la prevención de los riesgos. Aplicar los lineamientos de la norma en los controles del Sistema de Gestión para el análisis de riesgos logra minimizar su impacto negativo. Además de mejorar el rendimiento y la sostenibilidad de otros Sistemas de Gestión, como el de la calidad.

Cabe destacar, que la norma de gestión de riesgos ISO 31000 se adapta fácilmente a los procesos de modificación y cambios eficazmente, acoplándose a las modificaciones internas de la entidad, como la expansión o la reducción. Logra optimizar los recursos empleados en los procesos de prevención de riesgos. Reducción de costos, gracias a la disminución de incidentes o eventos generadores de riesgos. Finalmente, mejora de la planificación y reduce los incidentes que generan pérdidas inesperadas. Puntualmente, aplicar el ISO 31000 favorece a:

a. Mejora la eficiencia operativa de la organización en forma proactiva, y fomenta el liderazgo de la Alta Dirección.

b. Construye confianza entre las partes interesadas, que se ven beneficiadas con la prevención de los riesgos.

c. Aplica controles de Sistema de Gestión al análisis de riesgos para minimizar su impacto negativo.

d. Mejora el rendimiento y la sostenibilidad de otros Sistemas de Gestión, como el de la calidad.

e. Se adapta fácilmente a los cambios y las modificaciones de forma eficaz, sobre todo en la medida en la que la organización se expande.

f. Optimización de los recursos utilizados por la organización en la prevención de riesgos.

g. Reducción de costos, gracias a la disminución de incidentes o eventos generadores de riesgos.

h. Aprovechamiento de nuevas oportunidades.

i. Mejora de la planificación y reducción de incidentes generadores de pérdidas inesperadas. (ISOTOOLS EXCELLENCE, 2017)

Por otro lado, el ISO 27005, también una norma de gestión, se ocupa de la gestión de los riesgos relativos a la seguridad de información. La norma suministra las directrices para la gestión de riesgos, apoyándose fundamentalmente en los requisitos sobre esta cuestión definidos en la ISO 27001. La norma se puede aplicar a toda organización, que tenga la intención de mejorar su gestión de riesgos sobre seguridad de la información. El objetivo es generar una lista completa de los riesgos basados en eventos que tienen la capacidad de crear, aumentar, evitar, reducir, acelerar o retrasar el logro de sus objetivos. El ISO 27005, se ha creado para sustituir a las normas ISO anteriores como la ISO / IEC TR 13335-3:1998 (ISOTOOLS EXCELLENCE, 2017)

La modernidad se muestra con avances tecnológicos constantes, los cuales en el proceso de desarrollo e implementación posibilita la vulnerabilidad de los sistemas de seguridad -todo el tiempo hay nuevas formas de ciberataques-, por ello, es necesario adaptarse y mejorar continuamente al respecto de la gestión de la seguridad de la información. Para ello hay que lograr un correcto control de las entradas – información de la institución pertinente para la gestión del riesgo de la información- y salidas -delimitación de los criterios básicos, alcances, límites y organización del proceso de gestión del riesgo de la información-, así como de la contextualización y la institución de la gestión del riesgo de la información. (ICONTEC, 2008, P. 7)

3. CICLO PHVA COMO FACTOR DE PLANIFICACIÓN

Con respecto al ciclo PHVA, este se basa en planificar los objetivos y la manera de concretarlos en base a las políticas institucionales y los requerimientos de los clientes. Para lograr estos objetivos, se recomienda usar herramientas 5W2H; también hay que hacer la ejecución de lo planeado, haciendo pilotajes de los procesos a implementar. Esta etapa del ciclo, sirve para evidenciar las falencias internas de la implementación y todo aquello que se deba mejorar; Se requiere verificar que los objetivos se hayan realizado a través del seguimiento y medición de los procesos de acuerdo a las políticas internas de la institución y la planificación; por último, se sugiere actuar para realizar acciones de acuerdo a las mejoras de desempeño en los procesos, corrigiendo errores, estandarizando cada uno de ellos. Esto permite medir el alcance de las acciones realizadas, conocer el contexto y los criterios para la intervención. Así también, se logra identificar, analizar, valorar, tratar el riesgo y finalmente registrarlo e informarlo. Por lo antes expuesto, se pretende crear un software para la gestión de riesgos basado en los principios de la Norma ISO 27005 los cuales se van a actualizar y mejorar constantemente a través de la aplicación de las buenas prácticas y las herramientas de la Norma ISO 31000. Estas a su vez, serán aplicadas en base al ciclo PHVA, buscando generar confianza en el sistema de gestión de riesgos entre las partes involucradas, ya que su implementación permitirá minimizar el impacto negativo de los riesgos. Optimizando Las operaciones realizadas de forma eficiente, constante y proactiva.

La creación del software basado en la implementación de las normas ISO 31000 e ISO 27005, permitirá una adaptabilidad a cualquier proceso de cambio al interior de la organización de forma eficaz, ya que se logrará acoplarse a las modificaciones internas. Su creación y funcionamiento será realizado optimizando los recursos empleados, lo que reducirá el número de incidentes que generan pérdidas inesperadas, activando un correcto control de la información de la institución pertinente para la gestión del riesgo, la información de entradas y delimitación de los criterios básicos, alcances, límites y organización del proceso de gestión del riesgo de la información-salidas- así como de la contextualización y la institución de

la gestión del riesgo de la información. De esta manera lograremos definir el alcance, el contexto y que criterios usar para identificar, valorar, y tratar el riesgo, para finalmente registrar e informarlo.

Mejora la eficiencia operativa de la organización en forma proactiva, y fomenta el liderazgo de la Alta Dirección.	Delimitación de los criterios básicos, alcances, límites y organización del proceso de gestión del riesgo de la información de salidas	**Planeamiento**	Alcance, Contexto y Criterios.
Construye confianza entre las partes interesadas, que se ven beneficiadas con la prevención de los riesgos.			
Aplica controles de Sistema de Gestión al análisis de riesgos para minimizar su impacto negativo		**Hacer**	Identificación del Riesgo, Análisis del Riesgo,
Mejora el rendimiento y la sostenibilidad de otros Sistemas de Gestión, como el de la calidad.	control de la información de la institución pertinente para la gestión del riesgo de la información de entradas		
Se adapta fácilmente a los cambios y las modificaciones de forma eficaz, sobre todo en la medida en la que la organización se expande.		**Verificar**	Valoración del Riesgo,
Optimización de los recursos utilizados por la organización en la prevención de riesgos.			
Reducción de costos, gracias a la disminución de incidentes o eventos generadores de riesgos.		**Actuar**	Tratamiento del Riesgo, Registro e Informe
Aprovechamiento de nuevas oportunidades.			
Mejora de la planificación y reducción de incidentes generadores de pérdidas inesperadas			

Fuente: Elaboración propia (2021)

Con base a las especificaciones contenidas en las normas 31000 y 27005, se creará un software que ayude a la gestión de riesgos en la práctica del derecho forense. El cual albergará la información necesaria y estará a disposición de los usuarios a través de un sitio web. Su diseño instrucciones analizará los riesgos de la práctica del derecho forense, permitiendo así mayor fluidez y seguridad en las practicas durante el proceso.

4. INFRAESTRUCTURA PARA EL DISEÑO DEL SOFTWARE

La creación de un software aplicado a la gestión de riesgos del derecho, será bajo el enfoque descrito anteriormente, es decir, los ISO 31000 e ISO 27005, los cuales podrán usarse en las prácticas del derecho forense. Para el diseño del software de gestión de riesgos, se hará un diseño de la arquitectura de red, es decir, diseñar como se va dar la relación entre cliente y servidor, o dicho de otra forma, entre el solicitante de información y el proveedor de información. La arquitectura de red permitirá obtener información del usuario, enviar la información del usuario a la lógica de negocio para su procesamiento, recibir los resultados del procesamiento de la lógica de negocio y pre-

sentar estos resultados al usuario.

Lujan (2001), refiere que la arquitectura de red es un conjunto de procesos conectados de la demanda de información, por ejemplo, entre el cliente y el servidor en la que cada ordenador o proceso en la red es cliente o servidor. Los servidores son computadoras super potentes dedicadas a gestionar el tráfico de datos, de red, discos de ficheros, impresoras, aplicativos móviles entre otras cosas. Los clientes son computadoras, con menos capacidad, que se basan en los recursos que ofrecen los servidores. La arquitectura es pues, la relación de procesos de demanda y satisfacción de la demanda.

• Cliente: Son los terminales que realizan peticiones al servidor, solicitando un determinado servicio. Para aplicaciones Web, las peticiones se realizan a través de interfaces, las cuales son páginas Web interpretadas y mostradas por navegadores Web como Mozilla Firefox o Google Chrome.

• Servidor: Es el computador encargado de responder con sus propios recursos las peticiones de los usuarios es decir de forma directa, por lo tanto, no requiere de otra aplicación o servicio para generar estas respuestas. (Maguiña, 2017, p. 10). Los servidores no solo son materiales y/o computadores, sino también software. Es decir, programas informáticos que procesan información y cumplen con la demanda de información de los clientes. Estos servidores web realizan conexiones bidireccionales o unidireccionales con el cliente que ofrecen diseños de páginas web con información como enlaces, imágenes, videos y música entre otros. Para el diseño del software se usará el Lenguaje Unificado de Modelado (UML), con el cual se buscará especificar, visualizar, y construir los elementos de un sistema de software. Es decir, se dará el contenido a la interface del software, con lo que se diseñará la operabilidad del software.

Cuadro II. Elementos del diseño del software

Software	Características
Lenguaje de programación	PHP VER. 7.5
Servidor	Apache 3.5
Sistema operativo	Chrome
Servidor de base de datos	MySQL Server 7.5
Editor PHP	PSPAD ver. 5.1
Diseñador de base de datos	MySQL Workbench 6.2
IDE de manejo de datos	MySQL Workbench 6.2

Elaboración propia (2021)

4.1 Lenguaje UML

El UML es un lenguaje de programación, que está compuesto por elementos gráficos combinables que forman diagramas. Ya que el UML es un lenguaje que cuenta con reglas para combinar tales elementos. La finalidad es presentar múltiples perspectivas de un sistema, a las cuales se les conoce como modelo. Un modelo es una representación simplificada de la

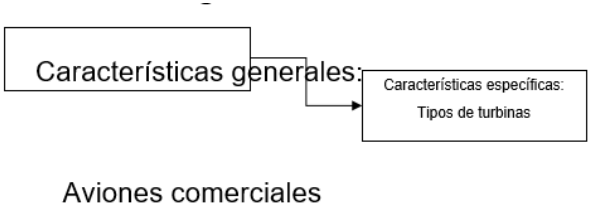
realidad; el modelo UML describe lo que supuestamente hará un sistema. El diagrama que se usará para este software será el diagrama de clases. Para desarrollar el diseño del software de gestión del riesgo, será considerado el modelo UML.

4.2 El diagrama de Clases

Un diagrama de clases tiene el propósito de describir las clases que conforman el modelado de un sistema informático, el diagrama se crea y se refina durante las fases de análisis y diseño, estando presente como guía en la implementación del sistema. (García y Pardo, 2018)

Los diagramas de clases recrean la estructura estática de un sistema. Las cosas que existen y que nos rodean se agrupan naturalmente en categorías. Una clase es una categoría o grupo de cosas que tienen atributos (propiedades) y acciones similares. Un ejemplo puede ser la clase "Aviones" que tiene atributos como el "modelo de avión", "la cantidad de motores", "la velocidad de crucero" y "la capacidad de carga útil". Entre las acciones de las cosas de esta clase se encuentran: "acelerar", "elevarse", "girar", "descender", "desacelerar". Un rectángulo es el símbolo que representa a la clase, y se divide en tres áreas. Un diagrama de clases está formado por varios rectángulos de este tipo conectados por líneas que representan las asociaciones o maneras en que las clases se relacionan entre sí.

Diagrama I. Estructura estática del sistema de clase



Cuadro III. Modelo de clases UML

CARACTERÍSTICAS	⟷	PROCESOS
Característica #1	⟷	Proceso #1
Característica #2	⟷	Proceso #2
Característica #3	⟷	Proceso #3

El diseño del modelo de diagrama de cuadros presentado, es la relación de generalización/especialización entre clases. En UML el modelo se representa mediante una flecha, cuya punta es un triángulo vacío. La flecha que representa el modelo va orientada desde la subclase a la superclase. Cuando de una superclase se derivan varias subclases existen dos notaciones diferentes. En la primera forma de representar esta situación se muestra una superclase a la que llegan tantas flechas como clases derivadas tiene. En la segunda representación se tiene una única punta de flecha que llega a la superclase, pero a la base del triángulo que hace de punta de flecha llegan tantos caminos como subclases haya. (García y Pardo, 2018)

5.RUP COMO DISCIPLINA PARA LA GESTIÓN DE PROYECTOS

El Rational Unified Process (RUP), es una disciplina encargada de asignar tareas y responsabilidades en una empresa, para la gestión de proyectos, a través de iteraciones tempranas se estiman tareas y horarios. Las iteraciones tempranas del RUP, se encargan principalmente del desarrollo del software -arquitectura-. El método RUP, se basa en cuatro fases: Inicio (alcance del proyecto), elaboración (análisis, definición y diseño del proyecto), construcción (implementación del proyecto), y transición (cierre del proyecto y producción). (Común y Bruno, 2016)

Entre sus principales características RUP se puede denotar el quien hace, que hace, cuando y como lo hace, se puede ver en esta metodología de desarrollo el desarrollo iterativo n veces, poder administrar requisitos, uso de arquitectura basada en componentes, control de cambios, modelado visual de software y verificación de la calidad del software.

El proceso iterativo e incremental consta de una secuencia de iteraciones. Cada iteración aborda una parte de la funcionalidad total, pasando por todos los flujos de trabajo, cada iteración al final es evaluada donde se pueden determinar si han aparecido nuevos requisitos o se deben realizar cambios a los existentes, afectando por lo tanto a las iteraciones siguientes, toda la retroalimentación de la iteración pasada permite reajustar los objetivos para las siguientes iteraciones, se observa en la imagen la manera en que funciona el ciclo de vida RUP. (Ibid)

6.RUP COMO DISCIPLINA PARA LA GESTIÓN DE PROYECTOS

El software deberá cumplir con las siguientes especificaciones, basadas en la norma ISO 31000, con las cuales se protegerá la información y gestionará los riesgos. En primer lugar, el software creara y protegerá el valor de la información, contribuyendo a los objetivos del software, como son la seguridad y la gestión de riesgos las cuales son importantes para garantizar el buen desarrollo de la práctica forense del derecho y llevar a tomar decisiones asertivas para que los resultados sean los más adecuados. En segundo lugar, Los procesos del software deberán estar integrados a la red de procesos de la organización. En tercer lugar, deberá controlar la

incertidumbre y mejorar la toma de decisiones. EN cuarto lugar, ser sistemático, estructurado y adecuado, brindando eficiencia y fiabilidad a los resultados. En quinto lugar, Estar hecha a medida. La gestión del riesgo está alineada con el contexto externo e interno de la organización y con su perfil de riesgo. En sexto lugar, Ser dinámica, iterativa y sensible al cambio. La organización debe velar para que la gestión del riesgo detecte y responda a los cambios de la empresa y de su entorno. Y en séptimo lugar, facilitar la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización.

7.SITIO WEB

Un sitio web es un conjunto de páginas relacionadas entre sí, es decir ficheros y sus recursos (imágenes, textos, videos, etc.). Las páginas web son creadas a partir de un lenguaje de programación, en este caso HTML, cuyos contenidos pueden ser iniciales (pagina de entrada) o principales (menú).

La página inicial, conocida como splash page en inglés, es la primera página que un usuario ve al visitar un sitio web. Normalmente, la página inicial se emplea para promocionar la compañía u organización a la que pertenece el sitio web, o para dar a conocer un producto o servicio particular (por ejemplo, para promocionar unos productos en oferta). También se suele emplear para informar al usuario de los requisitos (tipo y versión de navegador, resolución mínima, etc.) necesarios para visualizar correctamente el resto de páginas del sitio web. (Lujan, 2001, p. 62)

8. RIESGOS DE LA PRÁCTICA DEL DERECHO

Riesgo, según la Real Academia de la Lengua Española, significa contingencia o proximidad de daño. Todas las actividades humanas conllevan cierto riesgo, algunos más notorios que otros, unos son evidentes, y por ello se les pone más atención, y otros menos evidentes, y por ello menos atendidos. Las profesiones y oficios tienen sus propios riesgos, inherentes a ellos, y la profesión del derecho no es ajena a ello. La práctica del derecho, así como del derecho forense, conlleva asociados unos riesgos inherentes a la profesión, gestionar estos riesgos es importante para garantizar el buen desarrollo de la práctica forense del derecho y llevar a tomar decisiones asertivas para que los resultados sean los más adecuados. Los riesgos más comunes en el derecho, tiene que ver con la salvaguarda de la información, el secreto profesional.

El riesgo no tiene una forma definida, son percibidos como una situación poco clara, indefinida, por ello, tampoco se les puede dar una solución precisa, a menos que este a punto de suceder o este sucediendo, es decir, se haya materializado el riesgo. Las instituciones jurídicas, deben estar atentas a la mitigación de los riesgos para la sociedad, por ello deben de crear y reformular leyes y normas para salvaguardar a la sociedad (Beck, 1998; Hefendehl, 2002). Por otro

lado, es importante medir el riesgo de reincidencias delictivas, y con ella proteger el futuro de la sociedad. Existe reincidencia delictiva, en muchos exclusos, por lo que es menester de las ciencias jurídicas evaluar esos riesgos, y tomar decisiones oportunas (Martínez, 2016; Soler-González, 2018).

En base a los riesgos dentro del ejercicio profesional del derecho es necesario el desarrollo de un software que ayude a las instituciones jurídicas, a manejar y gestionar los riesgos inherentes a ellas. Por ende, la aplicación de los conocimientos de la ingeniería de software en conjunto con la ciencia jurídica permitirá gestionar esos riesgos. Así mismo, desarrollar estas actividades bajo el enfoque de las normas ISO 1000:2018 e ISO 27005:2008, se logrará mitigar los riesgos dentro del campo jurídico. (Martínez y Montes, 2018)

8.1 Procesamiento del riesgo

Para procesar los riesgos, el software creado realizara la filtración de la información a través de categorías, como riesgo, delito, proceso, contingencia, reincidencia entre otras. El software será utilizado por los abogados, secretarias, clientes y administradores.

La información será filtrada y almacena en carpetas, a las cuales se añadirán archivos con leyes o normas correspondientes, así como dependencias jurídicas, e instituciones conexas.

8.2 Admisibilidad para el uso del software durante el Proceso

Los administradores serán aquellos que administren la información y gestionen la apertura de cuentas de los abogados, secretarias y clientes, que serán los usuarios de las cuentas del software.

Cuadro IV. Operarios del software

ADMINISTRADOR	GESTIÓN DE LA INFORMACIÓN Y CUENTAS
Descripción de funciones	El administrador crea usuarios, modifica o elimina según sea requerido. Así como, almacenará y guardará la información
Procedimiento de ingreso	-Iniciar sesión como Administrador -Seleccionar la pestaña de "Usuarios" -Seleccionar la opción "Crear" -Ingresar los datos -Seleccionar "Aceptar" -Terminar sesión
Proceso de edición de cuentas e información	-Iniciar sesión como Administrador -Seleccionar la pestaña de "Usuarios" -Seleccionar Usuario a editar -Edita los campos -Seleccionar "Aceptar" -Terminar sesión
Proceso de eliminación de cuentas e información	-Iniciar sesión como Administrador -Seleccionar la pestaña de "Usuarios" -Seleccionar Usuario a eliminar -Selecciona la opción "Eliminar" -Seleccionar "Aceptar" -Terminar sesión

USUARIO	Adición y sustracción de información y uso de cuenta
Descripción de funciones	El usuario utilizará la cuenta para introducir y sustraer información sobre los riesgos.
Procedimiento de ingreso	-Iniciar sesión como Usuario -Seleccionar la pestaña de archivos -Seleccionar la opción cargar, descargar o modificar archivo -Ingresar los datos -Seleccionar "Aceptar" -Terminar sesión

Elaboración propia (2021)

De esta forma se utilizará el software, para gestionar los riesgos. La creación de un software basado en los ISOS 31000:2018 e ISO 27005:2008 para la gestión de riesgos en el ejercicio del derecho será importante para poder mitigar los riesgos. El software, es un ejemplo del uso de la ingeniería de software dentro del campo del derecho para crear valor y salvaguardar la información.

9. ANÁLISIS Y CONCLUSIONES

Crear un software para la gestión de riesgos dentro del ejercicio de las ciencias jurídicas, presenta el siguiente desafío, hacerse con conocimientos de otra disciplina, así mismo, combinarla con la propia ciencia para crear un conocimiento útil.

Del mismo modo, la creación del software para la gestión del riesgo, es la creación de una herramienta útil para para cualquier disciplina, y por lo tanto para las ciencias jurídicas. En base a lo expuesto en este artículo, podemos afirmar que la creación del software sirva para creación del valor al interior de las organizaciones y para protección de la información. Es en base a ello, creemos que conseguir mitigar los riesgos y sus efectos adversos es de suma importancia, ya que esta manera el profesional será más seguro. Por otro lado, el uso del software será amigable, y será fácil de usar.

La integración e implementación de las normas ISO usadas para el desarrollo del presente artículo, ayudaran a la perfectibilidad de las organizaciones publicas y privadas a mejorar continuamente los procesos que en estas se desarrollan; de esta forma creado y asegurando el valor de los procesos, así como de sus activos, en este caso la información, facilita la gestión de los riesgos que amenazan la información. Por lo que además, se debe considerar la aplicación de la metodología PHVA, puesto que su implementación ayuda al manejo de la eficiencia de los proceso y su implementación, así como, coadyuvando a las referidas a la eficacia y eficiencia de los mismos mejoras realizadas.

BIBLIOGRAFÍA CITADA

Adelaide South Australia, January 2010. School of Computer and Information Science. Division of Information Technology, Engineering, and the Environment, University of South Australia, pág. 19.

Beck, U. (1998). La sociedad del riesgo. Hacia una nueva modernidad. Paidós, España.

Común, U. Bruno, I. (2016). Desarrollo de un sistema de información, basado en la metodología RUP para mejorar el proceso de matrícula en el colegio Von Humboldt del Sur. (Tesis de licenciatura), Universidad Autónoma del Perú, Perú

García, F. y Pardo, C. (2018). Diagramas de Clase en UML 1.1. Universidad de Burgos, España.

Gerencie (2020) Ciclo PHVA. Recuperado de: https://www.gerencie.com/ciclo-phva.html#:~:text=El%20ciclo%20PHVA%20o%20ciclo,%2C%20Do%2C%20Check%2C%20Act.

Hefendehl, R. (2002) ¿Debe ocuparse el derecho penal de riesgos futuros? Revista Electrónica de Ciencia Penal y Criminología, 14(4), 1-13

ICONTEC (2008). Norma Técnica Colombiana NTC-ISO/IEC 27005:2008. Recuperado de: http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001071&ruta=/documentacion/0000001359/0000000107

ISOTOOLS EXCELLENCE (2017). La norma en Gestión de Riesgos ISO 31000 y sus beneficios. Recuperado de: https://www.isotools.org/2017/10/15/gestion-de-riesgos-iso-31000-y-sus-beneficios/

ISOTOOLS EXCELLENCE (2017). La gestión de la seguridad de la información. Recuperado de: https://www.isotools.org/2015/10/05/como-implantar-eficazmente-la-norma-iso- 27005/#La%20norma%20ISO%2027005%20es,definidos%20en%20la%20ISO%2027001

Luján, S. (2001). Programación en Internet: clientes web. Alicante: Editorial Club Universitario

Maguiña, R. (2017). Análisis y diseño de un sistema de gestión documentaria para un estudio de abogados. (Tesis de licenciatura), Universidad de Piura, Perú.

Martínez, L. (2015). Errores conceptuales en la estimación de riesgo de reincidencia. La importancia de diferenciar sensibilidad y valor predictivo, y estimaciones de riesgo absolutas y relativas. Revista Española de Investigación Criminológica, 3(14), 3-31

Martínez, L y Montes, F. (2018). El uso de valoraciones del riesgo de violencia en Derecho Penal: algunas cautelas necesarias, In-Dret Revista Para El Análisis Del Derecho, 1-47. Recuperado desde file:///C:/Users/raque/Downloads/337780-Text%20de%20l'article-486166-1-10-20180523.pdf

Soler-González, R. et al (2018). La gestión de riesgo: el ausente recurrente de la administración de empresas. Revista Ciencia UNEMI, 11(26), 51-62