Formulación de un modelo metodológico para gestionar los riesgos en las aplicaciones móviles.

Yazmín Lulú Álvarez Sánchez[1]

Andrés Mauricio Sanjuan Durán[2]

RESUMEN

En este artículo el objetivo principal es proponer un modelo metodológico para la gestión de riesgos en el desarrollo e implementación de aplicaciones móviles para aquellas organizaciones dedicadas al desarrollo de las mismas. Hoy día las empresas reconocen el gran beneficio que tiene el utilizar soluciones tecnológicas para fortalecer su sistema de negocio. Considerando el auge que tiene las aplicaciones móviles, es necesario diseñar modelo metodológico que nos permita gestionar los riesgos que se pueden presentar al momento de desarrollar e implementar en las empresas dichas aplicaciones y de esta manera poder reducir el riesgo que pueda presentarse, debido a que se puede tener consecuencias lamentables dentro una organización, los riesgos que pueden presentarse son muchas, esto conforme al tipo de aplicaciones móviles a las que se le puede gestionar los riesgos. El alcance del artículo parte de los problemas de riesgos que se presentan en las aplicaciones móviles y los planes para la gestión de riesgos que debe tener las organizaciones que utilizan las aplicaciones móviles para el buen funcionamiento de sus organizaciones. La metodología propuesta CVEM, enmarca la realización de una guía para la realización de la gestión de riesgos en aplicaciones móviles dentro de las organizaciones. Dentro de los resultados obtenidos esta la caracterización de riesgos y su clasificación, que permitió limitar el alcance del proyecto, posteriormente se validaron los dominios de la norma ISO 31000(**2018 ADMINISTRACIÓN Y GESTIÓN DE RIESGOS**) para poder encontrar los controles que cubrirán esas vulnerabilidades, mediante el plan de gestión de riesgos.

Palabras claves: Aplicaciones móviles, Gestión de riesgos, Metodología, tecnología**.**

---

[1] Yazmín Lulú Álvarez Sánchez, Ingeniera de Sistemas - Universidad Popular del Cesar , Estudiante de la Especialización en Auditoria de sistemas de la Universidad Antonio Nariño.

[2] Andrés Mauricio Sanjuán Duran, Ingeniero de sistemas de la Fundación Universitaria San Martín Sede Caribe, Estudiante de la Especialización en Auditoria de sistemas de la Universidad Antonio Nariño.

ABSTRACT

In this article the main objective is to propose a methodological model for risk management in the development and implementation of mobile applications for those organizations dedicated to their development. Nowadays, companies recognize the great benefit of using technological solutions to strengthen their business system. Considering the rise of mobile applications, it is necessary to design a methodological model that allows us to manage the risks that may arise when developing and implementing these applications in companies and thus be able to reduce the risk that may arise, because it can have unfortunate consequences within an organization, the risks that can arise are many, this according to the type of mobile applications to which the risks can be managed. The scope of the article is based on the risk problems that arise in mobile applications and the risk management plans that organization that use mobile applications must have for the proper functioning of their organizations. The proposed methodology CVEM, frames the realization of a guide for carrying out risk management in mobile applications within organizations. Among the results obtained is the characterization of risks and their classification, which allowed limiting the scope of the project, subsequently the domains of the ISO 31001 standard (2018 RISK ADMINISTRATION AND MANAGEMENT) were validated in order to find the controls that will cover these vulnerabilities, through the risk management plan.

Keywords: Mobile applications, Risk management, Methodology, technology.

INTRODUCCIÓN

El enfoque sobre gestión de riesgos en aplicaciones móviles se ha convertido en tema de estudio importante, donde la movilidad es una prioridad, en especial en las fuerzas comerciales. Con el avance tecnológico desarrollado a grandes pasos en el tiempo se exige acceso a la información de manera inmediata a través de las aplicaciones móviles del comercio, lo que les permiten ser más productivos con el fin de fortalecer las estrategias de negocio; debido a esto la gestión de riesgos es una actividad clave para garantizar y proteger la continuidad del negocio, los activos de información de la organización, las bases de datos, la infraestructura de red y las aplicaciones; toda compañía se encuentra constantemente expuesta a una serie de

riesgos y amenazas surgidas del uso de tecnologías de la información y las comunicaciones, creando la necesidad de proteger dichos activos, lo que la ha convertido en base importante para la cultura organizacional lo que logra aportar herramientas que contribuyen al logro de los objetivos y mejorar el desempeño de las organizaciones, a través de la revisión de sus sistemas de gestión y sus procesos, con el fin de visibilizar el mundo de eventualidades potenciales en lugar de hacer foco sobre las no conformidades ocurridas, únicamente. Como consecuencia, a nivel organizacional es de vital importancia realizar un análisis y gestión de riesgos sobre el parque de aplicaciones móviles, cuyo resultado conlleve a la implementación de controles apropiados, estableciendo las directrices para la implementación de una cultura organizacional, que permita proteger la privacidad de los usuarios lo que se vuelve cada vez más importante ante las numerosas amenazas que se puedan presentar al desarrollar apps móviles. El objetivo de este artículo es formular un modelo metodológico para gestionar los riesgos en las aplicaciones móviles. ¿Cómo sería una metodología apropiada a la gestión de riesgos para las aplicaciones móviles? Con base a esta necesidad planteada, en este artículo se presenta un modelo metodológico para la gestión de riesgos a aplicaciones móviles, estableciendo las directrices que permitan a la organización cumplir con las necesidades propias del negocio en sus diferentes áreas bajo un entorno seguro, maximizando las posibilidades de éxito y minimizando la pérdida de oportunidades. Para el desarrollo de este artículo se ha determinado usar el método empírico analítico, que es uno de los modelos para describir el método científico, basado en la experimentación y la lógica empírica. Junto a la observación de fenómenos y sus análisis estadísticos, cuyo enfoque está marcado por un estilo de pensamiento sensorial, por una orientación concreta-objetiva hacia las cosas, por un lenguaje numérico- aritmético, por una vía inductiva y por unas referencias de validación situadas en la realidad objetiva. (Pérez, 2016, p. 102).

METODOLOGÍA

El tipo de estudio que se aplicó a lo largo del desarrollo de este artículo fue Metodología de Gestión de Riesgos, ya que a través de ella se describen las directrices a seguir para la formulación de un modelo metodológico para la gestión de riesgos en las aplicaciones móviles. El artículo asimismo tiene un carácter documental, por tanto, se hizo un análisis documental que implicó “hacer una revisión previa de los estudios anteriores y de literatura relacionada que

permitió establecer que se ha dicho sobre el tema propuesto, desde que punto de vista y con qué resultados" (Galeano, 2004, pág. 116). A su vez tiene un carácter propositivo, pues formuló un modelo metodológico para la gestión de riesgos en aplicaciones móviles. Para dar cumplimiento a los objetivos específicos, la principal técnica de investigación fue la revisión documental, la cual tuvo como objetivo realizar una revisión de la literatura asociada con el tema, y tenía como propósito ubicar, clasificar y analizar la información detectada. El compendio de documentos con los cuales se realizó esta revisión documental, se conformó a partir de búsquedas sistemáticas en bibliotecas, además de rastreos en los principales motores de búsqueda y bases de datos disponibles en red, tales como SciELO, Dialnet, World Wide Science y Google Scholar. Los documentos encontrados fueron categorizados según su relevancia para los propósitos de este trabajo, en todo el trabajo de rastreo y ubicación de la información se priorizó la búsqueda de fuentes autorizadas, tales como libros, artículos de revista indexadas, investigaciones, tesis, y en general, documentación validada que aportaron elementos para la elaboración de este artículo.

Para dar cumplimiento al primer objetivo se realizó una revisión bibliográfica tendiente a identificar las características relevantes que deben cumplir las aplicaciones móviles en cuanto a su estructura y sus definiciones, diferentes usos y funcionamiento. Para el segundo objetivo se realizó una revisión bibliográfica que identificó las directrices a nivel organizacional para la gestión de riesgos y vulnerabilidades de las aplicaciones móviles con énfasis en las aplicaciones escogidas como objeto de estudio. Y para el tercer objetivo se permitió describir el modelo metodológico propuesto para la identificación de riesgos en aplicaciones móviles.

RESULTADOS

Aplicaciones Móviles

Una aplicación móvil o App, como comúnmente se le denomina, es "un software diseñado para funcionar en teléfonos inteligentes y otros dispositivos móviles" (San Mauro et al. 2014), generalmente se acepta que no todas las aplicaciones móviles son programas y que no todos los programas son aplicaciones móviles; una aplicación móvil es una pieza de software diseñada para cumplir un propósito específico o para facilitar una tarea determinada, mientras que un programa es una pieza de software que se diseña para cumplir una serie de tareas o para suplir un requerimiento más general. El desarrollo de aplicaciones móviles se ha expandido en los últimos 10 años, y las empresas encargadas de diseñarlas intentan realizar cada vez más mejoras al punto

que hay una gran competitividad entre ellas. De esta manera, las aplicaciones móviles y la telefonía móvil se han expandido y los individuos se ven abocados a su uso en la mayoría de los entornos que normalmente frecuentan. El principal tipo de clasificación de aplicaciones móviles son los tipos, entre ellas se encuentran las nativas, las híbridas y las web, y se extiende a todos las aplicaciones sin importar la empresa que las distribuye, ya sea Google, Apple, Blackberry, etc.

El tipo de desarrollo de aplicaciones, se refiere a la naturaleza del fabricante, es decir, si las aplicaciones fueron diseñadas para el SO del dispositivo o por el contrario fueron diseñadas para ser compatibles con cualquier SO. En la década de los 1990 aparecen las primeras aplicaciones móviles, éstas eran herramientas básicas, bastante simples en términos de usabilidad y diseño, entre ellas había apps diseñadas para cumplir las funciones más elementales del teléfono como gestores de contactos, editores de ringtone, entre otros. En el año 2007 la reconocida empresa Apple lanza su teléfono Iphone, a partir de allí, se dio comienzo a un mercado que cada vez está más extendido y que progresivamente presenta mejores y más funcionales aplicaciones. En "el año 2008 (…) se lanzó la App Store de Apple, una tienda virtual de apps donde los desarrolladores podían publicar sus aplicaciones y los usuarios descargarlas" (Herranz, 2017, pág. 7), mediante este programa Apple brinda la posibilidad de obtener aplicaciones externas y es así como Apple permite a los desarrolladores de aplicaciones desde cualquier país, promover su apps y las ventas de la misma. A partir de las innovaciones de Apple, otras empresas descubren un mercado con altísimo potencial, es así como Google con su SO Android emerge el dicho mercado y desarrolla la tienda Play Store, cuya ventaja es que muchas de sus aplicaciones son libres y tienen alta compatibilidad, no así las de su competencia de Apple. Dicha circunstancia conduce a un aumento en el alcance de las aplicaciones Android y contribuye a establecer un claro dominio del mercado de las apps. Dadas estas circunstancias, lo que comienza con unas pocas aplicaciones con una funcionalidad restringida, termina con millones de aplicaciones que cumplen múltiples funciones que favorecen a los usuarios, e incluso la creación de apps por parte de los usuarios de las mismas.

Aplicaciones Móviles para Android: Todas las aplicaciones para dispositivos Android, "están encapsuladas en un formato específico, conocido como APK «Application PacKage File»" (Erazo & Betancur, 2015, pág. 30), el formato APK es el utilizado para instalar y distribuir las aplicaciones de esta plataforma y aunque es un formato exclusivo para SO Android, es

compatible con múltiples dispositivos móviles. El sistema operativo Android clasifica sus aplicaciones en 3 clases: “Primer plano o foregroung, segundo plano o background, y lo que es denominado como widget o apps widget” (Gallego, 2014). Dada la necesidad de disminuir las vulnerabilidades en las aplicaciones móviles, la gestión de riesgos nos permite determinar los posibles impactos que pueden generarse de las vulnerabilidades y amenazas, para identificar las contramedidas necesarias, de aquí la Gestión de los riesgos más críticos presentes en dichas aplicaciones.

Tabla 1.Ejemplo de Posibles Escenarios de Riesgos en Aplicaciones Móviles.

Posibles escenarios de Riesgo	Descripción
Malas prácticas de autenticación	Las funciones de las aplicaciones relacionadas con la autenticación de los usuarios, a menudo se implementan incorrectamente, lo que permite a los atacantes comprometer contraseñas, claves o tokens de sesión, o explotar otras fallas de implementación para asumir las identidades de otros usuarios de forma temporal o permanente.
Exposición de datos sensibles	Muchas aplicaciones web y API no protegen adecuadamente los datos confidenciales, como finanzas, salud y datos de sus clientes. Los atacantes pueden robar o modificar los datos que están débilmente protegidos para cometer fraude con tarjetas de crédito, robo de identidad u otros delitos. Los datos confidenciales pueden verse comprometidos sin protección adicional, como el cifrado en reposo o en tránsito, y requieren precauciones especiales cuando se intercambian con el navegador.
Pérdida de control de acceso	Las restricciones sobre lo que los usuarios autenticados pueden hacer a menudo no se aplican correctamente. Los atacantes pueden explotar estas fallas para acceder a funciones y / o datos no autorizados, como acceder a las cuentas de otros usuarios, ver archivos confidenciales, modificar datos de otros usuarios, cambiar derechos de acceso, etc.
Configuración de Seguridad Incorrecta	La mala configuración de la seguridad es el problema más común. Esto suele deberse a configuraciones predeterminadas inseguras, configuraciones incompletas o por “default”, almacenamiento en la nube abierta, encabezados HTTP mal configurados y mensajes de error detallados que contienen información confidencial. No solo todos los sistemas operativos, marcos, bibliotecas y aplicaciones deben estar configurados de manera segura, sino que deben ser parchados / actualizados de manera oportuna.
Deserialización Insegura	La Deserialización insegura a menudo conduce a la ejecución remota de código. Incluso si las fallas de Deserialización no dan como resultado la ejecución remota de código, se pueden usar para realizar ataques, incluidos ataques de repetición, ataques de inyección y ataques de escalada de privilegios
Uso de componentes con vulnerabilidades conocidas	Los componentes, como bibliotecas, marcos y otros módulos de software, se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, tal ataque puede facilitar la pérdida grave de datos o la toma de control del servidor. Las aplicaciones y las API que utilizan componentes con vulnerabilidades conocidas pueden socavar las defensas de las aplicaciones para permitir o facilitar ataques.
Registro de logs y monitoreo insuficientes	El registro y monitoreo insuficientes, junto con una mala integración de respuesta a incidentes, permite a los atacantes atacar aún más los sistemas, mantener la persistencia, girar a más sistemas y manipular, extraer o destruir datos. La mayoría de los estudios de infracciones muestran que el tiempo para detectar una infracción es de más de 200 días, típicamente detectado por partes externas en lugar de procesos internos o monitoreo.

Dado la presentación de estos posibles escenarios de riesgo, se hace necesaria la formulación de un modelo metodológico para la gestión de riesgos en las aplicaciones móviles logrando contribuir de alguna manera en la mitigación o disminución de los mismos.

Metodologías para Gestión de Riesgo

El proceso de gestión de riesgo comienza con la identificación de las amenazas. Para reconocerlas adecuadamente existen diversas metodologías de gestión de riesgos, que pueden clasificarse en dos: deductivos e inductivos. Normalmente se sigue un procedimiento para reconocer cuáles son los fallos y los errores, que permitirá establecer una solución para cada uno de estos eventos. Los siguientes son algunos de estos:

ISO 31000:2018 ADMINISTRACIÓN Y GESTIÓN DE RIESGOS[1]

Esta norma va dirigida a las personas que protegen el valor de las organizaciones gestionando riesgos, tomando decisiones, estableciendo y logrando objetivos y mejorando el desempeño. La administración gestión de riesgos está basada en los principios, el marco de referencia y el proceso descritos en este documento. La administración/gestión de riesgos es parte de todas las actividades asociadas con la organización e incluye la interacción con las partes interesadas.

ALCANCE: La norma ISO 31000:2018[1] proporciona directrices sobre la gestión del riesgo a la que se enfrentan las empresas. Las aplicaciones de diferentes pautas, pueden personalizarse para cualquier organización y su contexto.

Ventajas de implantar la norma ISO 31000:2018[1]

Una empresa que aplica todas las directrices de la normativa consigue:

- ✓ Mejorar su eficiencia operativa.
- ✓ Contar con la mejora gobernabilidad interna de la empresa.
- ✓ Incrementar la confianza de partes externas.
- ✓ Mejorar el rendimiento y la sostenibilidad.
- ✓ Acentuar la calidad.
- ✓ Minimizar los costes.

---

[1] **ISO 31000:2018 ADMINISTRACIÓN Y GESTIÓN DE RIESGOS** – Elaborada por la Organización Internacional de Normalización. Esta norma ofrece lineamientos guía para administrar/gestionar los riesgos a los que las organizaciones se enfrentan. La aplicación de estos lineamientos puede adaptarse a cualquier organización y a su contexto.

Tiene como finalidad, establecer lineamientos, directrices para la gestión de riesgos en esta se destacan las siguientes etapas para la gestión:

- ✓ **Establecer el alcance:** se refiere a que la organización debe definir la dimensión, los niveles o procesos en los que gestionará actividades para la gestión del riesgo.
- ✓ **Definir el contexto:** realizar el análisis de su entorno tanto interno como externo, para definir los factores que pueden ser origen de riesgos.
- ✓ **Evaluar el riesgo:** para ello se debe realizar inicialmente la identificación del mismo, posteriormente realizar un análisis mediante variables que definan el nivel del riesgo, y por último la valoración que implica comparar el resultado del riesgo en el análisis vs el resultado de la valoración para establecer panes de tratamiento.
- ✓ **Plan de tratamiento:** establecer actividades, responsables, metas y fechas de cumplimiento para dar respuesta a los riesgos encontrados.
- ✓ **Seguimiento y revisión:** monitoreo de los resultados y establecimiento de nuevos planes de tratamiento de ser necesario.

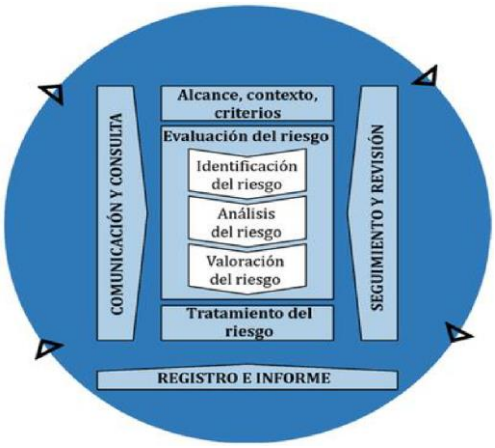

Figura 1. Proceso de Gestión de Riesgos
Fuente: Norma ISO 31000 (ISO, 2018, sección 6: Proceso)

---

[1] **ISO 31000:2018 ADMINISTRACIÓN Y GESTIÓN DE RIESGOS** – Elaborada por la Organización Internacional de Normalización. Esta norma ofrece lineamientos guía para administrar/gestionar los riesgos a los que las organizaciones se enfrentan. La aplicación de estos lineamientos puede adaptarse a cualquier organización y a su contexto.

Nota: En la figura 1. Se puede ver de manera clara el proceso de gestión del riesgo según Norma Internacional ISO 31000, dentro de los cuales están:

Identificación del riesgo: Es la parte del proceso de gestión de riesgos en la que conocemos e inspeccionamos los riesgos. El objetivo de la identificación del riesgo es conocer los sucesos que se pueden producir en la organización y las consecuencias que puedan tener sobre los objetivos de la empresa.
Análisis del riesgo: El análisis de riesgo involucra la consideración de las fuentes del riesgo, sus consecuencias y la probabilidad de que estas consecuencias puedan ocurrir.
Valoración del riesgo: permite la identificación y el análisis de los riesgos que enfrenta la institución para la consecución de los objetivos, tanto de fuentes internas como externas relevantes.
Tratamiento del mismo: El objetivo del tratamiento de riesgos según ISO 31000:2018 es diseñar, evaluar, seleccionar e implementar acciones para abordar los riesgos identificados dentro de una organización.

ISO 27005 GESTIÓN DE RIESGOS DE LA SEGURIDAD LA INFORMACIÓN

Este estándar esta principalmente dirigido a empresas aunque es útil para cualquier tipo de organización que desee mejorar su Sistema de Gestión de Seguridad de Información (SGSI) o que puedan sufrir ciertos problemas de seguridad en su empresa, para ello no es necesario aplicar toda la metodología del estándar, sino más bien centrarse en una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria. Por tanto, su principal objetivo es mejorar la gestión de riesgos de seguridad de la información en una organización dando a entender la metodología concreta para cada problema de seguridad de información, es decir, una metodología concreta no servirá para todos los problemas de Sistema de Gestión Riesgos de Seguridad de la Información en aplicaciones móviles. Establece lineamientos para la gestión de riesgos relacionados con la seguridad de la información, establece cuatro pasos fundamentales para la implementación de la misma:

- ✓ Establecer el contexto.
- ✓ Identificación de los riesgos relacionados con seguridad de la información.
- ✓ Análisis.
- ✓ Evaluación.

Al respecto también es importante tener en cuenta en el caso de los riesgos de seguridad de la información, establecer un inventario y calificación de activos de la información que se integran posteriormente a la gestión de los riesgos.

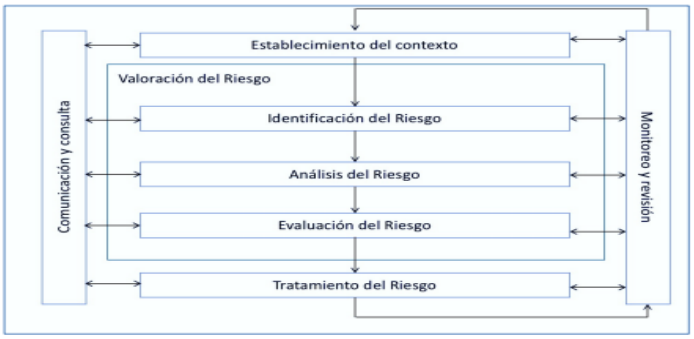

Figura 2. Procesos de gestión de riesgos según ISO 27005
Fuente: Norma ISO 27005

Nota: En la figura 2 podemos observa el proceso de gestión del riesgo según la norma Internacional ISO 27005 dentro de los cuales tenemos las etapas:

- **Definición de contexto:** es responsable de definir el ambiente, alcance, criterios de evaluación, y otros ajustes.
- **Análisis/Evaluación del riesgo:** permite la identificación del riesgo y la determinación de las acciones necesarias para reducir el riesgo a un nivel aceptable.
- **Tratamiento del riesgo**: los controles necesarios para el tratamiento del riesgo se definen a partir de los resultados obtenidos del análisis y la evaluación del riesgo.

La norma ICONTEC NTCISO/IEC 27001 especifica los controles que deberán ser implementados.

- **Aceptación del riesgo:** asegura los riesgos asumidos por la organización, estos se denominan riesgos residuales, cuya clasificación en esta categoría deberá justificarse.
- **Comunicación del riesgo:** se informa el riesgo y la forma como será tratado, para todas las áreas operacionales y sus gestores.
- **Seguimiento y análisis crítico:** son las actividades de acompañamiento de los resultados, implementación de controles y análisis crítico para el mejoramiento continuo del proceso de gestión del riesgo.

---

[1] **ISO 27005:2009 GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN –** Elaborada por la Organización Internacional de Normalización. Esta norma Proporciona directrices para la gestión del riesgo en una organización, dando soporte particular a los requisitos de un sistema de gestión de la seguridad de la información (SGSI) de acuerdo con la norma NTC-ISO/IEC 27001.

NORMA TECNICA COLOMBIANA NTC – ISO/IEC 27001:2013[1]

El diseño e implementación en una organización están influenciados por las necesidades y objetivos, los procesos empleados y el tamaño y estructura de una organización. Esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos. La adopción del modelo PHVA también reflejará los principios establecidos en las Directrices OCDE (2002)1 que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de gestión y reevaluación. Existen metodologías que apoyan la medición, la cuantificación de los riesgos, entre las más conocídas encontramos:

MAGERIT V3[1]: Metodología creada por Consejo Superior de Administración Electrónica de España, enfocada en la gestión de los riesgos relacionados con las tecnologías de la información y las comunicaciones, tomando en cuenta las dimensiones de disponibilidad, integridad y confidencialidad, establece un modelo que integra la gestión de riesgos con los pasos y lineamientos de la norma ISO 31000 y se complementa con la gestión de los activos que establece que se debe realizar una identificación , establecer la dependencia entre activos, y la valoración de los mismos.

INDICADOR CLAVE DE RIESGOS (KRI- KEY RISK INDICATORS)

En la gestión de riesgos, los KRI[2], ayudan a adelantarse en los problemas y/o oportunidades a las que tenga que enfrentarse una organización en el futuro, basándose en la observación de tendencias que puedan afectarles.

---

[1]**MAGERIT V3:** es la metodología de análisis y gestión de riesgos de los sistemas de información.

[2] Los indicadores de riesgo clave, conocidos como KRI (**Key Risk** Indicator), sirven para determinar el nivel de riesgo que tiene una organización ante una determinada amenaza o evento que pueda ocurrir e impactarle

Corresponde a indicadores que ayudan a conocer que tan posible es que se materialice un riesgo y el impacto que este generaría, ejemplo: el riesgo de interrupción del trabajo por causa de la interrupción del servicio de internet se podría medir de la siguiente forma, Horas acumuladas en el mes sin servicio de internet, para este tipo de indicadores es muy importante establecer los límites, ejemplo si el tiempo sin servicio es mayor o igual a 10 horas el riesgo es Alto, entre 5 y 9 horas es medio, y entre 0 y 5 horas es básico, es importante basarse en la mediciones históricas y establecer planes de tratamiento al respecto.

Para la gestión de Riesgos en aplicaciones móviles las normas mencionadas en el apartado anterior, permiten llevar a cabo el proceso de gestión de riesgos de manera ordenada y eficaz con el fin de lograr los objetivos de las organizaciones dentro de las cuales se desarrollan las aplicaciones móviles.

METODOLOGÍA PROPUESTA

Las organizaciones de todo tipo y tamaño enfrentan factores e influencias, internas y externas, que crean incertidumbre sobre si ellas lograrán o no sus objetivos. El efecto que esta incertidumbre tiene en los objetivos de una organización es el "riesgo". Todas las actividades de una organización implican riesgo. Las organizaciones gestionan el riesgo mediante su identificación y análisis; luego evaluando si el riesgo se debería modificar por medio del tratamiento del riesgo con el fin de satisfacer los criterios. A través de este proceso, las organizaciones se comunican y consultan con las partes involucradas, monitorean y revisan el riesgo y los controles que lo están modificando con el fin de garantizar que no se requiere tratamiento adicional para el mismo. Debido a la demanda de aplicaciones móviles que se desarrollan para diferentes usos, es necesario tratar el tema de gestión de riesgos. Para ello es necesario establecer una metodología apropiada que nos permita mirar de qué manera podemos realizar la gestión de riesgos en las aplicaciones móviles. Hoy día las aplicaciones móviles son vulnerables, por eso se necesita garantizar el buen funcionamiento de éstas para no correr riesgos. Es necesario que las organizaciones implementen unas políticas de gestión de riesgos para asegurar la continuidad del negocio en las aplicaciones móviles. Cuando utilizamos la gestión de riesgos podemos observar y planear con anticipación las posibles amenazas que pueda tener las

aplicaciones, tomando como ejemplo la norma internacional ISO 31000, proponemos la siguiente metodología que nos servirá como guía para la gestión de riesgos en aplicaciones móviles.

METODOLOGIA CVEM

La presente metodología permite documentar las actividades a realizar para la gestión del riesgo en aplicaciones móviles, tomando como referencia los pasos metodológicos de la norma internacional ISO 31000 (Gestión del riesgo Principios y Directrices).

Alcance: el alcance de esta metodología comprende la Gestión de Riesgo para aplicaciones móviles, en las organizaciones al igual que se pretende que esta metodología sea utilizada para armonizar los procesos de Gestión del riesgo en aplicaciones móviles.

Objetivo: Gestionar los riesgos en las aplicaciones móviles.

El modelo metodológico propuesto en este artículo se basa en la metodología de la norma ISO 31000, en el siguiente diagrama, se pone en contexto la metodología propuesta en este artículo dentro de cada etapa del ciclo.

Figura 3. Metodología para gestión de riesgos en aplicaciones móviles.

Fuente: Elaboración propia

Dentro de las etapas de la metodología propuesta tenemos las siguientes:

1. **CARACTERIZACIÓN DEL RIESGO**.

   Para el desarrollo de esta etapa se deben cumplir los siguientes procesos:

   1.1 Identificación del riesgo: Para las aplicaciones móviles, se deben identificar las fuentes de riesgo, las áreas de impacto, los eventos, causas y consecuencias potenciales, generando una lista de riesgos en base a dichos criterios. La identificación

del riesgo dependerá de la generación de una lista de posibles riesgos, donde se deben incluir todo tipo de riesgos independientemente de si su origen está bajo control o no. Para esto las organizaciones en las aplicaciones móviles deberán implementar técnicas y herramientas para la identificación de dichos riesgos adecuadas a sus objetivos y capacidades.

1.2 Análisis del riesgo: Mediante la exploración de todo el espacio de posibles resultados para una situación determinada, un buen análisis de riesgo puede identificar peligros y descubrir oportunidades. El análisis de riesgo es importante para la toma de decisiones, en donde las organizaciones en el caso de las aplicaciones móviles deberán elegir los diversos tipos y niveles de riesgo, involucrando las causas, fuentes, consecuencias y probabilidad de ocurrencia de las mismas. Sin embargo, durante el proceso de análisis de riesgo también se pueden descubrir resultados potenciales positivos. Mediante la exploración de todo el espacio de posibles resultados para una situación determinada, un buen análisis de riesgo puede identificar peligros y descubrir oportunidades. Habiendo ya identificado y clasificados los riesgos, se debe realizar el análisis de los mismos, es decir, se estudian la posibilidad y las consecuencias de cada factor de riesgo con el fin de establecer el nivel de riesgo. El análisis de los riesgos determinará cuáles son los factores de riesgo que potencialmente tendrían un mayor efecto sobre las aplicaciones móviles y, por lo tanto, deben ser gestionados con especial atención. Son las organizaciones las encargadas de establecer la tipología para realizar el análisis de riesgos de las aplicaciones móviles.

El enfoque utilizado dependerá de la naturaleza de las actividades bajo revisión y los tipos de riesgo, una vez definido el riesgo en su forma específica y medible. El análisis dependerá de la información disponible sobre el riesgo y de su origen. Para adelantarlo es necesario diseñar escalas que pueden ser cualitativas o cuantitativas. Teniendo la consecuencia de un riesgo bien definido se debe medir que tan importante y prioritario es gestionar el riesgo para las aplicaciones móviles, esto se realiza a través de dos variables:

- ✓ **Variable de probabilidad:** la probabilidad es de ocurrencia que tan probable es que el riesgo se materialice.

- ✓ **Variable de impacto:** el impacto es que tan grave es que el riesgo se materialice.

2. VALORACIÓN DE LOS RIESGOS

La valoración de los riesgos nos ayuda a establecer el nivel de criticidad de cada riesgo, en cuanto a las aplicaciones móviles permitirá clasificar los riesgos desde el más alto hasta el más bajo de acuerdo a la probabilidad de ocurrencia del mismo. Estos se pueden clasificar en altos medios y bajos de acuerdo a su criticidad definida como un indicador proporcional al riesgo que permite establecer la jerarquía o prioridades de procesos, sistemas y equipos, creando una estructura que facilita la toma de decisiones acertadas y efectivas, y permite direccionar el esfuerzo y los recursos a las áreas donde es más importante y/o necesario mejorar la confiabilidad y administrar el riesgo. *(Análisis de criticidad y estudio RCM del equipo de máxima criticidad de una planta desmotadora de algodón, s.f.).*

Una vez identificados todos los Riesgos y Oportunidades se debe determinar su valoración. Dado que los recursos para reducirlos suelen ser finitos, se necesita poder valorar cada uno de los riesgos para poder determinar su criticidad, y así dedicar los recursos disponibles en los más importantes.

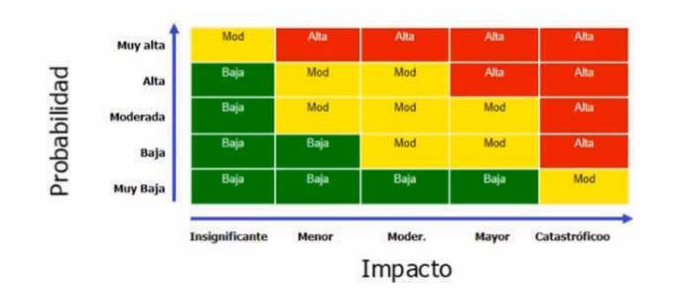

Figura 4. Matriz de administración de riesgos.

Fuente: https://www.ealde.es/matriz-evaluacion-riesgos/

Nota. En la figura 4. La matriz de riesgo nos sirve para tomar decisiones y establecer controles. Por medio de estos controles se pueden tomar medidas y mitigar el riesgo. Los colores indican la criticidad del riesgo desde el menos crítico hasta el más crítico, mediante la matriz de riesgo es posible evaluar la efectividad de la gestión de los riesgos

Tabla 2. Matriz de valoración del riesgo cruce de variables

Probabilidad				
	ALTO	M	A	A
	MEDIO	M	M	A
	BAJO	B	M	M
		BAJA	MEDIA	ALTA
		Impacto		

Fuente: Elaboración Propia

Nota. En la tabla 2, los riesgos se clasifican y los resultados que se obtienen salen de cruzar la variable e impacto, de esta manera se define la amenaza del riesgo.

3. EVALUACIÓN DE LOS RIESGOS

La evaluación de riesgos es un proceso mediante el cual se obtiene la información necesaria para estar en condiciones de tomar decisiones sobre la necesidad o no, de adoptar acciones preventivas, y en caso afirmativo el tipo de acciones que deben adoptarse. (Evaluación de Riesgos Laborales, 2015). Esta etapa permite que una organización tome decisiones respecto al tratamiento del riesgo, priorizando la mitigación del riesgo con facilidad. La evaluación de riesgos, toma en cuenta los criterios de riesgo y las medidas contra el análisis de riesgo para determinar:

- ✓ Qué riesgos tienen mayor prioridad.
- ✓ Efectividad de la definición de criterios.
- ✓ Éxito en el proceso de análisis de riesgos.
- ✓ Pautas para abordar los próximos pasos, (tratamiento de riesgos).
- ✓ El resultado de la evaluación de riesgos puede ser:
- ✓ Asignar más análisis.
- ✓ Mantener controles existentes.
- ✓ Reconsiderar los objetivos de la estrategia de riesgo en concordancia con los objetivos de la organización.

La evaluación periódica permite desarrollar una estrategia integral y madura de gestión de riesgos, ya que los cambios en los factores de riesgo, impacto, consecuencia y objetivos se pueden abordar en un plazo razonable. (Evaluación de riesgos en ISO 31000, 2017) En cuanto a

aplicaciones móviles se refiere, esta etapa nos permite detectar errores, por medio de un informe detallado en donde se muestre las falencias para luego hacer las recomendaciones de mejora para el uso de la aplicación. Los dos criterios clásicos que se utilizan para este tipo de evaluación, son la probabilidad y el impacto. Con un riesgo alto ya existe la probabilidad de que provoque aumentos significativos en el coste, el tiempo, el rendimiento y hay que tomar acciones significativas y en algunos casos de manera inmediata. Lo que se quiere lograr es transformar aquello que no sabemos en algo conocido, pero que no sabemos cuándo va a suceder, y tener claro que acción tomar en el momento que se haga realidad.

Para la evaluación de los riesgos existen tres tipos de métodos descritos en la figura 5.

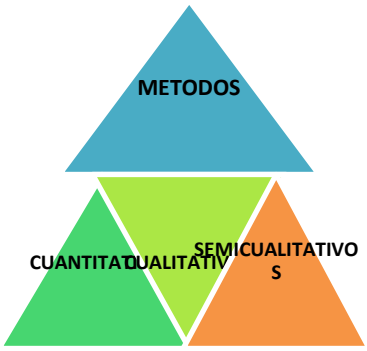

Figura 5. Métodos para evaluación de los riesgos

Fuente: Elaboración propia

En la figura 5 se muestra los diferentes métodos que pueden ser usados para la Evaluación de Riesgos en el caso de las aplicaciones móviles depende de la Organización la elección del método acorde a las características de las aplicaciones móviles la escogencia del método de evaluación de los riesgos.

Método cualitativo: En este el criterio y el conocimiento de expertos en el tema analizado es el imperante. Su principal ventaja se debe a su mayor facilidad de cálculo, al no implicar una valoración económica o de probabilidad.

Método semicualitativo: Se construye bajo un sistema de índices, teniendo en cuenta las situaciones que fueron analizadas para poder clasificar los riesgos que se puedan presentar, y a su vez, contar con un plan de acción.

Método cuantitativo: en este el análisis de riesgos es aquel que permite obtener una valoración numérica de la materialización de un evento, ya sea negativo o positivo, en términos de los criterios definidos, que pueden ser monetarios, operativos, técnicos, humanos, entre otros, lo que hace más tangible y objetivo el análisis.

En este artículo se tomo como referencia el método caualitavo, ya que estamos dando a conocer una metodología para poner en práctica, en gestión de riesgos a las aplicaciones móviles.

4. MITIGACIÓN DE LOS RIESGOS.

El proceso de tratamiento de riesgos consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos. Cualquier sistema de tratamiento de riesgos para aplicaciones móviles debe garantizar como mínimo:

- ✓ Un funcionamiento efectivo y eficiente de la aplicación móvil.
- ✓ Controles internos efectivos en el funcionamiento de las aplicaciones móviles
- ✓ Conformidad con las leyes y reglamentos vigentes.

(Análisis de Riesgos – Tratamiento del Riesgos, s.f.)

Esta etapa es vital dentro de la gestión de riesgos dado que el planear una respuesta para los riesgos de alta prioridad, nos ayuda a monitorizar los nuevos riesgos que puedan presentarse y ejecutar un plan de respuesta en el momento de la ocurrencia del riesgo. En muchas ocasiones la aparición de riesgos nos lleva a estar preparados y actualizar el plan de gestión de riesgos para cualquier organización, en este caso implementado para las aplicaciones móviles. Para la toma de decisiones con los riesgos identificados se tienen unos procesos de gestión de riesgos que sirven de guía y contienen la estrategia de mitigación, cada proceso depende del tipo de aplicación móvil. En esta etapa de mitigación del riesgo se pueden tomar 4 medidas diferentes:

- ✓ **Aceptación del riesgo:** decisión generada por la entidad de aceptar las consecuencias y probabilidad de un riesgo en particular, sin adelantar acciones de reducción y control.
- ✓ **Rechazo del riesgo:** decisión generada por la entidad de no aceptar las consecuencias y probabilidad de un riesgo en particular

- ✓ **Transferencia del riesgo:** e transfiere los riesgos asociados a un proyecto a una compañía de seguros y a una reaseguradora.
- ✓ Mitigación del riesgo: consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.

Si la empresa no toma una decisión, equivale a la aceptación del riesgo. La mitigación dentro del Proceso de Gestión de Riesgos trata de conducirlo a un nivel aceptable aplicando alguna de estas medidas. (El tratamiento de riesgos según ISO 31000, 2017).

Es necesario implementar la gestión de riesgo para las aplicaciones móviles, por esto es indispensable avanzar cada día para conocer, evaluar, encontrar y definir los riesgos de las aplicaciones y como mitigarlos, creando una comunidad que sea consciente de la inversión necesaria en la gestión de riesgos de aplicaciones móviles y compartiendo los resultados con el resto del mundo.

DISCUSIONES Y CONCLUSIONES

Es normal encontrar aplicaciones móviles con problemas de funcionamiento y debido a su gran auge, las empresas u organizaciones dedicadas al desarrollo e implementación de éstas, corren el riesgo de tener vulnerabilidades dentro de la misma organización. Es recomendable que las empresas implementen una buena política de gestión de riesgo para la mitigación de dichos eventos. Debe existir una relación costo beneficio al momento de implementar los controles que se crean necesarios para minimizar el riesgo de que las vulnerabilidades se materialicen, pues no es óptimo establecer controles que afecten de manera significativa la inversión de las organizaciones. El análisis en este artículo nos permite identificar las diferentes metodologías que pueden ser implementadas para gestión de riesgos y el tipo de fallas que podemos tener al no realizar un buen plan de gestión de riesgos en las aplicaciones móviles, al igual que un modelo metodológico con el que podemos llevar a cabo la gestión de riesgo en las aplicaciones móviles; y sobre todo el impacto que puede presentar en las organizaciones si no se tienen en cuenta las recomendaciones, para poder cumplir con satisfacción todos los requerimientos y poder así lograr los objetivos de cada organización en cuanto al desarrollo de aplicaciones móviles se refiere.

BIBLIOGRAFIA

- ✓ Amaya, D., (2013). Metodologías ágiles en el desarrollo de aplicaciones para dispositivos móviles. Estado actual. 12, pp. 111-124.
- ✓ Aponte, S. & Dávila, C. (2011). Sistemas operativos móviles: Funcionalidades, efectividad y aplicaciones útiles en Colombia. (Tesis de Pregrado) Universidad EAN, Facultad de Ingeniería de Sistemas, Bogotá Aranaz Tudela, J. (2009). Desarrollo de aplicaciones para dispositivos móviles sobre la plataforma Android de Google (Tesis de Maestría). Universidad Carlos Tercero, Madrid.
- ✓ BECERRA J. Germán. (1997) Auditoría de sistemas en el PAD. 2ª.ed. Editorial Edmez, Bogotá, Colombia, 110 p
- ✓ D´OLIVO y SAULEDA. Alternativa de participación de la auditoría interna en procesos de autoevaluación de controles, Uruguay
- ✓ ENYOYSAFERTECHNOLOGY, Eset Security Report Latinoamérica 2014 [en línea] 2014 Disponible en http://www.welivesecurity.com/wpcontent/uploads/2014/06/informe_esr14.pdf
- ✓ GUTIÉRREZ, SOLIS Y PORTAL. El rol del auditor interno en los procesos de autoevaluación de controles. México D.F.
- ✓ International Organization for Standardization. (2018). ISO 31000, Risk management.
- ✓ Lefcovich, M. (2009). La gestión del Riesgo. ed. Córdoba: El Cid Editor. Biblioteca UAN.
- ✓ OWASP, Los diez riesgos más críticos de Aplicaciones Web [en línea] 2013 Disponible en https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf
- ✓ RAMOS P, La realidad de la seguridad empresarial en Latinoamérica: ¿qué debemos hacer? [en línea] 2016 Disponible en http://www.welivesecurity.com/laes/2016/04/29/seguridadempresarial-latinoamerica-que-hacer/
- ✓ Universidad Nacional Autónoma de México. (nf). Capítulo III: Riesgos Informáticos. https://archivos.juridicas.unam.mx/www/bjv/libros/2/909/5.pdf