La importancia para la gestión de riesgos en entidades financieras

Erika Brissett Pardo Ramírez.
Brissett1@hotmail.com;
Especialización en Seguridad Informática
Universidad Piloto de Colombia – Bogotá, Colombia.

Resumen— Actualmente, las entidades financieras han optado por hacer una adecuada gestión de riesgos lo cual les permite conocer las vulnerabilidades y amenazas frente al negocio. Al tener identificados los riesgos podrán establecer medidas que puedan garantizar mayores niveles de seguridad de la información. Existen varias metodologías para la gestión de riesgos y algunas normas con enfoque de soporte a cuáles serán concertadas en este artículo. Al implementar estas metodologías y normas permitirán un mayor control y protección para los servicios tales como: inversiones de capital y gastos operacionales. Este artículo provee un panorama un poco más comprensible de las integraciones de los modelos y estándares, así como las semejanzas que existe entre estos.

Índice de Términos— gestión de riesgos, estándares, riesgo inherente, riesgo residual

Abstract — Currently, financial institutions have opted to do an adequate risk management which allows them to know the vulnerabilities and threats against the business. By having identified the risks, they can establish measures that can guarantee higher levels of information security. There are several methodologies for risk management and some standards with a support approach to which will be agreed in this article. By implementing these methodologies and standards will allow greater control and protection for services such as: capital investments and operational expenses. This article provides a slightly more comprehensible picture of the integrations of the models and standards, as well as the similarities that exist between them.

I. Introducción

En este momento, las entidades financieras hacen uso de la tecnología en sus procesos principales del negocio para el almacenamiento y tratamiento de información, siendo está considerada un activo importante que es imperativo proteger, bien sea por cumplimiento legal o por el simple hecho de proteger la información de sus clientes.

Las mejoras continuas tecnológicas en las organizaciones hacen que los análisis de riesgos se generen de forma frecuente. La gestión de riesgos es una metodología que permite identificar, analizar y responder a factores de riesgo, con el fin de que la organización mitigue y reduzca perdidas económicas o de información.

Del mismo modo, la gestión de riesgos en las entidades financieras radica en su mayor parte en una alianza con las nuevas tecnologías, ya que estas permiten que los servicios financieros, de inversión y de gastos de operación tengan un desempeño confiable para el negocio. Hoy en día, los servicios de tecnología se encuentran en un panorama cambiante esto hace que las organizaciones tomen decisiones estratégicas, sobre los controles débiles, es decir, es importante cubrir de extremo a extremo la tecnología y la seguridad de la información ya que hacen parte importante en estos controles para mitigar posibles riesgos, en tiempo atrás no era prioridad, pero en la actualidad las Entidades Financieras se están volviendo un objetivo para los atacantes.

Teniendo en cuenta lo anterior, este artículo proporciona una serie de recomendaciones las cuales encaminan en la gestión y análisis de riesgos para entidades financieras, lo que permite generar estrategias de protección que reduzcan las amenazas, evidenciando mejoras continuas a nivel de seguridad de la información, disminuyendo posibles impactos económicos en base a la ISO31000:2009, ISO27005:2011, circulares 052 de 2007 y la circular 048 de 2006.

II. Normas de Gestión en Tecnologías de la Información

Las normas y estándares han permitido que las organizaciones tengan mayor control y buenas prácticas en la gestión de riesgos, a continuación, se muestran algunas de ellas:

- COBIT

Es un marco de referencia COBIT (Objetivos de Control para Información y Tecnologías Relacionadas) lanzado por ISACA el 10 de abril de 2012, el cual se encarga de proveer una guía de mejores prácticas, dirigida a realizar controles y supervisiones de tecnología de la información. Este framework brinda una visión empresarial en los gobiernos de tecnología, contando con 4 dominios: Planificación y Organización (Plan and Organize)), Adquisición e Implantación (Acquire and Implement), Entrega y Soporte

(Deliver and Support) y Supervisión y Evaluación (Monitor and Evaluate).

- CRAMM

Es una metodología de gestión de riesgos fue creada en 1987 por la Agencia Central de Computadoras y Telecomunicaciones (CCTA), ahora llamada la Oficina de Gabinete, del gobierno del Reino Unido. Esta metodología está compuesta de tres etapas: Establecer objetivos de seguridad, evaluación de riesgos para el sistema propuesto y los requisitos de seguridad, identificación y selección de contramedidas acordes con las medidas de riesgos.

- MAGERIT

Es una metodología elaborada por el Consejo Superior de Administración Electrónica, se encarga del análisis de riesgos de los Sistemas de Información. Actualmente se encuentra en la version 3.

- RISK IT

Provee una visión integral y completa de todos los riesgos relacionados con el uso de Tecnologías de la Información y un tratamiento igualmente extenuante de la gestión de riesgos, desde el tono y la cultura en la parte superior, hasta los problemas operativos

- OCTAVE

Es una metodología OCTAVE (Operationally, Critical, Threat, Asset, Vulnerability, Evaluation) de análisis de riesgos desarrollada en el año 2001 por el SEI (Software Engineering Institute) operado por la Universidad Carnegie Mellon, que tiene por objeto facilitar la evaluación de riesgos en una organización, estudia los riesgos en base a tres principios: Confidencialidad, Integridad y Disponibilidad.

- ISO / IEC 27000

Estándar sobre Sistemas de Gestión de la Seguridad de la Información publicación realizada en el 2008.

- ISO / IEC 27005

La norma ISO 27005 fue publicada en inicio de junio de 2008 y reemplaza la norma ISO 13335-2 “Gestión de Seguridad de la Información y la tecnología de las comunicaciones”. Esta incluye recomendaciones para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información en sus seis anexos, donde incluye orientaciones tales como la identificación de activos y riesgos.

En el proceso de gestión de riesgos se debe contemplar la seguridad de la información para que se le realice su respectivo tratamiento. Previamente, debe haber un levantamiento de los activos de información ya que al identificarlos se podrán generar planes para la gestión de incidentes y así producir reducciones en los daños potenciales a las organizaciones. Del mismo modo, es importante generar conciencia del personal sobre los riesgos y controles esto con el fin de establecer controles para mitigar riesgos y eventos de una forma más ágil. Igualmente, tener documentación de los procesos de gestión de riesgo de seguridad de la información, asimismo debe incluirse que en estos análisis se encuentren alineados con los objetivos estratégicos.

III. Definiciones

A continuación, se muestran algunas definiciones que son implementadas en la gestión de riesgo:

- *Aceptación del riesgo:* Decisión informada a favor de tomar un riesgo.
- *Activo:* Recurso de un sistema de información o relacionado con éste.
- *Administración de riesgos:* Método lógico y sistemático para la identificación, medición, control y monitoreo de los riesgos derivados de cualquier actividad, función y proceso, con el objetivo de minimizar pérdidas y maximizar oportunidades.
- *Amenaza:* Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de la información de un sistema.
- *Controles:* Medidas tomadas para gestionar o mitigar el riesgo.
- *Gestión de riesgos:* Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.
- *Impacto:* Medir la consecuencia al materializarse en una amenaza.
- *Mapa de riesgos:* Relación de las amenazas a que están expuestos los activos.
- *Probabilidad:* Posibilidad de que un hecho se produzca.
- *Riesgo:* Posibilidad de que se produzca un impacto determinado en un activo o en toda la organización.
- *Riesgo Inherente:* Nivel del riesgo propio de la actividad, sin tener en cuenta el efecto de los controles [1].
- *Riesgo Residual:* Nivel resultante del riesgo después de la implementación de los controles [2].
- *Tratamiento de riesgos:* Proceso destinado a modificar el riesgo.
- *Vulnerabilidad:* posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

IV. Principios

Las entidades financieras deben estar comprometidas con los siguientes principios para la administración de riesgos [3]:

a) *La gestión del riesgo crea y protege el valor*
La gestión del riesgo contribuye al logro de los objetivos y a mejorar el rendimiento en temas de

cumplimiento legal y normativo, seguridad, calidad, gestión de proyectos, eficiencia en las operaciones, gobernabilidad, reputación, entre otros.

b) *La gestión del riesgo es una parte Integral de todos los procesos de la institución*
La gestión de riesgo hace parte de las responsabilidades de todos los procesos organizacionales.

c) *La gestión del riesgo es parte de la toma de decisiones*
La gestión del riesgo apoya a quienes toman las decisiones a que están seas informadas, con acciones priorizadas y diferenciando entre todas las posibles alternativas de acción.

d) *La gestión de riesgos aborda explícitamente la incertidumbre*
La gestión de riesgos tiene en cuenta la incertidumbre, la naturaleza de esa incertidumbre y cómo puede ser dirigida.

e) *La gestión del riesgo es sistemática, estructurada y oportuna*
La gestión del riesgo es sistemática, estructurada y oportuna.
Un enfoque sistemático, oportuno y estructurado de la gestión de riesgos contribuye a la eficiencia y a la obtención de resultados consistentes, comparables y confiables.

f) *La gestión de riesgos se basa en la mejor información disponible*
La gestión de riesgos se basa en la mejor información disponible.
Las entradas al proceso de gestión de riesgos se basan en fuentes de información como datos históricos,
experiencia, retroalimentación de los interesados, observación, previsiones y juicio de expertos. Sin embargo, para la toma de decisiones los fabricantes se debe tener en cuenta la posibilidad de divergencia entre los expertos.

g) *La gestión del riesgo está adaptada*
La gestión de riesgos está alineada con el contexto externo e interno y el perfil de riesgos de la organización.

h) *La gestión del riesgo tiene en cuenta los factores* humanos y culturales
La gestión de riesgos reconoce las capacidades, percepciones e intenciones de las personas externas e internas que pueden facilitar o dificultar el logro de los objetivos de la organización.

i) *La gestión de riesgos es transparente e inclusiva*
La participación adecuada y oportuna de las partes interesadas y, en particular, de los encargados de adoptar decisiones en todos los niveles de la organización, asegura que la gestión de riesgos sigue siendo relevante y actualizada.

j) *La gestión de riesgos es dinámica, iterativa y sensible al cambio*
La gestión del riesgo percibe y responde continuamente al cambio. A medida que suceden eventos externos e internos,
se generan cambios en los que se identifican nuevos riesgos.

k) *La gestión del riesgo facilita la mejora continua de la organización*
Las organizaciones deben desarrollar e implementar estrategias para mejorar su madurez en la gestión de riesgos.

V. Metodología del Sistema de Administración del Riesgo

La metodología del Sistema de Administración del Riesgo Operativo (SARO) considera la descripción de criterios de probabilidad e impacto, identificación de riesgos, análisis y evaluación de riesgos, planes de mitigación por medio de controles, protocolos de comunicación, indicadores de gestión, el análisis y la evaluación de riesgos, lo cual ha permitido que las Instituciones Financieras mejoren sus procesos y mecanismos de control.

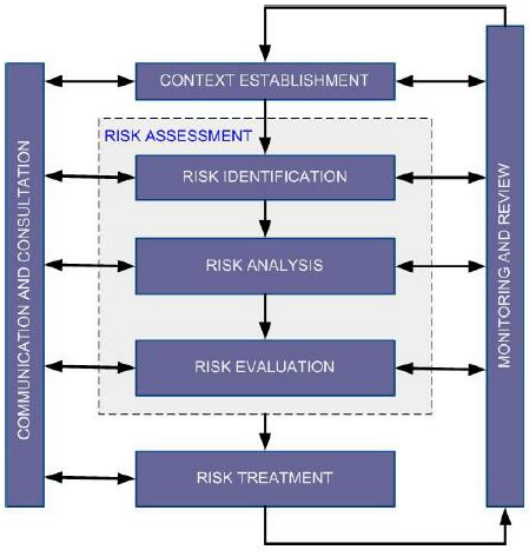

Fig. 1. Proceso de administración del riesgo [4]

A continuación, se muestra el proceso de gestión de riesgos el cual está especifico en la ISO31000[5]:

- Comunicación y consulta
- Establecimiento del contexto
- Valoración del riesgo
- Identificación del riesgo
- Análisis del riesgo
- Evaluación del riesgo
- Tratamiento del riesgo
- Monitoreo y revisión

La identificación y medición de riesgos se genera por procesos y en compañía de los líderes de proceso, en cuanto cada líder del proceso tiene los conocimientos y la experiencia en las actividades que se desarrollan y en los controles establecidos.

Es importante para tener éxito en la gestión de riesgos:

- Conocimiento y compromiso de la alta gerencia.
- Aceptación de la metodología que se aplicara.
- Integración de los controles con los objetivos estratégicos.
- Definición de los responsables de la gestión de riesgos

A continuación, se muestra el proceso de gestión de riesgos el cual está especifico en la ISO27005[6]:

- Planificar
- Hacer
- Verificar
- Actuar

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

Fig. 2. Alineación del SGSI y del proceso de gestión de riesgos de seguridad de la información [7]

En un Sistema de Gestión de Seguridad de la información(SGSI), se establece el contexto, la evaluación de riesgos, el desarrollo del plan de tratamiento de riesgos y la aceptación de riesgos.

VI. Definición de Criterios

Para lograr una adecuada metodología de administración de riesgos, es necesario establecer:

- Mapa de riesgos
- Definición de criterios de frecuencia e impacto.
- Severidad del riesgo

a) Mapa de riesgos

En el diseño del mapa de riesgos considera variables como la frecuencia y el impacto frente a la ocurrencia de un riesgo.

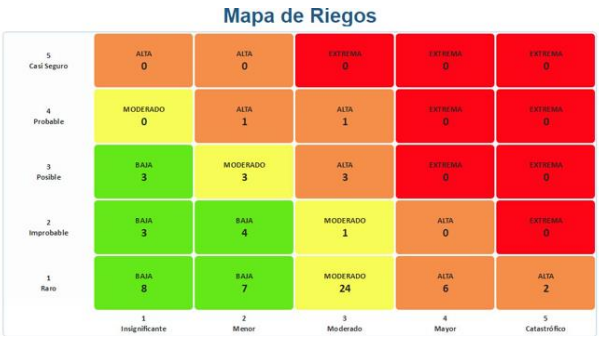

Fig. 3. Las mejores prácticas para gestionar los riesgos estratégicos [8]

Se definen los riesgos de niveles de severidad del riesgo, como, por ejemplo:

Bajo
Moderado
Alto
Extremo

Fig. 4. Niveles de severidad para análisis de riesgos

b) Criterios de frecuencia

La frecuencia es el número de eventos que podrían dar lugar a la materialización de eventos de riesgo, medido con respecto a una unidad de tiempo.

c)Criterios de impacto

El impacto es el resultado de un riesgo manifestado cualitativa o cuantitativamente, en donde se definen rangos sobre la posibilidad de resultados asociados a la materialización del riesgo.

d) Severidad del riesgo

Es la mezcla entre la frecuencia de ocurrencia y la magnitud del impacto del riesgo, este permite identificar el nivel de riesgo en los procesos.

e) Identificación de riesgos

Se deben identificar los riesgos en cada uno de los procesos de las organizaciones, generando un análisis de aquellos eventos que pueden llegasen a afectar los procesos u objetivos.

VII. Análisis de Riesgos

a) Identificación de causas

El análisis de riesgo consiste en identificar las causas que puedan llegar a materializarse en los riesgos identificados, los cuales son clasificados de acuerdo al factor de riesgo que las genera. Cada uno de los factores

tienen diversos componentes, cualquiera de ellos podría dar origen a un riesgo.

a) Factores de riesgo
Los factores de riesgo son seleccionados de acuerdo con su pertinencia en los contextos de las organizaciones. Como, por ejemplo:

- Infraestructura física
- Tecnología
- Eventos externos
- Entre otros.

b) Evaluación de riesgos
La evaluación de riesgos tiene como objetivo medir el nivel de riesgo al cual están expuestos los procesos, tendiendo como relevantes los criterios de frecuencia de ocurrencia y el impacto.

Existen dos enfoques para la evaluación del riesgo:

- Inherente a residual: Parte del riesgo inherente al cual están expuestos los procesos, para luego de esto determinar el riesgo residual.
- Residual a inherente: Parte del riesgo residual al cual están expuestos los procesos, para luego de esto determinar el riesgo inherente.

c) Mitigación de riesgos
Considerando que una vez se han calificado los riesgos, se procede con la identificación y evaluación de cada uno de los controles, teniendo presente el diseño y la ejecución de estos. El resultado de la alineación de estos criterios determina la efectividad del control.

VIII. Medición de efectividad del diseño de controles

En la medición se genera una evaluación de la configuración de los controles respectivamente a la mitigación del riesgo. En tanto que la evaluación de cada uno de los riesgos y controles se deben tener en consideración la experiencia de los equipos de trabajo, así como las mejores prácticas para evaluar que los controles que ya existen, estén diseñados de buena manera, antes, se podrán determinar planes de mejoramiento continuos.

En el diseño de los controles se debe tener en consideración:

a) Descripción de los controles
Se determina la periodicidad de la medición, los responsables, las actividades que se ejecutan y los soportes de las mismas.

b) Responsable:
Persona que es consciente de sus obligaciones.

c) Tipo de control:
Se asigna un tipo de control al riego, como, por ejemplo:

- Preventivo: Control anticipado ante un evento.
- Correctivo: Control que tiene como meta reparar cualquier tipo de evento.
- Detectivo: Control que identifica cualquier error.

d) Frecuencia del control:
Cada cuanto se ejecuta el control (cuando se requiera, mensual, diario, quincenal, permanente, anual).

e) Naturaleza: Este control puede ser manual, programado o automático.

f) Evidencia:
Criterio que determina si se deja evidencia de la ejecución del control.

g) Cobertura:
Porcentaje del total de actividades que es abarcado por el control.

IX. Medición de riesgos

Las metas y métodos de la medición de riesgos dependen el enfoque que se haya determinado en la evaluación inicial de riesgos. En caso de que sea seleccionado el enfoque inherente a residual el objetivo en esta etapa es la evaluación del riesgo residual.

Para medir los riesgos se debe contemplar los objetivos de los controles constituidos para mitigar que ocurran con frecuencia:

- Objetivo de control = disminuir frecuencia, se aplica el porcentaje de mitigación en la frecuencia.
- Objetivo de control = disminuir impacto, se aplica el porcentaje de mitigación a nivel de impacto.
- Objetivo de control = disminuir impacto y frecuencia, se aplica el porcentaje de mitigación a nivel de impacto y frecuencia.

A continuación, mostramos los enfoques para la medición de riesgos:

a) Medición del riesgo residual
b) Medición de riesgo inherente

X. Seguimiento y monitoreo

El seguimiento de los riesgos se genera por medio de registros y análisis de eventos. Esto permite verificar continuamente los procesos y una evaluación del sistema de administración de riesgos.

- *Monitoreo del funcionamiento del proceso:* Cada dueño de su proceso debe verificar el funcionamiento de los controles, para así establecer cambios y definir el impacto en el perfil de riesgo de los procesos, con el fin de determinar los planes que se ejecutaran.

- *Monitoreo del funcionamiento de sistema de administración de riesgos:* Cada dueño de su proceso debe verificar que los lineamientos definidos en el Sistema de Administración de Riesgos se lleven a cabo. Además, que se actualicen los procesos y generar los ajustes necesarios.

- *Registro de eventos:* Cada dueño de su proceso debe informar al responsable de la administración de riesgos los eventos que puedan llegar a presentarse y afectar alguno de los procesos.

  El responsable de la administración de riesgos deberá actualizar su registro de los eventos que se presentaron, así también, la evaluación del impacto en el mapa de riesgos y los controles establecidos en los procesos. Del mismo modo, en caso de que se requiera, es importante que se generen planes de acción para que minimicen los acontecimientos de eventos semejantes.

XI. TRATAMIENTO DE LOS RIESGOS

Para el caso de que los riesgos estén cualificados como extremos y altos, estarán incluidos en planes de mitigación y se les deberá generar el respectivo seguimiento mediante indicadores de riesgo y control.

Para el caso de los riesgos que estén cualificados como moderados o bajos serán monitoreados.

Las opciones existentes del tratamiento del riesgo deben seleccionarse en función del resultado de las evaluaciones de riesgo generadas, así como el costo planeado para la implementación y los beneficios.

Fig. 4. Las mejores prácticas para gestionar los riesgos estratégicos [9]

XII. CLASIFICACIÓN DE LOS EVENTOS

Los tipos de evento de riesgo se asocian de acuerdo a su naturaleza así:

- *Fraude interno:* Pérdidas provenientes de cualquier actuación encaminada a defraudar, por una parte, interna de la empresa.
- *Fraude externo:* Pérdidas provenientes de cualquier actuación encaminada a defraudar, por una parte, externa de la empresa.
- *Relaciones laborales:* Pérdidas derivadas de actos incompatibles con la legislación laboral.
- *Clientes:* Pérdidas derivadas de daños o perjuicios a activos de las empresas frente a clientes o de un servicio.
- *Daños a activos fijos:* Pérdidas derivadas de daños o perjuicios a activos físicos de las empresas frente a clientes o de un servicio.
- *Fallas tecnológicas:* Pérdidas derivadas a un incidente tecnológico.
- *Ejecución y administración de procesos:* Pérdidas derivadas
- *Reputacional:* Pérdidas derivadas que incurre una organización por desprestigio, mala reputación.
- *Legal:* Pérdidas derivadas que incurre al ser sancionada u obligada a pagar daños.

XII. CAPACITACIÓN

Las capacitaciones en riesgos deben estar contempladas con el fin de tener claridad de los conceptos, responsabilidades y esquemas para el tratamiento de los mismos, así como una frecuencia de revisión.

Cada programa de capacitación debe tener a los funcionarios de las organizaciones actualizados en el Sistema de Administración de Riesgos, se debe contar con mecanismos de evaluación de los procesos y controles para determinar la eficiencia y los resultados de los objetivos cumplidos.

Es responsabilidad de los dueños de los procesos capacitar a los funcionarios que están a su cargo referente a los riesgos y controles existentes en sus áreas, así también como la documentación existente.

XIII. CUMPLIMIENTO LEGAL

Es importante que en la gestión de riesgos se tenga en cuenta las normas y regulaciones del sector financiero como es el caso de las circulares 052 de 2007 y la circular 048 de 2006 con el fin de evitar riesgos reputacionales o sanciones económicas.

La gestión de riesgo de cumplimiento legal deduce que se deben conocer los controles que refieren a la mitigación de riesgo, así como la eficiencia a los que están sujetos. Además, se debe entender que están incluidos estándares, normas, códigos de conducta entre otros, los cuales son aplicables a las labores financieras, no obstante, hacen parte del cumplimiento normativo de cada país. Por ejemplo:

- Gestión de conflicto de intereses
- Ley de protección de datos personales
- Financiación del terrorismo

XIV. AUDITORÍAS

Como proceso de seguimiento y control de la gestión de riesgos, es necesario que se generen auditorias basadas en los riesgos.

Como, por ejemplo:

- *Auditoria Interna:* Se encarga de que en la ejecución del plan de auditoria se identifiquen las oportunidades de mejora concernientes a la eficiencia de los controles establecidos a los riesgos, estos deben estar en conocimiento de los dueños de los procesos con el fin de realizar las actualizaciones correspondientes.
- *Auditoria externa:* Se encarga de garantizar la razonabilidad de los estados financieros de una institución.
- *Auditoría legal*: Se encarga de cumplir los requisitos de una legislación o regulación en particular.

XV. INDICADORES

El monitoreo debe estar asociado con la entrega de indicadores para comparar los resultados de las metas planeadas y así generar acciones preventivas y correctivas en los posibles riesgos que se puedan presentar.

- *Indicadores claves de desempeño:* Permiten medir y cuantificar el grado de cumplimiento de los objetivos de los procesos y así evaluar si se está cumpliendo con el nivel de desempeño esperado.
- *Indicadores claves de control:* Permiten evaluar cómo está cambiando el perfil de riesgo y si está localizado en los niveles de tolerancia acordados.
- *Indicadores claves de riesgo:* Permite evaluar al dueño de los procesos el perfil de riesgo de estos. Para la medición de este indicador es necesario analizar las causas de los eventos de riesgo.

XVI. CONCLUSIONES

La gestión de riesgos de TI debe tener definidas evaluaciones de los costos, la valoración de activos y métricas alineadas con las estrategias del negocio. La generación de los análisis debe realizarse desde una perspectiva de extremo a extremo, en el marco global de los riesgos y respondiendo así a las diferentes necesidades del negocio.

Las organizaciones se enfrentan a riesgos estratégicos los cuales se encuentran en cambio constante. La naturaleza de estos riesgos y las causas potenciales a las que se enfrentan son cada vez más complicadas. La tecnología está en desarrollo constante lo cual genera incremento en la complejidad de los instrumentos financieros y operacionales, el impacto de una falla en alguno de sus controles u otros factores afectan a las instituciones financieras e impactan en su capacidad de reaccionar.

REFERENCIAS

[1] Circular Externa 048 de 2006. Superintendencia Financiera de Colombia.

[2] Circular Externa 048 de 2006. Superintendencia Financiera de Colombia.

[3] oficial referencia ISO 31000:2009 - gestión de riesgos - principios y directrices

[4] ISO (International Standard Organization). (2008). Tecnología de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información. Estándar de Seguridad ISO/IEC 27005.

[5] oficial referencia ISO 31000:2009 - gestión de riesgos - principios y directrices

[6] ISO (International Standard Organization). (2008). Tecnología de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información. Estándar de Seguridad ISO/IEC 27005.

[7] ISO (International Standard Organization). (2008). Tecnología de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información. Estándar de Seguridad ISO/IEC 27005.

[8] 27001 EALDE BUSINESS SCHOOL. Obtenido de https://www.ealde.es/las-mejores-practicas-para-gestionar-los-riesgos-estrategicos/

[9] 27001 NORMAS ISO. Obtenido de http://www.normas-iso.com/implantando-iso-27001/