ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

UNIDAD DE GESTIÓN DE POSTGRADOS

DEPARTAMENTO DE SEGURIDAD Y DEFENSA

MAESTRÍA EN SEGURIDAD Y RIESGO

III PROMOCIÓN

TEMA: "La Mejores prácticas aplicadas a un Análisis de Riesgos de seguridad de la información para las Entidades Financieras Controladas por La Superintendencia de Economía Popular y Solidaria (Cooperativas de Ahorro y Crédito) que conforman el grupo de Asistencia Tecnológica Cooperativa (Asistecooper)" Propuesta alternativa

AUTOR: DIEGO FERNANDO CEVALLOS GUERRA

DIRECTOR:

Mst. Arturo De La Torre

Sangolquí, Enero 2015

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. Diego Fernando Cevallos Guerra como requerimiento para la obtención del título de Master en Gerencia de Seguridad y Riesgos.

_____

24 de marzo de 2015

DECLARACIÓN DE RESPONSABILIDAD

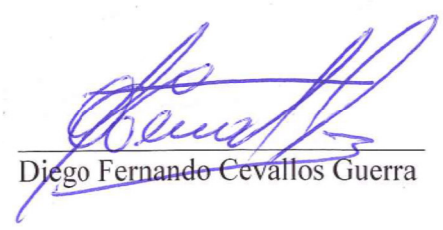
Diego Fernando Cevallos Guerra

Declaro que :

El proyecto de grado denominado "La Mejores prácticas aplicadas a un Análisis de Riesgos de seguridad de la información para las Entidades Financieras Controladas por La Superintendencia de Economía Popular y Solidaria (Cooperativas de Ahorro y Crédito) que conforman el grupo de Asistencia Tecnológica Cooperativa (Asistecooper)", ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del proyecto de grado en mención.

Sangolquí, Marzo del 2015

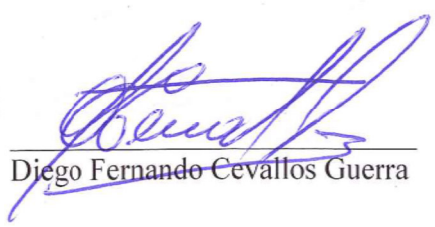


Diego Fernando Cevallos Guerra

AUTORIZACIÓN

Autorizo a la Universidad de las Fuerzas Armadas – ESPE la publicación, en la biblioteca virtual de la institución el trabajo "La Mejores prácticas aplicadas a un Análisis de Riesgos de seguridad de la información para las Entidades Financieras Controladas por La Superintendencia de Economía Popular y Solidaria (Cooperativas de Ahorro y Crédito) que conforman el grupo de Asistencia Tecnológica Cooperativa (Asistecooper)" cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolqui, Marzo del 2015



Diego Fernando Cevallos Guerra

DEDICATORIA

Dedico este trabajo de tesis al inspirador y motivador de todos los que tenemos la bendición de gozar la vida, cuyo nombre esta sobre todo nombre, Jesús, solamente es necesario aprender a escucharlo y tener el valor de obedecerlo, de esta manera los objetivos a conseguir no solo son alcanzados, sino que también se convierten en bendiciones, como lo sucedido con este trabajo.

Dedico también este trabajo a las 4 mujeres de mi vida, que son : mi esposa, mi dos hijas y mi nieta, mujeres que con sus virtudes y defectos me inspiran para mantenerme con un espíritu de superación.

AGRADECIMIENTOS

Mis agradecimientos eternos a mi patrocinador, quien se encargó de entregarme los recursos necesarios para yo culminar este trabajo, recursos como: sus bendiciones, misericordia, fe, esperanza, paciencia, persistencia, etc. Todos estos elementos me han permitido culminar con éxito este trabajo.

Gracias señor Jesús.

Mis agradecimientos a mi esposa, mis hijas y mi nieta, quienes al estar a mi lado, son el motivo de mi inspiración y fortaleza para seguir adelante en la vida.

Gracias familia.

Mis agradecimientos se extienden también a mis hermanas, sobrinos y amigos, quienes no apoyaron mucho en el desarrollo del tema, pero si fueron insistentes en reclamar la fecha de graduación.

Gracias familia y amigos.

Mis agradecimientos para el personal de la ESPE, coordinadores y docentes de la maestría en gerencia de seguridad y riesgos, tercera promoción, quienes entregaron su tiempo y conocimiento con alta calidad para que esta maestría cumpla con los objetivos propuestos.

Gracias señores coordinadores y docentes.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

En el Ecuador, el sector financiero, como principal usuario de las tecnologías de la información y conocedor de las amenazas a las que se encuentran expuestos los diferentes servicios financieros, algunas instituciones han tenido iniciativas muy particulares para proteger la integridad, disponibilidad y confidencialidad de la información, sin embargo, se puede afirmar que estas iniciativas no han sido muy generalizadas especialmente en las cooperativas de ahorro y crédito, ante esta situación, la Superintendencia de Bancos emitió una serie de normativas que obligan a las entidades financieras a implementar estrategias para mantener la seguridad de la información basadas en un análisis de riesgos con la finalidad de que las mencionadas estrategias sean objetivas y precisas en la protección de la información crítica para la continuidad del negocio. Las Normativas mencionadas están fundamentadas, en las denominadas mejores prácticas en seguridad de la información, desarrolladas por entidades internacionales públicas y privadas, en base a estudios especializados en el manejo de la información y los riesgos a los que está expuesta, como son : las normas ISO 27000, COBIT, ITIL. Con la finalidad de unificar los criterios que ofrecen las mejores prácticas para el desarrollos de un análisis de riesgos en seguridad de la información y las regulaciones emitidas por la entidad de control, se ha desarrollado una metodología que consolidan los criterios tanto de las mejores prácticas como en las normativas, lo que permitirá, obtener de una manera sencilla y objetiva los niveles de riesgo en los que se encuentra la información institucional

Palabras Clave :

- **ANÁLISIS DE RIESGOS.**
- **MEJORES PRÁCTICAS.**
- **SEGURIDAD DE LA INFORMACIÓN**
- **ENTIDADES FINANCIERAS**
- **SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA**.

ABSTRACT

In Ecuador, the financial sector as a major user of information technology and knowledgeable about the threats they are exposed to various financial services, some institutions have very specific initiatives to protect the integrity, availability and confidentiality information, however, we can say that these initiatives have not been very widespread especially in cooperative savings and credit, in this situation, the Superintendency of Banks issued a series of regulations requiring financial institutions to implement strategies to maintain information security based on a risk analysis in order that the above strategies are objective and accurate in protecting critical information for business continuity. The regulations mentioned are well founded, in so-called best practices in information security, developed by public and private international organizations, based on expertise in the management of information studies and the risks to which it is exposed, such as: the rules ISO 27000, COBIT, ITIL. In order to unify criteria that offer best practices for the development of a risk analysis and information security regulations issued by the controlling entity, has developed a methodology that consolidate the views of both best practices as in regulations, allowing to obtain a simple and objective risk levels where corporate information is located.

Keywords :

- **RISK ANALYSIS.**
- **BEST PRACTICES.**
- **INFORMATION SECURITY**
- **FINANCIAL INSTITUTIONS**
- **SUPERINTENDENCE OF POPULAR AND SOLIDARITY.**

CAPÍTULO 1

EL PROBLEMA DE INVESTIGACIÓN

1. Introducción

1.1. Antecedentes.

En la actualidad, los avances tecnológicos para el procesamiento de la información permiten mayor eficiencia y competitividad entre las instituciones financieras; no obstante también han dado lugar al surgimiento de amenazas que pretenden aprovechar las vulnerabilidades que éstas podrían tener con respecto a la seguridad de la información, amenazas que persiguen varios objetivos como: obtener dinero fácil, apropiarse de información confidencial, vulnerar activos de información, etc. Estas situaciones pueden generar afectaciones muy importantes como: pérdida de confianza por parte de los clientes, deterioro de la imagen institucional; o para el caso de las instituciones financieras: corrida de fondos, iliquidez, quiebra, etc.

Las investigaciones realizadas a nivel mundial por laboratorios de seguridad de la información, mantienen permanentemente monitoreadas las tendencias de las amenazas que tratan de vulnerar la seguridad de la información en las diferentes instituciones y en especial en el sector financiero.

Las estadísticas mencionan, según Kaspersky Lab:

- Que los ataques informáticos mediante el uso de programas maliciosos, crecieron en el 2013 en un 27,6% y alcanzaron los $28.4 millones, esto significa que fueron atacados 3,8 millones de usuarios, representando un crecimiento del 18.6%;
- El malware financiero o programas maliciosos para robar dinero, alcanzó los 19 millones de delitos informáticos, esta cantidad constituye los dos tercios de los ataques financieros realizados mediante software malicioso en el mundo.

- La suplantación de identidad para obtener datos confidenciales de los usuarios denominado pishing se duplicó en el 2013 en comparación con el 2012, de todos los ataques realizados, el 22% se los ejecutaron mediante sitios falsificados de bancos (Kaspersky Lab, 2014).

En el Ecuador, el artículo 222 de la Constitución; establece: "Art. 222.- Las superintendencias serán organismos técnicos con autonomía administrativa, económica y financiera y personería jurídica de derecho público, encargados de controlar instituciones públicas y privadas, a fin de que las actividades económicas y los servicios que presten, se sujeten a la ley y atiendan al interés general" (Asamblea Nacional, 2008).

En correspondencia a esta disposición constitucional, la Superintendencia de Bancos del Ecuador (antes Superintendencia de Bancos y Seguros del Ecuador), en su calidad de entidad encargada de la supervisión y control del sistema financiero, según lo determina el artículo 1 de la Ley General del Instituciones del Sistema Financiero (Congreso Nacional, Codificación 2002); consiente de los riesgos a los que se enfrenta la información en las entidades financieras y basándose en las mejores prácticas de general aceptación en riesgo operativo y seguridad de la información, en los años 2005 y 2012, emite las normativas: jb-2005-834 y jb-2012-2148, las mismas que son adoptadas por la Superintendencia de Economía Popular y Solidaria, para el control de las entidades financieras pertenecientes al sector Cooperativo. La normatividad mencionada instruye a las entidades financieras que deben realizar un análisis de riesgos en seguridad de la información con el objetivo de determinar lo siguiente:

- Si la tecnología implementada realmente es efectiva para el control de un incidente de seguridad de la información.
- Si la seguridad implementada está focalizada en los riesgos de más alta criticidad.
- Si es óptima la utilización de recursos para la implementación y administración de controles de seguridad de la información.

- Si la seguridad implementada está garantizando la continuidad del negocio en caso de un desastre natural.
- Si la seguridad implementada está garantizando la confidencialidad, integridad y disponibilidad de las transacciones realizadas por los socios o clientes a través de los diferentes medios electrónicos.

En la Ley General del Sistema Financiero, Título X De la Gestión y Administración de Riesgos, Capítulo V De la Gestión del Riesgo Operativo, Sección II Factores del Riesgo Operativo, artículo 4, numeral 4.3 relativo a "Tecnologías de Información", se indica (Junta Bancaria, 2005):

"4.3 Tecnología de Información.- Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea integra, confidencial y esté disponible para una apropiada toma de decisiones…" (Junta Bancaria, 2005).

No obstante de lo indicado, en nuestro país subsiste una alta incidencia de delitos informáticos, lo que pone en riesgo la estabilidad y aún existencia de algunas entidades financieras.

Al respecto surge una pregunta: ¿Si existen lineamientos técnicos(mejores prácticas) y una normativa legal que regulan mecanismos y procedimientos para garantizar una seguridad en la información de las entidades del sistema financiero, por qué aún se evidencian vulnerabilidades en la seguridad de la información especialmente a nivel de la cooperativas de ahorro y crédito?

En la presente investigación se analizan diversos aspectos vinculados a la seguridad informática, con el propósito de detectar falencias que deben ser corregidas a fin de precautelar los intereses institucionales, así como de los socios y clientes. Se hace énfasis en las cooperativas de ahorro y crédito por cuanto en la actualidad estas entidades se

encuentran en un proceso, tanto de regulación como de implementación de nuevos productos y sistemas tecnológicos para entregar servicios, los mismos que requieren mantener una fortalecida y específica seguridad de acuerdo a la realidad de cada entidad.

1.2. Formulación del problema.

Con los antecedentes mencionados se identifica la necesidad de desarrollar una metodología de análisis de riesgos basada en marcos de referencia de general aprobación y aceptación, para la identificación y valoración de activos y de riesgos, que permita a las cooperativas de ahorro y crédito realizar un diagnóstico de los riesgos a los que está expuesta la información institucional. De la necesidad identificada se generan las siguientes preguntas:

- ¿Cuáles son las mejores prácticas en identificación y valoración de activos de información y de riesgos?
- ¿Cuáles son las normativas en el ámbito de la seguridad de la información emitidas por la entidad de control?
- ¿Cuál es la relación existente entre las propuestas que mantienen las mejores prácticas sobre, la identificación y valoración de activos de información y de riesgos?
- ¿Cómo desarrollar un metodología de análisis de riesgos de seguridad de la información fundamentada en la relación existente entre las propuestas que mantienen las mejores prácticas en cuanto a la identificación y valoración de activos de información y riesgos?.
- ¿Cómo validar la metodología a través de un caso de estudio en una Cooperativa de ahorro y crédito?

1.3. Justificación.

La información constituye uno de los elementos vitales para que las instituciones tomen decisiones que les permitan ser: competitivas, productivas y trascedentes; por lo tanto, es necesario que se les provea una serie de elementos de seguridad que salvaguarden los atributos de confidencialidad, integridad y disponibilidad, que debe tener la información en las instituciones con el objetivo de evitar que sea manipulada, accedida o transferida de manera fraudulenta.

La aplicación de las normativas constitucionales y legales antes expuestas, no surten los efectos esperados, en muchos casos, por la implementación de estrategias de seguridad de manera empírica y no acorde a lo que instruyen las mejores prácticas en seguridad de la información y las normativas emitidas por las entidades de control, en las que se menciona que la implementación de las estrategias de seguridad debe darse en base a una metodología de análisis de riesgos, para que la estrategias de seguridad sean objetivas y precisas y evitar así las brechas de seguridad que pueden afectar a las instituciones en su imagen, reputación y confianza.

Para el establecimiento de esta metodología de análisis de riesgos es necesario el seguimiento de los siguientes pasos, proceso que en la actualidad no se lo cumple o se lo hace en forma parcial:

1. El conocimiento de las mejores prácticas para la identificación y valoración de activos de información y riesgos. Y la relación que existe entre estas.
2. El conocimiento de las normativas adoptadas por la Superintendencia de Economía Popular y Solidaria originalmente emitida por la Superintendencia de bancos del Ecuador que tratan sobre la Seguridad de la información en las instituciones financieras.

3. El conocimiento de la eficacia de diferentes salvaguardas de seguridad que mantienen las instituciones, para determinar objetivamente el nivel del riesgo en el que se encuentra los activos de información.

La no aplicación de los pasos mencionados conllevan a una percepción equivocada que la seguridad de la información implementada en las diferentes instituciones, está cubriendo con los activos de información realmente críticos para la continuidad del negocio y de las operaciones, manteniéndose vulnerables las instituciones frente a las amenazas pudiendo producir perdidas por la apropiación y accesos ilícito a la información o por destrucción de los activos de información por desastres naturales, accidentes o por acciones vandálicas.

En este escenario, se plantea el desarrollo de esta investigación tendiente a desarrollar una metodología de análisis de riesgos de seguridad de la información que sirva de base para diagnosticar de una manera objetiva el riesgo en el que se encuentra la información institucional, información que servirá de base para clasificar y priorizar los activos de información de acuerdo a sus niveles de riesgos y para la posterior selección de medidas de protección.

1.4. Identificación del problema.

En el Ecuador, la información sobre los ataques o delitos informáticos que se han producido en las entidades bancarias o cooperativas de ahorro y crédito es muy restringida y confidencial, ya que es crítica, en la medida que puede afectar a la reputación institucional y por lo tanto a la confianza de los clientes. Sin embargo, en base a datos publicados por la Fiscalía General del Estado (FGE), que es la receptora de las diferentes demandas realizadas por las personas víctimas de los delitos informáticos bancarios, es factible obtener una idea del impacto que generan las diferentes amenazas a las que está expuesta la información de las instituciones del sector financiero.

Según la Fiscalía General del Estado (2014), los delitos informáticos bancarios denunciados en el año 2009 totalizan 168; para el 2011, se incrementan a 3.129 casos, situación que obliga a las instituciones financieras a implementar controles de seguridad informática; para el 2012, los delitos informáticos disminuyen a 2.682, debido a los controles implementados; y en el año actual, 2014, se tienen registrados, hasta el mes de mayo, 877 casos. Esto significa que existe un promedio de 176 casos mensuales; por lo tanto, hasta finales del 2014, se estima que habrán al menos 2.112 delitos informáticos bancarios. Se debe mencionar, además, que de 600 delitos informáticos que se producen en el país, se estima que únicamente 1 es denunciado ante la fiscalía.

Los estudios y análisis efectuados por la antes citada institución determinan que:

- Las provincias que tienen el mayor porcentaje de incidencia en delitos informáticos, son: Pichincha con el 47.38%, Guayas con el 27,57% y El Oro con el 5.24%
- Los delitos informáticos receptados por la FGE confirman aquellas amenazas analizadas por los laboratorios de seguridad de la información a nivel mundial, como por ejemplo: fuga de información, interceptación de información (malware, spyware), suplantación de identidad (pishing), ataques a la integridad de la información institucional (Hackeo, virus, bootnet), etc. (Fiscalía General Del Estado Ecuatoriano, 2014).

De lo anotado es factible inferir que las estadísticas, tanto mundiales como del Ecuador, relativas a las amenazas contra la integridad, confidencialidad y disponibilidad de la información, especialmente en las entidades financieras, se mantienen evolucionando en sus técnicas e incrementándose en su número; esto exige que las instituciones sean muy objetivas y precisas en analizar y evaluar el riesgo al que puede estar expuesta la información institucional, para implementar los debidos controles y mitigar los riesgos.

Un error que se presenta con relativa frecuencia en las instituciones financieras, es la implementación de estrategias de seguridad informática con métodos empíricos, siguiendo

costumbres, modas, tradiciones, etc., sin realizar un análisis de riesgos para determinar, cuáles son los activos de información de mayor criticidad y que necesidades de seguridad tienen, Éste es uno de los factores que genera la problemática de los ataques informáticos a las instituciones, ya que no se tiene la certeza de que los recursos asignados para la implementación de seguridad de la información en las instituciones, están enfocados en los activos de información de mayor criticidad y cubren con las necesidades de seguridad de los mismos, generando de esta manera brechas de inseguridad que pueden afectar a la continuidad en las operaciones de la institución.

De la experiencia laboral del autor de esta tesis, se considera que entre los lineamientos técnicos (mejores prácticas) y el marco jurídico de regulación para la identificación y evaluación de activos de información y sus riesgos; y los sistemas de seguridad informática implementados en las cooperativas de ahorro y crédito, en un alto porcentaje, existe una brecha que limita el diagnóstico adecuado de las vulnerabilidades que mantienen los activos de información y por lo tanto una adecuada implementación de un sistema de seguridad de la información. El elemento faltante para eliminar la brecha mencionada es una metodología que vincule a los componentes referidos, sin embargo, esta afirmación requiere ser procesada y comprobada, por lo que sirve de base para la formulación de la pregunta de investigación del presente trabajo.

1.5. Formulación de la pregunta de investigación.

1.5.1. Pregunta de investigación.

¿Cómo las mejores prácticas en identificación y valoración de activos y riesgos, permiten el desarrollo de una metodología para el análisis de riesgos y la identificación del nivel de riesgo en el que se encuentra la información institucional?

1.5.2. Determinación de variables indicadores e índices.

Siendo la pregunta de investigación planteada de carácter predictiva, en la medida que anticipa con algún grado de certeza el comportamiento de la variable independiente, como también de carácter deductiva, por cuanto parte de inferencias lógicas deductivas para llegar a conclusiones particulares que después son comprobadas experimentalmente; es menester la identificación de las variables: independiente y dependiente, así como de sus correspondientes indicadores e índices (Tabla 1).

Tabla 1

Variables, indicadores e índices.

Variable independiente	Indicadores generales	Indicadores específicos	Índices
Las mejores prácticas en identificación y valoración de activos y riesgos.	Normas ISO 27000	Identificación de activos	
	Cobit	Valoración de activos	
	ITIL	Identificación de riesgos	
		Valoración de riesgos	

Continúa ⟶

Variable dependiente	Indicadores generales	Indicadores específicos	Índices
Metodología de análisis de riesgos.	Identificación de activos	Información Software Equipos Personas	Tipo de activo
	Valoración de activos	Confidencialidad Integridad Disponibilidad	Criticidad del activo
	Identificación de riesgos	Identificar activos Identificar amenazas Identificar impacto y probabilidad de ocurrencia	Elementos para la estimación del riesgo
	Valoración de riesgos	Activos de información y amenazas Valoración del impacto Probabilidad de ocurrencia	Nivel del riesgo

Fuentes: (ISO/IEC 27002, 2005); (IT Governance Institute, 2007); (ITIL, 2008)

1.5.3. Definiciones de variables, indicadores e índices.

Variable dependiente.- es aquella que cumple la función de causa o supuesta causa **(Morones)** en este caso de acuerdo a la pregunta de investigación, corresponde a las mejores prácticas.

Variable independiente.- es la que actúa como efecto o supuesto efecto en este caso corresponde a la metodología propuesta.

1.5.3.1. Indicadores generales de la variable independiente.

Corresponden a las mejores prácticas en identificación y valoración de activos y riesgos:

Normas ISO 27000 .- Son normas especializadas para la implementación de un sistema de gestión de seguridad de la información.

Cobit.- Es un marco referencia tomado como mejor práctica para el gobierno y administración de tecnologías de información.

ITIL.- Es un marco de referencia tomado como mejor práctica para la entrega de servicio en lo que se refiere a tecnología de información.

1.5.3.2. Indicadores específicos de la variable independiente.

Identificación de activos. Permite clasificar los activos de información agrupándolos de acuerdo a su naturaleza, por ejemplo: software, hardware, bases de datos, etc.

Valoración de activos. Permite valor al activo de acuerdo a los atributos de la seguridad de la información que son: confidencialidad, integridad y disponibilidad.

Identificación de riesgos. Permite identificar los elementos del riesgo, amenazas, impacto, probabilidad de ocurrencia.

Valoración de riesgos. Permite estimar el riesgo con los elementos identificados en el punto anterior.

1.5.3.3 Índices variable independiente.

En la variable independiente so se han definidos índices, debido a que los indicadores definidos requieren apoyarse en una metodología para generar un índice de medición, situación que se lo podrá observar en la variable dependiente.

1.5.3.4. Indicadores generales de la variable dependiente.

Los indicadores específicos definidos en la variable independiente, se convierten en los indicadores generales en la variable dependiente: identificación de activos, valoración de activos, identificación de riesgos, valoración de riesgos.

1.5.3.5. Indicadores específicos de la variable dependiente.

Los indicadores específicos correspondientes a:

- La identificación de activos hacen referencia a las diferentes opciones de clasificación de un activo, que proponen en común las mejores prácticas.
- La valoración de activos hacen referencia a los atributos sobre los cuales se debe valorar al activo.
- La identificación de riesgos hacen referencia a la identificación de los elementos para estimar el riesgo.
- La valoración de riesgos hacen referencia a la estimación del riesgo.

1.5.3.6. Índices variable dependiente.

Tipo de activo.- Este índice de carácter cualitativo permite clasificar los activos de información, obtendrá valores de acuerdo a lo establecido en los indicadores específicos.

Criticidad del activo.- Este índice de carácter cuantitativo permite obtener el nivel de criticidad de los activos de información para la continuidad del negocio y las operaciones.

Elementos para la estimación del riesgo.- Este índice permite establecer métricas para estimar el riesgo en cuanto a impacto y probabilidad de ocurrencia

Nivel de riesgo.- Este índice permite estimar el riesgo, calculándolo en base a los elementos identificados en el punto anterior.

1.6. Objetivos.

1.6.1. Objetivo General.

Desarrollar una metodología de análisis de riesgos en seguridad de la información basada en las mejores prácticas, para identificación y valoración de activos de información y de riesgos, que permita obtener de manera oportuna la identificación, evaluación y priorización del riesgo en el que se encuentra la información institucional.

1.6.2. Objetivos Específicos.

- Analizar las mejores prácticas para la identificación y valoración de activos de información y de riesgos.
- Analizar las normativas emitidas por la Superintendencia de Economía Popular y Solidaria en lo que se refiere a análisis de riesgos y seguridad de la información.
- Relacionar las propuestas de identificación y valoración de activos de información y de riesgos que mantienen las mejores prácticas, lo cual será la base para el desarrollo de la metodología de análisis de riesgos.
- Desarrollar un modelo de análisis de riesgos informáticos en base a las mejores prácticas analizadas y relacionadas, con la finalidad de obtener un mapa de riesgos que permita identificar objetivamente el nivel de riesgo en el que se encuentran los activos de información institucionales.
- Validar el modelo de análisis de riesgos, aplicándolo en una Cooperativa de ahorro y crédito.

CAPÍTULO II

MARCO REFERENCIAL

2.1. Estado del Arte.

Con respecto a la identificación y valoración de activos y riesgos existen diferentes enfoques que son necesarios conocerlos, se los puede agrupar en: marcos de referencia, metodologías de análisis de riesgos y análisis de impacto y probabilidad.

2.1.1 Marcos de referencia existentes.

- Normas ISO 27000 (ISO/IEC 27000, 2014) son un conjunto de lineamientos especializados en seguridad de la información, son un grupo de normativas de normativas relacionadas entre sí, que incluyen propuestas para la identificación y valoración de activos y riesgos.
- La Norma ISO/27001, (ICONTEC ISO/IEC 27001, 2006) manifiesta que debe implementarse un sistema de gestión de riesgos estableciendo requisitos que debe cumplir este sistema, sin embargo no define específicamente una metodología para análisis de riesgos.
- La Norma ISO/27005, (ISO-27005) establece una guía metodológica para realizar un análisis de riesgos, y se debe hacer énfasis que solamente es una guía en donde establece los siguientes pasos a seguir: identificación del riesgo, estimación del riesgo, evaluación del riesgo, monitoreo del riesgo y aceptación del riesgo.

Existen otros marcos de referencia que no son especializados en seguridad de la información, sin embargo mantienen en su contexto lineamientos para la identificación y valoración de activos y riesgos y son :

- CobiT, (IT Governance Institute, 2007) establece un marco de trabajo para la gestión de la tecnología de la información orientado al negocio y a los procesos, mantiene 4

dominios que son : Planificación y organización(PO), Adquisición e implementación(AI), Entrega y soporte (ES) y Monitoreo y Evaluación (ME).

Específicamente en el dominio de planificación y organización (PO) se establece requerimientos para la gestión del riesgo y en el dominio Entrega y Soporte (ES) se especifica un proceso de aseguramiento de continuidad del servicio.

En estos dominios, a fin de satisfacer los objetivos del negocio se definen siete criterios en términos de requerimientos de información, los cuales son : efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento, confiabilidad.En cuanto a los recursos o activos de información se consideran los siguientes: efectividad, eficiencia, confidencialidad, integridad y disponibilidad.

- ITIL(Information Technology Infraestructure Library) (ITIL, 2008) entrega una serie de procedimientos que tienen la finalidad de entregar a las organizaciones una referencia para que las operaciones de TI sean de calidad y eficientes. Este marco de referencia, en cuanto a los recursos o activos que deben ser identificados y valorados para el análisis de riesgos, establece los siguientes: organización, procesos, conocimiento, personas, información, aplicaciones, infraestructura y capital financiero y su valoración propone realizarlo en base a su disponibilidad.

Las propuestas que tienen los marcos de referencia existentes para la identificación y valoración de activos y riesgos, fueron identificadas y comparadas, constituyéndose en un insumo fundamental y común para el desarrollo de la metodología de análisis de riesgos propuesta en esta investigación.

2.1.2. Metodologías de análisis de riesgos existentes.

- CRAMM (SIEMENS, 2013) : Es una Metodología de análisis y gestión de riesgos desarrollada por la agencia central de telecomunicaciones (CCTA) del Gobierno del Reino Unido. Esta metodología es un antecedente para la norma BS799-3 y al

liberarse la versión 5 está ya contiene la actualización del BS799, por lo tanto la compatibilidad con la familia de las normas ISO27000.

Tiene un enfoque organizado y su alcance abarca a medios de información tecnológicas o no tecnológicas, para su evaluación la tecnología se divide en tres etapas :

1. Identificación y valoración de activos.
2. Identificación de amenazas y vulnerabilidades.
3. Contramedidas selección y recomendaciones.

Cramm, (Seguridad informática, 2014) puede definirse como una Metodología, para el análisis y gestión de riesgos que:

- Aplica sus conceptos de una manera formal, disciplinada y estructurada.
- Es Orientada a proteger la confidencialidad, integridad y disponibilidad de un sistema y de sus activos.
- Aunque es considerada cuantitativa, utiliza evaluaciones cuantitativas y cualitativas, y por esto se considera mixta.

Cramm, (Seguridad informática, 2014) incluye una amplia gama de herramientas de evaluación de riesgo que son totalmente compatibles con 27001 y ISO que se ocupan de tareas como:

- Activos de modelado de dependencia
- Evaluación de impacto empresarial
- Identificación y evaluación de amenazas y vulnerabilidades
- Evaluar los niveles de riesgo
- La identificación de los controles necesarios y justificados sobre la base de la evaluación del riesgo.
- Un enfoque flexible para la evaluación de riesgos.

Para la aplicación de esta metodología existe un software especializado denominado "Cramm Manager" comercializado en el Reino Unido por Insight Consulting. (Seguridad informática, 2014)

- **MAGERIT** : (Seguridad informática, 2014), Es una metodología de análisis y gestión de riesgos creada en España, que ofrece un método sistemático para analizar los riesgos producto del uso de las tecnologías de la información.

  La metodología se basa en :

  - El impacto que puede tener la empresa por la violación de la seguridad.
  - Identifica las amenazas que puede llegar a afectar las instituciones.
  - Identifica vulnerabilidades.
  - Determina los controles o salvaguardas.

  La metodología está alineada a los estándares ISO en gestión riesgos y seguridad de la información.

  Para la aplicación de esta metodología existe un software denominado PILAR, con el cual se puede realizar análisis cualitativo y cuantitativo de riesgos, manteniendo un orden, como el siguiente :

  - Identificar los activos más significativos.
  - Identificar el valor relativo de los activos.
  - Identificar las amenazas más relevantes.
  - Identificar las salvaguardas presentes en el sistema.
  - Establecer los activos críticos.

- **OCTAVE** (Operationally Critical Threat , Asset and vulnerability Evaluation) (Carnegie Melon university, 2014). Es una metodología de análisis de riesgos en seguridad para tecnologías de la información, enfocada a que las organizaciones sean capaces de :

- Evaluar y controlar los riesgos en la seguridad de la información, por si mismos.
- Tomar decisiones adecuadas en base , basadas en el análisis de sus riesgos.
- Enfocarse en el aseguramiento de sus activos tecnológicos principales.
- Preservar información clasificada.

Los aspectos importantes de esta metodología :

- Asegura la continuidad de operación de la empresa.
- Definición de riesgos y amenazas basadas en los activos críticos.
- Establece estrategias para mitigar los riesgos.
- Se enfoca en la conservación de la información.
- Ayuda a la organización a cumplir regulaciones de la seguridad de la información.

Las metodologías propuestas mantienen un fin común que es: evaluar el riesgo en el que se encuentran los activos de información, objetivo que no es diferente con la propuesta de esta investigación. La diferencia se encuentra en que las metodologías descritas anteriormente exigen inversiones bastante altas para su implementación, administración y mantenimiento ya que requieren de recursos especializados para su total aprovechamiento. Son herramientas diseñadas en países europeos, siendo necesario adaptarlos a las realidades de las instituciones en el Ecuador lo cual implica invertir más recursos económicos y humanos cada vez que exista una modificación establecida por las entidades de control.

La propuesta de esta investigación es el desarrollo de una metodología de análisis de riesgos, que sea económica, de fácil aplicación, flexible y objetiva, orientada específicamente a las entidades financieras.

2.1.3. Análisis de impacto y probabilidad.

Los laboratorios especializados en seguridad de la información mantienen un monitoreo de los diferentes incidentes que se presentan a nivel mundial, información que es de gran utilidad para que las instituciones tengan como referencia para establecer criterios en la evaluación del riesgo en cuanto a impacto y probabilidad de ocurrencia de un incidente. A continuación se presentan las opiniones de algunos estudios:

Según Ponemon Institute y Websense Inc. (Websense, 2014)

Menciona, que las probabilidades de ocurrencia de un incidente de seguridad está en niveles muy altos, debido a que los controles de seguridad no son implementados, ni actualizados de acuerdo a las realidad del riesgo que mantienen las instituciones, especialmente porque no existe compromiso de parte de los dirigentes para implementar un sistema de gestión de seguridad de la información que se ocupe de identificar y valorar los activos de información y los riesgos a los que se enfrentan.

Según PWC Asesores Empresariales. (PWC Asesores Empresariales, 2014)

Las tasas de crecimiento de los ataques informáticos determinan que las instituciones están expuestas a tener altos impactos frente a la materialización de alguna de las amenazas analizadas, además al no tener los controles debidamente diseñados, implementados y monitoreados la probabilidad de ocurrencia y éxito en los ataques informáticos es muy alta.

Según Kapersky. (Kaspersky Lab, 2014)

Los ataques a las entidades financieras es incremental año a año, han producido impactos económicos bastantes significativos especialmente en las entidades financieras.

2.2. Marco Teórico.

A continuación se describen las mejores prácticas que servirán de base para el desarrollo de la metodología de análisis de riesgos en seguridad de la información. Los

numerales 2.2.1 al 2.2.6, contienen una descripción resumida de la cobertura que tienen cada una de las mejores prácticas.

Los numerales 2.2.7 al 2.2.18, contienen, las diferentes propuestas para el levantamiento de activos de información y de riesgos, emitidas por las mejores prácticas, elementos fundamentales para realizar un análisis de riesgos en seguridad de la información, la cual es producto de un entendimiento y una investigación de todo el contexto de cada una de las mejores prácticas, considerando que no todas ellas tienen como especialidad la seguridad de la información y tampoco proponen una metodología para el análisis de riesgos.

Los numerales 2.2.19 al 2.2.20, contienen respectivamente estadísticas de los incidentes en seguridad de la información y estadísticas de la eficiencia de los controles o salvaguardas para mitigar los riesgos informáticos.

2.2.1. Norma ISO 27000.

La Norma ISO 27000 **(ISO/IEC 27000, 2014)**, provee una visión general de todas las normas que son parte de la familia ISO 27000, explicando su alcance; contiene definiciones de los diferentes términos que son utilizados en las distintas Normas de la familia; además, aporta las bases del porque es importante la implementación de un sistema de gestión de la seguridad de la información y entrega una descripción muy general del procedimiento que se debe seguir en la implementación, monitorización, mantenimiento y mejora de un sistema de gestión de seguridad de la información**.**

2.2.2. Norma ISO 27001.

La Norma ISO 27001 (**ICONTEC ISO/IEC 17799, 2006)** tiene origen en la Norma ISO 17999, la cual es un código de buenas prácticas para la administración de la seguridad

de la información de una institución, que permiten garantizar la confidencialidad, disponibilidad e integridad de la información.

A su vez, la Norma ISO 17999 tiene su origen en la British Standard BS 7799 **(ICONTEC ISO/IEC 17799, 2006),** la cual consta de dos partes, en la primera parte se tiene la normalización, que se convirtió en la norma ISO/IEC 17999:2000, la segunda parte: es la certificación que hasta el año 2005 se la trabajaba en base a BS 7799-2, ahora se lo hace con la Norma ISO 27001 **(ICONTEC ISO/IEC 27001, 2006).**

La Norma ISO 27001, especifica los requisitos para: implementar, ejecutar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información, especifica también los requerimientos para la implementación de controles de seguridad de la información adaptados a las necesidades de la organización. En el Anexo A de la Norma ISO 27001, hace referencia a los objetivos de control y controles que debe mantener un sistema de gestión de seguridad de la información, los mismos que son desarrollados en la Norma ISO 27002.

2.2.3. Norma ISO 27002.

La Norma ISO 27002, **(ISO/IEC 27002, 2005)**, establece 39 objetivos de control en seguridad de la información y detalla 133 controles agrupándolos en 11 dominios. Este documento es utilizado como una guía para implementar los sistemas de gestión de seguridad de la información en base a prácticas eficaces. En el Anexo 2 de esta norma se puede observar de forma desglosada los dominios y controles de seguridad.

2.2.4. Norma ISO 27005.

La Norma ISO 27005, **(ICONTEC ISO/IEC 27005, 2009).** proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación

satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos, definiendo cual es el proceso para la gestión del riesgo como se puede observar en la figura 1.

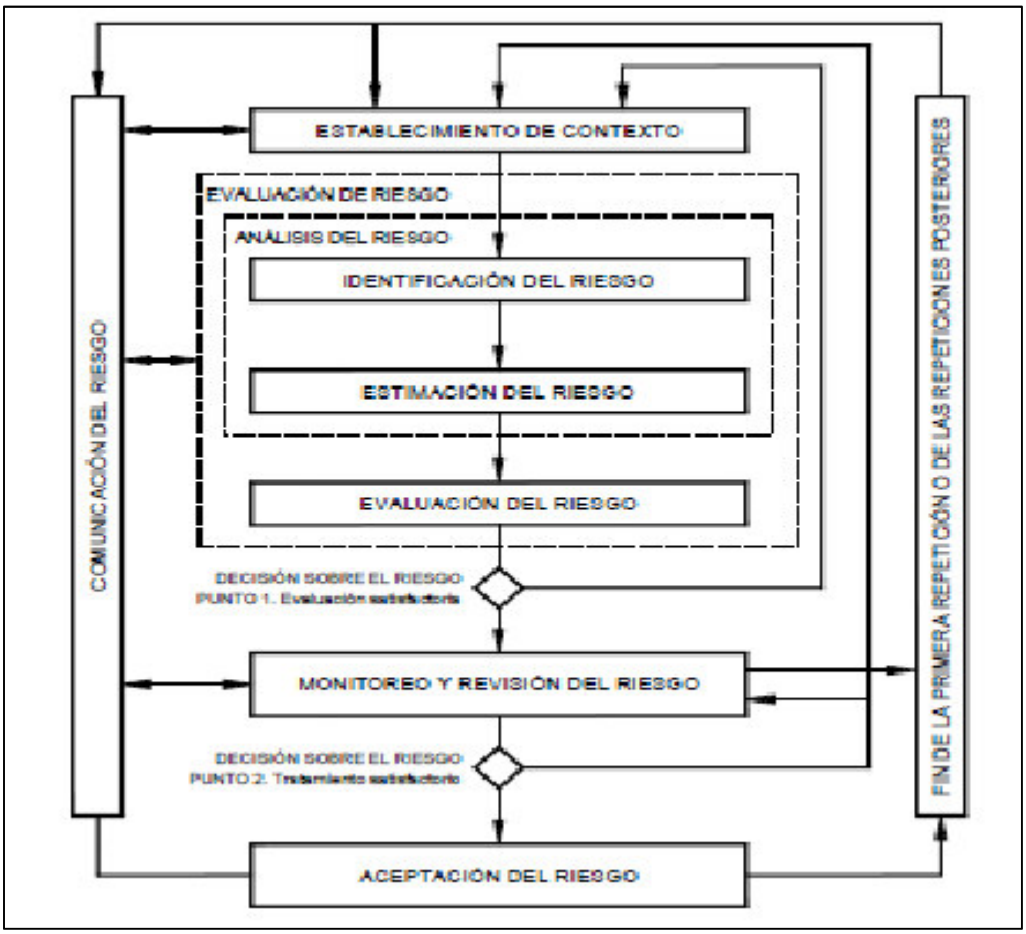


Figura 1: Proceso de gestión del riesgo en la seguridad de la información.
Fuente: (ICONTEC ISO/IEC 27005, 2009).

2.2.5. Cobit 4.1.

El estándar COBIT 4.1 **(IT Governance Institute, 2007)** se aplica a todos los sistemas de información; está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos, naturalmente agrupados, para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

La misión de COBIT es investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes, auditores y gerentes de seguridad de la información.

Los productos COBIT se han organizado en tres niveles diseñados para dar soporte a:

- Administración y consejos ejecutivos
- Administración del negocio y de TI
- Profesionales en Gobierno, aseguramiento, control y seguridad

El estándar tiene las siguientes características:

- Orientado al negocio
- Alineado con estándares y regulaciones "de facto"
- Basado en una revisión crítica y analítica de las tareas y actividades en TI
- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA)

La estructura conceptual se puede enfocar desde tres puntos de vista:

a) Los criterios empresariales que deben satisfacer la información
b) Los recursos de las TI
c) Los procesos de TI

Los criterios deben considerar los requerimientos de información: de Calidad, fiduciarios y de seguridad.

- **Requerimientos de Calidad:** Calidad, Costo y Entrega.
- **Requerimientos Fiduciarios:** Efectividad y Eficiencia operacional, Confiabilidad de los reportes financieros y Cumplimiento le leyes y regulaciones.

- **Efectividad:** La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.
- **Eficiencia:** Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).
- **Confiabilidad:** proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.
- **Cumplimiento:** de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.
- **Requerimientos de Seguridad:** Confidencialidad, Integridad y Disponibilidad.
- **Confidencialidad:** Protección de la información sensible contra divulgación no autorizada.
- **Integridad:** Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.
- **Disponibilidad:** accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.

En COBIT se establecen los siguientes recursos en TI necesarios para alcanzar los objetivos de negocio:

- **Aplicaciones:** Incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- **Información:** Son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
- **Infraestructura:** es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc.,

así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

- **Personas:** son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

La estructura de COBIT se define a partir de una premisa simple y pragmática: "Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos".

COBIT (ITG, 2007) se divide en tres niveles:

1. **Dominios:** Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
2. **Procesos:** Conjuntos o series de actividades unidas con delimitación o cortes de control.
3. **Actividades**: Acciones requeridas para lograr un resultado medible.

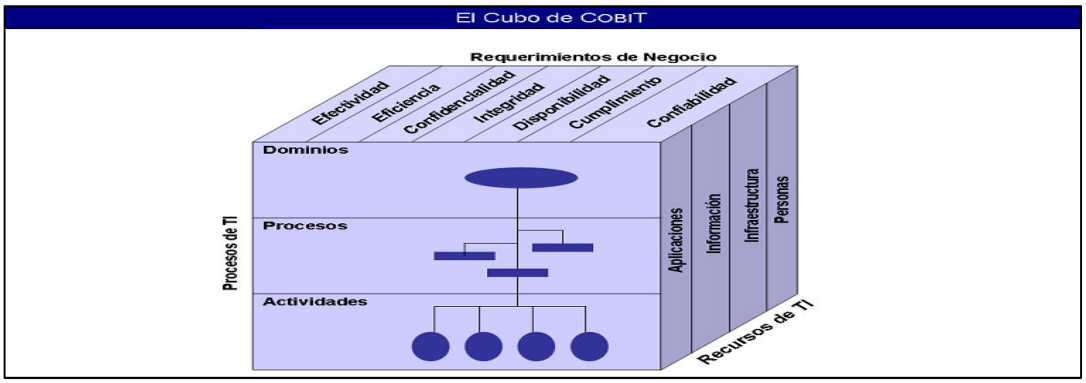


Figura 2: Cubo Cobit, muestra la relación entre procesos de TI,s.
Fuente: (IT Governance Institute, 2007).

COBIT (IT Governance Institute, 2007), define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear, sobre las cuales deben actuar políticas, estándares y procedimientos de seguridad de la información.

2.2.6. ITIL

ITIL(Information Technology Infraestructure Library) es un conjunto de prácticas y conceptos para la gestión de los servicios de TI, el desarrollo de tecnologías de información y las operaciones relacionadas con la misma.

ITIL entrega una serie de procedimientos que tienen la finalidad de entregar a las organizaciones una referencia para que las operaciones de TI sean de calidad y eficientes.

2.2.7. Identificación de Activos según la Norma ISO-27001.

La Tabla 2 contiene los ítems que respaldan la identificación de activos según la Norma ISO 27001 **(ICONTEC ISO/IEC 27001, 2006).**

Tabla 2

Control A.7 Gestión de Activos.

A.7	**Gestión de Activos**	
A.7.1	**Responsabilidad sobre los activos.**	
Objetivo:	**Alcanzar y mantener una protección adecuada de los activos de la Organización**	
A.7.1.1	Inventario de activos.	Control: Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
A.7.1.2	Responsable de los activos.	Control: Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.
A.7.1.3	Acuerdo sobre el uso aceptable de los activos	Control: Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

Fuente: (ICONTEC ISO/IEC 27001, 2006).

En la Norma ISO 27002 (ISO/IEC 27002, 2005) manifiesta que existen muchos tipos de activos, incluyendo:

a) **Información:** Bases de datos y archivos de datos, contratos y acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada
b) **Activos de Software:** Software de aplicación, software del sistema, herramientas de desarrollo y utilidades**.**
c) **Activos físicos:** Equipos de computación, equipos de comunicaciones, medios removibles y otros equipos**.**

d) **Servicios:** Servicios de computación y comunicaciones, servicios generales como por ejemplo iluminación, calefacción, energía y aire acondicionado**.**

e) **Personas:** Sus calificaciones, habilidades y experiencia**.**

f) **Intangibles:** Reputación e imagen de la organización**.**

2.2.8. Valoración de Activos según la Norma ISO-27001.

La Tabla 3 contiene los ítems que respaldan la valoración de activos según la Norma ISO 27001.

Tabla 3

Control A.7 Clasificación de la información.

A.7	**Gestión de Activos**	
A.7.2	**Clasificación de la Información**	
Objetivo:	**Asegurar que la información recibe el nivel de protección adecuado**	
A.7.2.1	Directrices de clasificación	Control: La clasificación se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y de la importancia para la organización.
A.7.2.2	Etiquetado y manejo de Información	Control: Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.

Fuente: (ICONTEC ISO/IEC 27001, 2006).

La Norma ISO 27002 (ISO/IEC 27002, 2005), establece que la valoración de los activos se lo puede realizar de acuerdo a su confidencialidad, integridad y disponibilidad, esto debe tener una estrecha relación con las necesidades del negocio respecto a compartir o restringir el acceso a la información, además las categorías de clasificación que se van aplicar para la clasificación deben ser muy razonables debido a que esquemas demasiado complejos pueden volverse engorros y de uso costoso o no ser prácticos.

La Norma ISO27002 en la guía de implementación hace referencia a controles que también deben ser considerados para la clasificación de la información, Tabla 4.

Tabla 4

Controles asociados a la clasificación de activos.

A.11.1.1	Política de control de accesos	Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.
A.7.1.2	Responsable de los activos	Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.
A.10.7.2	Eliminación de soportes	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.

Fuente: (ICONTEC ISO/IEC 27001, 2006).

2.2.9. Identificación de Riesgos según la Norma ISO-27001.

En la sección 4.2.1 de la Norma ISO 27001 (ICONTEC ISO/IEC 27001, 2006), se encuentran definidos los siguientes requisitos para la identificación de riesgo:

c) **Definir el enfoque organizacional para la valoración del riesgo.**

1. Identificar una metodología de valoración del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de seguridad de la información del negocio, identificados.
2. Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables.

d) **Identificar los riesgos.**

1. Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
2. Identificar las amenazas en relación a los activos.
3. Identificar las vulnerabilidades que podrían ser aprovechadas por dichas amenazas.
4. Identificar los impactos que la pérdida la confidencialidad, integridad y disponibilidad puede tener sobre estos activos. (ICONTEC ISO/IEC 27001, 2006)

2.2.10. Valoración del Riesgo según la Norma ISO-27001.

En la sección 4.2.1 de la Norma ISO 27001 (ICONTEC ISO/IEC 27001, 2006), se encuentran definidos los siguientes requisitos para la valoración del riesgo:

c) Analizar y evaluar los riesgos.

1. Valorar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos.
2. Valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente.
3. Estimar los niveles de los riesgos.
4. Determinar la aceptación de riesgo o la necesidad de su tratamiento a partir de los criterios establecidos en el numeral 4.2.1, literal c. (ICONTEC ISO/IEC 27001, 2006).

En la Norma ISO 27005 (ICONTEC ISO/IEC 27005, 2009)**.**en las fases de identificación, estimación y evaluación del análisis de riesgos manifiesta que la valoración del riesgo consta de las siguientes actividades:

- Análisis de riesgo consta de:
  - Identificación del riesgo, Numeral 8.2.1.
  - Estimación del riesgo, Numeral 8.3.1.
  - Evaluación del riesgo, Numeral 8.3. Tiene relación directa con lo el numeral 4.2.1 de la Norma ISO-27001 que de igual manera trata sobre los requisitos para la valoración del riesgo. (ICONTEC ISO/IEC 27005, 2009).

2.2.11. Identificación de Activos según COBIT.

COBIT (IT Governance Institute, 2007) especifica los recursos de TI necesarios para alcanzar los objetivos de negocio constituyéndose en una referencia para la identificación de los activos:

- **Aplicaciones:** Incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- **Información:** Son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
- **Infraestructura:** es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- **Personas:** son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, o contratadas, de acuerdo a como se requieran. (ICONTEC ISO/IEC 27005, 2009)

La estructura de COBIT se define a partir de una premisa simple y pragmática: "Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos" (IT Governance Institute, 2007).

2.2.12. Valoración de Activos según COBIT.

Los criterios para la valoración de los activos de información según COBIT son los siguientes:

Tabla 5

Criterios de valoración de activos.

Criterios	Detalle
Efectividad	Tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable
Eficiencia	Consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
Confidencialidad	Se refiere a la protección de información sensitiva contra revelación no autorizada.
Integridad	Está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
Disponibilidad	Se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
Cumplimiento	Tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos extremadamente, así como políticas internas.
Confiabilidad	Se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

Fuente: (IT Governance Institute, 2007).

2.2.13. Identificación de Riesgos según COBIT.

Cobit (IT Governance Institute, 2007) contiene en el Dominio P09 Planear y Organizar el proceso Evaluar y Administrar los Riesgos de TI en donde se menciona que deben existir:

- Criterios comunes en la institución para identificar y medir los riesgos.
- Estrategias para mitigación de riesgos para llevarlos a un nivel aceptable.
- Metodologías para identificar amenazas y vulnerabilidades para determinar el impacto que causen sobre las metas que tiene el negocio en caso de que se materialicen.

El Dominio mencionado contiene diferentes sub-dominios para la identificación de riesgos Tabla 6.

Tabla 6

P09 Evaluar y Administrar los riesgos TI.

Objetivo de Control		Detalle
PO9.1	Marco de Trabajo de Administración de Riesgos	Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.
PO9.2	Establecimiento del Contexto del Riesgo	Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.
PO9.3	Identificación de Eventos	Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de a empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.

Fuente: (IT Governance Institute, 2007).

2.2.14. Valoración de Riesgos según COBIT.

El Dominio P09 Planear y Organizar contiene el proceso Evaluar y Administrar los Riesgos de TI en donde se detallan los diferentes sub-dominios para la evaluación de riesgos, Tabla 7.

Tabla 7:

P09 Evaluar y Administrar los riesgos de TI.

Sub-Dominio	Objetivo de Control	Detalle
PO9.4	Evaluación de Riesgos de TI	Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.
PO9.5	Respuesta a los Riesgos	Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.
PO9.6	Mantenimiento y Monitoreo de un Plan de Acción de Riesgos	Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

Fuente : (IT Governance Institute, 2007).

2.2.15. Identificación de Activos según ITIL.

ITIL en el Capítulo 3 en la Fase: Ciclo de vida: Estrategia del servicio, en la sección 3.2 Conceptos Básicos, se definen los activos de servicio denominados Recursos y Capacidades, estos tipos de activos son utilizados por las instituciones para crear valor en la forma de productos o servicios. La definición según ITIL de estos tipos de activos son las siguientes:

"Los **recursos** suelen estar basados en experiencias, requieren mucho conocimiento e información y están íntimamente relacionados con las personas, sistemas, procesos y tecnologías de una organización. La adquisición de recursos resulta relativamente sencilla en comparación con la adquisición de capacidades" (Van, Bon Jan, 2008).

"Las **capacidades** se desarrolla a lo largo de los años. La extensión y profundización de experiencias adquiridas con distintos tipos de clientes, mercados, contratos y servicios facilita el desarrollo de capacidades propias. La experiencia se consigue resolviendo problemas, enfrentándose a distintas situaciones, gestionando riesgos y analizando errores. Los proveedores de servicios deben desarrollar capacidades distintivas para poder fidelizar a los clientes con servicios que sean difíciles de encontrar en la competencia. También deben realizar importantes inversiones en educación y formación para seguir desarrollando sus activos estratégicos" (Van, Bon Jan, 2008).

"Las capacidades por si solas no pueden generar valor sin los recursos adecuados. La capacidad productiva de un proveedor de servicios depende de la disponibilidad de los recursos. Las capacidades se emplean para desarrollar, implementar y coordinar la capacidad productiva" (Van, Bon Jan, 2008).

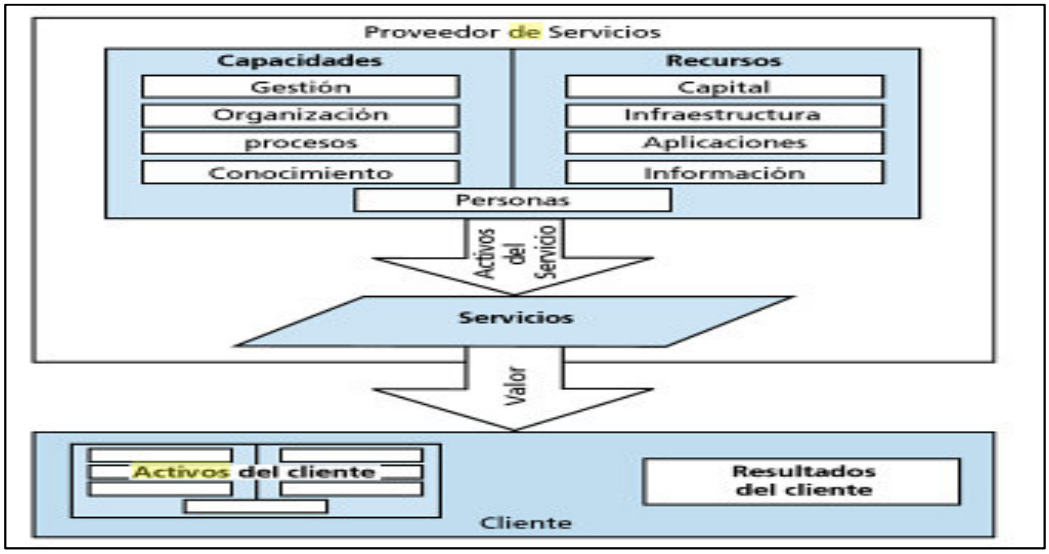


Figura 3:Los recursos y las capacidades son la base para la creación de valor. Fuente: (Van, Bon Jan, 2008).

Tipos de activo.

En la Tabla 8 se detallan los tipos de activos, constituyéndose en una referencia muy útil para la identificación de activos.

Tabla 8

Tipos de activos.

Tipo de activo	Descripción
Gestión	Gestión es un sistema que incluye liderazgo, administración, política, rendimiento, regulaciones e incentivos; esta capa cultiva, coordina y supervisa los otros tipos de activos.
Organización	Los activos organizacionales son configuraciones activas de las personas, procesos, aplicaciones e infraestructuras que implementan todas las actividades de la organización; esta capa incluye las jerarquías funcionales, grupos de redes sociales, equipos y personas y todos los sistemas que se utilicen para trabajar juntos hacia objetivos colectivos.
Procesos	Los activos de proceso consisten en algoritmos, métodos, procedimientos y rutinas que impulsan la implementación y administración de las actividades y las interacciones

Continúa ⟶

Conocimiento	Los activos de conocimiento son acumulaciones de realizaciones, experiencia, información, conocimiento y propiedad intelectual que están asociadas con actividades específicas y contextos.
Personas	Las personas como activos representan la capacidad de análisis, percepción, creatividad, educación, evaluación, liderazgo, comunicación, coordinación, empatía y confianza.
Información	Los activos de información son colecciones, patrones y abstracciones significativas de datos que se aplican en el contexto de los clientes, contratos, servicios, eventos, proyectos y producción.
Aplicaciones	Los activos de aplicación son muy variados en tipo e incluyen artefactos, automatización y herramientas para apoyar el desempeño de otros tipos de activos; las aplicaciones derivan su valor de sus relaciones con otros activos.
Infraestructura	Los activos de infraestructura existen en forma de capas que se definen por sus relaciones de apoyo a otros activos (personas y aplicaciones, en particular).
Capital Financiero	Los activos financieros son necesarios a fin de apoyar la propiedad o el uso de todo tipo de activos.

Fuente: (Van, Bon Jan, 2008).

2.2.16. Valoración de Activos según ITIL.

ITIL en los capítulos 4: Fase de diseño del Servicio y Capitulo 10: Introducción a funciones y procesos, específicamente en el numeral 10.4 Gestión de la Disponibilidad ITIL presenta diferentes menciones para valorar los activos como los siguientes:

- **Valorando datos por su disponibilidad:** Este enfoque mira qué procesos del negocio se afectarían si no se dispusiera de una porción determinada de los datos, y que costo le representaría esto a la Organización (Van, Bon Jan, 2008, págs. 212-220).

- **Valoración de pérdida de datos:** Este enfoque examina el costo de tener que reemplazar los datos si se pierden o son destruidos (Van, Bon Jan, 2008, págs. 212-220).
- **Valorando datos teniendo en cuenta el ciclo de vida:** Este enfoque se centra en cuestiones tales como cómo se crean los datos, cómo se hacen disponibles, y cómo se archivan; el ciclo de vida difiere (y por lo tanto, también lo hacen los costos) dependiendo de la demanda, o si estos pasos pueden ser realizados por un parte interna o externa (Van, Bon Jan, 2008, págs. 212-220).

Y propone clasificarlos en tres niveles:

- **Datos operacionales:** Estos son los datos necesarios para el funcionamiento de la organización y son menos específicos (Van, Bon Jan, 2008, págs. 212-220).
- **Datos tácticos**: Estos son los datos necesarios para la línea o administración superior; entre otras cosas, esto se refiere a los datos periódicos, analizados a partir de los sistemas de información de gestión (Van, Bon Jan, 2008, págs. 212-220).
- **Datos estratégicos:** Se refiere a las tendencias a largo plazo en comparación con información externa (mercado) (Van, Bon Jan, 2008, págs. 212-220).

En el numeral 10.4 manifiesta que La medición es extremadamente importante y propone tres perspectivas para la medición:

- **Perspectiva del negocio**: Mira la disponibilidad de TI en términos de su contribución o impacto en las funciones vitales del negocio (Van, Bon Jan, 2008, págs. 212-220).
- **Perspectiva del usuario:** Ve la disponibilidad de los servicios de TI como una combinación de tres factores: frecuencia, alcance en duración e impacto (cuántos usuarios o partes de la organización son afectados) y también tiempos de respuesta (Van, Bon Jan, 2008, págs. 212-220).

- **Perspectiva del proveedor de servicio de IT**: Ve la disponibilidad de los servicios y sus componentes desde el punto de vista de disponibilidad, confiabilidad y continuidad (Van, Bon Jan, 2008, págs. 212-220).

ITIL define dos conceptos para valorar un servicio:

- **Utilidad:** Aptitud para el propósito. Corresponde a los atributos del servicio que tienen un efecto positivo sobre el rendimiento de las actividades, los objetos y as tareas con un resultado específico. Utilidad representa el aumento de una posible ganancia (Van, Bon Jan, 2008, págs. 212-220).
- **Garantía:** Idoneidad para el uso. Disponibilidad y confiabilidad en la continuidad y seguridad. Soportes de garantía para la disminución de posibles pérdidas (Van, Bon Jan, 2008, págs. 212-220).

ITIL afirma que la creación de valor es una combinación de los efectos de utilidad y garantía, que ambos son necesarios para la creación de valor para el cliente.

La garantía asegura la utilidad de un servicio haciendo que esté disponible y que ofrezca suficiente capacidad, continuidad y seguridad.

- **Disponibilidad:** La disponibilidad es el aspecto más fundamental en la prestación de servicios a un cliente. Ofrece al cliente la garantía de que los servicios están disponibles según las condiciones acordadas.
- **Capacidad:** Sin la supervisión efectiva de los problemas de capacidad, los proveedores de servicios no se encuentran en condiciones de ofrecer la utilidad de la mayoría de los servicios.
- **Continuidad:** La continuidad garantiza que el servicio soporta al negocio incluso durante momentos de gran dificultad o en condiciones de desastre.
- **Seguridad:** Garantiza a los clientes que pueden hacer uso del servicio de manera segura.

2.2.17. Identificación de Riesgos según ITIL.

ITIL (Van, Bon Jan, 2008) hace referencia a CMDB (configuration managment database) es una base de datos donde constan todos los elementos de configuración y sus relaciones, los cuales van desde los servicios que ofrece TI, hasta la infraestructura que apoya el funcionamiento de estos servicios (servidores, redes, routers, etc.), incluyendo también personas, documentación, proveedores. Mantener una correcta CMDB, permite disponer de información necesaria para tomar decisiones sobre cualquier cambio que se realice en los elementos de configuración y mantener dimensionado el impacto que puede causar, ITIL a través de sus procesos de Gestión de configuración y Gestión de activos, sugiere que los diferentes elementos de configuración mantengan los siguientes atributos de seguridad: Confidencialidad, Integridad / Confiabilidad, Disponibilidad / Continuidad. También plantea que en el proceso de control de cambios, realice un análisis de riesgos en donde se evalúen:

- El impacto sobre los procesos del negocio.
- El impacto sobre los procesos de TI.
- Cual es el nivel de seguridad requerido.

Riesgos de contratos: (un contrato incluye acuerdos formal y legalmente vinculantes entre el negocio y los proveedores de servicios) – Los riesgos hacen imposible que el proveedor satisfaga los acuerdos contractuales, son riesgos estratégicos, porque no sólo amenazan la producción actual, sino también dañan la confianza para futuras interacciones. El impacto de los riesgos del contrato, los peligros subyacentes y sus debilidades no puede limitarse a una función específica del proceso. El cliente no hace distinción del origen de los riesgos. La coordinación durante todo el ciclo es necesaria a fin de administrar eficazmente los riesgos (Van, Bon Jan, 2008).

Riesgos de diseño: Los clientes esperan servicios para tener un impacto específico en el rendimiento de sus activos, lo que es una utilidad desde su perspectiva. Siempre existe el

riesgo que los servicios alcancen resultados no deseados. Esto es un riesgo de rendimiento. Un pobre rendimiento generalmente es el resultado de un mal diseño (Van, Bon Jan, 2008).

Riesgos operacionales: Cada organización se ocupa de los riesgos operacionales. Visto desde una perspectiva de gestión de servicio, existen dos tipos de distinguir: los riesgos para las unidades de negocio y los riesgos para las unidades de servicio (Van, Bon Jan, 2008).

Riesgos de mercado: La gestión eficaz de servicio ayuda a reducir los riesgos competitivos mediante el aumento de la escala y el alcance de la demanda de un catálogo de servicios. Otro enfoque es modificar el contenido del catálogo de servicios para que los clientes puedan encontrar la profundidad y amplitud que están buscando. Pueden reducir los riesgos de mercado a través de:

- **Diferenciación:** desde la perspectiva del cliente, los activos que son escasos y complementarios son interesantes. Los proveedores de servicios pueden concentrarse en proporcionar activos importantes que no hayan sido proporcionados por terceros. Los mercados desatendidos y carentes de servicios ofrecen oportunidades atractivas (Van, Bon Jan, 2008).
- **Consolidación:** la consolidación de la demanda reduce los riesgos financieros para proveedores de servicios, así como los riesgos operacionales para el cliente. (Van, Bon Jan, 2008).

2.2.18. Valoración de Riesgos según ITIL.

ITIL (Van, Bon Jan, 2008), En el capítulo de Gestión de la disponibilidad manifiesta que el objetivo de esta gestión es monitorear, analizar e informar sobre los siguientes elementos de la información:

Disponibilidad: El servicio o la capacidad del componente para funcionar según lo acordado con el cliente.

Confiabilidad: El tiempo de que un servicio o componente puede funcionar sin interrupción conforme a los acuerdos.

Recuperación: La velocidad y la eficacia de la reparación de un componente o servicio después de una falla; en otras palabras, cuán rápido se reanudará el funcionamiento normal.

Servicio: La capacidad de un proveedor externo para cumplir con los acuerdos de contrato.

Y afirma que para asegurar estos elementos se debe realizar en el diseño del servicio un análisis y gestión de riesgos como actividades proactivas.

Por otro lado en la Gestión de Continuidad de Servicio de TI cuyo objetivo es apoyar a la continuidad del negocio al asegurar que las de TI puedan reanudarse con los plazos acordados para lo cual es necesario que se realice lo siguiente:

- Acuerdos sobre alcance del plan de continuidad del negocio.
- Un análisis de impacto de negocio para calificar el impacto de calamidades.
- Análisis e identificación de riesgos (incluyendo medidas necesarias).
- La creación de una estrategia global de continuidad de negocio.
- La creación de planes de continuidad del negocio.
- Pruebas de los planes.
- Mantenimiento continúo de los planes.

2.2.19. Riesgos y Tendencias.

A continuación se presentan diferentes investigaciones realizadas por laboratorios de injerencia mundial en materia de seguridad de la información, estas empresas de manera permanente mantienen un análisis y monitoreo de las amenazas informáticas y sus tendencias.

Se debe recalcar que los resultados producto de los análisis desarrollados por los laboratorios de seguridad de la información a nivel mundial, se constituyen en una base

muy importante para establecer los criterios de medición del riesgo en cuanto a impacto y probabilidad de ocurrencia, ya que los estudios mencionan las tasas de incremento de las amenazas informáticas y los impactos económicos que han representado.

2.2.19.1. Según Kaspersky Lab.

"Según los datos provenientes de los subsistemas de protección de los productos de Kaspersky Lab, en el 2013 la cantidad de ataques financieros, ya sean phishing o mediante el uso de programas maliciosos, ha crecido notablemente" (Kaspersky Lab, 2014).

Las principales cifras obtenidas durante la investigación son las siguientes:

- "El 31,45% de todos los ataques phishing en 2013 afectó al sector financiero" (Kaspersky Lab, 2014).
- "El 22,2% de los ataques se realizó mediante sitios falsificados de bancos; el porcentaje de phishing bancario se ha duplicado en comparación con 2012" (Kaspersky Lab, 2014).
- "El 59,5% de los ataques phishing bancarios explotaban los nombres de 25 bancos internacionales. El resto de ataques se repartió entre más de 1000 otros bancos" (Kaspersky Lab, 2014).
- "El 38,92% de las reacciones de las tecnologías de defensa de Kaspersky Lab en equipos Mac ocurrieron al visitar páginas phishing "financieras" (Kaspersky Lab, 2014).
- "La cantidad de ataques informáticos realizados usando programas maliciosos dirigidos al robo de datos financieros en 2013 creció en un 27,6% y alcanzó los 28,4 millones" (Kapersky Lab, 2014).
- "La cantidad de usuarios atacados fue de 3,8 millones y el crecimiento en el año de un 18,6% " (Kapersky Lab, 2014).
- "La cantidad de usuarios que se toparon con ataques financieros realizados mediante programas maliciosos en 2013 fue del 6,2% del total de usuarios atacados. En

comparación con 2012 este índice ha crecido en 1,3 puntos porcentuales" (Kapersky Lab, 2014).

- "Entre los programas maliciosos financieros se desarrollaron más activamente los instrumentos relacionados con Bitcoin, pero el papel principal lo sigue jugando el robo de dinero de cuentas bancarias, por ejemplo el programas malicioso Zeus" (Kapersky Lab, 2014).
- "En la colección de Kaspersky Lab la cantidad de aplicaciones maliciosas para Android en el segundo semestre de 2013 casi se ha quintuplicado, desde 265 muestras en junio hasta 1321 en diciembre" (Kapersky Lab, 2014).
- "En 2013 los expertos de Kaspersky Lab descubrieron por primera vez programas troyanos para Android capaces de robar dinero de las cuentas bancarias de los usuarios" (Kapersky Lab, 2014).

En el área financiera los ataques informáticos dirigidos al robo de datos afectó a las entidades en $28.4 millones y se debe considerar que la tasa de crecimiento anual de estos ataques es del 27.6%. Se puede observar también el incremento de un 18,6% que existe en cuanto a los usuarios atacados en el año 2013, fueron 3.8 millones de usuarios, ya sea por suplantación de identidad (pishing), programas maliciosos u otros tipos de ataques.

Estos resultados se los debe tomar como referencia para la evaluación del riesgo en lo que se refiere a la probabilidad de ocurrencia de un ataque informático y del impacto que puede causar la materialización de una amenaza, determinando el nivel del riesgo informático en el que se encuentra determinada institución.

2.2.19.2. Según PWC Asesores Empresariales.

Pwc Asesores empresariales realizó un estudio desde febrero del 2013 a abril del 2013, el alcance fue el siguiente:

- 115 países.

- 9600 encuestados entre ellos CEOs, CISOs, CIOs VPs y directores de IT y de seguridad.
- Más de 40 preguntas sobre los controles de privacidad y seguridad de la información y su alineamiento con los objetivos del negocio.
- 39% de los encuestados corresponden a compañías de más de 500 millones de ingresos anuales.
- De los encuestados el 36% son de Norte América, 26% de Europa, 21% Asia Pacífico, 16% Sudamérica, 2% Medio Oriente y África.
- 993 incluyen a las empresas de servicios financieros.
- Margen de error menos del 1%, los valores no pueden sumar el 100% debido al redondeo. (PWC Asesores Empresariales, 2014)

Resultados:

Los resultados obtenidos de esta encuesta fueron los siguientes:

- Se obtuvo los porcentajes de las empresas que mantienen desactualizados los controles de seguridad frente a las nuevas amenazas que existen actualmente. Figura 4.
- Hubo un incremento en el 2013 de un 25% de incidentes de seguridad de la información con respecto al 2012. Figura 5.
- Los costos financieros por incidentes de seguridad con respecto al año 2012 han incrementado en un 18%. Figura 6.

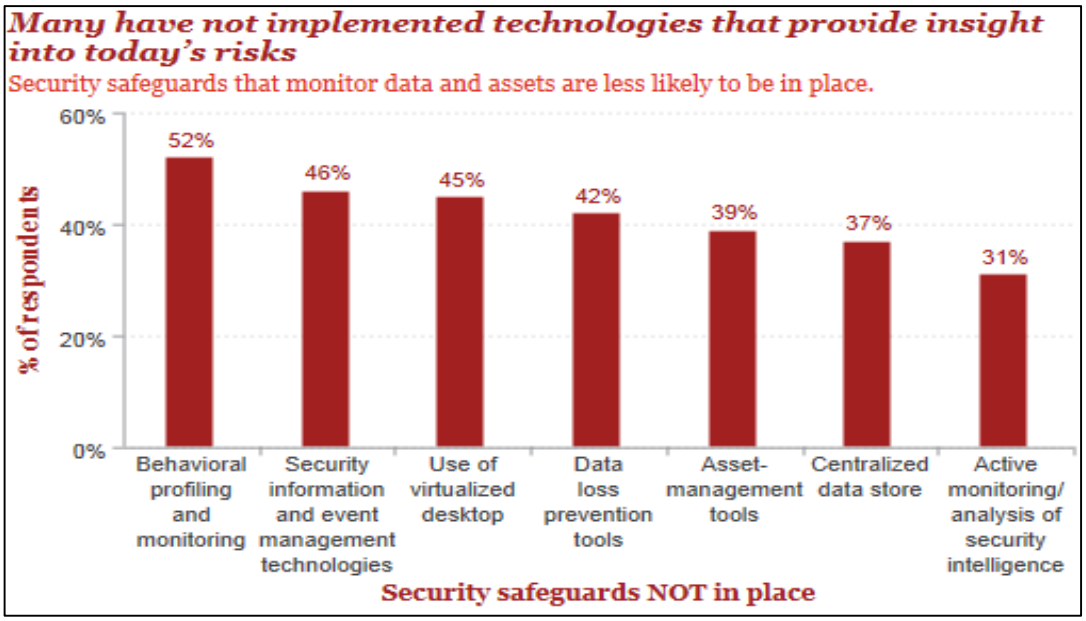


Figura 4: "Many Have not implemented technologies that provide insight into today´s risk"
Fuente : (PWC Asesores Empresariales, 2014).

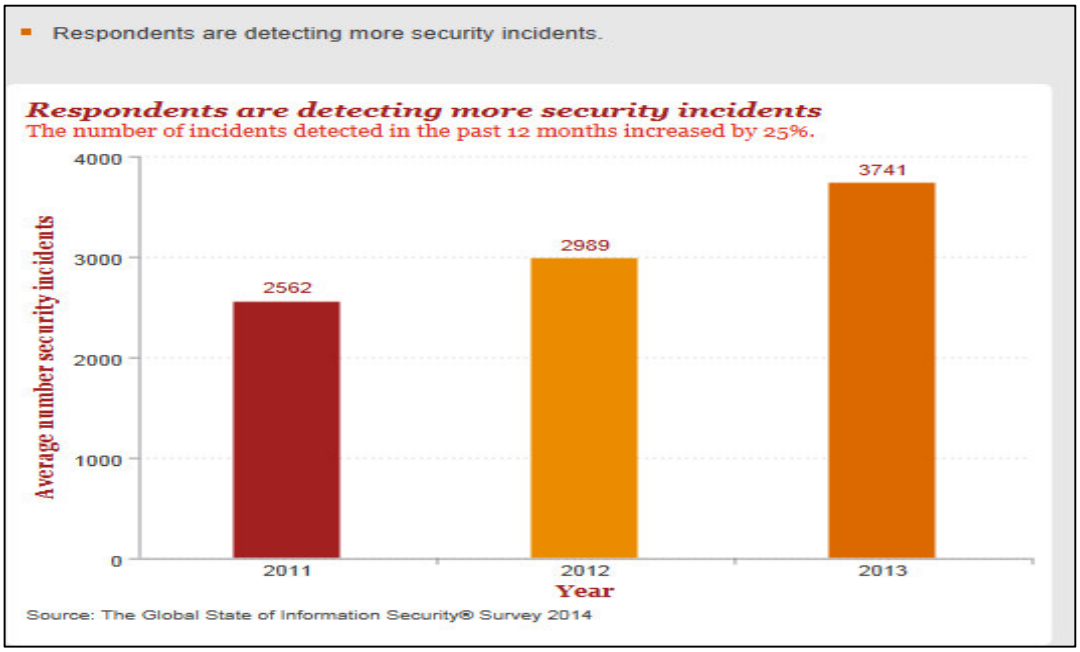


Figura 5: "Respondents are detecting more security incidents"
Fuente: (PWC Asesores Empresariales, 2014).

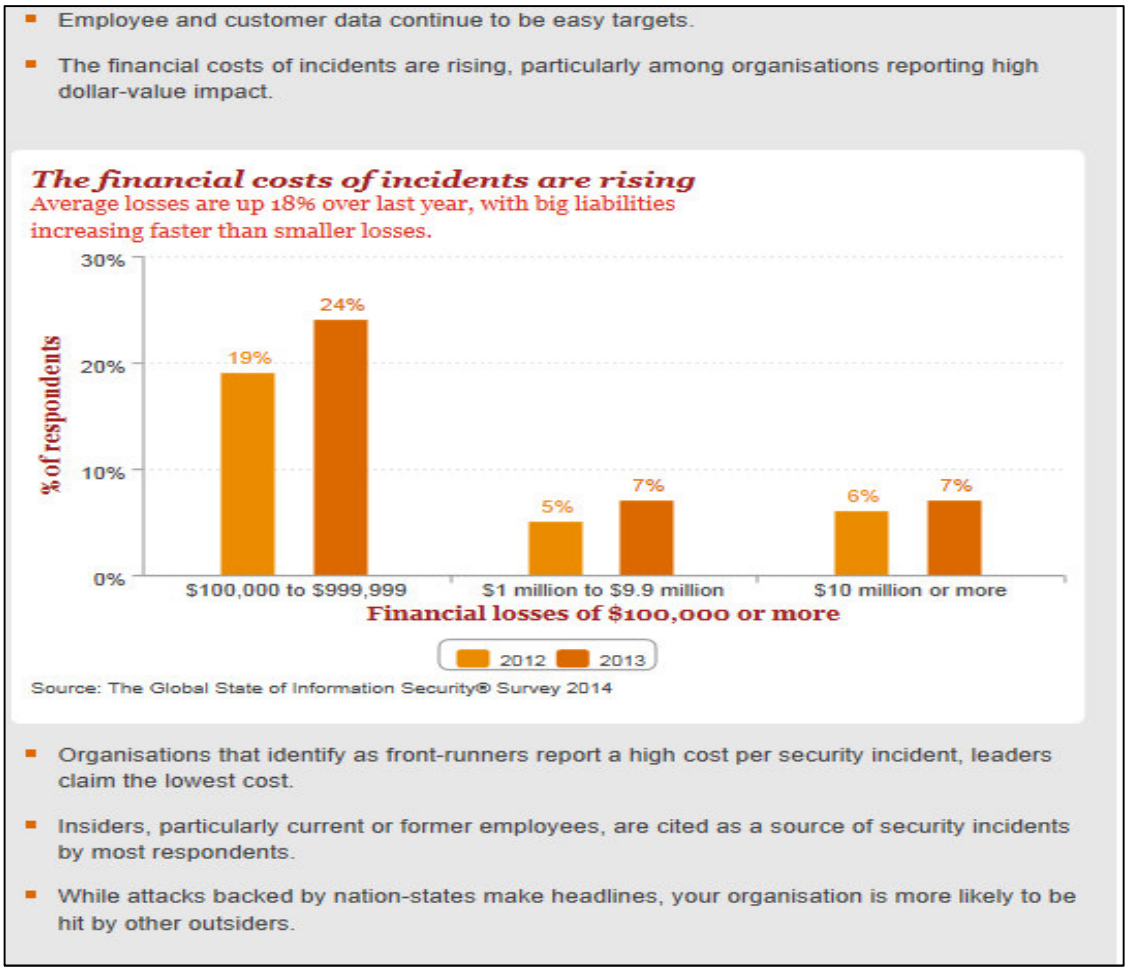


Figura 6: "The financial costs of incidents are rising"
Fuente: (PWC Asesores Empresariales, 2014)

Las tasas de crecimiento de los ataques informáticos determinan que las instituciones están expuestas a tener altos impactos frente a la materialización de alguna de las amenazas analizadas, además al no tener los controles debidamente diseñados, implementados y monitoreados la probabilidad de ocurrencia y éxito en los ataques informáticos es muy alta.

2.2.19.3 Según el informe Cisco. (CISCO, 2014)

La evaluación de las amenazas realizadas por Cisco se basó en información obtenida de la siguiente manera:

- 16 mil millones de peticiones web son inspeccionados todos los días a través de Cisco Cloud Security Web.
- 93 mil millones de mensajes de correo electrónico se inspeccionan todos los días por la solución de correo electrónico alojado de Cisco.
- 200.000 direcciones IP son evaluados diariamente.
- 400.000 ejemplares de malware son evaluados diariamente.
- 33 millones de archivos de puntos finales se evalúan todos los días.
- 28 millones de Conexiones de red son evaluados cada día.

Amenazas detectadas por Cisco:

- 4,5 mil millones de mensajes de correo electrónico se bloquean todos los días.
- 80 millones de peticiones web se bloquean todos los días.
- 6.450 detecciones de archivos de punto final se producen cada día.
- detecciones de red de punto final se producen cada día.
- 50.000 intrusiones en la red se detectan todos los días.

De los resultados obtenidos, se puede deducir que la seguridad perimetral en las diferentes instituciones deben ser muy fortalecidas y de monitoreo permanente, ya que son ataques que se realizan desde el exterior de las entidades, haciendo uso de los canales de comunicación que tienen las instituciones con sus colaboradores y con sus clientes, especialmente por el internet, además se debe recalcar que el monitoreo debe ser permanente, más aún, en el caso de las entidades financieras, las cuales prestan sus servicios transaccionales a través de medios electrónicos las 24 horas del día, por lo tanto la seguridad debe ser monitoreada por 7 días a la semana, 24 horas del día y los 365 días del año y no restringirse a las horas y días laborables. El diseño de una estructura de seguridad perimetral acorde a las necesidades de las instituciones y con monitoreo permanente, son factores de gran relevancia para la mitigación del riesgo.

2.2.19.4 Según Websense Inc.

En el informe denominado “Informe de Amenazas 2014 Websense” (Websense, 2014)**,** se destacan los siguientes puntos:

- Websense previno en el año 2013, 4.1 mil millones de ataques informáticos.
- El objetivo de los ataques era evadir seguridades tradicionales, poner en peligro sistemas y obtener datos confidenciales a través de redes infectadas.
- Si bien el robo de datos fue el objetivo común de los atacantes, la motivación prevalente para atacar fue la obtención de beneficios económicos, sin embargo existieron otros motivos como el hacer daño a la imagen y competitividad de una empresa, ataques relacionados con la política para desprestigiar gobiernos o para robar secretos de estado.
- En el informe se menciona de un modelo denominado cadena de ataque, que es utilizado como procedimiento por los atacantes y está compuesto de siete etapas : Reconocimiento, señuelo, redireccionamiento, kit de explotaciones, archivo detonante, llamada a casa, robo de datos.

El informe de igual manera hace notar el gran número de ataques informáticos a los que están expuestas las instituciones, sin embargo cabe destacar que también se hace mención sobre las diferentes intenciones que tienen los ataques informáticos y que son ejecutados por organizaciones que mantienen procedimiento elaborados, situaciones que deben ser muy tomadas en cuenta por las personas que se encargan de la seguridad de la información en las instituciones para que las estrategias de seguridad a implementarse tenga un alto nivel de análisis e implementación.

2.2.19.5 Según Ponemon Institute y Websense Inc. (Ponemon Institute, 2014)

El estudio fue realizado mediante una encuesta a 4.881 profesionales de la seguridad en 15 países, con un promedio de 10 años de experiencia en el área, los resultados dicen lo siguiente:

- Los profesionales de la seguridad manifiestan que sus sistemas de seguridad no tienen la especialización necesaria como para cubrir los actuales ataques cibernéticos y fugas de información ya que es necesario mantener un sistema de inteligencia que permita anticipar, identificar y reducir las amenazas y los sistemas de seguridad no lo tienen en su mayoría.
- El 50% manifiestan que sus organizaciones no están cubiertas para ataques cibernéticos avanzados.
- El 63% de los encuestados tienen la duda que la fuga de información confidencial de sus organizaciones este controlada.
- El 69% de los encuestados manifiestan que las amenazas de seguridad se materializan debido a los huecos de seguridad que mantienen los sistemas implementados en las empresas.
- El 44% de las empresas tuvo ataques cibernéticos importantes durante el año.
- El 59% de las organizaciones no tienen un buen conocimiento de los intentos de ataque y además no tienen a disposición un sistema de inteligencia que permita prever las amenazas.
- El 51% de los encuestados mencionan que no están seguros que sus sistemas de seguridad informen sobre las causas raíz de los ataques.
- El 89% de encuestados no tienen en cuenta la relación que puede existir entre la pérdida potencial de ingresos, debido a la fuga de datos confidenciales.
- Ponemon Institute indica que el costo promedio por fuga u otros ataques a la información confidencial de una empresa es de $5,4 millones.

- El 48% de los encuestados manifiestan no tener un buen conocimiento sobre seguridad de la información.

Los resultados obtenidos en el informe ponen en manifiesto lo siguiente:

- Los dirigentes en las instituciones no mantienen un criterio firme y objetivo de la relación que debe existir entre el cumplimiento de los objetivos del negocio y la seguridad que debe mantener la información institucional, motivo por el cual los presupuestos para implementar y administrar la seguridad de la información son mínimos o no existen.
- En las instituciones tanto directivos como personal tienen muy poca o ninguna capacitación sobre temas de seguridad de la información.
- Las instituciones no tienen la debida certeza de que los controles implementados para la seguridad de la información sean capaces de cubrir ataques avanzados de última generación.

El mantener las debilidades mencionadas en una institución, solo lleva a deducir que la información institucional mantiene un nivel de riesgo muy alto, debido a que no existe un compromiso por parte de los dirigentes para implementar un sistema de gestión de seguridad de la información que se ocupe de identificar y valorar los activos de información y los riesgos a los que se enfrentan.

2.2.20. Controles o Salvaguardas.

En esta sección se presentan diferentes investigaciones realizadas por laboratorios encargados de certificar las tecnologías que actualmente se tienen a disposición para controlar algunos de los ataques informáticos analizados en la sección anterior.

Se debe recalcar que las evaluaciones sobre la efectividad de las tecnologías de seguridad, se constituyen en una base fundamental para establecer criterios en lo que se refiere a la evaluación del riesgo en lo que se refiere a su mitigación.

2.2.20.1. Según NSSLabs. (NSS Labs, 2013)

Anti-Pishing

Los ataques de pishing son de gran afectación especialmente en el sector financiero, para determinar cuál es el alcance de los diferentes productos de protección de punto final en cuanto al pishing, se obtuvo el análisis de 5 productos de consumo masivo, denominadas suites de protección que además proporcionan protección contra troyanos, bootkits, spyware, rootkits y obviamente contra el pishing, los resultados obtenidos son los presentados en la figura 7.

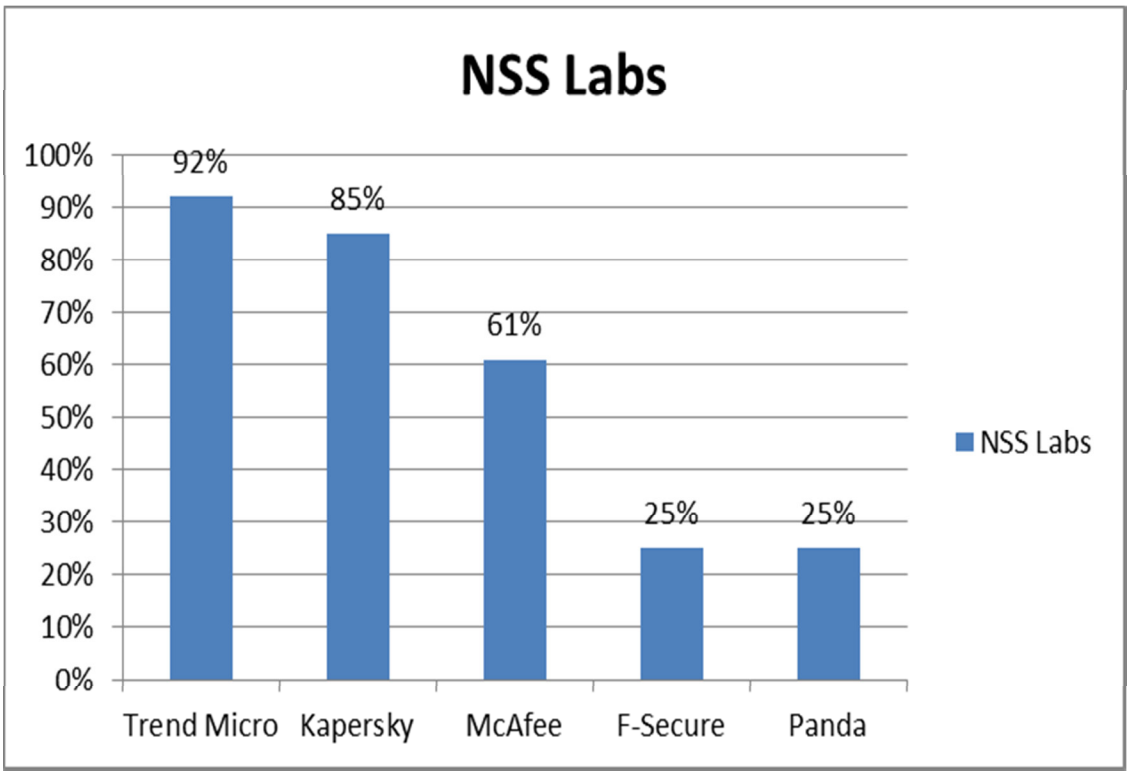


Figura 7: Tasa de eficacia de protección contra el pishing.
Fuente: (NSS Labs, 2013)

Los resultados de la evaluación sobre la efectividad de los aplicativos de punto final demuestran que ninguno de ellos llegan a una efectividad del 100%, límite que debe ser considerado para cuando se evalúe el riesgo informático.

Anti-malware (Ataques de Ingeniería Social).

Los navegadores para internet son los aplicativos de defensa de primera instancia contra los ataques de ingeniería social, en el análisis se incluyeron 8 navegadores, de los cuales se pudo determinar los diferentes niveles de efectividad, como se puede observar en la figura 8.

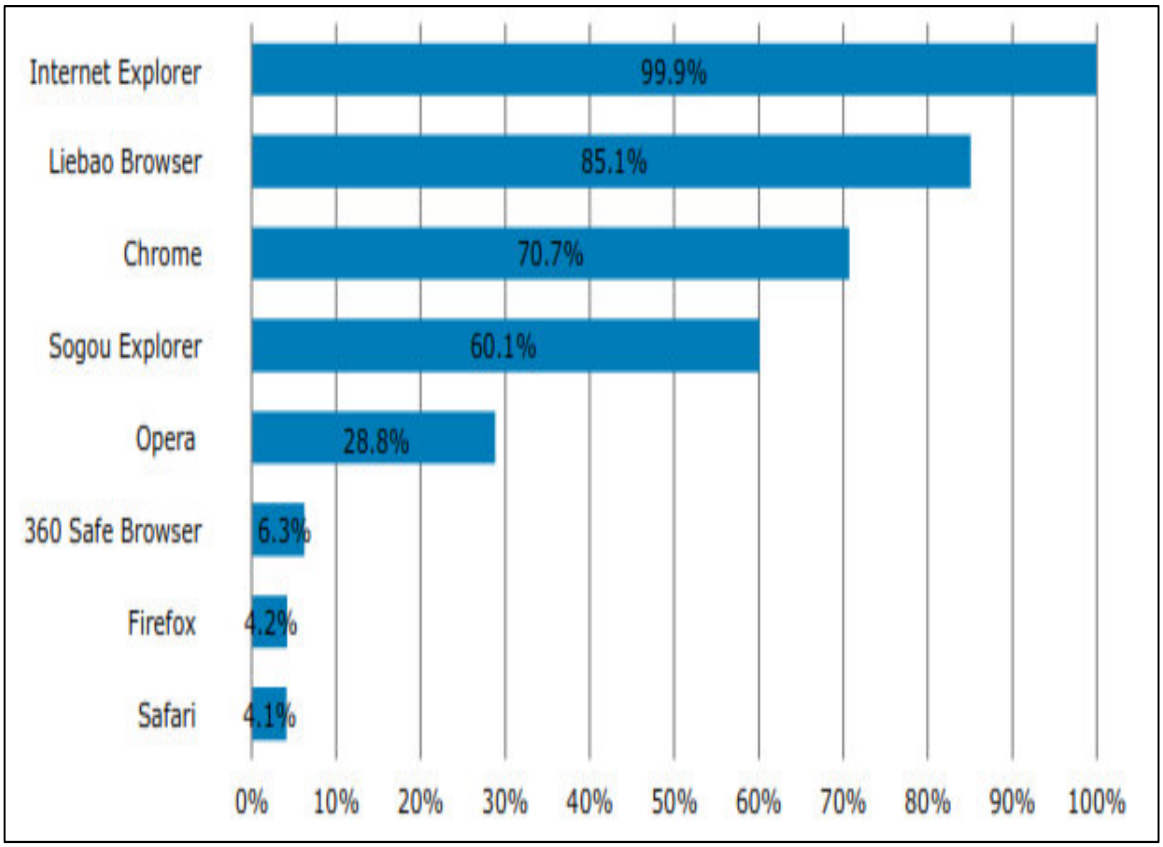


Figura 8: Tasa de eficacia en el bloqueo de ataques de ingeniería social.
Fuente: (NSS Labs, 2013)

Es necesario mencionar que el nivel de efectividad de los navegadores, no debe ser considerado como un elemento total para la mitigación del riesgo de ataque del malware, sino como un elemento adicional que contribuye controlar la amenaza del malware, debido

a que existen diferentes tipos de malware que posiblemente no sean mitigados por los exploradores. De igual forma se debe notar que el control no llega al 100% de efectividad.

2.2.20.2. Según AV Comparatives. (AV Comparatives, 2013)

Pishing

En el estudio realizado se puso a prueba 5 productos de diferentes marcas con la finalidad de establecer el porcentaje de protección que tienen cada uno de ellos frente al ataque de pishing, los resultados se pueden observar en la figura 9.

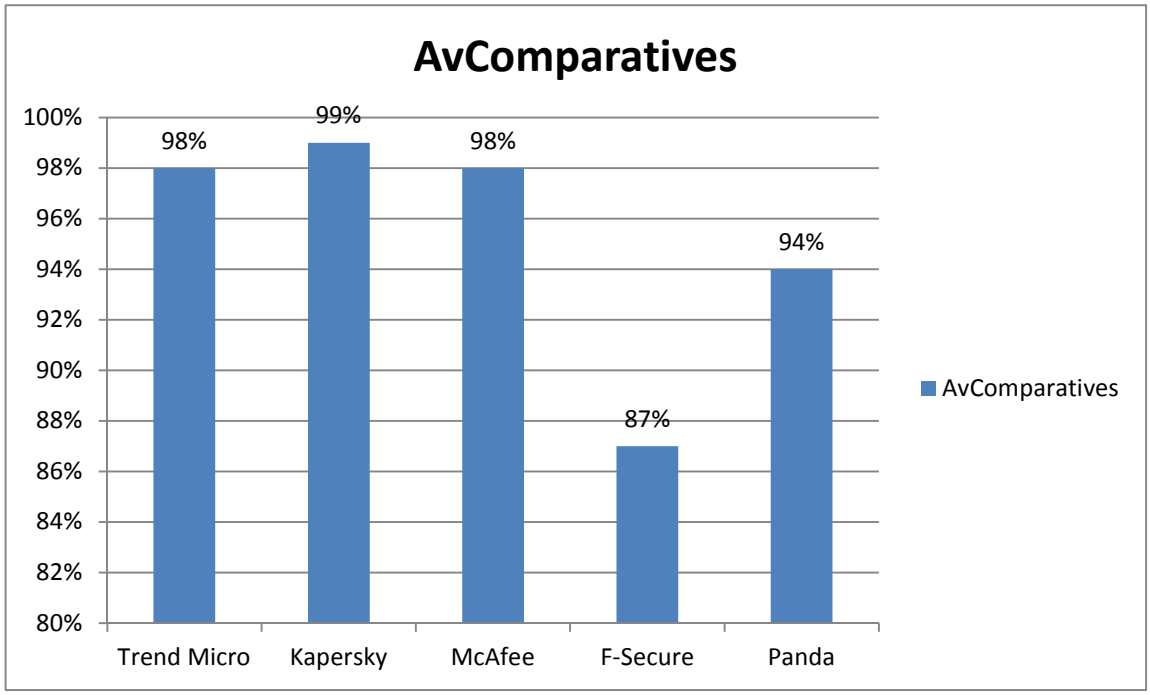


Figura 9: Tasa de eficacia de protección contra el pishing.
Fuente: (AV Comparatives, 2013).

En este análisis se evaluaron los mismos productos anti-pishing que en la sección 2.1.1 l y como se puede observar, los niveles de efectividad son diferentes, esta diferencia debe ser debidamente interpretada para establecer métricas en la evaluación de los controles que

mantenga la institución o que se implemente en la misma para la evaluación del riesgo informático.

Malware.

Con el objetivo de establecer la eficiencia de protección contra el malware, se aplicó a 16 diferentes productos 11 diferentes casos de ataques de malware y para la calificación se lo realizó considerando la información de las tablas 9 y 10:

Tabla 9

Criterios para calificar la eficiencia en el control del malware.

Eliminación del malware	Asignación
Removió el Malware y solo quedaron rastros insignificantes	A
Removió el Malware pero algunos ejecutables o registros fueron modificados	B
Removió el Malware pero existen problemas potenciales (Mensajes de error, Archivos de hosts comprometidos, deshabilitados registros del sistema, detección de loops)	C
Solo el Malware fue neutralizado pero otros archivos maliciosos no fueron removidos y el sistema ya no puede ser usado con normalidad	D
Acciones	
La eliminación del malware es en modo normal.	A
La eliminación del malware requiere de una reiniciación del sistema en modo seguro y de la intervención de otros utilitarios o procedimientos manuales	B
La eliminación requiere que el disco se rescatado o reparado	C
La eliminación del malware requiere contactar soporte o similares; La eliminación del malware fue fallida	D

Fuente : AV Comparatives.

Tabla 10

Tabla de puntaje asignado por calificación.

Asignación	Puntaje	Puntaje	Descripción
AA	100	86-100	Avanzado +
AB	90	71-85	Avanzado +
AC	80	56-70	Estándar
BA	70	<56	Para investigar
BB	60		
BC	50		
CA	40		
CB	30		
CC	20		
DD	0		

Fuente : AV Comparatives.

Los resultados obtenidos en la calificación de los 16 productos se los puede observar en la figura 10.

	Sample											Points
	1	2	3	4	5	6	7	8	9	10	11	∅
AhnLab	DD	AA	AA	AA	BA	BA	AA	AA	AA	AB	DD	75
Avast	AA	AA	AA	AA	AA	AA	BA	AA	CA	AA	BC	87
AVIRA	AA	AA	AA	AA	AA	AA	AA	AA	BA	BB	AC	92
Bitdefender	AA	AA	AA	AA	AA	AA	AA	AA	AA	AB	AC	97
BullGuard	AA	BA	BA	BA	BA	AA	AA	BA	AA	BC	DD	73
Emsisoft	AA	AA	AA	AA	BA	AA	AA	AA	CA	BB	DD	79
eScan	AA	AA	AA	AA	BA	BA	AA	AA	AA	AB	DD	85
ESET	AA	AA	AA	AA	AA	AA	BA	AA	AA	BC	BC	88
F-Secure	AA	DD	AA	AA	AA	AA	AA	AA	AA	BC	BC	82
Fortinet	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	DD	91
G DATA	AA	AA	AA	BA	BA	BA	AA	AA	CA	DD	BC	73
Kaspersky Lab	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AC	98
Microsoft	AA	AA	BA	AA	AA	AA	AA	BA	AA	BA	DD	83
Panda	AA	AA	AA	AA	AA	AA	BA	AA	AA	AB	DD	87
Sophos	AA	AA	AA	AA	BA	AA	AA	AA	BA	BC	BC	85
ThreatTrack Vipre	BA	BA	BA	AA	BA	BA	BA	BA	CA	AB	DD	65

Figura 10: Calificación la eficiencia para controlar el malware.
Fuente:(AV Comparatives, 2013).

En esta evaluación se obtuvo los niveles de eficacia de diferentes productos anti-malware, calificaciones que sirven de referencia para medir el nivel de riesgo de acuerdo al control que se mantenga implementado en las diferentes instituciones.

UTM networking.

El UTM tiene la función de identificar y detectar el tráfico malicioso que pretende ingresar hacia la infraestructura tecnológica de una institución, por lo tanto es necesario obtener un criterio sobre la capacidad que puede tener un firewall para detectar y bloquear el tráfico malicioso, con la finalidad de que esta tecnología sea implementada, actualizada o evaluada para determinar si el firewall-ips está cumpliendo con el objetivo de mitigar el riesgo de un ataque informático. A continuación se presentan el análisis de algunos firewall-ips en cuanto a: eficacia en entregar seguridad, la capacidad de procesamiento, y el tiempo de latencia. Elementos fundamentales que deben ser evaluados conjuntamente con las necesidades de seguridad de cada institución para mitigar el nivel de riesgo en el que se encuentra la información institucional.

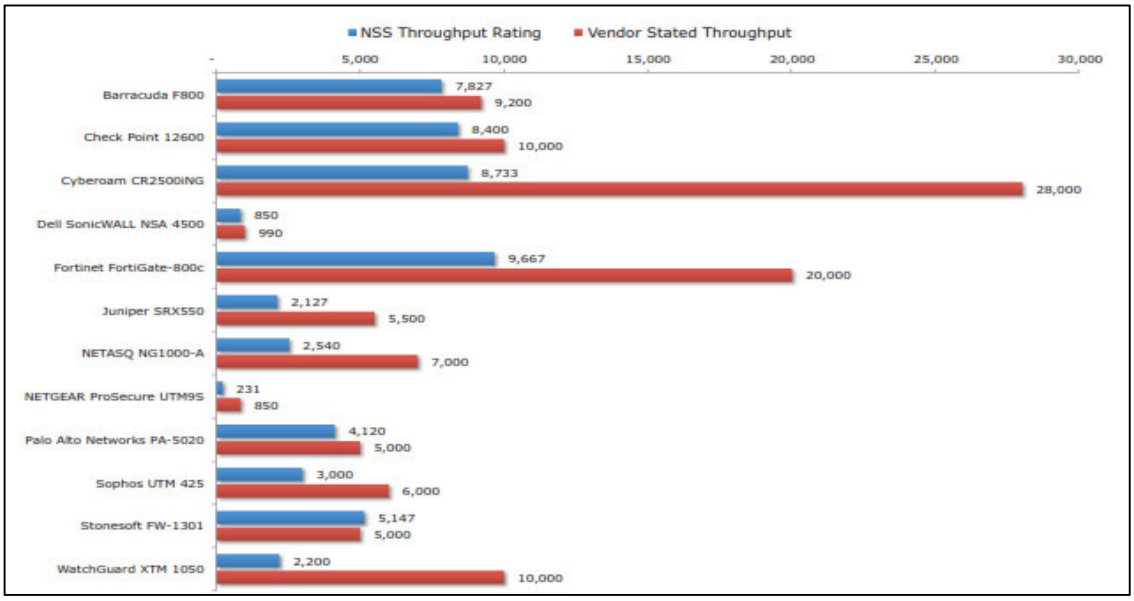


Figura 11: Evaluación de la eficacia en detección y bloqueo en Mbps.
Fuente: (AV Comparatives, 2013).

Product	64 Byte Packets - Latency (µs)	128 Byte Packets - Latency (µs)	256 Byte Packets - Latency (µs)	512 Byte Packets - Latency (µs)	1024 Byte Packets - Latency (µs)	1514 Byte Packets - Latency (µs)
Barracuda F800	273	163	108	104	103	109
Check Point 12600	75	124	99	82	102	109
Cyberoam CR2500iNG	1,185	845	452	385	302	270
Dell SonicWALL NSA 4500	30	31	32	33	37	42
Fortinet FortiGate-800c	5	6	6	7	8	9
Juniper SRX550	12	12	12	13	14	16
NETASQ NG1000-A	36	36	43	46	47	36
NETGEAR ProSecure UTM9S	232	237	243	255	337	603
Palo Alto Networks PA-5020	15	19	22	26	33	38
Sophos UTM 425	59	61	60	63	92	169
Stonesoft FW-1301	50	84	51	54	82	81
WatchGuard XTM 1050	136	156	182	269	460	705

Figura 12: Latencia de los firewalls en microsegundos.
Fuente: (AV Comparatives, 2013).

2.3. Marco Conceptual.

2.3.1. Sistema de gestión de seguridad de la información (SGSI).

"Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información (**ICONTEC ISO/IEC 27001, 2006, pág. 3**).

2.3.2. La Seguridad de la Información.

La seguridad de la información es un conjunto apropiado de controles que permiten preservar la confidencialidad, integridad y disponibilidad de la información con la finalidad de entregar la debida protección a la información institucional contra las diferentes amenazas que se pueden presentar según el entorno donde la institución desarrolle sus actividades, asegurando la continuidad del negocio, minimizando el riesgo al

que se encuentra expuesta la información, maximizando el retorno de las inversiones y oportunidades del negocio (**ICONTEC ISO/IEC 17799, 2006, pág. 2**).

2.3.3. Riesgo Informático.

Es la posibilidad de que una amenaza explote o se aproveche de las vulnerabilidades que mantiene un activo de información provocando un determinado impacto en la institución. Generalmente y de acuerdo a la definición al riesgo se lo mide por la relación impacto por probabilidad **(ICONTEC ISO/IEC 27005, 2009, pág. 2).**

2.3.5. Análisis de Riesgos.

Es el estudio de:

- Las amenazas que están en el entorno donde se desarrollan las actividades de la institución.
- Las vulnerabilidades que mantienen los activos de información.
- La Probabilidad que la amenaza explote la vulnerabilidad que mantiene el activo.
- El impacto que generé en el negocio.

2.3.4. Gestión del Riesgo.

Es un conjunto de estrategias debidamente coordinadas en la institución para manejar la incertidumbre proveniente de la amenaza, las estrategias pueden ser: transferir el riesgo, mitigar el riesgo, aceptar el riesgo (Cevallos, 2014).

2.3.5. Evento de Seguridad de la Información.

Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad (**ICONTEC ISO/IEC 17799, 2006, pág. 2**).

2.3.6. Incidente de Seguridad de la información.

Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información **(ICONTEC ISO/IEC 17799, 2006, pág. 2**).

2.3.7. Control.

"Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

NOTA. El control también se utiliza como sinónimo de salvaguarda o contramedida" (ICONTEC ISO/IEC 17799, 2006, pág. 1).

2.3.8. Integridad.

"Propiedad de salvaguardar la exactitud y estado completo de los activos" (ICONTEC ISO/IEC 27001, 2006, pág. 3).

2.3.9. Reducción del Riesgo.

"Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

NOTA En el contexto de esta norma, el término "posibilidad" se utiliza en lugar del término "probabilidad" para la reducción del riesgo" (ICONTEC ISO/IEC 27005, 2009, pág. 2).

2.3.10. Retención del Riesgo.

"Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

NOTA En el contexto de los riesgos en la seguridad de la información, únicamente se consideran las consecuencias negativas (pérdidas) para la retención del riesgo" (ICONTEC ISO/IEC 27005, 2009, pág. 2).

2.3.11. Transferencia del Riesgo.

"Compartir con otra de las partes la pérdida o la ganancia de un riesgo.

NOTA En el contexto de los riesgos en la seguridad de la información, únicamente se consideran las consecuencias negativas (pérdidas) para la transferencia del riesgo" (ICONTEC ISO/IEC 27005, 2009, pág. 2).

2.3.12. Tratamiento del Riesgo.

"Proceso de selección e implementación de medidas para modificar el riesgo" (ICONTEC ISO/IEC 17799, 2006, pág. 2).

2.3.13. Valoración del Riesgo.

"Proceso global de análisis y evaluación del riesgo" (ICONTEC ISO/IEC 27001, 2006, pág. 4).

2.3.14. Vulnerabilidad.

La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas (ICONTEC ISO/IEC 17799, 2006, pág. 3).

2.3.15. Proceso

"Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas". (ICONTEC ISO/IEC 27001, 2006)

2.3.16. Subproceso.

Conjunto de actividades que forman parte de un proceso.

2.3.17 Riesgo inherente.

Es el riesgo que mantiene el activo de información cuando no existe ningún tipo de control o salvaguarda. (ICONTEC ISO/IEC 27001, 2006)

2.3.18 Riesgo residual.

Es el riesgo que permanece en el activo, aún con la implementación de controles o salvaguardas.

2.4. Marco Legal.

La Superintendencia de Bancos y Seguros del Ecuador, consiente del incremento del delito informático y sobre todo sensibles del riesgo a los que están sometidos los capitales

depositados en las diferentes entidades financieras, emitió el 25 de octubre del 2005 la resolución No JB-2005-834 (Anexo1), documento que en la sección II trata sobre el tema "Factores de riesgo Operativo" donde manifiesta lo siguiente : "……La resolución imparte una serie de disposiciones aplicables al sistema financiero a fin de contar con un sistema de gestión efectivo para la administración del riesgo operativo que permita identificar, medir, controlar/mitigar los riesgos derivados de fallas o insuficiencias en los procesos, personas, tecnologías de información y eventos externos, incluyendo el riesgo legal…" (**Superintendencia de Bancos, 2005**).

En materia de Seguridad de la Información, la Resolución JB-2005-834 abarca disposiciones, en las que se señala que las instituciones deben disponer de políticas, procesos y procedimientos que aseguren:

- Que el sistema de administración de seguridad de la información satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas.
- Que exista continuidad en la operación de la institución frente a eventos imprevistos en las tecnologías de información.
- Que los planes de contingencia y continuidad garanticen la capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio, implementando además un proceso de administración de la continuidad del negocio.

Como respaldo a la normativa JB-2005-834 la Superintendencia emite el 19 de Junio del 2012, la normativa JB-2012-2148, en donde se especifica las seguridades que deben implementar las entidades financieras, en los canales electrónicos por medio de los cuales prestan servicios transaccionales a sus clientes.

Cabe mencionar que las resoluciones JB-2005-834 y JB-2012-2148, en todo su contexto han sido adoptadas por la Superintendencia de Economía Popular y Solidaria y son de estricto cumplimiento para las entidades financieras que son controladas por esta

entidad (cooperativas de ahorro y crédito). A continuación se describen cada una de las normativas mencionadas.

2.4.1. Normativa JB-2005-834

La resolución JB-2005-834, emitida en Octubre del 2005 por la Superintendencia de Bancos y seguros y adoptada en todo su contexto por la Superintendencia de Economía Popular y Solidaria (Junta Bancaria del Ecuador, 2005), establece un conjunto de principios que proporcionan a las Entidades financieras un marco para la gestión y supervisión efectiva del riesgo operativo; también es de uso para entidades de supervisión al momento de evaluar políticas y prácticas de gestión del riesgo operativo. Además, el alcance de la norma depende de factores tales como: el tamaño, la sofisticación y complejidad de las entidades financieras para las que aplica. La resolución imparte una serie de disposiciones aplicables al sistema financiero a fin de contar con un sistema de gestión efectivo para la administración del riesgo operativo, que permita identificar, medir, controlar/mitigar los riesgos derivados de fallas o insuficiencias en los procesos, personas, tecnologías de información y eventos externos, incluyendo el riesgo legal.

La resolución recomienda que se cumpla con sus directrices respecto a la administración de los procesos, personas, tecnología de la información y eventos externos, agrupando sus procesos por línea de negocio, identificando para cada una de éstas sus eventos de riesgo, las mismas que están agrupadas de la siguiente manera: Fraude Interno, Fraude Externo, Prácticas Laborales y Seguridad del Ambiente de Trabajo, prácticas relacionadas con los clientes, productos y negocios, daños a los activos físicos, fallas de tecnología de información y, deficiencias en la ejecución de procesos, operaciones y relaciones con proveedores y terceros.

La norma menciona dentro del riesgo operativo a los riesgos en tecnologías de la información**.** La tecnología es el factor que quizás tiene mayor alcance y complejidad de todos los que integran el riesgo operativo, esto se debe a dos causas principales: las

tecnologías de información se extienden por todos los procesos y niveles de decisión de la Institución, además, siguen siendo un tema muy complejo y técnico, manejado por especialistas, quienes son presionados cada vez más en la entrega de servicios oportunos y de calidad.

Se debe considerar que para contar con una apropiada gestión del riesgo, las instituciones deben disponer de políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de las tecnologías de información para garantizar lo siguiente:

- Soportar adecuadamente los requerimientos de operación actuales y futuros de la entidad;
- Satisfacer los requerimientos de la entidad;
- Administrar adecuadamente los recursos y servicios provistos por terceros y monitorear la efectividad y eficiencia del servicio.
- Satisfacer los objetivos del negocio en lo referente a adquisición, desarrollo, implementación y mantenimiento de aplicaciones;
- Administrar y monitorear correctamente la infraestructura tecnológica que soporta las operaciones.

En materia de Seguridad de la Información, la Resolución JB-2005-834 abarca otras disposiciones, en las que se señala que las instituciones deben disponer de políticas, procesos y procedimientos que aseguren:

- Que el sistema de administración de seguridad de la información satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas.
- Que exista continuidad en la operación de la institución frente a eventos imprevistos en las tecnologías de información.
- Que los planes de contingencia y continuidad garanticen la capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del

negocio, implementando además un proceso de administración de la continuidad del negocio.

2.4.2. Normativa JB-2012-2148.

La norma JB-2012-2148 emitida en Junio del 2012 por la Superintendencia de Bancos y Seguros adoptada en su totalidad por la Superintendencia de Economía Popular y Solidaria, (Junta Bancaria del Ecuador, 2012), establece un conjunto de controles que se deben implementar en los diferentes canales electrónicos, para que las entidades financieras entreguen los servicios transaccionales a sus clientes. La Resolución JB-2012-2148 dispone lo siguiente:

- Los controles de seguridad que se implementen en los canales electrónicos deben basarse en las mejores prácticas vigentes a nivel internacional y además deben estar sometidas a un monitoreo permanente.
- Deben ser implementados los elementos de seguridad en los canales electrónicos como: cajeros automáticos, Páginas web transaccionales, Servicios telefónicos transacciones, dispositivos de banca móvil, POS, etc.

Los elementos de seguridad que exige la normativa son los siguientes:

- Encriptación o cifrado de accesos, canales de comunicación y bases de datos.
- Seguridad perimetral (firewall, IDP, Antispam, etc).
- Procedimientos de administración de la seguridad.
- Procedimientos para el monitoreo de la seguridad.
- Mensajería para informar al cliente de los movimientos en sus cuentas por medio de los canales electrónicos.
- Seguridad en transacciones que se realicen vía call center.
- Seguridad física y lógica en cajeros automáticos.

- Capacitación a los usuarios o clientes sobre la seguridad que mantienen los canales electrónicos y como debe colaborar el usuario o cliente.

Las normativas descritas anteriormente son de cumplimiento obligatorio para las entidades financieras, las cuales tienen establecidas diferentes fechas de cumplimiento, extendiéndose hasta junio del 2015.

CAPÍTULO III

METODOLOGÍA PROPUESTA

3.1. Metodología propuesta para el análisis de riesgos.

La metodología propuesta para el análisis de riesgos está compuesta por los siguientes pasos:

- Correlación de las mejores prácticas analizadas en el marco teórico en lo que se refiere a identificación y valoración de activos y riesgos.
- Establecimiento de criterios para la identificación y valoración de Activos y riesgos.
- Establecimiento de criterios para la identificación de los procesos críticos de la institución.
- Evaluación de los activos de información.
- Evaluación del riesgo informático.

3.1.1. Correlación de las Mejores Prácticas para la identificación y valoración de activos y riesgos.

En base al conocimiento de las propuestas que contienen las mejores prácticas para la identificación y valoración de activos y riesgos (numerales 2.2.7 al 2.2.18), fue necesario establecer una línea base, donde se consolidaron las propuestas descritas, esta línea base se constituyó en un insumo fundamental para desarrollar la metodología de análisis de riesgos en seguridad la información.

Para establecer la línea base o la consolidación de las propuestas sobre identificación y valoración de activos y riesgos se tomaron los atributos de cada una de las propuestas, bajo las siguientes consideraciones:

1. La base fundamental para realizar la consolidación de los atributos que mantienen las diferente propuestas en cuanto a identificación y valoración de activos y riesgos son los que mantienen las normas ISO27000, los cuales tendrán prevalencia sobre los atributos de las otras dos mejores prácticas analizadas, en razón de que las normas ISO27000 son estándares que tienen especialización en seguridad de la información.
2. Como premisa, se tomaran los atributos que tengan en común por lo menos en dos de las tres mejores prácticas analizadas. Sin embargo, si es necesario incluir un atributo que no sea común en las tres mejores prácticas, y que se considere necesario evaluar, se lo podrá realizar, ya que por la naturaleza de la institución, situación geográfica, normativa legal u otras particularidades, pueden existir riesgos que se requieran evaluar.

A continuación se pueden observar, las diferentes matrices, producto de la consolidación de las propuestas en identificación y evaluación de activos y riesgos planteadas por las mejores prácticas, así como también la definición de sus atributos.

3.1.1.1. Relación de los atributos en la Identificación de activos.

Tabla 11

Identificación de Activos.

	ISO27000	COBIT	ITIL
Identificación de activos	Información	Información	Información
	Software	Aplicaciones	Aplicaciones
	Equipos	Infraestructura	Infraestructura
	Servicios		
	Personas	Personas	Personas
	Reputación		
			Gestión
			Organización
			Procesos
			Conocimiento
			Capital Financiero

Fuente : (ICONTEC ISO/IEC 27005, 2009); (IT Governance Institute, 2007); (ITIL, 2008)

3.1.1.2. Definición de los atributos para la identificación de activos.

Información.- es toda fuente de datos estructurada acordes a la naturaleza de la institución, entre otras son las siguientes: bases de datos y archivos de datos, contratos y acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada, etc

Software o aplicaciones.- es todo aplicativo o componente que forman parte de las tecnologías de información por ejemplo: Software de aplicación, software del sistema, herramientas de desarrollo, software de colaboración, software de seguridad. etc.

Equipos o Infraestructura.- Tecnología que hace posible el procesamiento electrónico de la información, servidores, computadores, equipos de comunicación, dispositivos y demás equipos que apoyen a la gestión electrónica de la información.

Personas.- Todo el personal que es parte del proceso con sus respectivas habilidades y conocimientos.

Servicios.- Son los servicios suministrados por terceros, como: energía eléctrica, agua, telecomunicaciones, internet, etc.

Reputación.- Se refiere al nivel de confianza que tiene la marca ante sus clientes o usuarios, se lo denomina imagen.

Organización.- Estructura organizativa y jerárquica de una institución, departamento o área.

Gestión.- Actividades necesarias para conseguir un objetivo.

Conocimiento.- este elemento está implícito en el atributo personas, se refiere al grado de conocimiento que puede tener una persona de un proceso crítico para la institución.

Capital financiero. Recursos económicos necesarios para ejecutar un proceso.

3.1.1.3. Relación de los atributos en la Valoración de activos

Tabla 12

Valoración de Activos.

	ISO27000	COBIT	ITIL
Valoración de activos		Efectividad	
		Eficiencia	
	Confidencialidad	Confidencialidad	
	Integridad	Integridad	
	Disponibilidad	Disponibilidad	Disponibilidad
		Cumplimiento	
		Confiabilidad	
			Continuidad
			Capacidad
			Seguridad

Fuente : (ICONTEC ISO/IEC 27005, 2009); (IT Governance Institute, 2007); (ITIL, 2008)

3.1.1.4 Definición de los atributos en la valoración de activos.

Confidencialidad.- se refiere a la protección de información sensitiva contra revelación no autorizada. (ITG, 2007)

Integridad.- está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio. (ITG, 2007).

Disponibilidad.- se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas. (ITG, 2007)

Efectividad.- tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

Eficiencia.- consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos. (ITG, 2007)

Cumplimiento.- tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas. (ITG, 2007)

Confiabilidad.- se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno. (ITG, 2007)

3.1.1.5. Relación de los atributos en la identificación de riesgos.

Tabla 13

Identificación de riesgos.

	ISO27000	COBIT	ITIL
Identificación de riesgos	1.- Identificar los riesgos.	PO9 Evaluar y administrar los riesgos de TI	1.Análisis de Riesgos
	2.- Identificar los Activos	PO9.1 Marco de Trabajo de Administración de Riesgos	2. Identificación de Riesgos
	3.- Identificar las amenazas.	PO9.2 Establecimiento del Contexto del Riesgo	
	4.- Identificar las Vulnerabilidades	PO9.3 Identificación de Eventos	
	5.- Identificar los impactos que la pérdida de la confidencialidad, integridad y disponibilidad puede tener sobre estos activos.		

Fuente : (ICONTEC ISO/IEC 27005, 2009); (IT Governance Institute, 2007); (ITIL, 2008)

3.1.1.6. Definición de los atributos en la identificación de riesgos.

Identificar una metodología de valoración del riesgo. Este atributo hace referencia a que las instituciones deben identificar e implementar una metodología de análisis de riesgos acordes a los requisitos legales y de seguridad de la información.

Identificar Activos. Se entiende por activo todo aquello que tiene valor para la institución y que aportan para el cumplimiento de los objetivos y el mantenimiento de una marca, imagen o reputación.

Identificar Amenazas.- Se refiere a algo que puede dañar el activo de información como por ejemplo: virus, intrusión, desastres naturales, robo, etc.

Identificar las Vulnerabilidades.- Se refiere a aquellas debilidades que tiene el activo que pueden ser aprovechadas para ser atacadas o dañadas.

3.1.1.7. Relación de los atributos en la Valoración de riesgos.

Tabla 14

Valoración de riesgos.

	ISO27000	COBIT	ITIL
Valoración de riesgos	1. Analizar y evaluar los riesgos.		Gestión de Riesgos
	2. Valorar el impacto al negocio que podría causar una falla en la seguridad.	PO9.4 Evaluación de Riesgos de TI	Evalúa Riesgos
	3. Valorar la posibilidad realista de que ocurra una falla en la seguridad		
	4. Estimar los niveles de los riesgos.		Define el Nivel aceptable de riesgos
	5. Determinar la aceptación de riesgo o la necesidad de su tratamiento.	PO9.5 Respuesta a los Riesgos	Identifica respuesta adecuada del riesgo.

Fuente : (ICONTEC ISO/IEC 27005, 2009); (IT Governance Institute, 2007); (ITIL, 2008)

3.1.1.8. Definición de atributos en la valoración de riesgos.

Analizar y evaluar riesgos.-Se refiere a establecer una metodología de análisis de riesgos para gestionar el riesgo, analizándolo y evaluándolo.

Valor el impacto como consecuencia de una falla de seguridad.- Se debe valorar el impacto monetario, de imagen o reputacional, etc. que puede causar una falla de seguridad.

Valorar la posibilidad realista de que ocurra una falla de seguridad.- Se refiere a establecer la probabilidad de ocurrencia de que una amenaza se materialice para lo cual se debe considerar las amenazas y vulnerabilidades existentes.

Estimar los niveles de los riesgos. Es necesario establecer métricas que determinen los niveles de riesgos extremos, bajos y sus intermedios.

Determinar la aceptación de riesgo o la necesidad de su tratamiento.- En base a la estimación de los niveles de riesgos e identificado el impacto, se establecerá la acción a tomar con cada uno de los riesgos, aceptándolos o tratándolos.

3.1.1.9 Criterios consolidados para la identificación y valoración de activos y riesgos.

La tabla 15, finalmente es la consolidación de los atributos de las diferentes propuestas para la identificación y valoración de activos y de riesgos.

Tabla 15

Criterios consolidados para identificación y valoración de activos.

Instancia	Atributos para la identificación y valoración de activos y riesgos.			
Identificación de activos	Información	Aplicaciones	Infraestructura	Personas
Valoración de activos	Confidencialidad	Integridad	Disponibilidad	
Identificación de Riesgos	Identificar activos	Identificar amenazas	Identificar vulnerabilidades	
Valoración de riesgos	Evaluar el impacto al negocio	Evaluar la probabilidad que se materialice el riesgo	Estimar niveles de riesgo	

Fuente : (ICONTEC ISO/IEC 27005, 2009); (IT Governance Institute, 2007); **(ITIL, 2008)**

3.1.1.10 Criterios para la identificación de los Procesos Críticos.

Para la identificación y evaluación de activos y riesgos, se identificaron los procesos que son indispensables para la continuidad del negocio y sus operaciones, considerando que si sucediera alguna falla de seguridad en estos procesos críticos podría generar un impacto negativo en la institución. (Junta Bancaria del Ecuador, 2005);

La normativa JB-2005-834, (Junta Bancaria del Ecuador, 2005), manifiesta lo siguiente:

> **En la Sección II.- FACTORES DE RIESGO OPERATIVO en el artículo 4 en el inciso 4.1 Procesos:**
>
> Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:
>
> **4.1.1 Procesos gobernantes o estratégicos.-** Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros.
>
> **4.1.2 Procesos productivos, fundamentales u operativos.-** Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,
>
> **4.1.3 Procesos habilitantes, de soporte o apoyo.-** Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal

competente, reducir los riesgos del trabajo, preservar la calidad delos materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos.

Identificados los procesos críticos, se implantarán mecanismos o alternativas que ayuden a la entidad a evitar incurrir en pérdidas o poner en riesgo la continuidad del negocio y sus operaciones (Junta Bancaria del Ecuador, 2005).

En las instituciones financieras como son las cooperativas de Ahorro y crédito, los procesos antes mencionados generalmente contienen los siguientes sub-procesos:

- **Procesos gobernantes o estratégicos.**
  - **Gestión de la estrategia.-** Son todos aquellos procesos que generan actividades estratégicas para el negocio, como: planes estratégicos, presupuestos, merketing estratégico.
  - Gestión del Gobierno Corporativo.- En las cooperativas de ahorro y crédito son todas las actividades de administración realizadas por el consejo de administración, consejo de vigilancia y la gerencia general.
  - **Administración del Riesgo.** Es el proceso cuyas actividades se encargan de monitorear los riesgos de liquidez, mercado, y legal.
  - **Gestión Prevención del lavado de dinero.-** Son las actividades que se enfoquen en monitorear el cumplimiento de las normativas de lavado de dinero para las entidades financieras
- **Procesos Productivos, fundamentales u operativos.**
  - **Gestión de operaciones.-** Son todas las actividades que apoyan a la operación diaria en las instituciones financieras como: atención al cliente, cajas, gestión de transferencias monetarias, control de las transacciones por canales electrónicos de atención, etc.

- **Gestión de productos y servicios.-** Son las actividades que los desarrollo marketing con su personal, para la implementación o mejoramiento de productos financieros.
- **Gestión comercial (captaciones).-** Son las actividades donde se comercializan los diferentes productos de ahorro e inversiones.
- **Gestión comercial (colocaciones).-**Son las actividades donde se comercializan los diferentes productos de crédito.
- **Gestión de cobranzas.-** Son las actividades que se realizan para la recuperación del dinero cuyos créditos han caído en mora.

- **Procesos habilitantes o de apoyo.**
  - **Gestión de talento humano.-** Son las actividades que se realizan para que el talento humano requerido en los diferentes procesos, sea suficiente de calidad.
  - **Gestión de tecnología.-**Son las actividades que se realizan para procesar, custodiar y mantener la disponibilidad de la información, tanto para funcionarios como para clientes.
  - **Gestión administrativa.-**Son las actividades de administración y mantenimiento de los activos físicos institucionales, ocupándose de las relaciones contractuales con los proveedores de diferentes servicios.
  - **Gestión financiera.-** Son las actividades de registro contable y emisión de estados financieros y reportes exigidos por los organismos de control.
  - **Gestión de asesoría jurídica.-** Son las actividades jurídicas administrativas o jurídicas de negocio.
  - **Gestión de control institucional.** Son las actividades de control que realiza la gerencia general en cuanto al cumplimiento de objetivos, metas, presupuestos, etc.

- **Gestión de auditoria interna.** Son las actividades de auditoria en sus diferentes coberturas como: auditoria financiera, auditoria de cumplimientos, auditoria informática, auditoria de gestión.

Para calificarlos como críticos a los procesos institucionales se tuvo en cuenta la definición de procesos críticos que mantiene la normativa JB-2005-834, dice lo siguiente

"Sección I.- ÁMBITO, DEFINICIONES Y ALCANCE. ARTÍCULO 1. INCISO 2.6:

Proceso crítico.- Es el indispensable para la continuidad del negocio y las operaciones de la institución controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo" (Junta Bancaria del Ecuador, 2005).

A continuación en la tabla 16, se presenta una matriz con la que se realizó la identificación de los procesos críticos institucionales.

Tabla 16

Matriz de Procesos y Sub-Procesos.

Procesos	Sub-Procesos	Procesos Críticos	Responsable del Proceso
Gobernantes o Estratégicos	Gestión de la Estrategia	S	Gerencia General Gerente Financiero Gerente de Marketing
	Gestión de Gobierno Corporativo	N	Gerencia General Consejo De Administración
	Administración del Riesgo	S	Gerente de Riesgos
	Gestión Prevención de lavado de activos	S	Jefe de Cumplimiento

Continúa →

Productivos, fundamentales u operativos	Gestión de Operaciones	S	Gerente de Operaciones
	Gestión de Productos Y Servicios		Gerente de Marketing
	Gestión Comercial (Captaciones)	S	Gerente de Negocios
	Gestión Comercial (Colocaciones)	S	Gerente de Negocios
	Gestión de Cobranzas	S	Gerente de Negocios
Habilitantes de soporte o apoyo	Gestión del Talento Humano	N	Gerente de Talento Humano
	Gestión de Tecnología	S	Gerente de Tecnología
	Gestión Administrativa	N	Gerencia de Operaciones
	Gestión Financiera	S	Gerente Financiero
	Gestión Asesoría Jurídica	N	Asesor Jurídico
	Gestión Control Institucional	S	Gerente General
	Gestión de Auditoría Interna	S	Auditor Interno

Fuente : (Superintendencia de Bancos, 2005)

3.1.2. Identificación de los activos de información.

Una vez establecidos los criterios para la identificación y valoración de activos y riesgos y seleccionados los procesos críticos, se procedió a levantar un inventario de todos los activos de información que conforman estos procesos, la identificación de los activos se lo realizó de acuerdo a la Tabla 15, de la sección 3.1.1.9 Criterios consolidados para la identificación de activos y riesgos. En donde se identificó los atributos o tipos de activos que se deben considerar para la identificación y clasificación de los activos de información, los atributos son los siguientes: información, aplicaciones, infraestructura y personas.

En la tabla 17 se presenta una matriz, con la que se realizó el levantamiento y clasificación de los activos de información.

Tabla 17

Matriz para inventario de Activos de Información.

Id. Activo	Nombre de activo	Propietario	Administrador	Tipo de activo
I1	Servidor Core Bancario	Tecnología	Jefe de Infraestructura	Infraestructura
S1	Aplicativo Bancario	Proveedor	Jefe de sistemas	Software
F3	Bases de datos crédito	Negocios	Gerente de negocios	Información
I7	Base de datos Clientes	Negocios	Gerente de negocios	Información
F1	Base de datos Inversiones	Negocios	Gerente de negocios	Información
F2	Bases de datos Cuentas de ahorro	Negocios	Gerente de negocios	Información
I2	Servidor E_mail	Tecnología	Jefe de Infraestructura	Infraestructura

Descripción de la tabla 17.

Id. Activo.- Es un código que a discreción del analista lo puede asignar al activo, el cual puede ser un secuencial.

Nombre del Activo.- Es el nombre que identifica al activo ejemplo: servidor, red, mail, base de datos, etc.

Propietario.- Es el lugar donde está localizado y custodiado el activo.

Administrador.- Es la persona que administra el equipo, manteniéndole en las mejores condiciones para que preste un servicio.

Tipo de activo.- Esto va de acuerdo a lo establecido en los criterios para la identificación de los activos definido en Tabla 15, de la sección 3.1.1.9 Criterios consolidados para la identificación de activos y riesgos.

3.1.3. Evaluación de los activos de información.

La evaluación de los activos de información se lo realizó en base a lo establecido en la Tabla 15, de la sección 3.1.1.9 Criterios consolidados para la identificación de activos y riesgos. En donde se identificaron los atributos para la evaluación de los activos y son: confidencialidad, integridad y disponibilidad.

La evaluación de los activos de información tiene tres objetivos:

1. Asignar una calificación en los diferentes procesos críticos a cada uno de los activos de información.
2. Obtener una calificación total o global que determine el nivel de importancia de cada uno de los activos, para lo cual, se sumaron las calificaciones asignadas a los activos de información en cada uno de los procesos críticos, este resultado mientras más alto sea más alta será la importancia del activo y viceversa.
3. Obtener una calificación total del activo de información que determine el nivel de criticidad del activo en la continuidad del negocio y de los procesos. Para lo cual se calculó el promedio de todas las calificaciones asignadas a los activos de información en cada uno de los procesos críticos identificados.

Para cumplir con los objetivos antes mencionados, fue necesario establecer métricas para calificar los activos, primero en base a los atributos de confidencialidad, integridad y disponibilidad y segundo, métricas para establecer el nivel de criticidad de los activos de información.

3.1.3.1 Métricas de calificación de activos por atributos.

En la tabla 18 se presentan diferentes opciones en las que se podrían situar los atributos de la información y a cada una de esas opciones se les ha asignado un valor cuantitativo y un color, con la finalidad de identificar el nivel de criticidad del activo de información con respecto a cada uno de los atributos.

Tabla 18

Métricas para la evaluación de activos de información.

Atributo	Calificación	Descripción
Confidencialidad	1	La información o el servicio son Públicos, el acceso no autorizado al activo de información o al servicio no tienen ningún impacto en el proceso ni en la institución.
	2	La información o el servicio es de Uso Interno, el acceso no autorizado podría afectar al proceso o poner en riesgo a la institución.
	3	La información o el servicio es de carácter restringida, el acceso no autorizado podría afectar en mayor grado a la institución o al proceso.
	4	La información o el servicio es Confidencial, el acceso no autorizado podría afectar muy gravemente a la institución.

Continúa ⟶

Atributo	Calificación	Descripción
Integridad	1	La información o el servicio no son críticos, pueden ser restablecidos fácilmente, si se detectan errores no hay riesgo para el proceso ni para la institución
	2	La información o el servicio son necesarios para la toma de decisiones o la continuidad del negocio. Su reconstrucción es más compleja y hay riesgo de fraude, error o problemas en la continuidad del proceso o del negocio.
	3	La información o el servicio son críticos, su restablecimiento es muy complejo. Hay riesgo de fraude, error que puede afectar a la institución de una manera muy importante.
	4	La información es básica para la toma de decisiones. Su reconstrucción es sumamente compleja y los riesgos de fraude o error pueden ser catastróficos para la institución.
Disponibilidad	1	El tiempo para recuperar la información o el servicio no es crítico puede esperar hasta que se lo pueda restablecer sin afectar al proceso o al negocio y la no disponibilidad no afecta a la institución o al proceso.
	2	El tiempo de recuperación de la información o del servicio podrá ser máximo de una semana.
	3	El tiempo de recuperación de la información o del servicio deberá ser máximo de 2 días.
	4	El tiempo de recuperación de la información o del servicio deberá ser máximo de 4 horas, para iniciar el procesamiento normal.

3.1.3.2. Métricas de nivel de criticidad del activo.

En la tabla 19, se pueden observar las métricas para identificar el nivel de criticidad que tienen los activos de información calificados.

Tabla 19

Métricas para la evaluar el nivel de criticidad de los activos de información.

	Criticidad del activo	Descripción
4	**Muy Crítico**	En caso de pérdida, acceso o difusión no autorizada hay Alta probabilidad de pérdida financiera.
3	**Crítico**	En caso de pérdida, acceso o difusión no autorizada de la información hay posible probabilidad de pérdida financiera.
2	**Importante**	En caso de pérdida, acceso o difusión no autorizada hay Alta probabilidad de pérdida operativa.
1	**Bajo**	En caso de pérdida o difusión no autorizada hay Posible probabilidad de pérdida operativa.

3.1.3.3 Calificación de los activos de información.

A continuación en la Tabla 20, se presenta un matriz en donde se cumplen los tres objetivos de la evaluación de activos de información, antes mencionados.

Tabla 20

Matriz para evaluación de Activos.

Identificación del Activo					Procesos críticos										
					Gestión de la Estrategia			Administración del Riesgo			Gestión Prevención de lavado de activos				
Id. Activo	**Nombre de activo**	**Propietario**	**Administrador**	**Tipo de activo**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**Promedio**	**Evaluación del activo**
I1	Servidor Core Bancario	Tecnología	Jefe de Infraestructura	Infraestructura	1	1	1	4	4	4	4	4	4	3	**27**
S1	Aplicativo Bancario	Proveedor	Jefe de sistemas	Software	1	1	1	4	4	4	4	4	4	3	**27**
F3	Bases de datos crédito	Negocios	Gerente de negocios	Información	1	1	4	4	4	4	1	1	1	2	**21**
I7	Base de datos Clientes	Negocios	Gerente de negocios	Información	1	1	4	4	4	4	4	4	4	3	**30**

Descripción de la Tabla 20.

Procesos Críticos._ En la fila superior se deben incluir todos los procesos críticos identificados en la correspondiente matriz (Tabla 16).

C,I,D.- Estas son las siglas de los atributos de Confidencialidad, Integridad y Disponibilidad, en estas celdas se asignarán las calificaciones a los activos de acuerdo a las métricas establecidas en la Tabla 18.

Promedio. Es cálculo del promedio de todas las calificaciones asignadas al activo de información en los diferentes procesos críticos, este valor representa el nivel de criticidad del activo.

Evaluación del activo.- Es la suma total de las calificaciones asignadas a cada uno de los atributos en los respectivos procesos críticos. Mientras mayor es el valor más crítico es el activo de información y viceversa.

3.1.4. Evaluación del riesgo informático.

Con los resultados obtenidos en la identificación y evaluación de los activos de información, en cuanto al nivel de importancia y de criticidad que tiene cada uno de ellos, como paso siguiente se procedió a evaluar el nivel de riesgo en el que se encuentran los activos de información, para lo que serán utilizadas las siguientes formulas:

- **Riesgo inherente = Impacto * Probabilidad de Ocurrencia.**
- **Riesgo Residual = Riesgo inherente – (Riesgo Inherente * Nivel de mitigación del control)**

Para que las formulas cumplan con el objetivo de calcular el nivel de riesgo, fue necesario establecer métricas para sus componentes: impacto, probabilidad de ocurrencia y nivel de mitigación del control.

En vista de que las instituciones financieras no mantienen datos estadísticos que permitan determinar con certeza y total objetividad: la probabilidad de ocurrencia de que una amenaza afecte al activo de información, el porcentaje de eficiencia que tuvo un determinado control ante un ataque y el impacto en términos monetarios. El establecimiento de las métricas se lo realizó en base a criterios cualitativos, criterios que indudablemente dependen de factores como: la percepción, incidentes sucedidos en el pasado, experiencias, etc. por lo tanto las métricas serán datos que no tienen una precisión absoluta.

Sin embargo, con la finalidad de mitigar el nivel de subjetividad en la definición de las métricas, se tomó en consideración los estudios realizados por los laboratorios de seguridad de la información, mencionados en el marco teórico, de donde se pudo obtener una referencia sobre: la probabilidad de ocurrencia de un delito informático (frecuencia), la eficiencia que tienen los controles o salvaguardas para proteger los activos de información y del nivel de impacto.

3.1.4.1. Métricas para medir la probabilidad de ocurrencia.

La probabilidad de ocurrencia, hace referencia a la posibilidad de que una amenaza se aproveche de las vulnerabilidades de un activo de información y lo afecte de manera negativa, por lo tanto fue necesario establecer métricas que identifiquen distintas instancias, determinando la probabilidad de ocurrencia de un evento de riesgo.

Como se pudo observar, en las diferentes estadísticas obtenidas por los laboratorios de seguridad de la información y por la fiscalía general de la nación, demuestran que la probabilidad de que una amenaza ataque a un activo de información es muy alta, primero porque las tecnologías utilizadas son muy sofisticadas y pueden ejecutar un ataque en periodos de tiempo muy cortos y segundo porque según las estadísticas los ataques informáticos para las instituciones financieras se incrementan, también, en periodos muy cortos de tiempo.

En base a lo mencionado, en la Tabla 21 se definieron, métricas con criterio cualitativo para evaluar la probabilidad de ocurrencia de un evento de riesgo, se puede observar que a cada uno de los niveles se lo ha asignado un valor, el cual se lo utilizará para calcular el riesgo con las formulas planteadas para dicho efecto.

Tabla 21

Probabilidad de Ocurrencia.

Probabilidad de Ocurrencia (Frecuencia)	Descripción	Valor
Muy Alta	El incidente se puede producir diariamente e incluso varias veces en el día.	0.99
Alta	El incidente se puede producir mensualmente.	0.80
Moderada	El incidente se puede producir una vez al año.	0.60
Baja	El incidente sucedió hace más de un año.	0.40
Muy Baja	El incidente no ha sucedido en la institución o la probabilidad que suceda es muy baja.	0.20

3.1.4.2. Métricas para medir el impacto.

El impacto se refiere a la degradación que puede sufrir un activo de información afectando a la normal continuidad del negocio y de sus operaciones y por lo tanto a la reputación y confianza institucional, trayendo consigo pérdidas financieras.

Como se pudo observar, en las diferentes estadísticas obtenidas por los laboratorios de seguridad de la información, los impactos monetarios son de muchos millones de dólares los que han tenido que soportar las instituciones del sector financiero a causa de los ataques informáticos.

En base a lo mencionado, en la Tabla 22 se definieron métricas con criterio cualitativo para evaluar el nivel de impacto que puede ocasionar la afectación de una amenaza a un activo de información, se puede observar también, que a cada uno de los niveles se lo ha asignado un valor, el cual se lo utilizará para calcular el riesgo con las formulas planteadas para dicho efecto.

Tabla 22

Impacto

Nivel de Impacto	Descripción	Valor
Superior	El activo sufre daños irreparables y la continuidad del negocio y sus operaciones, generan una pérdida financiera más allá de lo tolerable.	1.00
Mayor	El activo sufre daños que se pueden solucionar en longitudes de tiempo críticos y pueden generar pérdidas financieras muy altas que lleguen al borde de lo tolerable.	0.80
Importante	El activo sufre daños, existe restricción en las operaciones, que se pueden solucionar en tiempos tolerables, las pérdidas financieras son tolerables.	0.60
Menor	El activo sufre daños, pero puede seguir operando, no existen pérdidas financieras. Las soluciones se lo pueden realizar en espacios de tiempo que no afecte la continuidad del negocio	0.40
Inferior	El activo no sufre daños que le impidan continuar operando	0.20

3.1.4.3. Métricas para medir la Eficiencia del Control.

La eficiencia del control hace referencia a la capacidad que tiene el mismo para mitigar el impacto que podría causar la afectación de una amenaza en un activo de información.

Los controles de seguridad de la información pueden estar constituidos por elementos como: tecnología, políticas, estándares, procedimientos y talento humano. Cada uno de estos controles pueden tener una o varias de las siguientes características:

Preventivo.- el control alerta antes de que la amenaza afecte al activo de información.

Detectivo.- el control detecta la fuente de la amenaza que afectó al activo de información.

Correctivo.- el control detecta la fuente de la amenaza y toma medidas correctivas.

Automático.- El control genera alertas automáticas sin intervención humana.

Manual.- El control requiere de intervención humana, para generar alertas.

Medibles.-Se puede medir la eficiencia del control.

La Tabla 23 contiene las métricas con criterio cualitativo para evaluar la eficiencia del control, considerando en cada métrica los tipos de controles y las características que pueden tener y que fueron descritas anteriormente, se puede observar también que a cada nivel de eficiencia se ha asignado un porcentaje de cobertura del control, el cual se lo utilizará para calcular el nivel de riesgo con las formulas planteadas para dicho efecto.

Tabla 23

Eficiencia del control.

Eficiencia	Descripción	Cobertura del control %
Muy Fuerte	El control es preventivo, automático, existen procedimientos establecidos y socializados cuando se presentan incidentes detectados por el control, la efectividad del control es comprobada.	71%-90%
F**uerte**	El control es preventivo, manual y/o automático, existen procedimientos establecidos y socializados cuando se presentan incidentes detectados por el control, la efectividad del control es comprobada.	51%-70%
Moderado	El control es informativo y/o detectivo, manual y/o automático, existen procedimientos establecidos y socializados cuando se presentan incidentes.	31%-50%
Débil	El control es informativo y/o detectivo, manual frente a incidentes se ejecutan acciones varias por conocimiento del personal, costumbre o lógica, ya que no existen procedimientos establecidos y socializados.	11%-30%
Muy Débil	El control es disuasivo su efectividad no es comprobada o el control no existe.	1%-10%

3.1.4.4 Métricas para identificar el nivel de riesgo informático.

La tabla 24 contiene las métricas con criterio cualitativo de los niveles de riesgo informático en los que puede incurrir los resultados obtenidos de la aplicación de las fórmulas para calcular el nivel de riesgo, a cada nivele se le ha asignado un valor y un color para determinar la criticidad del riesgo.

Tabla 24

Niveles de riesgo Informático.

Métrica	Nivel de Riesgo	Descripción
81%-100%	**EXTREMO**	Este nivel de riesgo implica que el impacto puede ser catastrófico para la institución ya que puede sobrepasar los límites financieros tolerables, las amenazas tienen una probabilidad de ocurrencia muy alta.
61%-80%	**MUY ALTO**	Este nivel de riesgo, implica que el impacto puede llevar a altas pérdidas financieras, las cuales se pueden desbordar de los límites tolerables, sino se toman medidas emergentes para cubrir con las vulnerabilidades del activo de información, ya que la probabilidad de ocurrencia de que una amenaza afecte al activo es alta.
41%-60%	**ALTO**	Este nivel de riesgo implica que el impacto puede generar pérdidas financieras tolerables para la institución, la probabilidad de ocurrencia es moderada, es decir el incidente puede suceder una vez al año.
21%-40%	**MODERADO**	Este nivel de riesgo, implica que el impacto no genera pérdidas financieras, pero tiene afectaciones operativas.
0%-20%	**BAJO**	Este nivel de riesgo, implica que los daños que puede tener un activo de información no tiene un impacto ni financiero ni operativo.

3.1.4.5. Métricas para identificar el nivel de seguridad.

La tabla 25 contiene las métricas con criterio cualitativo de los niveles de seguridad en los que puede incurrir los resultados obtenidos de la aplicación de las fórmulas para calcular el nivel de seguridad, a estos niveles se les ha asignado un valor y un color para determinar el nivel de seguridad.

Tabla 25

Niveles de Seguridad.

Métrica	Nivel de eficiencia	Descripción
81%-100%	**EXCELENTE**	Este implica, que los controles tienen una eficiencia muy fuerte de acuerdo a la tabla 27
61%-80%	**MUY ALTO**	Este implica, que los controles tienen una eficiencia Fuerte de acuerdo a la tabla 27
41%-60%	**ALTO**	Este implica, que los controles tienen una eficiencia moderada de acuerdo a la tabla 27
21%-40%	**BAJO**	Este implica, que los controles tienen una eficiencia débil de acuerdo a la tabla 27
0%-20%	**MUY BAJO**	Este implica, que los controles tienen una eficiencia muy débil de acuerdo a la tabla 27

3.1.4.6. Cálculo del Riesgo Informático.

Una vez que se establecieron las fórmulas para calcular el nivel del riesgo (riesgo residual y riesgo inherente), y las métricas que ayudaron a cumplir con el objetivo de las formulas, a continuación, se ejecutaron los pasos que se deben seguir para calcular el nivel de riesgo en el que se encuentran los activos de información, considerando las amenazas que les pueden afectar y los controles existentes que colaboran con la mitigación del impacto que puede causar la amenaza, los pasos a seguir son los siguientes :

3.1.4.6.1. Identificación de amenazas y controles o salvaguardas.

Para realizar una identificación de las amenazas que pueden afectar los activos de información, fue necesario tener en consideración los siguientes factores: el tipo de negocio, localización geográfica, tecnología instalada, la capacitación del personal, cultura.

Se debe mencionar que cada uno de los factores antes mencionados establecen la diferencia entre las instituciones en lo que se refiere al nivel del riesgo que mantienen los activos de información.

Con la finalidad de tener una línea base que sirva de referencia para la identificación de las amenazas, se tomó como referencia el anexo 3 de la Norma ISO 27005 (ICONTEC ISO/IEC 27005, 2009).

En la Tabla 26, se presenta una matriz que fue utilizada para el levantamiento de las amenazas y de los controles o salvaguardas existentes:

Tabla 26

Matriz para el levantamiento de amenazas y controles

	AMENAZAS			
Controles o salvaguardas	Divulgación de información confidencial	Acceso no autorizado a la información física Y/o digital.	Incumplimiento de políticas de seguridad física o lógica	Ausencia de políticas y procedimientos de seguridad física o lógica aprobados por CDA.
Corte de conexiones en la red por inactividad en las estaciones de trabajo *				
Informar al usuario sobre su último ingreso a los servicios transaccionales electrónicos. *				
Proceso de desvinculación, vacaciones, permisos del talento humano **				

Descripción de la Tabla 26.

Amenazas.- En esta fila y con orientación vertical, se deben colocar cada una de las amenazas identificadas.

Controles y salvaguardas.- En esta columna se deben incluir cada uno de los controles o salvaguardas identificados.

3.1.4.6.1. Evaluación de la eficiencia de los controles o salvaguardas.

Una vez identificadas las amenazas y los controles o salvaguardas, se procederá a evaluar la eficiencia de los controles con respecto a las amenazas identificadas.

Para realizar la evaluación de la eficiencia de los controles, se utilizará la matriz propuesta en la Tabla 27, incrementado una variante, como se puede observar a continuación.

Tabla 27

Matriz para evaluación de la eficiencia de los controles

	AMENAZAS			
Controles o salvaguardas	Divulgación de información confidencial	Acceso no autorizado a la información física Y/o digital.	Incumplimiento de políticas de seguridad física o lógica	Ausencia de políticas y procedimientos de seguridad física o lógica aprobados por CDA.
Corte de conexiones en la red por inactividad en las estaciones de trabajo *	90%			
Informar al usuario sobre su último ingreso a los servicios transaccionales electrónicos. *		50%		
Eficiencia del control	88%	70%	75%	80%

Descripción de la tabla 27.

Amenazas.- En esta fila y con orientación vertical, se deben colocar cada una de las amenazas identificadas.

Controles y salvaguardas.- En esta columna se deben incluir cada uno de los controles o salvaguardas identificados.

Eficiencia del control.- La calificación de la eficiencia del control se lo realizará en la celda que relacione al control con la amenaza. Esta calificación se lo realizará de acuerdo a lo establecido en la sección 3.1.4.3 Métricas para medir la eficiencia del control, Tabla 23.

Eficiencia Promedio del Control.- Es el promedio de las calificaciones asignadas a la eficiencia del control por cada una de las amenazas. Este valor será utilizado para calcular el riesgo residual.

3.1.4.6.2. Calculo del riesgo inherente y residual por cada activo.

Los resultados obtenidos en: la identificación de activos (sección 3.1.2), la evaluación de activos (sección 3.1.3), la identificación de amenazas y controles o salvaguardas (sección 3.4.6.1) y la evaluación de controles o salvaguardas (sección 3.1.4.6.1),), se constituyeron en el insumo con el que fue factible calcular el nivel del riesgo (riesgo inherente y el riesgo residual).

Para realizar esta calificación se deben consolidar los resultados obtenidos en cada una de las secciones mencionadas, de esta manera se obtuvo una matriz en donde se relacionaron los activos de información identificados en los procesos críticos, las amenazas que podrían afectar al activo de información y los controles o salvaguardas que protegen el activo, con esta información se procedió a calificar por cada uno de los activos de información, los diferentes elementos que conforman las fórmulas de cálculo del riesgo, que son : Impacto, probabilidad de ocurrencia, Nivel del control o eficiencia del control. La calificación de cada uno de estos rubros se los realizará en base a las métricas definidas en las secciones : 3.1.4.1 Métricas para medir la probabilidad de ocurrencia,3.1.4.2 Métricas para medir el impacto y 3.1.4.3 Métricas para medir la eficiencia del control.

A continuación, en la tabla 28, se presenta una matriz, donde se consolidaron los resultados obtenidos, la calificación de los rubros : eficiencia del control, impacto y probabilidad de ocurrencia y el cálculo del nivel del riesgo, resultados que tienen un color

asignado en base a las métricas establecidas para identificar el nivel de riesgo, definidas en la sección 3.1.4.4.

Tabla 28

Matriz para evaluación del riesgo informático.

			Amenazas															
			Fuga de información digital					**Divulgación de información confidencial**					**Acceso no autorizado a la información física y/o digital.**					
Id. Activo	**Activos de información**	**Calificación del activo**	Eficiencia del control	Probabilidad de ocurrencia	Impacto	Riesgo inherente	Riesgo residual	Eficiencia del control	Probabilidad de ocurrencia	Impacto	Riesgo inherente	Riesgo residual	Eficiencia del control	Probabilidad de ocurrencia	Impacto	Riesgo inherente	Riesgo residual	**Promedio del riesgo informático residual**
F3	Bases de datos crédito	**21**	75	0.99	0.80	0.79	0.20	76	0.99	1.00	0.99	0.24	76	0.99	1.00	0.99	0.24	0.22
I7	Base de datos Clientes	**30**	75	0.99	0.60	0.59	0.15	76	0.99	0.60	0.59	0.14	76	0.99	0.60	0.59	0.14	0.14
F1	Base de datos Inversiones	**24**	75	0.99	0.80	0.79	0.20	76	0.99	0.80	0.79	0.19	76	0.99	0.80	0.79	0.19	0.19
F2	Bases de datos Cuentas de ahorro	**24**	75	0.99	1.00	0.99	0.25	76	0.99	0.80	0.79	0.19	76	0.99	0.80	0.79	0.19	0.21
I2	Servidor E_mail	**13**	75	0.99	0.80	0.79	0.20	76	0.99	0.80	0.79	0.19	76	0.99	0.80	0.79	0.19	0.19

Descripción de la tabla 28.

Amenazas.- Son las amenazas identificadas en la tabla 26 de la sección 3.1.4.6.1 Identificación de amenazas y controles o salvaguardas.

Activos de información.- Los activos de información son los identificados en la tabla 17 de la sección 3.1.2 Identificación de los activos de información.

Calificación de los activos.- Es la calificación asignada a los activos de información en la tabla 18 de la sección 3.1.3. Calificación de los activos de información.

Eficiencia del control.- Por cada una de las amenazas y si el control es aplicable al activo de información, se debe incluir el valor promedio obtenido en la tabla 27 de la sección 3.1.4.6.1 Evaluación de la eficiencia de los controles o salvaguarda. Si el control no es aplicable para el activo se lo debe llenar con la letra N.

Probabilidad de ocurrencia.- El valor de esta celda debe ir de acuerdo a las métricas establecidas en la tabla 21, en la sección 3.1.4.1 Métricas para medir la probabilidad de ocurrencia.

Impacto.- El valor de celda debe ir de acuerdo a las métricas establecidas en la tabla 22, en la sección 3.1.4.2 Métricas para medir el Impacto.

Riesgo Inherente.- Para el cálculo del riesgo inherente se aplicará la siguiente fórmula: Riesgo inherente = Impacto * Probabilidad de Ocurrencia.

Riesgo Residual.- Para el cálculo del riesgo residual se debe aplicar la siguiente fórmula:

Riesgo Residual = Riesgo inherente – (Riesgo Inherente * Nivel de mitigación del control)

Niveles de riesgo.- Los niveles de riesgos están identificados por los colores asignados al resultado del cálculo del riesgo inherente y residual, que están de acuerdo a las métricas para identificar el nivel de riesgo, definidas en la sección 3.1.4.4 Métricas para identificar el nivel de riesgo informático.

3.1.4.7. Calculo del riesgo informático total.

Una vez que se obtuvo el nivel de riesgo informático residual por cada uno de los activos de información se procederió a obtener el riesgo informático total, aplicando la siguiente fórmula:

Fórmula: Rt = (Promedio(X)) * 100

Donde : Rt = Riesgo Informático total

X = Riesgo Residual

Variable: X >= 0.20

El valor de la variable se lo define como mayor o igual a 0.20 por que es donde inician los riesgos de nivel moderado, de acuerdo a las métricas establecidas para identificar el nivel de riesgo en la tabla 24 de la sección 3.1.4.4 Métricas para identificar el nivel de riesgo.

A continuación en la tabla 29, se presenta una matriz en donde se puede identificar por cada uno de los activos el valor promedio del riesgo residual, este valor es el que se asignará a la variable X de la fórmula planteada para obtener el valor del riesgo informático total.

Para el caso de la matriz el riesgo informático residual total es el siguiente:

- Rt = 0.30 * 100
- Rt = 30%

El riesgo total del 30% de acuerdo a lo establecido en la tabla 24 de la sección 3.1.4.4 Métricas para identificar el nivel de riesgo. El Riesgo total informático tiene un nivel moderado.

Tabla 29

Riesgo informático residual Promedio.

Id. Activo	Activos de información	Calificación del activo	Riesgo informático residual promedio
F23	Base de datos de firmas	3	0.26
F7	Manuales (políticas, procedimientos estándares)	3	0.30
P1	Administrador de base de datos	2	0.50
P2	Operador	3	0.35
P3	Personal de apoyo IT	3	0.36
I3	Servidor WEB transaccional	3	0.26
F22	Documentos valorados	1	0.26
I4	Switch transaccional (atm, Ventanilla compartida)	2	0.26
F13	Actas consejo de vigilancia	2	0.26
F14	Informes de auditoría y control interno	3	0.26
F11	Estatutos	3	0.26
I12	Grabaciones CCTV	3	0.26
	Riesgo Informático residual total		0.30

3.1.4.8 Cálculo del nivel de seguridad informática.

Para el cálculo del nivel de seguridad informático se aplicó siguiente fórmula:

Seguridad informática = 1 – Riesgo informático total.

Dónde:

- La constante 1 representa que la entidad es propietaria de un 100% de seguridad.
- El riesgo informático total es el calculado en el punto 3.1.4.7

Para el caso presentado en el tabla 29, es el siguiente:

Seguridad informática = 1 – 30%

Seguridad informática = 70%

La seguridad informática del 70% y de acuerdo a lo establecido en la tabla 25, en la sección 3.1.4.5 Métricas para identificar el nivel de seguridad. Esto valor quiere decir que la seguridad tiene un nivel Muy Alto.

CAPÍTULO 4

APLICACIÓN DE LA METODOLOGÍA PROPUESTA

4.1. Aplicación.

La metodología anteriormente detallada fue aplicada a una Cooperativa de ahorro y crédito, a la que denominaremos Cooperativa de Ahorro y crédito Cooperación. Como actividades previas a la aplicación de la metodología de análisis de riesgos, se realizaron las siguientes:

1. Se hizo una exposición al grupo de gerentes y miembros del consejo de administración sobre los riesgos a los que se enfrentan actualmente las entidades financieras con respecto a la seguridad de la información institucional.

2. Se hizo conocer las normativas emitidas por la Superintendencia de economía popular como son: JB-2005-834 y JB-2012-2148.

3. Se hizo conocer las mejores prácticas sobre las cuales está fundamentada la metodología propuesta.

4. Conjuntamente con la gerencia general, la gerencia financiera y la gerencia de riesgos de la institución se establecieron las métricas para los niveles de impacto, niveles de probabilidad de ocurrencia, niveles de riesgo, niveles para la valoración de los activos y niveles para la evaluación de los controles y salvaguardas.

5. Se adjunta a la monografía un disco compacto que contiene una matriz Excel que integra las diferentes matrices que se presentaron en las diferentes secciones de identificación, y valoración de activos y riesgos. En esta matriz se encuentra desarrollado el análisis de riesgos de la Cooperativa de ahorro y crédito Cooperación.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones.

1. Cada una de las mejores prácticas analizadas (Cobit, ITIL, Normas ISO27000), contienen lineamientos para la identificación y valoración de activos de información, como también para la identificación y valoración de riesgos, dichos lineamientos coinciden con el objetivo que persiguen y por lo tanto son la base fundamental para el desarrollo de la metodología propuesta.

2. El aporte que entregan las mejores prácticas en lo que se refiere a identificación y valoración de activos y de riesgos, facultaron para que la metodología de análisis de riesgos propuesta, contenga etapas ordenadas, concretas y con valoraciones o clasificaciones específicas, para la identificación y valoración de activos y de riesgos.

3. Al integrar en la metodología de análisis de riesgos de seguridad de la información propuesta, los lineamientos para la identificación y valoración de activos y de riesgos que mantienen las mejores prácticas, se obtuvieron resultados: concretos, objetivos, ordenados y priorizados. Lo que permitirá a las instituciones ser objetivas en las estrategias de seguridad de la información a implementar.

4. Considerando que la normativa emitida por la Superintendencia de bancos y seguros en lo que se refiere a administración, control y seguridad de las tecnologías de información, tienen como base las mejores prácticas analizadas en este trabajo, se puede sacar como conclusión, que al aplicar la metodología propuesta se está cumpliendo tanto con la normativa de la entidad de control para las entidades financieras, como con lo establecido en las mejores prácticas para la identificación y valoración de activos y de riesgos.

5. La metodología contiene una serie de matrices, de fácil entendimiento y manejo, con las que se realizan el levantamiento y la evaluación de: activos, amenazas, controles

y riesgos; sin embargo, conforme se incremente el volumen de información tanto de amenazas como de controles por cada uno de los activos, la administración y la correlación de la información en las diferentes matrices se vuelve compleja.

5.2. Recomendaciones.

1. Se recomienda a las entidades financieras, aplicar la metodología propuesta con la finalidad de obtener evaluaciones objetivas en cuanto a las brechas de seguridad de la información que tienen las instituciones, con respecto a las amenazas identificadas y al cumplimiento de la normatividad de los organismos de control.

2. La aplicación de la metodología propuesta es recomendable para cualquier institución o empresa que requiera una evaluación de riesgos en seguridad de la información, puesto que está desarrollada en base a las mejores prácticas. Y especialmente recomendable para las entidades financieras ya que además de alinearse a las mejores prácticas, permite cumplir con las normativas de seguridad de la información emitidas por los organismos de control, y que son de aplicación obligatoria.

3. Se recomienda la aplicación de esta metodología en las entidades financieras, ya que los resultados que se obtienen, además de ofrecer eficacia en la implementación de un sistema de gestión de seguridad de la información, permiten optimizar el uso de los recursos tales como: tiempo, talento humano, tecnología, dinero, etc.

4. La información que se genera en el levantamiento de activos, amenazas, controles o salvaguardas y en la evaluación de riesgos, es incremental y su volumen puede ser muy significativo, complicándose la administración y la correlación de la información en hojas electrónicas, por lo tanto se recomienda el desarrollo de un aplicativo para el análisis de riesgos, considerando las definiciones, procesos y métodos planteados en esta metodología

Anexo 1: Normativa JB-2005-834 Superintendencia de Bancos y Seguros.

BIBLIOGRAFÍA

ICONTEC ISO/IEC 27001. (22 de 03 de 2006). Norma técnica NTC_ISO/IEC Colombiana 27001. *Norma técnica NTC_ISO/IEC Colombiana 27001*. Bogotá, Colombia: ICONTEC.

AV Comparatives. (08 de 2013). *AV comparatives.* Recuperado el 09 de 07 de 2014, de AV Comparatives: http://www.av-comparatives.org/wp-content/uploads/2013/08/avc_aph_201308_en.pdf

Carnegie Melon university. (2014). *CERT DIVISION.* Recuperado el 08 de 12 de 2014, de CERT DIVISION: http://www.cert.org/resilience/products-services/octave/octave-method.cfm

Cevallos, D. (19 de 07 de 2014). La Mejores prácticas aplicadas a un Análisis de Riesgos de seguridad de la información para las Entidades Financieras Controladas por La Superintendencia de Economía Popular y Solidaria (Cooperativas de Ahorro y Crédito) que conforman el grupo de Asistenc. Quito, Pichincha, Ecuador.

CISCO. (2014). *Latest Malware Trends Available Now.* Recuperado el 20 de 08 de 2014, de Latest Malware Trends Available Now: https://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html?keycode=000350063

ESET. (enero de 2013). *Resumen de amenzas de enero*. Recuperado el 09 de 06 de 2013, de Resumen de amenzas de enero: http://blogs.eset-la.com/laboratorio/2013/01/30/resumen-amenazas-enero-2013/

ESET. (2014). *Tendencias 2014: el desafío de la privacidad en internet*. Recuperado el 26 de 05 de 2014, de Tendencias 2014: el desafío de la privacidad en internet: http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

Fiscalía General Del Estado Ecuatoriano. (11 de 08 de 2014). *Los delítos informáticos.* Recuperado el 21 de 11 de 2014, de Los delítos informáticos: http://www.fiscalia.gob.ec/index.php/sala-de-prensa/2421-el-coip-contempla-una-pena-de-tres-a-cinco-a%C3%B1os-de-prisi%C3%B3n-por-robos-de-cuentas-bancarias.html

Haley, K. (08 de 04 de 2014). *Symantec* . Recuperado el 26 de 05 de 2014, de Symantec revela que las fugas de datos crecieron 62% en 2013: http://tecno.americaeconomia.com/noticias/symantec-revela-que-las-fugas-de-datos-crecieron-62-en-2013

ICONTEC ISO/IEC 17799. (22 de 09 de 2006). Norma Técnica Colombiana NTC-ISO-IEC 17799. *Norma Técnica Colombiana NTC-ISO-IEC 17799*. Bogotá, Colombia: ICONTEC.

ICONTEC ISO/IEC 27005. (19 de 08 de 2009). Norma Técnica NTC-ISO/IEC 27005. 66. Bogotá, Colombia: ICONTEC.

ISO/IEC 27000. (2014). *International Standard ISO/IEC 27000*. Recuperado el 20 de 07 de 2014, de www.iso.org

ISO/IEC 27002. (2005). *PORTAL DE SOLUCIONES TÉCNICAS Y ORGANIZATIVAS A LOS CONTROLES DE ISO/IEC 27002*. Recuperado el 07 de 2014, de http://www.iso27002.es/

ISO-27005. (s.f.). TÉCNICAS DE SEGURIDAD.GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN. En ICONTEC, *NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27005* (pág. 66). COLOMBIA: ICONTEC.

IT Governance Institute. (2007). COBIT 4.1. En I. G. Institute, *COBIT 4.1*.

ITG. (2007). COBIT 4.1. En I. G. Institute, *COBIT 4.1* (pág. 209). united states of américa.

ITIL. (2008). Fundamentos de la Gestión de Servicios de TI Basada en ITIL. En J. V. Bon, *Fundamentos de la Gestión de Servicios de TI Basada en ITIL.* Van Haren publishing zalt bonnel (www.vanharen.net).

Junta Bancaria del Ecuador. (2005). *Superintendencia de Bancos y Seguros del Ecuador.* Recuperado el 20 de 07 de 2014, de JB-2005-834: http://www.sbs.gob.ec/practg/p_index

Junta Bancaria del Ecuador. (2005). *Superintendencia de Bancos y Seguros del Ecuador.* Recuperado el 20 de 07 de 2014, de http://www.sbs.gob.ec/practg/p_index

Junta Bancaria del Ecuador. (06 de 2012). *Resolución JB-2012-2148.* Obtenido de http://www.sbs.gob.ec/practg/p_index

Kapersky Lab. (2013). *Global Corporate It Security Risk : 2013.*

Kapersky Lab. (13 de 02 de 2013). *Kapersky Lab*. Recuperado el 27 de 05 de 2013, de Kapersky Lab.

Kapersky Lab. (09 de 04 de 2014). *Las amenazas informáticas financieras en 2013. Parte 2: el malware.* Recuperado el 07 de 08 de 2014, de Las amenazas informáticas financieras en 2013. Parte 2: el malware: http://www.viruslist.com/sp/analysis?pubid=207271251

Kapersky Lab. (02 de 04 de 2014). *Las amenazas informáticas financieras en 2013. Primera parte: phishing*. Recuperado el 07 de 08 de 2014, de Las amenazas informáticas financieras en 2013. Primera parte: phishing: http://www.viruslist.com/sp/analysis?pubid=207271250

Kapersky, L. (03 de 04 de 2014). *Kaspersky Lab: alrededor de un tercio de todos los ataques de phishing están destinados al robo de dinero*. Recuperado el 26 de 05 de 2014, de Kaspersky Lab: alrededor de un tercio de todos los ataques de phishing están destinados al robo de dinero: http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/kaspersky-lab-alrededor-de-un-tercio-de-todos

Labs, M. (enero de 2013). *Mcafee predice amenaza cibernética para 2013*. Recuperado el 08 de 06 de 2013, de McAfee Labs prevé las siguientes tendencias para 2013:: McAfee Labs prevé las siguientes tendencias para 2013

Labs, M. (2014). *Mcafee threats prediction 2014*. Recuperado el 26 de 05 de 2014, de Mcafee threats prediction 2014: http://mcaf.ee/utjz4

Mcafee, L. (2014). *Mcafee threats prediction*. Recuperado el 26 de 05 de 2014, de Mcafee threats prediction 2014: http://mcaf.ee/utjz4

Morones, G. (s.f.). *Métodos y técnicas de la investigación científica.* Recuperado el 30 de 11 de 2014, de Métodos y técnicas de la investigación científica: http://biblioteca.ucv.cl/site/servicios/documentos/metodologias_investigacion.pdf

NSS Labs. (2013). *NSS Labs.* Recuperado el 09 de 06 de 2014, de NSS Labs: https://www.nsslabs.com/reports/2013-consumer-avepp-comparative-analysis-phishing-protection

Ponemon Institute. (06 de 2014). *websense.* Recuperado el 21 de 08 de 2014, de websen: http://www.websense.com/content/2014-ponemon-report-part-2-thank-you.aspx?cmpid=EmailPonemon2ESAug14&mkt_tok=3RkMMJWWfF9wsRoku6nMd%2B%2FhmjTEU5z16OUpWaSwgokz2EFye%2BLIHETpodcMS8ZgMa%2BTFAwTG5toziV8R7DEJM1u0dMQWxHq

PWC Asesores Empresariales. (2014). *The Global State of Information Security Survey 2014.* Recuperado el 07 de 08 de 2014, de The Global State of Information Security Survey 2014: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

Seguridad informática. (01 de 03 de 2014). *Herramienta de Evaluacion de Riesgo-CRAMM.* Recuperado el 09 de 12 de 2014, de Herramienta de Evaluacion de Riesgo-CRAMM: https://seguridadinformaticaufps.wikispaces.com/Herramienta+de+Evaluacion+de+Riesgo-CRAMM

Sergey Lozhkin, I. S. (03 de 04 de 2014). *Kaspersky Lab*. Recuperado el 26 de 05 de 2014, de alrededor de un tercio de todos los ataques de phishing están destinados al robo de dinero : http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/kaspersky-lab-alrededor-de-un-tercio-de-todos

SIEMENS. (28 de 09 de 2013). *CRAMM*. Recuperado el 08 de 12 de 2014, de http://archive.today/FVQg1

SOPHOS. (04 de 2014). *Security threat report.* Recuperado el 14 de 08 de 2014, de Security threat report: http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf

Superintendencia de Bancos. (2005). Normas Generales para la aplicación de la ley general de instituciones del sistema financiero. *Resolución JB-2005-834*. Quito, Pichincha, Ecuador.

Symantec. (15 de Noviembre de 2012). *5 Predicciones de Seguridad de Symantec para 2013*. Recuperado el 31 de 01 de 2013, de 5 Predicciones de Seguridad de Symantec para 2013: http://www.symantec.com/connect/blogs/5-predicciones-de-seguridad-de-symantec-para-2013

Sysmantec. (08 de 04 de 2014). *Symantec revela que las fugas de datos crecieron 62% en 2013*. Recuperado el 26 de 05 de 2014, de Symantec revela que las fugas de datos

crecieron 62% en 2013: http://tecno.americaeconomia.com/noticias/symantec-revela-que-las-fugas-de-datos-crecieron-62-en-2013

Van, Bon Jan. (2008). Fundamentos de la Gestión de Servicios de TI Basada en ITIL. En J. V. Bon, *Fundamentos de la Gestión de Servicios de TI Basada en ITIL.* Van Haren publishing zalt bonnel (www.vanharen.net).

Websense. (01 de 03 de 2014). *Informe de amenzas 2014 websense.* Recuperado el 08 de 21 de 2014, de Informe de amenzas 2014 websense: http://www.websense.com/assets/webinars/2014-threat-report/NA/index.htm