UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS POSTGRADO

TRABAJO DE GRADUACIÓN:

"DISEÑO DEL MODELO DE GESTIÓN DE RIESGOS. CASO PRÁCTICO EMPRESA DE FACTORAJE."

PARA OPTAR AL GRADO DE:

MAESTRO EN SEGURIDAD Y GESTION DE RIESGOS INFORMÁTICOS.

ASESOR:

MG. RENE ARTURO ANGULO ARRIAZA.

PRESENTADO POR:

LCDA. MARÍA AZUCENA BONILLA RIVERA
ING. EDGAR GIOVANNI PEÑA RIVAS.

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.

Agosto de 2018.

Tabla de contenido

1. INTRODUCCIÓN

La gestión de riesgo informático, ha aumentado a medida la tecnología se posiciona en puntos estratégicos en todos los tipos de empresas, tanto públicas como privadas. El principal objetivo de la presente investigación es apoyar a una empresa de factoraje a identificar, evaluar, mitigar o transferir los riesgos informáticos, a través de la creación de un “modelo de gestión de riesgos” el cual se entiende como un proceso estructurado y secuencial de identificación, análisis y cuantificación de las probabilidades de ocurrencia de una determinada amenaza, cuya materialización podría provocar pérdidas o deterioros (humanos y materiales) y otros efectos secundarios.

La propuesta del modelo de gestión del riesgo hará uso de un proceso sistémico que desarrolla la evaluación de riesgos, la elaboración de estrategias para manejarlos, el desarrollo de herramientas para medirlo, y la implementación de medidas preventivas que mitiguen el riesgo; para ello se tomarán como herramientas de trabajo buenas prácticas (COBIT 5, RISK IT), normas ISO (31000, 31010, 27005) según el campo de aplicación.

Es por ello que el presente trabajo se trazó como propósito principal, el diseño de un modelo de gestión de riesgos informáticos para una empresa real de factoraje, que, por temas de confidencialidad, se prohíbe la publicación de su nombre; permitiéndoles así apoyarles en los procesos de gestión de riesgos en el área de tecnologías de información identificación, valoración y seguimiento.

2. METODOLOGÍA DE TRABAJO.

2.1 Objetivos de la investigación.

Objetivo General.

- Desarrollar un Modelo de Gestión del Riesgo basado en buenas prácticas comúnmente aceptadas aplicado a un caso práctico en la empresa de factoraje.

Objetivos Específicos.

- Comprender el enfoque de las normas ISO en cuanto a la gestión del riesgo para que pueda ser aplicada a la metodología.
- Definir una metodología que ayude a la toma de decisiones con los resultados de la Gestión del Riesgo.
- Aplicar paso a paso la metodología desarrollada en la empresa Factoraje para verificar el grado de riesgo en la que se encuentra de acuerdo al análisis.

2.2 PLANTEAMIENTO DEL PROBLEMA

2.2.1 Antecedentes del problema

Todas las organizaciones, grandes o pequeñas, de capital privado o del ámbito público, industrial o de servicios, enfrentan factores internos y externos que generan incertidumbre en alcanzar sus objetivos. Esta falta de certeza es lo que se define como “Riesgo” y es inherente a todas las actividades.

La globalización de la economía, las crisis financieras, la disputa por los recursos, la desigualdad social, el cambio demográfico, la amenaza del cambio climático, por mencionar algunos, son los retos que enfrentamos en las economías y las sociedades; retos que impactan positiva o negativamente a las organizaciones. Todos estos factores significan cambios, y estos cambios se enmarcan en un entorno de incertidumbre y riesgo.

La Gestión de Riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejar y mitigar el riesgo utilizando recursos gerenciales.

La presente investigación es apoyar a una empresa de factoraje, a identificar, evaluar y mitigar los riesgos informáticos, a través de la creación de un “Modelo de Gestión de Riesgos” el cual se entiende como un proceso estructurado y secuencial de identificación, análisis y cuantificación de las probabilidades de ocurrencia de una determinada amenaza, cuya materialización podría provocar pérdidas o deterioros (humanos y materiales) y otros efectos secundarios.

2.3 HIPÓTESIS

Con el desarrollo de un Modelo de Gestión del Riesgo basado en buenas prácticas y aplicado al área de TI, se contribuirá a identificar el grado de riesgo y a la misma vez su mitigación.

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Estudio descriptivo

Para el presente estudio se realizará una investigación bibliográfica y directamente con la empresa, donde se analizarán los procesos y activos que se tienen en el área de tecnología de la información y servirá para la realización del análisis y planteamiento del sistema de gestión de riesgos.

3.2 Investigación bibliográfica

Se utilizará para obtener información contenida en documentos, que permitan localizar, identificar y acceder métodos empleados para la gestión de riesgos.

4. MARCO TEORICO.

4.1 COBIT

COBIT, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores, se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes.

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el

recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

Los principios y catalizadores de COBIT 5 son genéricos y útiles para las Organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público.

Los 5 Principios de COBIT 5 nos hace referencia en lo siguiente**:**

1. Satisfacer las necesidades de las Partes Interesadas.
2. Cubrir la Compañía de Forma Integral.
3. Aplicar un solo Marco Integrado.
4. Habilitar un Enfoque Holístico.
5. Separar el Gobierno de la Administración.

COBIT 5 une los **cinco principios** que permiten a la Organización construir un marco efectivo de **Gobierno y Administración** basado en una serie holística de **catalizadores**, que optimizan la inversión en **tecnología e información**, así como su uso en beneficio de las partes interesadas.

Las metas en cascada de COBIT 5 traducen las necesidades de las Partes Interesadas en metas específicas, accionables y personalizadas dentro del contexto de la organización, de las metas relacionadas con la TI y de las metas catalizadoras.

Los beneficios de las Metas en Cascada de COBIT 5 es:

- Permite la definición de prioridades para la implementación, mejora y aseguramiento del gobierno empresarial de TI basado en objetivos (estratégicos) de la empresa y su riesgo relacionado.
- En la práctica, las metas en cascada:
    - Definen objetivos y metas relevantes y tangibles en varios niveles de responsabilidad.
    - Filtra la base de conocimiento de COBIT 5, basado en objetivos empresariales para obtener las guías relevantes para su inclusión en proyectos específicos de implementación, mejoramiento o aseguramiento.

- Identifica claramente y comunica como los catalizadores (a veces de manera muy operativa) son importantes para lograr los objetivos empresariales.

Según COBIT 5 los catalizadores son los elementos que hacen que los procesos y políticas se desenvuelvan de una manera más fácil dentro de las organizaciones, y que en consecuencia se van reflejar en el rendimiento y alcance de objetivos.

Los catalizadores según COBIT 5 son:

- Factores que, individualmente y colectivamente, tienen influencia en que algo funcione – en el caso de COBIT, el Gobierno y Gestión de la TI empresarial.
- Manejados por las metas en Cascada, es decir los objetivos relacionados con TI de alto nivel definen aquello que los diferentes catalizadores deben lograr.
- Descritos en el marco de referencia COBIT 5 en siete categorías.

Beneficios de implementación de COBIT son:

- Mejor alineación, con base a su enfoque de negocios.
- Propiedad y responsabilidades claras.
- Optimización de los costos de las TI
- Una visión, entendible para la gerencia, de lo que hace TI
- Entendimiento compartido entre todos los interesados, con base a un lenguaje común.

4.2 APO12 Gestionar el riesgo.

APO12 (Gestionar el riesgo): Permite identificar, evaluar y reducir los riesgos relacionados a las TI de forma continua, dentro de los niveles de tolerancia establecidos teniendo en cuenta los requerimientos de la dirección.

El proceso de gestión de riesgos APO12 de COBIT 5 para Riesgos, por medio de sus fases, permite establecer el análisis de riesgos; el cual establece inicialmente en: recolectar datos, analizar el riesgo, mantener un perfil de riesgo,

expresar el riesgo, definir un portafolio de acciones para la gestión del riesgo y responder al riesgo.

Las fases para el análisis de riesgo son identificadas, en la figura 1 de acuerdo al proceso APO12 tal y como se muestra continuación.

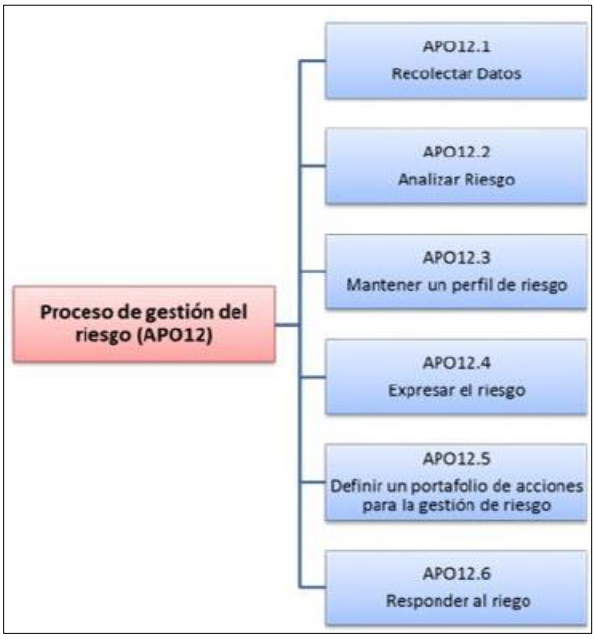

Figura 1: Proceso de Gestión del Riesgo COBIT

Basándose en las referencias del APO12 en la siguiente tabla se incluye una matriz RACI para cada uno de las fases de la gestión de riesgos, así como entradas y salidas.

Matriz RACI APO12

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
APO12.01 Recopilar datos.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
APO12.02 Analizar el riesgo.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
APO12.03 Mantener un perfil de riesgo.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
APO12.04 Expresar el riesgo.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
APO12.05 Definir un portafolio de acciones para la gestión de riesgos.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
APO12.06 Responder al riesgo.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

Apo12.01 Recolectar datos.

La información y el conocimiento constituyen la base para la realización de la gestión de riesgos, pues el conocimiento que se obtenga de esta actividad será de vital importancia a la hora de administrar el riesgo.

APO12 Prácticas, Entradas/Salidas y Actividades del Proceso

Práctica de Gestión	Entradas		Salidas	
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.	**De**	**Descripción**	**Descripción**	**A**
	EDM03.01	Evaluación de actividades de gestión de riesgos	Datos en el entorno de operación relacionados con el riesgo	Interno
	EDM03.02	• Procesos aprobados para medir la gestión de riesgos • Objetivos clave a ser monitorizados por la gestión de riesgos • Políticas de gestión de riesgos	Datos en eventos de riesgo y en factores contribuyentes	Interno
	APO02.02	Brechas y riesgos relacionados con capacidades actuales	Elementos y factores de riesgo emergentes	EDM03.01 APO01.03 APO02.02
	APO02.05	Evaluación del riesgo		
	APO10.04	Riesgo de entrega de proveedores identificado		
	DSS02.07	Estado de incidentes e informe de tendencias		

Apo12.02 Analizar el Riesgo

La creación de valor significa la obtención de beneficiar a un costo óptimo de recursos mientras se optimiza el riesgo, COBIT 5 ayuda a las empresas a crear ese valor a partir de las TI mediante el mantenimiento de un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y del uso de recursos, la entidad debe reconocer y conocer cuáles son los riesgos a los cuales se enfrenta, para poder prevenirlos de una forma segura mediante un plan de estrategias bien planteadas con el fin de evitar daños que repercutan en pérdidas y su mal funcionamiento.

Práctica de Gestión	Entradas		Salidas	
APO12.02 Analizar el riesgo. Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.	**De**	**Descripción**	**Descripción**	**A**
	DSS04.02	Análisis de impacto en el negocio	Alcance de los esfuerzos de análisis de riesgos	Interno
	DSS05.01	Evaluaciones de amenazas potenciales	Escenarios de riesgo de TI	Interno
	Fuera del Ámbito de COBIT	Avisos de amenaza	Resultados de análisis de riesgos	EDM03.03 APO01.03 APO02.02 BAI01.10
Actividades				
1. Definir la amplitud y profundidad apropiadas para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.				
2. Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta.				
3. Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.				
4. Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.				
5. Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/capturar. Proponer la respuesta al riesgo óptima.				
6. Especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requerimientos y expectativas para los controles clave que son apropiados para las respuestas de mitigación de riesgos.				
7. Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de empresa y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.				

Apo12.03 Matriz de Riesgo:

La Matriz de Riesgos es una herramienta de gestión que permite determinar objetivamente cuáles son los riesgos relevantes para la seguridad que enfrenta una organización, pretende exponer una visualización aproximada y a la vez global de aquellos riesgos identificados que impactan a una entidad, permitiendo detectar y evaluar a simple vista si la gestión que se ha venido desarrollando ha sido efectiva.

APO12 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
APO12.03 Mantener un perfil de riesgo. Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.	**De**	**Descripción**	**Descripción**	**A**
	EDM03.01	• Niveles aprobados de tolerancia el riesgo • Guía de apetito al riesgo	Escenarios de riesgo documentados por línea de negocio y función	Interno
	APO10.04	Riesgo de entrega de proveedores identificado	Perfil de riesgo agregado, incluyendo el estado de las acciones de gestión del riesgo	EDM03.02 APO02.02
	DSS05.01	Evaluaciones de amenazas potenciales		
Actividades				
1. Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.				
2. Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.				
3. Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.				
4. De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.				
5. Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.				
6. Capturar información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la empresa.				
7. Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil de riesgo de TI de la empresa.				

Apo12.04 Expresar el Riesgo

Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada que comunica los riesgos evaluados relacionados con los activos de las organizaciones, de esta forma se puede dar una respuesta eficiente para el tratamiento del riesgo.

Práctica de Gestión	Entradas		Salidas	
APO12.04 Expresar el riesgo. Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.	**De**	**Descripción**	**Descripción**	**A**
			Análisis de riesgos e informes del perfil de riesgos para las partes interesadas	EDM03.03 EDM05.02 APO10.04 MEA02.08
			Revisión de resultados de evaluaciones de riesgos de terceras partes	EDM03.03 APO10.04 MEA02.01
			Oportunidades para la aceptación de un riesgo mayor	EDM03.03
Actividades				
1. Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.				
2. Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable, exposiciones de diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.				
3. Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.				
4. Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo. Revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales.				
5. De forma periódica, para áreas con un riesgo relativo y una paridad de capacidad del riesgo, identificar oportunidades relacionadas con TI que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.				

Apo12.05 Definir un portafolio de acciones para la Gestión de Riesgos

Para definir las propuestas que deben hacer frente a los riesgos, se debe considerar el nivel de riesgo y las actividades clasificadas según los criterios de Cobit5 para riesgos:

Práctica de Gestión	Entradas		Salidas	
APO12.05 Definir un portafolio de acciones para la gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.	**De**	**Descripción**	**Descripción**	**A**
			Propuestas de proyecto para reducir el riesgo	APO02.02 APO13.02
Actividades				
1. Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.				
2. Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio.				
3. Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.				

Apo12.06 Responder al Riesgo

Después de un análisis minucioso y conforme de riesgo, obteniendo los niveles de apetito de riesgo, así como su tolerancia, y planeadas las actividades de acuerdo a su magnitud, la respuesta debe ser establecida a través de los planes.

APO12 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*

Práctica de Gestión	Entradas		Salidas	
APO12.06 Responder al riesgo. Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.	**De**	**Descripción**	**Descripción**	**A**
	EDM03.03	Acciones correctoras para tratar las desviaciones de gestión de riesgos	Planes de respuesta para incidentes relacionados con el riesgo	DSS02.05
			Comunicaciones del impacto del riesgo	APO01.04 APO08.04 DSS04.02
			Causas raíz relacionadas con el riesgo	DSS02.03 DSS03.01 DSS03.02 DSS04.02 MEA02.04 MEA02.07 MEA02.08

Actividades
1. Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.
2. Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.
3. Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.
4. Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.

4.3 APO13: GESTIONAR LA SEGURIDAD.

Este proceso del APO consiste en definir, operar y monitorear un sistema de gestión de seguridad de la información.

Matriz RACI APO 13

Matriz RACI APO13																									
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
APO13.01 Establecer y mantener un SGSI.		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13.03 Supervisar y revisar el SGSI.					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

APO13.01 Este es un enlace esencial para traducir el proceso de riesgo en servicios de seguridad efectivos, Este enfoque debe estar alineado con los requisitos del negocio y procesos comerciales.

APO13 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
APO13.01 Establecer y mantener un SGSI. Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.	**De**	**Descripción**	**Descripción**	**A**
	Fuera del Ámbito de COBIT	Enfoque de seguridad de la empresa	Política de SGSI	Interno
			Declaración de alcance del SGSI	APO01.02 DSS06.03
Actividades				
1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.				
2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.				
3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.				
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.				
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.				
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.				
7. Comunicar el enfoque de SGSI.				

APO13.02 Y APO13.03 El SGSI global debe ser monitoreado y revisado regularmente a través de revisiones de gestión y auditorías de seguridad. Un el tema subyacente aquí es una cultura de seguridad y mejora continua.

APO13 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*

Prácticas de Gestión	Entradas		Salidas	
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.	**De**	**Descripción**	**Descripción**	**A**
	APO02.04	Diferencias y cambios necesarios para alcanzar la capacidad objetivo	Plan de tratamiento de riesgos de seguridad de la información	Todo EDM Todo APO Todo BAI Todo DSS Todo MEA
	APO03.02	Descripciones de dominios de partida y definición de arquitectura	Casos de negocio de seguridad de información	APO02.05
	APO12.05	Propuestas de proyectos para reducir el riesgo		

Actividades

1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.
2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.
4. Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.
5. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.
6. Recomendar programas de formación y concienciación en seguridad de la información.
7. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.

Prácticas de Gestión	Entradas		Salidas	
APO13.03 Supervisar y revisar el SGSI. Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.	**De**	**Descripción**	**Descripción**	**A**
	DSS02.02	Incidentes clasificados y priorizados y requerimientos de servicios	Informes de auditoría del SGSI	MEA02.01
			Recomendaciones para mejorar el SGSI	Interno

Actividades

1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.
2. Realizar auditorías internas al SGSI a intervalos planificados.
3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.
4. Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.
5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.

4.4 ISO 31000

ISO 31000:2009 es una referencia para integrar el proceso de gestión del riesgo dentro del gobierno corporativo de la organización, incidiendo en su estrategia, planificación, política, valores, cultura, procesos de información etc., es decir, que se trata de una norma de gestión en toda regla.

La norma está estructurada en tres elementos claves:

- **Principios para la gestión de riesgos**, necesarios para garantizar una efectiva gestión de riesgos. Son los siguientes: crear y proteger el valor, estar integrada en todos los procesos de la organización, ser parte de la toma de decisiones, tratar explícitamente la incertidumbre, ser sistemática, estructurada y oportuna, basarse en la mejor información disponible, alinearse al contexto y al perfil de riesgos de la organización, tener en cuenta los factores humanos y culturales, ser transparente e inclusiva, ser dinámica sensible al cambio y, por último, facilitar la mejora continua.
- **Marco de trabajo**. Se refiere a la estructura de soporte que lleva a la empresa a integrar la gestión del riesgo en la gestión de la organización. Dicha estructura ha de basarse en el cumplimiento de una serie de premisas: la existencia de una política de gestión de riesgos, de indicadores de desempeño, el alineamiento de los objetivos de gestión de riesgos con los objetivos empresariales, asegurarse del cumplimiento legal y normativo, garantizar los recursos adecuados para garantizar la gestión del riesgo, establecer medios para la comunicación interna y externa y todo ello partiendo de un conocimiento exhaustivo de la organización y de su contexto.
- **Proceso de gestión de riesgos**. Se trata del elemento fundamental de la norma; en él se describe el proceso de gestión, propiamente dicho. El proceso parte del establecimiento previo de canales de comunicación y consulta de cara a garantizar las vías de entrada de información. A partir de ahí arranca un proceso que abarca las siguientes fases:

    - Establecimiento del contexto. Analizando el contexto interno y el externo, desde todos los puntos de vista, el alcance del análisis y del

proyecto de evaluación, la metodologías y criterios de evaluación y la relación con otros proyectos.

- Identificación de riesgos: sucesos y causas
- Análisis del riesgo, estimando la probabilidad y las consecuencias teniendo en cuenta los controles existentes
- Evaluar los riesgos, según diversas metodologías o apoyándose en la norma ISO 31010.
- Establecer decisiones: evitar el riesgo, aceptarlo o incrementarlo para generar una oportunidad, eliminar la fuente del riesgo, cambiar la probabilidad, cambiar las consecuencias, compartir el riesgo con terceros (incluyendo contratos y financiación) o mantener el riesgo por decisión propia.

Tratamiento de los riesgos, dependiendo de la estrategia decidida, identificando opciones de tratamiento, evaluándolas, seleccionando las opciones y preparando e implementando los planes de tratamiento.

Por último, la norma establece la obligación de implementar un proceso de seguimiento y medición de la evaluación de riesgos, ya que el contexto y otros factores pueden variar con el paso del tiempo. En la figura 2, se muestra el detalle de los principios, marco y procesos adaptados por dicha norma.

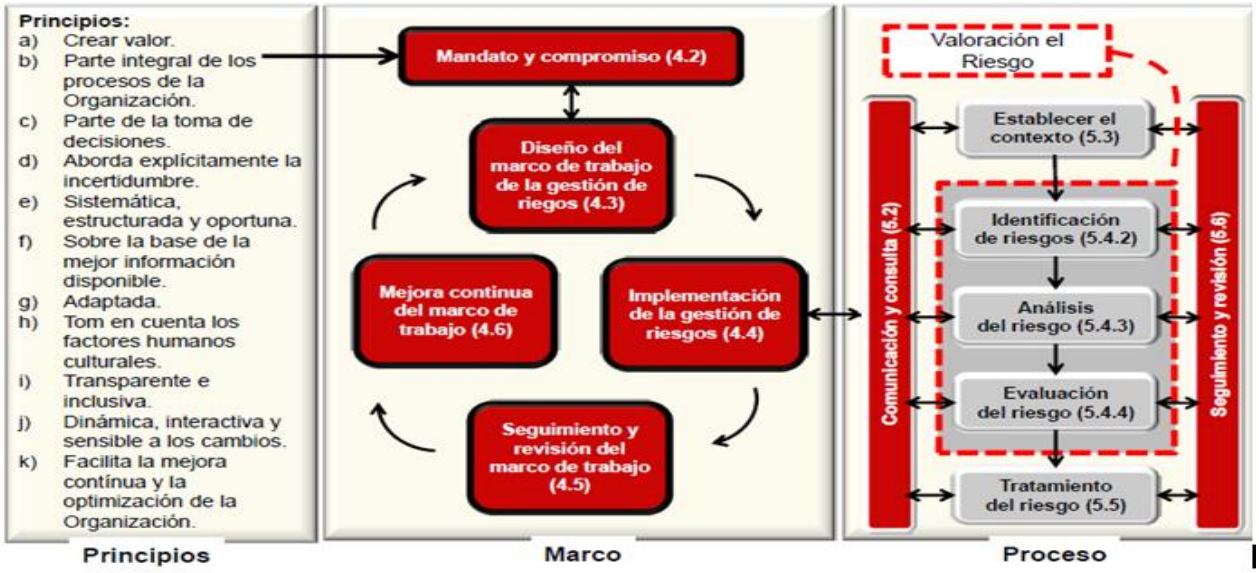

Figura 2: Principios, marco y proceso ISO 31000[1]

[1] Imagen tomada de la norma ISO 31000:2009

4.5 ISO 31010 TÉCNICAS DE APRECIACIÓN DEL RIESGO

Esta norma internacional es una norma de apoyo de la Norma ISO 31000, y proporciona directrices para la selección y aplicación de técnicas sistemáticas para la apreciación del riesgo.

Especifica las técnicas y Herramientas de Evaluación de riesgo en un proceso de Gestión de riesgo que pueden ser usadas dependiendo de la necesidad de la organización, las técnicas descritas en la norma pueden ser clasificadas de diferentes maneras con el fin de facilitar la comprensión de sus aplicaciones, elementos de entrada, procesos, resultados, relativas fortalezas y limitaciones.
La norma lista 31 técnicas para la evaluación de Riesgo según la figura 3, proporciona una Guía para la selección y aplicación de cada una de estas Técnicas en las etapas de Identificación, Análisis y Evaluación del riesgo según la propuesta de la norma ISO 31000.

TÉNCICAS DE EVALUACIÓN DE RIESGOS					
MÉTODOS DE CONSULTA	**MÉTODOS DE SOPORTE**	**ANÁLISIS DE ESCENARIOS**	**ANÁLISIS DE FUNCIÓN**	**EVALUACIÓN DE CONTROLES**	**MÉTODOS ESTADÍSTICOS**
1. Check – List 2. Análisis Preliminar de riesgos 3. Listas de ejemplos	4. Lluvia de ideas 5. Entrevista estructurada o semi-estructurada 6. Técnica Delphi 7. Técnica estructurada What if? (SWIFT) 8. Evaluación de la fiabilidad humana (HRA) 9. Análisis de Riesgos Preliminar	10. Análisis Causa Raíz (RCA) 11. Evaluación de Toxicidad 12. Análisis de Impacto al negocio (BIA) 13. Análisis de árbol de fallas (FTA) 14. Análisis de árbol de acontecimientos (ETA) 15. Análisis de causa – consecuencia 16. Análisis causa – efecto	17. Análisis de modo de fallos y efectos (AMEF – FMEA) 18. Fiabilidad de centro de mantenimiento (RCM) 19. Análisis de errores de diseño (Sneak) 20. Análisis de Peligros de Operabilidad (HAZOP) 21. Análisis de Peligros y Puntos Críticos de Control (HCCAP)	22. Análisis de capas de protección (LOPA) 23. Análisis de fallos y sucesos iniciadores (Bow Tie) 24. Análisis de circuitos de fugas	25. Análisis Markov 26. Simulación Monte Carlo 27. Estadística y redes Bayesianas 28. Curvas FN 29. Ïndices de Riesgo 30. Matrices de probabilidad y consecuencia 31. Análisis de decisión multi-criterio (MCDA)

Figura 3: Técnicas para la evaluación de riesgo

4.6 ISO 27005: Seguridad de la información y de las comunicaciones.

La norma 27005 es un estándar internacional utilizada para la gestión de riesgos de seguridad de la información[2].

Esta norma actualiza a la antigua ISO 13335, partes 3 y 4, basada en la siguiente figura 4.

Figura 4: procesos para la gestión del riesgo en la seguridad de la información y sus actividades.

La norma ISO 27005 en el proceso de gestión del riesgo en la seguridad de la información consta de:

- El establecimiento del contexto. (Numeral 7 de la norma)
- Evaluación del riesgo. (Numeral 8 de la norma)
- Tratamiento del riesgo (Numeral 9 de la norma)
- Aceptación del riesgo (Numeral 10 de la norma)
- Comunicación del riesgo (Numeral 11 de la norma)

[2] Esta norma fue creada su primera edición en cancelación y reemplazo a las normas ISO/IEC TR 13335-3:1998, e ISO/IEC TR 13335-4:2000, de las cuales constituye una revisión técnica. Dicha norma proporciona las directrices para la gestión del riesgo en la seguridad de la información que una empresa debe tomar en cuenta, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) según la norma ISO/IEC 27001.

- Monitoreo y revisión del riesgo (Numeral 12 de la norma).

Según la ISO 27005 la gestión del riesgo en la seguridad de la información debería contribuir a:

- La identificación de los riesgos;
- La evaluación de los riesgos en términos de sus consecuencias para el negocio y la probabilidad de su ocurrencia;
- La comunicación y entendimiento de la probabilidad y las consecuencias de estos riesgos;
- El establecimiento del orden de prioridad para el tratamiento de los riesgos;
- La priorización de las acciones para reducir la ocurrencia de los riesgos;
- La participación de los interesados cuando se toman las decisiones sobre gestión del riesgo y mantenerlos informados sobre el estado de la gestión del riesgo;
- La eficacia del monitoreo del tratamiento del riesgo;
- El monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos;
- La captura de información para mejorar el enfoque de la gestión de riesgos;
- La educación de los directores y del personal acerca de los riesgos y las acciones que se toman para mitigarlos.

Según la ISO 27005 es aconsejable seleccionar o desarrollar un enfoque adecuado para la gestión del riesgo que aborde los criterios básicos tales como: **Criterios de evaluación del riesgo, criterios de impacto, criterios de aceptación del riesgo.**

- **Criterios de evaluación del riesgo.**

Recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización.

Teniendo en cuenta:

- el valor estratégico del proceso de información del negocio;
- la criticidad de los activos de información involucrados;

- los requisitos legales y reglamentarios, así como las obligaciones contractuales;
- la importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio;
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

- **Criterio de Impacto.**

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la organización, causados por un evento de seguridad de la información.

Considerando los siguientes aspectos:

- nivel de clasificación de los activos de información impactados;
- brechas en la seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad);
- operaciones deterioradas (partes internas o terceras partes);
- pérdida del negocio y del valor financiero;
- alteración de planes y fechas límites;
- daños para la reputación;
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

- **Criterios de la aceptación del riesgo.**

Se recomienda desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas.

Durante el desarrollo, se deberían considerar los siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples; con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas.
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado.

- los diferentes criterios de aceptación del riesgo se pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes, podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos, si esto se especifica como un requisito contractual;
- los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

- **Valoración del riesgo en la seguridad de la información.**

La valoración del riesgo consta de las siguientes actividades:

- Análisis del riesgo el cual consiste en:
    - **Identificación del riesgo**: El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida. Esta valoración consta de la identificación de los activos a proteger dentro del contexto, la asignación del propietario del activo, identificación de las amenazas, identificación de los controles existentes, identificación de las vulnerabilidades y la identificación de las consecuencias.

    - **Estimación del riesgo:** en base a metodologías, las cuales pueden ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias. La estimación se basa en evaluación de las consecuencias, probabilidad de incidentes, nivel de estimación del riesgo.

    - **Evaluación del riesgo**: Consiste en comparar los niveles de riesgo frente a los criterios para la evaluación del riesgo y sus criterios de aceptación.

La valoración del riesgo determina el valor de los activos de información, identifica las amenazas y vulnerabilidades aplicables que existen (o que podrían existir), identifica los controles existentes y sus efectos en el riesgo identificado, determina las consecuencias potenciales y, finalmente, prioriza los riesgos derivados y los clasifica frente a los criterios de evaluación del riesgo determinados en el contexto establecido.

- **Tratamiento del riesgo**

La organización adopta en base a la evaluación realizada del riesgo el tratamiento aplicado al activo de información, este puede clasificar como una de las siguientes opciones:

- Reducir el riesgo: Aplicar controles para disminuir la probabilidad de ocurrencia o el impacto sobre el activo
- Aceptar el riesgo: En el caso de que el control sea más costoso que el activo a proteger.
- Evitar el riesgo: Cuando se decide cancelar procesos o actividades que generan un riesgo alto.
- Transferir el riesgo: Cuando se administra a través de terceros.

Aceptación del riesgo en la seguridad de la información.

En el caso se opte como un tratamiento del riesgo el Aceptar, esta decisión debe ser documentada y registrada por Alta Dirección.

Comunicación De Los Riesgos.

La información acerca del riesgo se debería intercambiar y/o compartir entre la persona que toma la decisión y las otras partes involucradas.

Monitoreo y revisión del riesgo en la seguridad de la información.

Los riesgos y sus factores deben ser periódicamente revisados y la información que resulte de las revisiones debe servir como insumo para las siguientes iteraciones del Sistema.

4.7 RISK IT

Es un marco creado para el gobierno corporativo asociado a las TIC (como se muestra en la Figura 5) que ayuda a la gestión eficaz de los riesgos de TI, basado en un conjunto de principios y guías, procesos de negocios y directrices de gestión que se ajustan a dichos principios.

Figura 5: Gobierno Corporativo

Risk IT está distribuido en dos documentos principales:

- **El Marco de Referencia** (“The Risk IT Framework “), muestra el repertorio de dominios y procesos ligados al Gobierno de los Riesgos Corporativos, asociados al uso de las TI; y,

- **la Guía para el Especialista** (“The Risk IT Practitioner Guide “), ofrece una visión en mayor detalle de ciertos aspectos concretos (creación de escenarios de riesgo específicos, basados en escenarios genéricos; creación de mapas de riesgo; definición de criterios de impacto y su relevancia para el negocio.

Según Risk it los riesgos pueden clasificarse de varias formas:

- El valor de los riesgos de TI permitidos – Asociado con las oportunidades no aprovechadas para mejorar la eficiencia o efectividad de los procesos de negocio, o la capacidad de soportar nuevas iniciativas, a través del uso de la tecnología.
- Programas de TI y riesgos en las entregas de proyectos – Asociada a la contribución de IT sobre nuevas soluciones de negocio, generalmente en forma de proyectos y programas.
- Operaciones de TI y riesgos en las entregas de servicios – Asociadas con todos los aspectos relacionados con los servicios y sistemas de TI, los cuales puede producir pérdidas o reducción del valor a la organización.

La conexión con el negocio se fundamenta en los principios en los que se basa el marco mostrado en la figura 6.

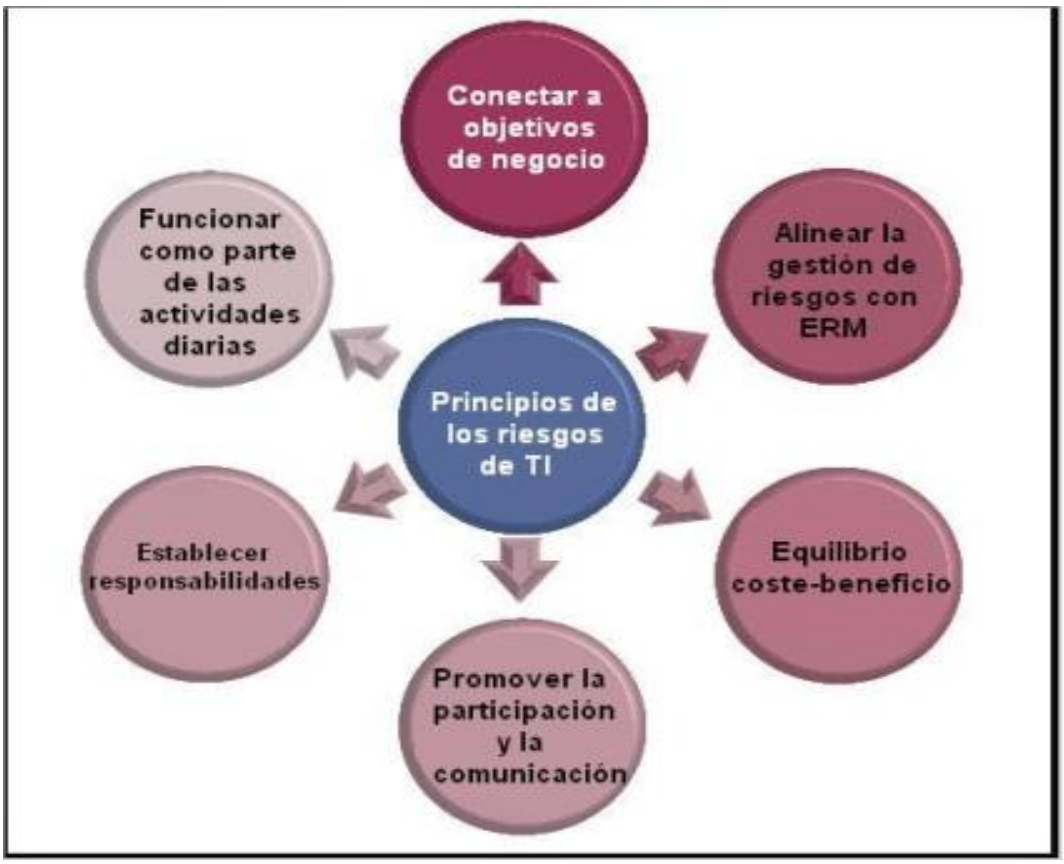

Figura 6: Principios del Riesgo

4.7.1 FUNDAMENTOS DEL GOBIERNO DE TI

Esta trata sobre algunos de los componentes esenciales del dominio de Gobierno del Riesgo. Las cuales hablan brevemente acerca de:

- Apetito de riesgo y tolerancia al riesgo.
- Responsabilidad y rendición de cuentas sobre la gestión de riesgos de TI.
- Sensibilización y comunicación.
- Cultura del riesgo.

Apetito de riesgo y tolerancia.

Según COSO ERM define el apetito de riesgo y tolerancia de la siguiente manera:

- **Apetito del riesgo**: es la cantidad de riesgo que una organización u otra entidad está dispuesta a aceptar en el cumplimiento de su misión (o visión).
- **Tolerancia del riesgo**: es la variación aceptable en relación a la consecución de un objetivo (y con frecuencia se mide mejor en las mismas unidades que las que se utiliza para medir los objetivos relacionados).

Mediante la gestión de riesgos de TI, se ha desarrollado un modelo de proceso que les será familiar a los usuarios de COBIT viéndolo desde IT. Se facilitan guías sobre las actividades clave dentro de cada proceso, las responsabilidades para el proceso, los flujos de información entre los procesos y la gestión del rendimiento del proceso.

El marco de RISK IT se basa en los riesgos de TI. En otras palabras, el riesgo organizacional está relacionado con el uso de las TI. La conexión con la organización se basa en los principios en los que se construye el marco, es decir, el gobierno efectivo de la organización y gestión de los riesgos de TI, Algunos de ellos son[3].

[3] Marco de Riesgos de TI, Disponible enhttp://www.info.unlp.edu.ar/uploads/docs/risk_it.pdf, acceso el 11de mayo de 2014.

El ámbito según RISK IT se clasifica en: ver figura 7:

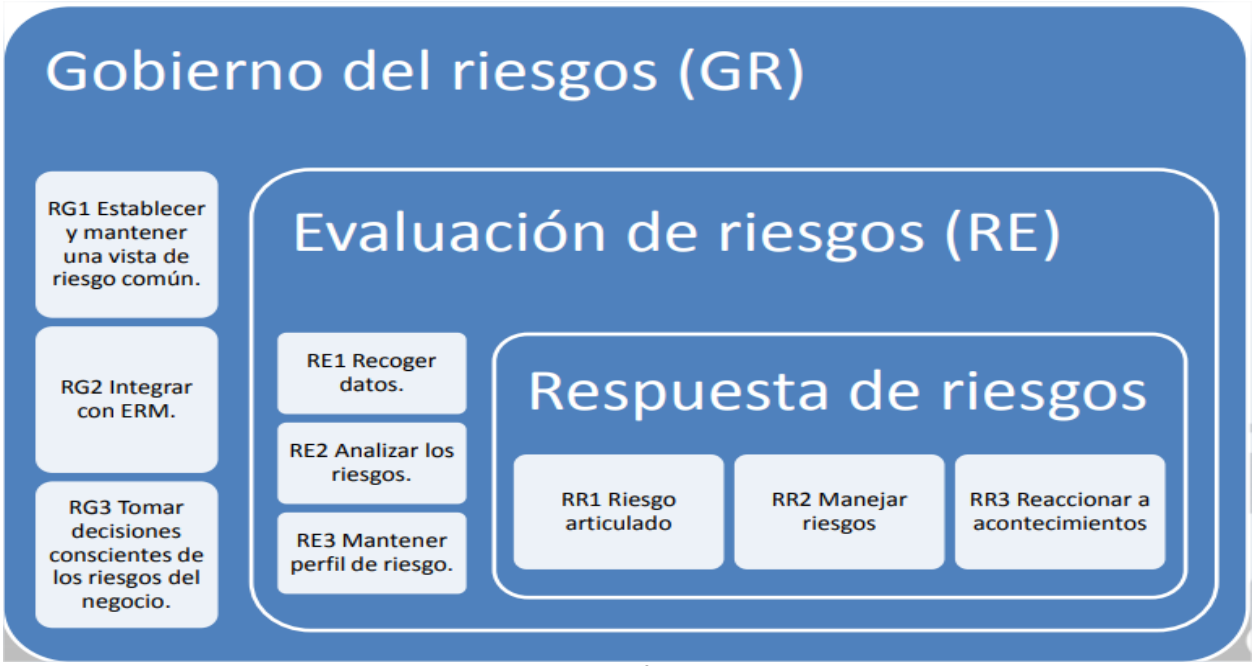

Figura 7: Clasificación del Riesgo

- **Comunicación según RISK IT** La comunicación de riesgo de TI abarca una amplia gama de flujos de información. Según Risk IT distingue entre los siguientes principales de tipos de comunicación de riesgos TI, según Figura 8.

Figura 8: Principales tipos de comunicación

- **Cultura de riesgos.**

La gestión de riesgos consiste en ayudar a las organizaciones a asumir mayores riesgos en la búsqueda de la rentabilidad. El conocimiento del riesgo también implica que todos los niveles dentro de una organización son conscientes de cómo y por qué para responder a los eventos adversos de TI.

La cultura del riesgo incluye:

- El comportamiento hacia la toma del riesgo
- ¿Cuál es el grado de riesgo que siente la organización que puede asumir y qué riesgos está dispuesta a tomar?
- El comportamiento hacia la política siguiente
- ¿En qué medida la gente va a aceptar y / o cumplir con la política?
- El comportamiento hacia resultados negativos
- ¿Cómo la organización se ocupa de los resultados negativos, es decir, acontecimientos de pérdida u oportunidades perdidas? ¿Aprenderá ellos de esto y tratarán de adaptarse, o se culpará sin tratar la causa de origen?

4.8 REVISION DE BUENAS PRÁCTICAS.

4.8.1 ISO31000

Buenas Practicas	Propósito
Comunicación y Consulta	Esta fase es importante dado que en ellas dan sus opiniones acerca del riesgo con base a la percepción de cada una de las partes involucradas, la Comunicación y la consulta debe desarrollar planes que aborden aspectos del propio riesgo, sus causas y consecuencias y las medidas que se tomen para tratarlo.
Establecimiento del Contexto	La organización considera sus objetivos, define los parámetros externos e internos que se van a considerar al gestionar el riesgo y establece el alcance y los criterios del riesgo para el resto del proceso.

Valoración-Identificación del Riesgo	El objeto de esta fase es generar una lista exhaustiva de riesgos con base en aquellos eventos que podrían crear, aumentar, prevenir, degradar acelerar o retrasar el logro de los objetivos.
Valoración-Análisis del Riesgo	La entrada de esta etapa es la lista de riesgos previamente identificados y el objetivo es desarrollar un entendimiento y comprensión acerca del riesgo y sus causas, utilizando como criterios la probabilidad de ocurrencia y el impacto de sus consecuencias, esto permite calcular el nivel de riesgo en función de estas dos variables. El análisis del riesgo proporciona elementos de entrada para tomar decisiones sobre cuáles son los riesgos y las causas a los que se les debe dar un tratamiento inmediato, cuales admiten acciones a mediano plazo y cuáles pueden ser aceptados sin tener nuevas acciones, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados.
Valoración-Evaluación del Riesgo	Toma como entrada los resultados de la identificación y del análisis del riesgo y tiene como objetivo ayudar a la toma de decisiones, determinando los riesgos a tratar, la forma de tratamiento más adecuada para adaptar los riesgos adversos a un nivel tolerable y conocer la priorización para implementar el tratamiento determinado.
Tratamiento de Riesgos	Involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. El tratamiento suministra control sobre los riesgos o los modifica.
Monitoreo Y Revisión	Este proceso de monitoreo y revisión se ejecuta sobre los planes de tratamiento del riesgo y proporciona una medida del funcionamiento de los mismos, cuyos resultados, registrados en informes

	internos y externos, se pueden incorporar en la gestión del funcionamiento global de la organización, en su medición y en las actividades externas e internas.
Registro	Los registros brindan la base para la mejora de los métodos y las herramientas, así como del proceso global, permiten el mejoramiento continuo en la organización, permite que la información sea reutilizada con fines de gestión.

4.8.2 ISO 31010

Buenas Practicas	Propósito
Evaluar el método de "Evaluación de toxicidad"	Se aplicará para analizar e identificar las posibles vías por las que el activo especifico podría estar expuesto al peligro. Utilizando la información sobre el nivel de exposición y la naturaleza del daño causado en un nivel de exposición determinado, combinándose para dar una medida de la probabilidad que el daño ocurra.
Adoptar el método de análisis del árbol de fallas	Esta técnica se utilizará para evaluar los eventos no deseados y determinar todas las posibles maneras que las que podría ocurrir, creando un diagrama de árbol lógico. Este árbol se considerará para evaluar las formas de reducir o eliminar las posibles causas y fuentes.
Adoptar el método de Análisis del árbol de eventos	Esta técnica hará uso del razonamiento inductivo para evaluar las probabilidades de diferentes sucesos sobre los posibles resultados.
Análisis de escenario	Se utilizará para analizar los futuros escenarios basándose en los riesgos presentes y diferentes, considerando que en cada uno de estos escenarios podría ocurrir un incidente. Esto se puede aplicar de manera cualitativa y cuantitativamente.

Adoptar el método de análisis de causa y efecto	Se utiliza para clarificar las causas de un problema. Clasifica las diversas causas que se piensa que afectan los resultados, señalando con flechas la relación causa – efecto entre ellas.
Implementar el método LOPA (capas de análisis de la protección)	También llamado análisis de barrera, se utilizará para determinar si se tienen las suficientes capas de seguridad para hacer frente a un escenario de accidente, es decir, si el riesgo puede ser tolerado.
Implementar el método de análisis del método de corbatín	Es la manera esquemática para describir y analizar la ruta de un riesgo desde las causas hasta las consecuencias. Puede ser considerado como una combinación de pensamiento del árbol de fallas analizando la causa de un evento (representado por el nudo de una corbata de lazo) y un árbol de eventos analizando las consecuencias.

4.8.3 ISO 27005

Buenas Practicas	Propósito
Evaluación de las restricciones técnicas	Permite evaluar la infraestructura, hardware y software y en todos aquellos lugares donde se albergan a los procesos.
Análisis de las restricciones de tiempo	El tiempo que se requiere para implementar los controles de seguridad se debería considerar con respecto a la capacidad de actualizar el sistema de información; si el tiempo para la implementación es muy prolongado, los riesgos para los cuales se diseñó el control pueden haber cambiado. El tiempo es un factor determinante para la selección de soluciones y prioridades.
Identificación de los tipos de activos y evaluación del riesgo	Para realizar la valoración de los activos, es necesario que la organización identifique primero sus activos (con un grado adecuado de detalles). Se pueden diferenciar dos clases de activos.

Realizar una valoración de los activos	Luego de identificar los activos se debe pactar la escala que se va a utilizar y los criterios para la asignación de una ubicación particular en esa escala para cada uno de los activos, con base en la valoración. Debido a la diversidad de activos que se encuentran en la mayoría de las organizaciones, es probable que algunos activos que tengan un valor monetario conocido sean valorados en la moneda local en donde están presentes, mientras otros que tiene un valor más cualitativo se les puede asignar un rango de valores, por ejemplo, desde "muy bajo" hasta "muy alto".
Evaluar el impacto sobre los activos	Un incidente en la seguridad de la información puede tener impacto en más de uno de los activos o únicamente en una parte de uno de los activos. El impacto se relaciona con el grado de éxito del incidente. En consecuencia, existe una diferencia importante entre el valor del activo y el impacto resultante de un incidente.

4.8.4 COBIT 5 APO12

Buenas Practicas	Propósito
Recopila Datos	Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con el riesgo de TI, con capacidad para varios tipos de eventos, múltiples categorías de riesgo de TI y de múltiples factores de riesgo.
	Registrar los datos pertinentes acerca del entorno corporativo interno y externo que puedan desempeñar un papel importante en la gestión de riesgo de TI
	Registrar datos sobre los eventos de riesgo que hayan causado o puedan causar impactos a los catalizadores del beneficio/valor de TI, a la entrega de programas y

	proyectos de TI, y/o las operaciones y a las prestaciones de servicios de TI, capturar la información relevante de los asuntos relacionados, incidentes, problemas e investigaciones.
Analizar el Riesgo	Definir el alcance y la profundidad adecuada de las actividades de análisis de riesgo teniendo en cuenta todos los factores de riesgo y la criticidad de los activos del negocio.
	Construir y analizar periódicamente los escenarios de riesgo de TI.
	Estimar la frecuencia y la magnitud de la pérdida o ganancia asociada con los escenarios de riesgo de TI. Considerar todos los factores de riesgo aplicables, evaluar los controles operativos conocidos y estimar los niveles e riesgo residual.
Expresar el Riesgo	Reportar los resultados del análisis de riesgo a todas las partes interesadas afectadas en los términos y formatos útiles para respaldar las decisiones empresariales.
	Ayudar a los tomadores de decisiones a comprender los peores casos y los escenarios más probables, las exposiciones de debida diligencia y la reputación significativa, consideraciones legales o reglamentarias.
	Revisar los resultados de las evaluaciones objetivas de terceros, de auditoria interna y las revisiones de controles de calidad y asignarlos al perfil de riesgo.
Definir el portafolio de acciones para la gestión del Riesgo	Mantener un inventario de actividades de control implantadas para gestionar el riesgo y que permitan que los riesgos se adecuen al apetito del riesgo y la tolerancia. Clasificar las actividades de control y asignarlas a las declaraciones de riesgo de TI específicas y a las agregaciones de riesgo de TI.

Responder al Riesgo	Aplicar un plan de respuesta adecuado para minimizar el impacto cuando se produzcan incidentes de riesgo.
	Preparar, mantener y aprobar planes que documenten pasos específicos a tomar cuando el evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave.
	Categorizar incidentes, y comparar la exposición real respecto a los umbrales de tolerancia del riesgo.

4.8.5 COBIT 5 APO 13

Buenas Practicas	Propósito
Establecer y mantener un SGSI	Establecer y mantener un SGSI que proporcione un enfoque estándar, formal continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que este alineados con los requerimientos de negocio y la gestión de la seguridad de la empresa.
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información	Mantener un plan de seguridad de la información que describa como se gestionan y alinean los riesgos de seguridad de la información con la estrategia y la arquitectura de la empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basen en casos de negocio aprobados, se implementan como parte integral del desarrollo de las soluciones y servicios.
Supervisar y revisar el SGSI	Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de la información. Recolectar y analizar datos sobre el SGSI y la

	mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.

4.8.6 RISK IT

Buenas Practicas	Propósito
Adoptar un componente del Gobierno de riesgos para la evaluación.	El gobierno de riesgo discute componente como: ● El apetito del riesgo y tolerancia. ● Responsabilidades y redición de cuentas sobre la gestión de riesgo ● Sensibilización y comunicación ● Cultura del riesgo
Adoptar alguna metodología para la evaluación del apetito del riesgo	Según Risk It define el apetito del riesgo como la cantidad de riesgo que una entidad está dispuesta a aceptar cuando se trata de alcanzar sus objetivos, este se puede definir mediante un mapa de calor.
Creación de técnicas, indicadores claves o flujo para la comunicación de riesgos	Risk it presenta el flujo importante para la comunicación del riesgo basado en la expectativa, capacidad y el estado del riesgo.
Creación de funciones para la gestión de riesgo	Dichas funciones asumen la responsabilidad o rendición de cuentas para una o más actividades dentro de un proceso.
Creación de escenarios de riesgos	Crear escenarios que le permita a la organización identificar: Actores, tipos de amenazas, Acciones que gestiona el riesgo, activos o recursos, Tiempo estimado.

5. DESARROLLO DE LA METODOLOGIA

5.1 Introducción.

Este documento presenta una metodología para gestionar riesgos de TI para cuya base se han utilizado puntos importantes de las normas ISO 31000, ISO/IEC 27005, COBIT5 específicamente APO 12 Y 13, Risk IT, ISO 31010 teniendo en cuenta que estos indican que se requiere para la gestión de riesgos. Además, incluye recomendaciones y buenas prácticas para el manejo de riesgos y la seguridad.

En este punto el desarrollo y uso de metodologías integradas y ágiles para gestionar riesgos y en especial el tecnológico, es importante con el fin de minimizar el impacto que pueda causar la violación de alguna de las dimensiones de la seguridad esto corresponde a la confidencialidad, integridad, disponibilidad de la información.

5.2 Alcance

El modelo de Gestión de Riesgo se realiza para la empresa de factoraje específicamente en el área de TI en el cual se analizarán, evaluaran y se proporcionaran recomendaciones para el tratamiento de la gestión del riesgo, siguiendo los lineamientos y mejoras de las normas que hablan sobre el riesgo.

De acuerdo a una metodología se establecerán buenas prácticas para la determinación de controles que la empresa de Factoraje debe implementar para la mitigación del riesgo.

5.3 Referencias normativas.

Los documentos siguientes son indispensables para el desarrollo y la aplicación del presente trabajo.

5.4 Contexto de la Gestión del Riesgo.

Con base a la lectura de las normas antes planteadas se ha estructurado un modelo de gestión de riesgo el cual busca servir como guía para identificar los riesgos de la empresa de Factoraje.

A continuación, en la figura 9 se detallan los procesos y sus relaciones, de los pasos a seguir para el desarrollo de esta metodología.

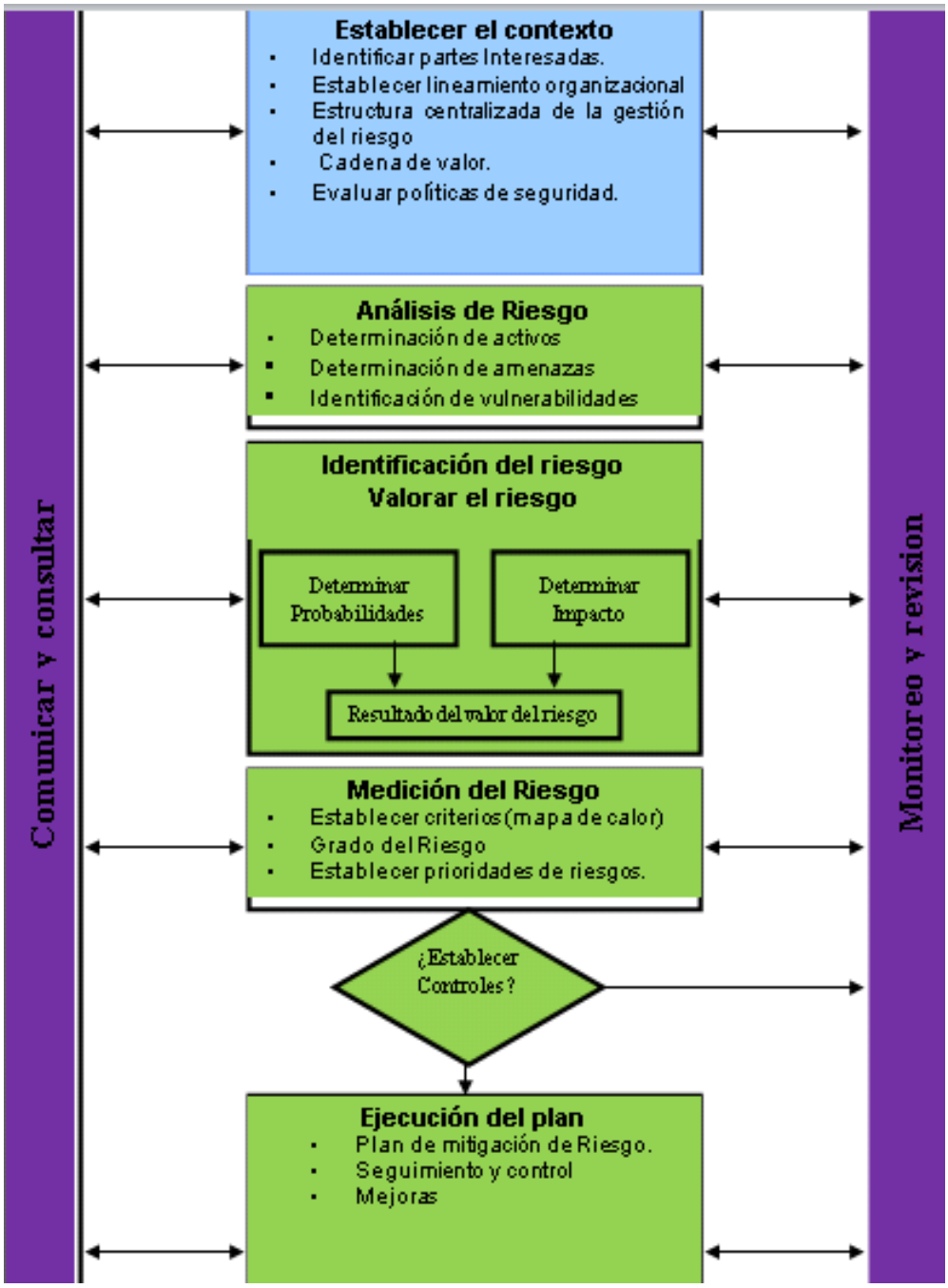

Figura 9. Modelo de gestión del riesgo

5.4.1 Definición del contexto y planificación del riesgo.

Establecer el contexto define los parámetros básicos dentro de los cuales se gestionan los riesgos y establece el alcance para el resto del proceso de gestión del riesgo. El contexto incluye el ambiente interno y externo los cuales se irán definiendo el desarrollo de la metodología.

5.4.2 Identificar las partes interesadas.

Descripción general.

El primer paso para la gestión del riesgo será la determinación de las partes interesadas, lo cual deberá listarse un detalle de todas las partes involucradas en el negocio, luego se debe seleccionar de ese detalle, las partes interesadas pertinentes.

Una parte interesada pertinente

Será aquella que se vea impactada directamente por temas financieros (multas, procesos), reputaciones (pérdida de imagen, prestigio, credibilidad). El listado seleccionado servirá para determinar los activos de información asociados, este detalle de activos deberá relacionarse con los procesos de misión crítica de la empresa, concluyendo al finalizar con un detalle de activos sobre los cuales las siguientes etapas trabajaran sus detalles.

La presente metodología establece en el anexo 1, una plantilla para el levantamiento de las partes interesadas, en ella se detalle los elementos a considerar para que sean partes interesadas pertinentes, en la cual se deben de tomar en consideración los siguientes puntos según figura 10:

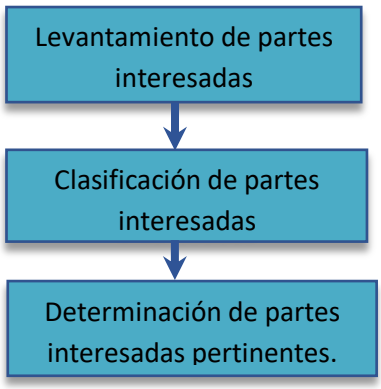

Figura 10, elementos considerados para partes interesadas pertinentes

De manera general los grupos de interés que intervienen en el funcionamiento de una empresa inciden en sus resultados, los cuales se pueden mencionar:

a. Clientes.
b. Proveedores / suministradores.
c. Personas de la Organización.
d. Socios.

e. Accionistas.
f. Administración.
g. Sociedad.

5.4.3 Establecer lineamiento organizacional

La dirección tendrá que decir cómo se dispersaran las actividades relacionadas con la gestión del riesgo; la metodología no pretende imponer un criterio, más bien se recomienda analizar en función de la realidad.

La política organizacional es la directriz u orientación que tendría que ser divulgada, entendida e interiorizada por todos los miembros de la organización, en ella se contemplan las normas y responsabilidades de cada área de la organización.

Según las buenas prácticas, es recomendable que las organizaciones opten por una estructura, recomendado en este proceso de investigación las siguientes:

a. Estructura centralizada para la gestión de riesgo.
b. Estructura descentralizada para la gestión del riesgo.

5.4.3.1 Estructura centralizada para la gestión de riesgo.

La dirección podrá crear un departamento de gestión del riesgo, área funcional que será responsable de la gestión del riesgo con ayuda de diferentes departamentos. En la figura 11, se muestra un ejemplo de un diagrama con su estructura organizacional.

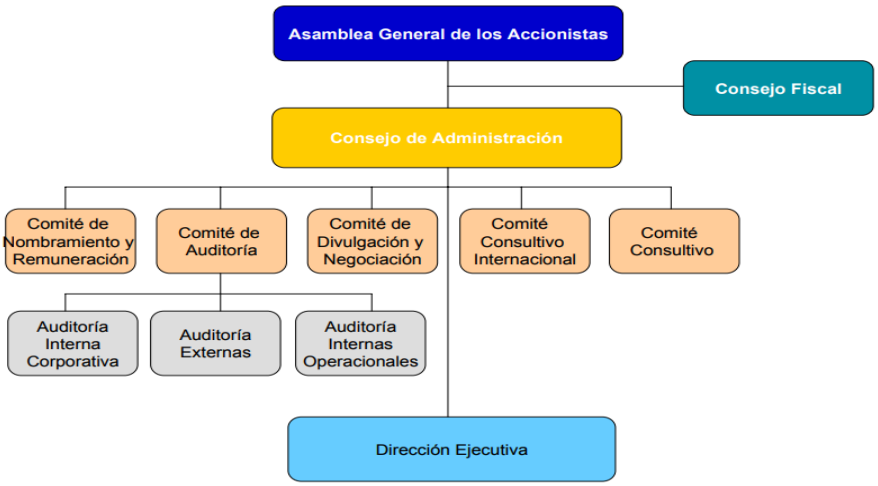

Figura. 11 Diagrama organizacional general

5.4.4 Establecer cadena de valor

Controlar cada eslabón de la cadena de valor permitirá a la empresa gestionar sus riesgos, maximizar las oportunidades de innovación, de eficiencia y sobre todo, aumentar su competitividad.

El no controlar los riesgos, derivados por ejemplo de proveedores directos o de segunda o tercera línea, podría provocar serios perjuicios a la operación, a la reputación y a la sostenibilidad de la empresa u organización.

Por ello el encargado o el área responsable de gestionar el riesgo deberá de identificar aquellos procesos relacionados con la cadena de valor para un buen resultado de sus servicios o productos. En la figura 12 se muestra algunos riesgos que deben controlarse para no afectar la cadena de valor:

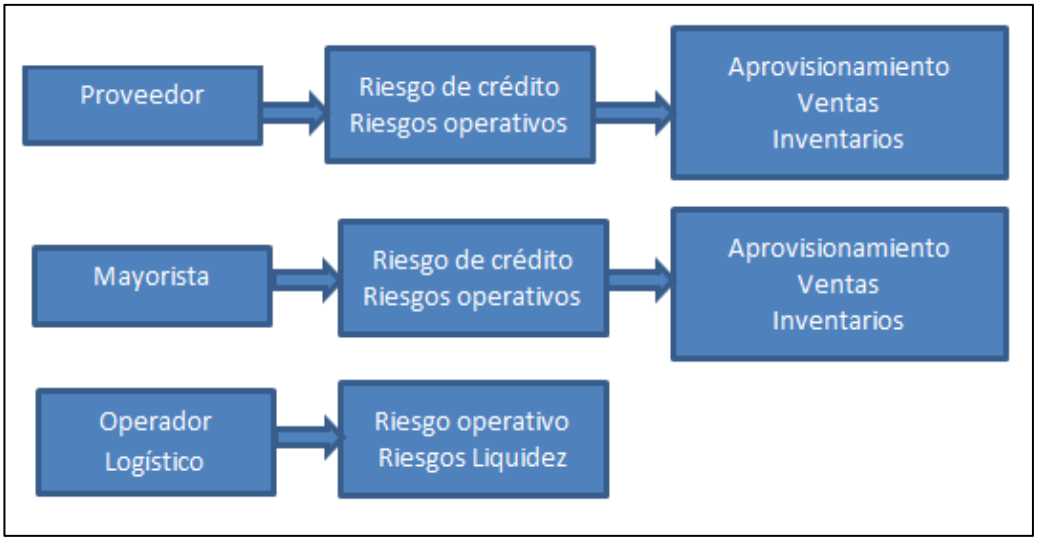

Figura 12. Riesgos que pueden afectar la cadena de valor

Dado que rara vez en una cadena los efectos de la ocurrencia de un riesgo suelen quedar contenidos en el nodo o vínculo en el que se verifica, resulta crucial para la estabilidad y el buen desempeño de una cadena es desarrollar estrategias de gestión de riesgos que identifiquen los riesgos a los que se encuentran expuestas cada eslabón de la cadena de valor que la empresa establezca, la probabilidad de ocurrencia de tales riesgos y los efectos que podrían tener la cadena y sus actores.

5.4.5 Definir el contexto

- **Evaluar Políticas de seguridad.**

La organización, deberá de tener claramente definida una política para la gestión de riesgos, sobre la cual se construirán las políticas asociadas al detalle de los activos y la gestión de riesgos de IT. En caso de tener un área de gestión de riesgos deberá de alinearse la política a dicha área, de no ser así, deberá redactarse la política de gestión de riesgo, considerando los siguientes elementos:

a) Área geográfica.
b) Proceso claves determinados en la cadena de valor.

Generalmente, la mayoría de empresas no poseen políticas de riesgo, el departamento de IT, al igual que los responsables de las diversas áreas deberán proveer y mantener la seguridad de los activos tomando como base las políticas de seguridad. Existen diversas normas que inciden en la adquisición y el uso de los bienes y servicios, las cuales se deberán acatar por aquellas instancias que intervengan directa o indirectamente en ello.

Las políticas son guías que se crean para orientar la acción; son lineamientos generales a observar en la toma de decisiones, sobre algún problema que se repite una y otra vez dentro de una organización. En este sentido, las políticas son criterios generales de ejecución que complementan el logro de los objetivos y facilitan la implementación de las estrategias. Las políticas deben ser dictadas desde el nivel jerárquico más alto de la empresa.

5.4.6 Análisis de riesgo

- **Determinación de activos.**
    - **Identificar los activos**

Un activo es algo que representa un valor o una utilidad para cualquier organización. Los activos precisan protección para asegurar las operaciones del negocio y la continuidad de la empresa.

La forma de la clasificación de los activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, ya que con base a su valor y de acuerdo a otras características particulares requiere un tipo de manejo especial.

Todos los activos de TI que son debidamente administrados, deben ser clasificados por su encargado considerando las siguientes propiedades:

- Confidencialidad: Garantizar que la información será accedida únicamente por personal autorizado.
- Integridad: Garantizar que la información será modificada únicamente por personal autorizado.
- Disponibilidad: Garantizar que la información estará disponible en el momento que sea requerido por el personal autorizado y para los fines que fue creada.

Los activos se pueden clasificar de la siguiente manera:

- **Activos de información:** Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
- **Activos de software:** Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas
- **Recurso humano:** Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
- **Servicio:** Servicios de computación y comunicaciones, tales como internet, páginas de consulta, directorios compartidos e Intranet
- **Hardware:** Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos
- **Otros:** activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso

En el anexo 4 se muestra un cuadro que le permitirá a la organización la identificación de los activos.

- **Valoración de los activos**

Una vez identificado los activos, el siguiente paso es hacer la valoración de estos. Esto se refiere al valor que se le asigna a cada activo de acuerdo al grado de importancia, además siempre resguardando la disponibilidad, integridad, confidencialidad y disponibilidad de cada uno de ellos.

En el anexo 5 se presenta la clasificación y valoración de los activos.

- **Determinación de las amenazas.**
  - **Identificar las amenazas.**

Las **amenazas** a las que se puede enfrentar la empresa Factoraje, pueden ser muy variadas, a modo de ejemplo:

Desastres Naturales: Este grupo de amenazas comprende los eventos que tienen su origen en las fuerzas de la naturaleza, estos desastres afectan a la información e integridad del sistema, ejemplos:

- Temblor, huracán, inundación, rayos.

Ataques Maliciosos: Estas amenazas están enfocadas a los ataques maliciosos de destrucción como el uso de explosivos y armas químicas o de acceso como el acceso a servicios, ejemplos:

- **Explosivos, vandalismo, intensión de robo, manipulación de equipo, manipulación de datos.**

- Fallas de energía: Este tipo de amenazas está enfocada a la explotación de las fallas de carga de energía, ejemplos:

- **Falla de suministro eléctrico, subidas de voltaje,**

- Fallas de comunicación: Esta clase reúne las amenazas dirigidas a los sistemas de comunicaciones, ejemplos:

- **Falla Degradación de sistemas de comunicaciones, falla/Degradación de equipo informático**

- Software: Las amenazas de software incluyen posibles fallas dentro del diseño, desarrollo e implementación del software, ejemplos:

- **Uso de software por usuarios no autorizados, uso de software en forma no autorizada, uso ilegal de software, software malicioso, código troyano, engaño DNS, falla de software/corrupción**

- Comunicaciones: Las principales amenazas que se presentan en esta categoría son la no disponibilidad de red, y la infiltración a las comunicaciones, ejemplos:

- Acceso a la red por usuario no autorizado, uso de instalaciones de red en forma no autorizada, comunicaciones a rutas no autorizadas, mal uso de puertos de acceso remoto para administración/diagnostico.

- Error humano: errores accidentales o deliberados de las personas que interactúan con la información, por ejemplo:

- acciones no autorizadas como uso de software o hardware no autorizados
- funcionamiento incorrecto por abuso o robo de derechos de acceso o errores en el uso, falta de disponibilidad, etc.
- información comprometida por robo de equipos, desvelado de secretos, espionaje, etc.

- **Valoración de las amenazas**

Después de obtener una relación de todos los activos disponibles en nuestra organización, habrá que **identificar y conocer las amenazas** susceptibles de causar daños en la información, los procesos y los soportes.

Con tal de ser eficaces en la tarea de identificación de las amenazas y **la valoración de los daños** que pueden producir, es recomendable contrastar la información de que disponemos con los propietarios de los activos, usuarios, expertos, etc.

En lo que respecta a la valoración de los daños, estas serán algunas de las preguntas que debemos formularnos:

¿Qué valor tiene este activo para la empresa?
¿Cómo repercute en los beneficios de la empresa?
¿Cuánto valdría para la competencia?
¿Cuánto costaría recuperarlo o volverlo a generar?
¿Cuánto costó adquirirlo o su desarrollo?
¿A qué responsabilidades legales o contractuales nos enfrentamos si se ve comprometido?

Es necesario hacer un análisis de riesgo, para ello se valorarán las amenazas y vulnerabilidades que afecten a los activos escogidos para el análisis e impacto que ocasionaría que algunas de las amenazas ocurrieran, sobre la base de conocimiento y experiencia dentro de la organización.
Como ejemplo de metodología de Análisis de Riesgos que utilizaremos como referencia se mostrara en las siguientes tablas.

Estimación de la probabilidad de ocurrencia de una amenaza sobre cada activo:

Probabilidad de ocurrencia de la amenaza	Guía
Baja	**Una media de una vez cada 5 años**
Media	**Una media de una vez al año**
Alta	**Una media de 3 veces al año**
Muy alta	**Una media de una vez al mes**

Estimación de la vulnerabilidad de cada activo, es decir, la facilidad de las amenazas para causar daños en el mismo:

Vulnerabilidad	Guía
Baja	**Una media de una vez cada 5 años**
Media	**Una media de una vez al año**
Alta	**Una media de 3 veces al año**
Muy alta	**Una media de una vez al mes**

- **Identificación de vulnerabilidades**

Tal y como hemos comentado anteriormente, una vulnerabilidad es toda aquella circunstancia o característica de un activo que permite la materialización de ataques que comprometen la confidencialidad, integridad o disponibilidad del mismo. Por ejemplo, ***comunicaciones***: Esta clase comprende las vulnerabilidades relacionadas con la posible intercepción de información por personas no autorizadas y con fallas en la disponibilidad del servicio: Transferencia de contraseñas/claves viables en texto visible, líneas de comunicación no protegidas.

Hay que identificar las debilidades en el entorno de la organización y valorar que tan vulnerable es el activo en una escala razonable por ejemplo (alto-medio-bajo; en rangos del 1 a 5; etc.). Hay que tener en cuenta que la presencia de una vulnerabilidad por sí misma no causa daño. Para que esta vulnerabilidad se materialice debe existir una amenaza que pueda explotarla. Algunos ejemplos de vulnerabilidades son:

1. La ausencia de copias de seguridad, que compromete la disponibilidad de los activos.
2. Tener usuarios sin formación adecuada, que compromete la confidencialidad, la integridad y la disponibilidad de los activos, ya que pueden filtrar información o cometer errores sin ser conscientes del fallo.
3. Ausencia de control de cambios, que compromete la integridad y la disponibilidad de los activos.

- **Identificar el riesgo**

Los riesgos deben ser identificados de manera que se puedan entender antes de ser analizados y gestionados correctamente. Esta identificación debe tener un enfoque detallado que permita abarcar todos los eventos posibles, de modo que se clasifiquen los riesgos en las categorías definidas en la estrategia de gestión del riesgo, de tal manera que los riesgos formen una línea base para el inicio de actividades en la gestión de riesgo.

Los riesgos deben ser revisados periódicamente para examinar las posibles fuentes de riesgo y revisar las condiciones cambiantes, revisando los riesgos que se pasaron por alto o aquellos que no existían en la última revisión.

En la siguiente tabla se muestra diferentes técnicas para la identificación del riesgo:

Técnica/Metodología	Aplicación
Lluvia de ideas	Identificación de riesgos y de sus características en forma grupal
Análisis/causa y efecto	Identificación de causas y efectos de un riesgo
Lista de chequeo y cuestionarios	Identificación de riesgos con guías estandarizadas, amplias y ajustables a todo tipo de empresa, pueden ayudar a elaborar el catálogo general de riesgos de una empresa
Inspección	Identificación de riesgos que pueden ser observados en instalaciones o en el desarrollo de un proceso
Entrevista	Identificación de riesgos que requieren el conocimiento y experiencia de personas clave
Flujograma	Identificación de riesgos en los procesos
Análisis de Información	Identificación de riesgos a través del análisis de información financiera, manuales técnicos, registro de siniestralidad y otros eventos, y del estudio de contratos laborales y comerciales

En el anexo 2 se presenta una matriz para la identificación del riesgo.

- **Valorar el riesgo**

La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados como elementos de control, con el objetivo de establecer prioridades para su manejo y fijación de políticas.

Una vez se hayan identificado los riesgos, se deberá determinar qué se va hacer con ellos. La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados como elementos de control, con el objetivo de establecer prioridades para su manejo y fijación de políticas.

En el anexo 3 le presentamos las tablas donde le permitirá sacar un listado para la valoración del riesgo.

- **Impacto y probabilidad**

Una de las formas en que se pueden apoyar para asignar un valor a la probabilidad de ocurrencia es la siguiente:

- El valor de la probabilidad (del 1 al 10) estará de acuerdo a los factores de riesgo.
- Y el valor del impacto (del 1 al 10) de acuerdo a los efectos.

En la figura 13 se presenta un ejemplo de valor del impacto por la probabilidad en mapa de calor:

		IMPACTO		
		Leve (1)	**Moderado (5)**	**Desastroso (10)**
PROBABILIDAD	**Probable (10)**	10 Riesgo Moderado	50 Riesgo Importante	100 Riesgo Inaceptable
	Posible (5)	5 Riesgo Tolerable	25 Riesgo Moderado	50 Riesgo Importante
	Improbable (1)	1 Riesgo Aceptable	5 Riesgo Tolerable	10 Riesgo Moderado

Figura 13. Matriz de probabilidad del Impacto

5.4.7 Aplicación del procedimiento para medir el riesgo.

Una vez identificados los riesgos asociados a los distintos procesos, es necesario establecer una metodología para medirlos y priorizarlos.

Metodología de implementación del mapa de riesgo.
Herramienta propuesta.

Mapa de Riesgo

El Mapa de Riesgos ha proporcionado la herramienta necesaria, para llevar a cabo las actividades de localizar, controlar, dar seguimiento y representar en forma gráfica, los agentes generadores de riesgos que ocasionan accidentes.

El objetivo es elevar la capacidad y la calidad en el funcionamiento de la institución, garantizando la eficiencia y la eficacia de los procesos.

Medición del riesgo

Para medir la probabilidad de ocurrencia de un evento de riesgo se establecerán los siguientes criterios:

Se determinará del valor del impacto por el valor de la probabilidad. Determinado el nivel de riesgo inherente de los eventos de riesgo, el Encargado de Riesgos o quien esté a cargo del riesgo, identificará las actividades de control que mitigan los riesgos identificados.

Se confeccionará un Mapa de Riesgos que determinará los riesgos que poseen mayor exposición, permitiéndoles priorizar en cada uno para obtener mejores esfuerzos, tal y como se muestra en el ejemplo de la figura 14.

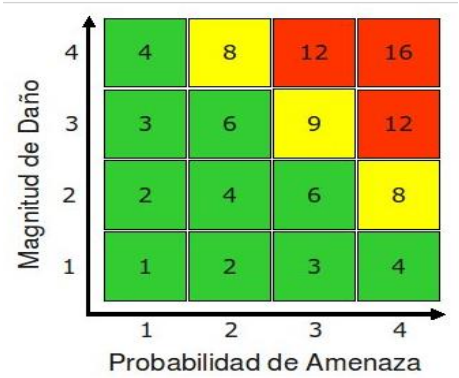

Figura 14. Tabla de valoración del Impacto probabilidad

5.4.8 Desarrollo del plan de mitigación del riesgo

Una vez realizado el análisis de los riesgos con base en los aspectos de probabilidad e impacto, se recomienda utilizar la matriz de priorización que permite determinar cuáles requieren de un tratamiento inmediato.

Esta matriz se realiza en primera instancia al interior de cada una de las dependencias los resultados que de aquí se deriven servirán para socializarlos con el mapa de riesgos

En el anexo 6, se estructura el plan para la mitigación del riesgo, en donde se establecen las actividades a realizar para la mitigación del riesgo, estableciendo responsables, fechas de inicio y finalización de la acción a realizar.

MEJORA CONTINUA

5.4.9 Seguimiento y control

Una vez diseñado y validado el plan para administrar los riesgos, en el mapa de riesgos, es necesario monitorearlo teniendo en cuenta que estos nunca dejan de representar una amenaza para la organización.

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

El monitoreo debe estar a cargo de los responsables de los procesos y de la Oficina de control Interno, su finalidad principal será la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo. La Oficina de Control Interno dentro de su función asesora comunicará y presentará luego del seguimiento y evaluación sus resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas.

5.4.10 Definición de metas y métricas.

Las métricas basadas en la seguridad de la información permiten evaluar si los controles de seguridad, políticas y procedimientos son efectivos.
Las métricas de seguridad de la información monitorean el cumplimiento de las metas y objetivos cuantificando el nivel de implementación de los controles de seguridad y efectividad de los mismos e identificando posibles actividades de mejora.

5.4.11 Mejora

En esta etapa se debe, en función de toda la información recabada en las etapas de monitoreo, métricas y revisión se deben adoptar las decisiones y redefiniciones necesarias para corregir los aspectos y controles que no estén logrando la efectividad esperada y replantearse el acierto o no de los controles planteados, así como la vigencia de los objetivos de control.

Es así que en esta etapa deberá tenerse en cuenta:

- Definir acciones correctivas y preventivas.
- Evaluar sugerencias y definir la implementación de mejoras.
- Revisar el plan de mejora continua.
- Obtener el “ok” de la Dirección si es necesario de los cambios propuestos.
- Obtener los recursos para llevarlos a cabo.
- Comunicar estos cambios y mejoras.

6.0 APLICACION DE LA METODOLOGIA DE GESTION DE RIESGO

- **Identificar partes interesadas.**

De acuerdo a la información proporcionada por la empresa de factoraje, se ha identificado sus partes interesadas según lo escrito en el numeral 5.4.2 de la metodología proporcionada, las cuales se presentan en la tabla1:

Código	Nombre parte interesada.	Descripción parte interesada.	Procesos asociados	Tipo de impacto
				Financiero/Reputacional /No relevante.
001	Desembolso	Personas que se encargan de la atención personalizada al cliente, gestionar nuevas operaciones de manera ágil	Cesiones	Reputacional
002	Empleados	Persona que ejecuta labores con el fin de obtener remuneración	Ambiente idóneo para desempeñar la labor	Reputacional
003	Junta Directiva	Accionistas y directores	Se encargan de la toma de decisiones críticas de inversiones	Financiero
004	Comité de Riesgos	Personas a cargo de evaluar situaciones que pueden afectar a la empresa ya sea negativa o positivamente, elaboración de normativas que previenen el riesgo	Evaluación de casos, evaluación de inversiones para someterlo a junta directiva	Financiero
005	Comité de Crédito	Personas que evalúan nuevos clientes o cambios en línea de crédito asignada, elaboración de políticas que ayudan a la colocación de buenos clientes	Nuevas contrataciones y cambio de línea de crédito.	Financiero / Reputacional
006	Comité de Cobranza	Personas que toman decisiones con respecto a incidencias y elaboran políticas para la prevención de nuevas incidencias	Cobranza	Financiero

Tabla 1. Identificación de partes Interesadas

- **Establecer lineamientos organizacionales.**

De acuerdo a la orientación propuesta en la metodología, la empresa de factoraje posee una estructura organizacional centralizada, la cual se muestra a continuación en la figura 1:

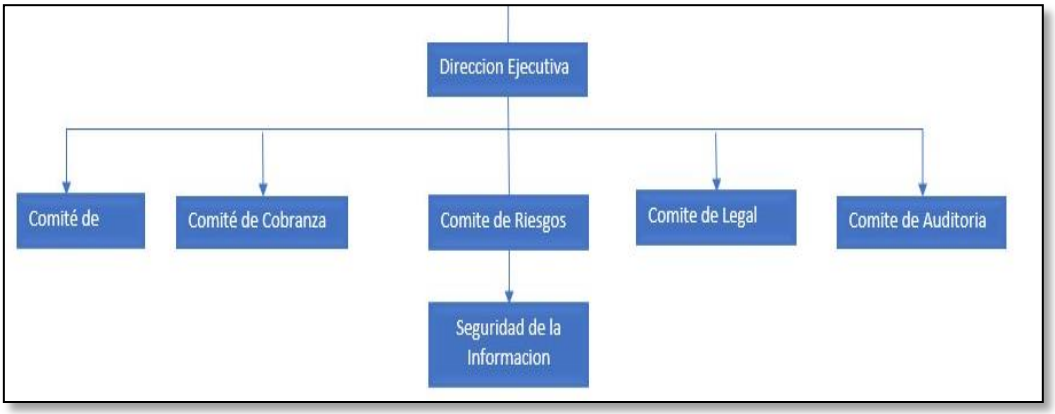

Figura 1. Lineamientos organizacionales

- **Establecer cadena de valor.**

En la verificación de la aplicación de la cadena de valor en la empresa de factoraje se pudo evidenciar que si se tiene definido cada uno de sus procesos los cuales le conllevan a la competitividad en el mercado y maximizar las oportunidades de innovación y gestionar el riesgo; sin embargo, no se contaba con un diagrama por lo cual en conjunto con la empresa se estableció el siguiente diagrama, como cadena de valor (Figura2).

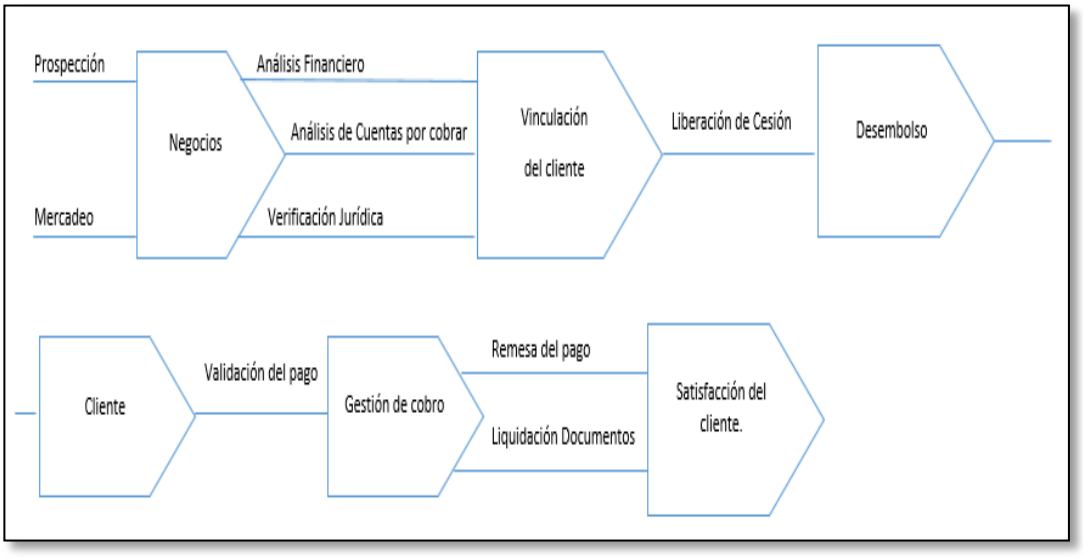

Figura 2. Cadena de Valor

- **Evaluar políticas de seguridad.**

La empresa de factoraje cuenta con una política de gestión de riesgo que aún no ha sido aprobada por junta directiva, sin embargo, es necesario su aprobación; por ello actualmente se ha procedido por parte de la dirección a revisar dicha política.

- **Identificación de activos.**

Después de identificar los riesgos se procede a la identificación de los activos, en la presente tabla la empresa de factoraje identifico los diferentes tipos de activos con los que cuentan; a continuación, se muestras un listado según tabla 1.

#	Activos	Descripción
1	Activos Físicos	**Servidores**
2	Activos Físicos	**UPS**
3	Activos de software	**Sistema de factoraje**
4	Activos de software	**Sistema Contable**
5	Activos de software	**Sistema de respaldo**
6	Activos de software	**Sistema de capital de trabajo**
7	Activos de software	**Sistema de Acceso a Mi Cuenta**
8	Imágenes y reputación de la empresa	**Página WEB**
10	Activos Físicos	**Firewall**
11	Activos Físicos	**Switch**
12	Activos Físicos	**Router**
13	Servicios	**Cámaras de Seguridad**
14	Documentos impresos	**Documentos negociables**
15	Activos Físicos	**Computadoras personales**
16	Activos Físicos	**Computadoras portátiles**
17	Activos de software	**Sistema de gestión documental y workflow**
18	Personas	**Personal**
19	Activo de software	**Antivirus**

Tabla 1. Identificación de activos

Con la identificación de los activos, se realiza una matriz en la cual se presentan las respectivas amenazas, así como las vulnerabilidades, a continuación, se detalla el valor que se le ha dado a cada activo con base a criterios de seguridad.

Criterios de seguridad que se utilizaron:

CONFIDENCIALIDAD	VALOR
Información que puede ser conocida y utilizada por todos los agentes de la organización	1
Información que solo puede ser conocida y utilizada por un grupo de agentes que la necesitan para realizar su trabajo	2
Información que solo puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio a la organización o terceros.	3

INTEGRIDAD	VALOR
Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta las actividades de la organización	1
Información cuya modificación no autorizada puede repararse aunque podría ocasionar un perjuicio a la organización o terceros	2
Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para la organización o terceros	3
Información cuya modificación no autorizada no podría repararse, impidiendo la realización de actividades	4

DISPONIBILIDAD	VALOR
Información cuya inaccesibilidad no afecta la actividad normal de la organización	1
Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para la organización	2
Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la organización	3
Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la organización.	4

Valor de los activos

SIGNIFICADO	VALOR
MUY ALTA	8 a 9
ALTA	6 a 7
MEDIO	4 a 5
BAJA	2 a 3
MUY BAJA	0 a 1

Probabilidad

FRECUENCIA	DEFINICION	VALOR
MUY BAJA	Baja probabilidad de ocurrencia, puede ocurrir solo en ocasiones excepcionales	**1**
BAJA	Limitada probabilidad de ocurrencia, podría ocurrir en pocas circunstancias	**2**
MEDIA	Mediana probabilidad de ocurrencia, puede ocurrir en algún momento	**3**
ALTA	Significativa probabilidad de ocurrencia, probablemente ocurrirá en la mayoría de las circunstancias	**4**
MUY ALTA	Alta probabilidad de ocurrencia, se espera que ocurra en la mayoría de las circunstancias.	**5**

Estimación del Impacto

CRITERIO	SIGNIFICADO	VALOR
MB	**MUY BAJA**	**1**
	BAJA	**2**
M	**MEDIA**	**3**
A	**ALTA**	**4**
MA	**MUY ALTA**	**5**

Se utilizaron tablas de criterios de estimación de impacto y la probabilidad, para darle un valor a las vulnerabilidades y amenazas que están asociadas al activo, esto con el fin de medir el riesgo para que posterior se pueda tener un resultado de los riesgos que se deben de tratar, lo cual en la tabla 5, se muestra el resultado obtenido.

- **Identificación del riesgo.**

Para la identificación de riesgo, en conjunto con el comité de riesgo de la empresa de factoraje, vieron a bien utilizar la técnica lluvia de ideas, de los cuales se listaron los siguientes riesgos según tabla 2

N	Riesgos y aspectos
	Riesgos Externos
1	Suspensión de servicio eléctrico
2	Vandalismo
3	Hackers
4	Desastres naturales
5	Falla servicio de internet
	Riesgos Internos
1	No se cuenta con contingencia de equipo de aire acondicionado.
2	Falla de servidores o perdida de los mismos
3	Falta de respaldo en el servicio eléctrico
4	Deficiencia en pruebas de restauración de backup
5	Sabotaje

Tabla 2. Identificación de Riesgos.

- **Valoración de riesgo.**

Luego de haber identificado los riesgos en la tabla anterior, se realizó la evaluación de cada riesgo y se realizó la valoración según los siguientes valores.

Probabilidad	**Muy probable**	**3**
	Posible	**2**
	Improbable	**1**

Impacto	**Desastroso**	**3**
	Moderado	**2**
	Leve	**1**

De lo cual se obtuvo el siguiente resultado, según tabla 3.

N	Riesgos y aspectos	Factores de Riesgo		
		Impacto	Probabilidad	Resultado
Riesgos Externos				
1	Suspensión de servicio eléctrico	2	3	Muy probable
2	Vandalismo	3	2	Muy probable
3	Hackers	3	3	Muy probable
4	Desastres naturales	2	2	Posible
5	Falla servicio de internet	1	2	Posible
Riesgos Internos				
1	No se cuenta con contingencia de equipo de aire acondicionado.	3	3	Muy probable
2	Falla de servidores o perdida de los mismos	3	2	Muy probable
3	Falta de respaldo en el servicio eléctrico.	3	1	Muy probable
4	Deficiencia en pruebas de restauración de backup	2	2	Posible
5	Sabotaje	1	2	Posible

Tabla 3. Resultado de la identificación de riesgos

Continuación en la siguiente matriz (tabla 4), se muestra todo el análisis realizado para la obtención del valor del riesgo.

Activos	Descripción	C	I	D	Valor del activo	Vulnerabilidad	Amenaza	Probabilidad	Estim. Impacto	Valor del Riesgo
Servidores	Contenedor de software	3	3	3	3	Falta de actualización del SO	Errores en las aplicaciones	**3.00**	**3.00**	**9.00**
UPS	Respaldo de energía eléctrica	3	3	3	4	Sobrecargar eléctrica	Daño en los equipos, perdida de información.	**3.00**	**2.00**	**6.00**
Sistema de factoraje	Procesar operación de factoraje	3	3	3	7	Configuración inadecuada del sistema.	Alteración en los datos de los clientes.	**2.00**	**5.00**	**10.00**
Sistema Contable	Procesar información que proviene de los diferentes sistemas	3	3	3	2	Configuración inadecuada del sistema.	Falsa información a los usuarios finales	**3.00**	**2.00**	**6.00**
Sistemas operativos	Sistema operativo instalado en los equipos para las operaciones diarias	2	3	2	3	Falta de actualización del software	Errores en las aplicaciones	**3.00**	**2.00**	**6.00**
Sistema de capital de trabajo	Procesar operaciones de créditos	3	3	2	1	Configuración inadecuada del sistema.	Falsa información a los usuarios finales	**2.00**	**2.00**	**4.00**
Sistema de Acceso a Mi Cuenta	Presentación de estados de cuenta	3	3	3	1	Configuración inadecuada del sistema.	Falsa información a los usuarios finales	**1.00**	**2.00**	**2.00**
Firewall	Filtro de navegación y otorgamiento de permisos de ingreso	3	3	3	4	Falta de seguridad física	Ataque físico, virus, robo de información	**3.00**	**3.00**	**9.00**
Switch	Control de equipos en la red	2	3	2	5	Falla de comunicación	Retraso en las operaciones afectadas	**3.00**	**3.00**	**9.00**
Router	Direccionamiento de información y control	2	3	2	4	Falla de comunicación	Retraso en las operaciones afectadas	**3.00**	**3.00**	**9.00**
Computadoras	Procesamiento de texto y operaciones en los diferentes	2	3	2	2	falta de recursos en los equipos	Falla en la ejecución en las aplicaciones y vulnerables a ataques	**3.00**	**2.00**	**6.00**

	sistemas informáticos									
Documentos negociables (Quedan, facturas, etc.)	Documentos que se financiaron.	3	3	2	4	Documentos falsos a ser financiados	Fraude con mutuo acuerdo con la empresa pagadora	**9.00**	**3.00**	**6.00**
Persona	Empleados internos calificados para el puesto	2	3	4	6	Empleados inconformes con su cargo	Compartir información con la competencia	**7.00**	**4.00**	**4.00**
Sistema de garantías entre factorajes.	Software de verificación de documentos por financiar	3	3	2	5	Configuración inadecuada del sistema.	Falsa información entre empresas de factoraje.	**9.00**	**1.00**	**2.00**
Sistema de gestión documental y workflow	Software de digitalización de documentos del cliente y medición de tiempos de elaboración de cesion.	2	3	4	4	Configuración inadecuada del sistema.	Extracción de datos.	**7.00**	**4.00**	**9.00**
Antivirus	Programa para detectar y eliminar virus.	2	3	4	5			**7.00**	**4.00**	**9.00**
Office 2016	Paquete de programa de	2	3	2	4	Falta de actualización del software	Errores en la carga de componentes	**7.00**	**2.00**	**9.00**
Documentos operativos del manejo del negocio	Programa gestor donde se almacena la información.	2	3	2	4			**5.00**	**3.00**	**6.00**
Base de Datos de Información		2	3	3	4			**7.00**	**6.00**	**6.00**

Tabla 4. Resultado del análisis del criterio de probabilidad e impacto

Para la medición del riesgo se utilizó la siguiente tabla con criterios.

Aquí se evalúan los riesgos críticos, bajo los parámetros de impacto y probabilidad para determinar el riesgo inherente de estos. Por otro lado, se identifican las actividades de control que mitigan los riesgos críticos, con el objeto de determinar el nivel de riesgo residual para cada uno de los eventos de riesgo, según tabla 5.

GRADO DE RIESGO		
NIVEL	**CALIFICACION**	**EVALUACION**
Insignificante	5	Nula probabilidad de impacto
Bajo	10	Poca probabilidad con poco impacto
Moderado	15	Mediana probabilidad con medio impacto
Alto	20	Mediana probabilidad con alto impacto
Critico	25	Alta probabilidad con alto impacto

Tabla 5. Criterios de Impacto

		IMPACTO				
		Insignificante (1)	***Bajo (2)***	***Moderado (3)***	***Alto (4)***	***Critico (5)***
PROBABILIDAD	***Critico (5)***	***5***	***10***	***15***	***20***	***25***
	Alto (4)	***4***	***8***	***12***	***16***	***20***
	Moderado(3)	***3***	***6***	***9***	***12***	***15***
	Bajo (2)	***2***	***4***	***6***	***8***	***10***
	Insignificante (1)	***1***	***2***	***3***	***4***	***5***

Con el resultado del valor del impacto por la probabilidad se obtiene el valor del riesgo para cada activo, por lo que a continuación en la tabla 6, se muestran los resultados y la acción a realizar, (esto según resultado en mapa de calor)

No	Área	Probabilidad	Estim. Impacto	Valor del Riesgo	Condición
1	Servidores	3,00	4,00	12,00	Reformular controles
2	UPS	3,00	4,00	12,00	Reformular controles
3	Sistema de factoraje	2,00	5,00	10,00	Requiere monitoreo
4	Sistema Contable	3,00	3,00	9,00	Requiere monitoreo
5	Sistemas operativos	3,00	3,00	9,00	Requiere monitoreo
6	Sistema de capital de trabajo	2,00	2,00	4,00	Riesgo Controlado
7	Sistema de Acceso a Mi Cuenta	3,00	3,00	9,00	Requiere monitoreo
8	Firewall	2,00	4,00	8,00	Requiere monitoreo
9	Switch	3,00	4,00	12,00	Reformular controles
10	Router	3,00	4,00	12,00	Reformular controles
11	Computadoras	3,00	4,00	12,00	Reformular controles
12	Documentos negociables (Quedan, facturas, etc.)	3,00	5,00	15,00	Reformular controles
14	Sistema de garantías entre factorajes.	1,00	4,00	4,00	Riesgo Controlado
15	Sistema de gestión documental y workflow	4,00	3,00	12,00	Reformular controles
16	Antivirus	4,00	4,00	16,00	Reformular controles
17	Office 2016	2,00	2,00	4,00	Riesgo Controlado
18	Documentos operativos del manejo del negocio	3,00	3,00	9,00	Requiere monitoreo
19	Base de Datos de Información	4,00	4,00	16,00	Reformular controles
	Promedio	**2,83**	**3,61**	**10,28**	**Reformular controles**

Tabla 6. Resultado del Valor del riesgo

Según el cálculo de porcentaje manejado en el mapa de calor (figura 3), se obtienen la lista de los activos que se le deben de tratar con mayor prioridad, considerando que, según el criterio de grado de riesgo, el promedio establecido el resultado es **"Mediana Probabilidad con Medio Impacto"**

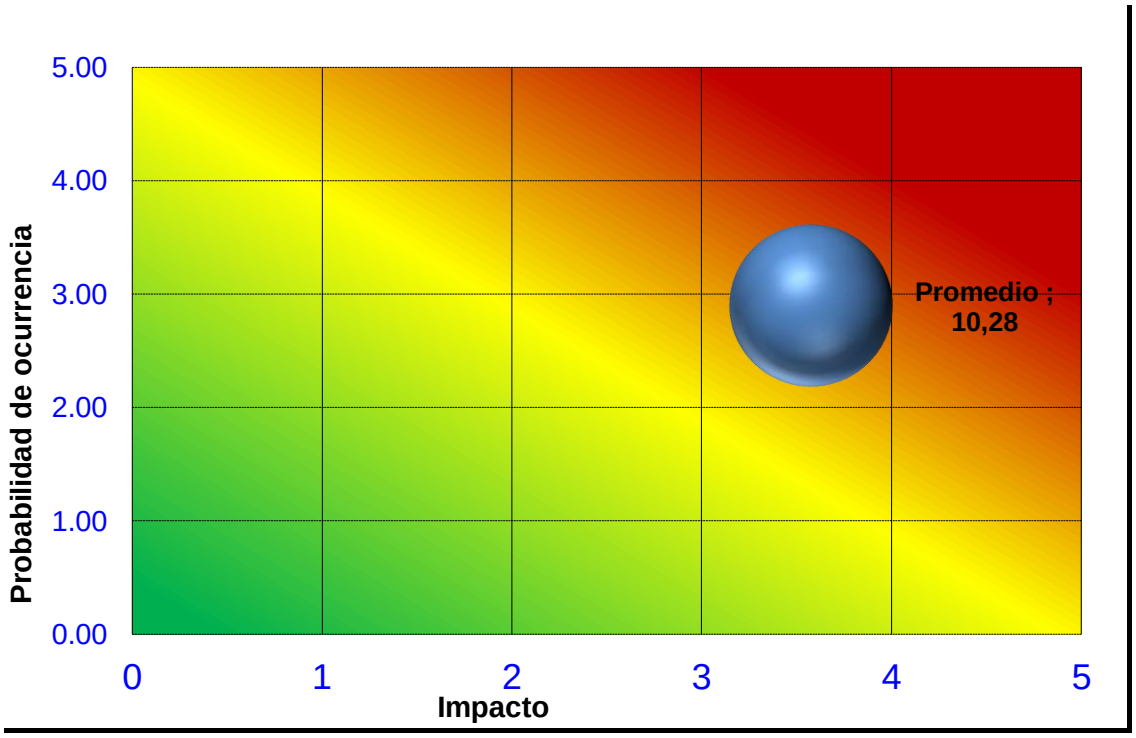

Figura 3. Mapa de calor

Priorización de Riesgos

Dado que el resultado de la medición de Riesgo fue "**Mediana Probabilidad con Medio Impacto",** para los activos que están dentro de este rango se debe establecer un plan de mitigación riesgo, tomando como prioritarios a aquellos activos con valor de riesgo **moderado** y con condición "**Reformular controles**", mostrados en la tabla 7, para la mitigación de los mismos.

La empresa Factoraje, para mitigar los riesgos de los activos que se consideraron como vulnerables, se establece el siguiente Plan de mitigación de Riesgos, según figura 7.

N	Objetivos	Activo	Riesgo	Valor del riesgo	Actividad a realizar	Responsable	Fecha de Inicio Ejecución	Fecha de Fin de Ejecución
	Reducir, evitar el riesgo	Servidores	Errores en las aplicaciones	Moderado	Establecer políticas de actualización	TI	**03-09-2018**	**15-09-2018**
	Reducir, evitar el riesgo	UPS	Daño en los equipos.	Moderado	Colocar un regulador de voltaje antes del UPS	TI	**08-09-2018**	**28-09-2018**
	Reducir, evitar el riesgo	Switch	Perdida de comunicación	Moderado	Establecer procedimientos de configuración	TI	**03-09-2018**	**15-09-2018**
	Reducir, evitar el riesgo	Router	Perdida de comunicación	Moderado	Contratar a un segundo proveedor de servicio	TI	**14-09-2018**	**25-09-2018**
	Reducir, evitar el riesgo	Computadoras	No contar con información para la toma decisiones.	Moderado	Adquisición de programas	TI	**25-09-2018**	**22-10-2018**
	Reducir, evitar el riesgo	Documentos negociables (Quedan, facturas, etc.)	Fraude con mutuo acuerdo con la empresa pagadora	Moderado	Implementación de firmas de autorización de pagos.	Finanzas	**14-09-2018**	**25-09-2018**
	Reducir, evitar el riesgo	Sistema de gestión documental y workflow	Errores en las aplicaciones.	Moderado	Establecimiento de procedimientos	TI	**13-09-2018**	**28-09-2018**
	Reducir, evitar el riesgo	Antivirus	Daños, en los equipos, pérdida de datos.	Moderado	Procedimiento de control de actualización de antivirus	TI	**03-09-2018**	**15-09-2018**
	Reducir, evitar el riesgo	Base de Datos de Información.	Robo de información	Moderado	Establecer y mejorar las políticas de acceso a las bases de Datos	TI	**20-09-2018**	**12-10-2018**

Figura 7. Plan de mitigación de Riesgo

MEJORA CONTINUA

Seguimiento y control

En esta etapa final es necesario informar al personal de las áreas implicadas sobre los activos evaluados con sus respectivas amenazas y salvaguardas factibles.

En el presente análisis de riesgos se han considerado los activos que forman parte de los principales servicios que brinda la empresa de factoraje a sus clientes, entre los cuales están: acceso a diferentes sistemas utilizados para el departamento financiero y operativo, proveer el acceso a la intranet e internet de forma alámbrica e inalámbrica y almacenar de forma segura la información que se genera diariamente, entre otras.
Después de haber identificado y analizado nuestros activos incluyendo la valorización del riesgo, se le recomienda a la empresa Factoraje llevar su respectivo seguimiento de los resultados, verificando que cada actividad o acción planteada en el Plan de mitigación de riesgo se cumpla, para que el objetivo sea siempre velar por la seguridad de la Información.

De acuerdo a lo anterior y de manera complementaria con el desarrollo de la metodología realizada, de la manera más atenta solicitamos dar a conocer el contenido del presente informe a los involucrados en Gestionar el Riesgo, a fin de darle seguimiento a los resultados encontrados.

Implementación de metas y métricas

La implementación de las métricas se ha realizado con base a la identificación de los activos y la probabilidad de que un riesgo se desarrolle, a continuación, en la tabla 8 se describen.

Métrica	Indicadores	Activos de medición
Número de virus o códigos malignos detectados.	99% de Eficacia en la identificación de virus	Antivirus
Actualización de antivirus	Validación de actualizaciones semanales en el 100% de equipos del personal.	Antivirus
Cumplimiento de las reglas de seguridad	Nivel de cumplimiento de los objetivos del manual de políticas de seguridad.	Manual de política de seguridad
Actualización de todo los SO con los últimos parches	Actualización de los sistemas operativos Windows en las computadoras de los empleados	Sistema Operativo
Implementación de política de contraseñas en los equipos	Todos los equipos tienen que poseer contraseña personalizada por los usuarios.	Equipos de computo
Realización de respaldos en las bases de datos y comprobación de las copias de seguridad	Realización diaria de respaldos y verificación semanalmente de restauración de los backup realizados, 100% de verificaciones sin error	Base de datos
Disminución de contraseñas débiles tras las campañas de concienciación	Parametrización a través de active directory por GPO para establecer un estándar en la creación de contraseñas.	Active Directory
Porcentaje de empleados nuevos y antiguos que recibieron curso de inducción a la política de seguridad.	100% de empleados que pasaron el curso.	Empleados
Porcentaje de acceso a páginas no permitidas Vs Acceso a páginas permitidas Vs Intentos de acceso a páginas restringidas	% de acceso a páginas no permitidas + % acceso a páginas restringidas < 25, gestionado a través del firewall	Firewall

Tabla 8. Desarrollo de Métricas

7.0 CONCLUSIONES

Los resultados obtenidos durante la aplicación de la metodología en la empresa de Factoraje permitieron a la organización, reconocer la necesidad de implementar un plan de gestión de riesgos que permita mitigar los riesgos más críticos, hasta que decidan desarrollar un Plan de Tratamiento de Riesgo en el que se considere la contratación de personal especializado en seguridad, análisis de documentos y registros de incidentes, resultados de entrevistas al personal.

En el presente trabajo fueron descritos los conceptos e importancia de los términos relacionados con la gestión del riesgo presente en la seguridad de la información que es administrada mediante los diversos equipos, servicios y personal del área de TI; además de conocer los estándares, metodologías y herramientas que posibilitan el desarrollo del análisis de riesgo en una organización y lo importante que realizar este análisis para estar preparados ante un evento, y así velar siempre por la confidencialidad, disponibilidad e integridad de la información.

8.0 Recomendaciones

- Desarrollar un análisis de riesgos de tipo cuantitativo considerando varios aspectos, como son: las consecuencias económicas de la materialización de una amenaza en cada activo, el costo del despliegue y mantenimiento de las salvaguardas; y estimar la probabilidad de ocurrencia de amenazas basándose en registros reales.

- Considerar los períodos de tiempo de recuperación de los procesos antes que las pérdidas se conviertan en irreparables y un análisis de aplicaciones críticas para definir prioridades de procesos.

- Continuar con el seguimiento y mejora de los resultados del análisis de riesgo realizado, esto con el fin de seguir mitigando los riesgos a través del cumplimento de los controles o acciones establecidas en el plan de mitigación de riesgo.

- Sensibilización y conocimiento de la gestión de riesgos en los empleados de Factoraje.

9.0 TERMINOS

- **Amenaza**: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.
- **Vulnerabilidad:** debilidad que presentan los activos y que facilita la materialización de las amenazas.
- **Impacto o consecuencia** de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad. El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo.
- **Probabilidad**: es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza.
- **Riesgo:** Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra
- **Activo:** Un activo es un bien que la empresa posee y que puede convertirse en dinero u otros medios líquidos equivalentes.
- **Confidencialidad:** se conoce como una forma de **prevenir la divulgación de la información** a personas o sistemas que no se encuentran autorizados
- **Disponibilidad:** Es un pilar fundamental de la **seguridad de la información**, nada hacemos teniendo segura e integra nuestra información, si no va a estar disponible **cuando el usuario o sistema necesite realizar una consulta**
- **Integridad:** Cuando hablamos de integridad en seguridad de la información nos referimos a cómo los datos se mantienen intactos libre de **modificaciones o alteraciones por terceros**, cuando una violación modifica algo en la base de datos, sea por accidente o intencionado se pierde la integridad y falla el proceso
- **Apetito al Riesgo:** es el nivel de **riesgo** que la empresa quiere aceptar y su tolerancia es la desviación respecto a este nivel. La capacidad es el máximo de **riesgo** que una organización puede soportar en la persecución de sus objetivos

-

10.0 REFERENCIA BIBLIOGRAFICA

- ✓ https://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf
- ✓ http://bibliotecadigital.usb.edu.co/bitstream/10819/2543/1/Identificar_Herramientas_Implementadas_Gerencia_Riesgo_Guañarita_2015.pdf
- ✓ http://www.oas.org/juridico/pdfs/mesicic5_cl_insitu_dnsc_ane8.pdf
- ✓ http://www.mbgproyectos.com/iso-31000-iso-31010-e-iso-22301/
- ✓ https://repositorio.escuelaing.edu.co/bitstream/001/226/1/EC-Especialización%20en%20Gestion%20Integrada%20QHSE-1072493699.pdf
- ✓ http://dspace.utpl.edu.ec/bitstream/123456789/11218/1/Pena%20Zhindon_Monica_del_Rocio.pdf
- ✓ https://prezi.com/ohiyv_5feeg9/iso-31010-tecnicas-de-evaluacion-de-riesgos/
- ✓ https://idus.us.es/xmlui/bitstream/handle/11441/26883/Q_Tesis_MUEP.pdf?sequence=1
- ✓ http://www.cicctic.unam.mx/cic/mas_cic/servicios/cgcp/download/Seminario_ISO_9001_2015/Presentacion%20Ing%20Jonathan%20Melendez%20Gonzalez.pdf
- ✓ http://bibliotecadigital.usb.edu.co/bitstream/10819/3063/1/Tecnicas_evaluacion_riesgo_santofimio_2015.pdf
- ✓ ISO (International Standard Organization). ISO-IEC 27005 Tecnologías de la Información – Técnicas de seguridad – Gestión del riesgo en la seguridad de la información.
- ✓ ISO (International Standard Organization). (2009). Norma Internacional ISO 31010, Gestión de Riesgos - Técnicas de valoración del riesgo.
- ✓ ISO (International Standard Organization). (2009). ISO 31000 Gestión del riesgo – Principios y Directrices

11.0 ANEXOS

ANEXO 1.

Tabla para el levantamiento de partes interesadas / partes interesadas pertinentes.

Código	Nombre parte interesada.	Descripción parte interesada.	Procesos asociados	Tipo de impacto Financiero/Reputacional/No relevante.
001	Clientes	Se interactúa bastante con el cliente, es un buen punto de interacción para saber cuáles son las necesidades, conocer sus expectativas.	Contratos, especificaciones técnicas, los productos que solicitan.	Reputacional
002	Empleados	Los requerimientos de sindicatos u otras organizaciones que aglutinen los intereses de los empleados.	Los requerimientos en cuanto a estructura o instalaciones que los empleados consideren indispensables para asegurar la calidad de los productos.	Reputacional
003	Accionistas	Son todas aquellas personas que tienen iniciativas para el bien de las acciones de la empresa,	Promueven la disminución de los costes y el aumento de las utilidades	Financiero

Anexo 2.

Identificación de Riesgos

N	Riesgos y aspectos	Factores de Riesgo	
		Impacto	Probabilidad
	Riesgos Externos		
1			
2			
3			
4			
5			
	Riesgos Internos		
1			
2			
3			
4			
5			

Anexo 3

Cuadro para la valoración del riesgo.

N	Probabilidad	Impacto	Resultado
Riesgo1			
Riesgo2			
Riesgo3			

Probabilidad	**Muy probable**	**3**
	Posible	**2**
	Improbable	**1**

Impacto	**Desastroso**	**3**
	Moderado	**2**
	Leve	**1**

Anexo 4

Tabla de Identificación de los activos de la organización

#	Activos	Descripción

Anexo 5.

Valoración de los activos – Escala estándar

Activos	Descripción	C	I	D	Valor del activo	Vulnerabilidad	Amenaza	Probabilidad	Estim. Impacto	Valor del Riesgo
Activo 1	Descripción 1	3	3	3	3	Vulnerabilidad 1	Amenaza 1	**3.00**	**3.00**	**9.00**
Activo 2	Descripción 2	3	3	3	4	Vulnerabilidad 2	Amenaza 2	**3.00**	**2.00**	**6.00**
Activo 3	Descripción 3	3	3	3	7	Vulnerabilidad 3	Amenaza 3	**2.00**	**5.00**	**10.00**
Activo 4	Descripción 4	3	3	3	2	Vulnerabilidad 4	Amenaza 4	**3.00**	**2.00**	**6.00**
Activo 5	Descripción 5	2	3	2	3	Vulnerabilidad 5	Amenaza 5	**3.00**	**2.00**	**6.00**
							total	2.64	2.64	6.95

Nivel de Clasificación

Nivel	Descripción
1	Bajo
2	Moderado
3	Alto

Anexo 6

Plan de mitigación de Riesgo

N	Objetivos	Activo	Riesgo	Valor del riesgo	Actividad a realizar	Responsable	Fecha de Inicio Ejecución	Fecha de Fin de Ejecución
	Objetivo1							
	Objetivo 2							
	Objetivo 3							
	Objetivo 4							
	Objetivo 5							