UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONÓMICAS

"EVALUACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS, EN UNA EMPRESA DE SERVICIOS ESPECIALIZADA EN EL PROCESAMIENTO DE DOCUMENTOS EN FORMA ELECTRÓNICA, UTILIZANDO LA NORMATIVA ISO 31000:2009"

TESIS

PRESENTADA A LA JUNTA DIRECTIVA DE LA

FACULTAD DE CIENCIAS ECONÓMICAS

Por

SENDER ALFREDO VELÁSQUEZ HERNÁNDEZ

PREVIO A CONFERÍRSELE EL TÍTULO DE

CONTADOR PÚBLICO Y AUDITOR

EN EL GRADO ACADÉMICO DE

LICENCIADO

Guatemala, febrero de 2017

MIEMBROS DE LA JUNTA DIRECTIVA
FACULTAD DE CIENCIAS ECONÓMICAS

Decano	Lic. Luis Antonio Suárez Roldán
Secretario	Lic. Carlos Roberto Cabrera Morales
Vocal Primero	Lic. Carlos Alberto Hernández Gálvez
Vocal Segundo	MSc. Byron Giovanni Mejía Victorio
Vocal Tercero	Vacante
Vocal Cuarto	P.C. Marlon Geovani Aquino Abdalla
Vocal Quinto	P.C. Carlos Roberto Turcios Pérez

PROFESIONALES QUE REALIZARON LOS EXÁMENES
DE ÁREAS PRÁCTICAS BÁSICAS

Área matemática-estadística	Lic. Felipe Hernández Sincal
Área contabilidad	Lic. Luis Alfredo Guzmán Maldonado
Área auditoría	Lic. Rubén Eduardo del Águila Rafael

PROFESIONALES QUE REALIZARON
EL EXAMEN PRIVADO DE TESIS

Presidente	Lic. Carlos Vicente Solórzano Soto
Secretario	Lic. Hugo Francisco Herrera Sánchez
Examinador	Lic. Othir Misael Cardona Sales

Guatemala 31 de agosto de 2016

Licenciado Luis Antonio Suárez Roldán
Decano, Facultad de ciencias Económicas
Universidad de San Carlos de Guatemala
Presente

Lic. Suárez:

Tengo el agrado de dirigirme a usted con relación a la designación contenida en Dictamen AUD-181-2016 de fecha 08 de julio de 2016 emitida por la Decanatura de la Facultad de ciencias Económicas, fui designado como asesor de tesis del alumno Sender Alfredo Velásquez Hernández, quien efectuó la investigación del punto de tesis titulado **"EVALUACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS, EN UNA EMPRESA DE SERVICIOS ESPECIALIZADA EN EL PROCESAMIENTO DE DOCUMENTOS EN FORMA ELECTRÓNICA, UTILIZANDO LA NORMATIVA ISO 31000:2009"**, el cual deberá presentar para poder someterse al examen privado de graduación profesional, previo a optar el título de Contador Público y Auditor en el grado académico de Licenciado.

El trabajo realizado por el alumno Sender Alfredo Velásquez Hernández reúne los requisitos profesionales exigidos por la Universidad de San Carlos de Guatemala y estimo que es un buen aporte tanto para los estudiantes como para los catedráticos interesados en conocer el tema en mención.

Atentamente,

Lic. Erik Roberto Flores López
Contador Público y Auditor
Colegiado No. 303

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONOMICAS
EDIFICIO "S-8"
Ciudad Universitaria zona 12
GUATEMALA, CENTROAMERICA

DECANATO DE LA FACULTAD DE CIENCIAS ECONÓMICAS, GUATEMALA, DIECIOCHO DE NOVIEMBRE DE DOS MIL DIECISÉIS.

Con base en el Punto CUARTO, inciso 4.5, subinciso 4.5.1 del Acta 23-2016 de la sesión celebrada por la Junta Directiva de la Facultad el 8 de noviembre de 2016, se conoció el Acta AUDITORÍA 217-2016 de aprobación del Examen Privado de Tesis, de fecha 29 de septiembre de 2016 y el trabajo de Tesis denominado: "EVALUACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS, EN UNA EMPRESA DE SERVICIOS ESPECIALIZADA EN EL PROCESAMIENTO DE DOCUMENTOS EN FORMA ELECTRÓNICA, UTILIZANDO LA NORMATIVA ISO 31000:2009", que para su graduación profesional presentó el estudiante **SENDER ALFREDO VELÁSQUEZ HERNÁNDEZ,** autorizándose su impresión.

Atentamente,

"ID Y ENSEÑAD A TODOS"

CARLOS ROBERTO CABRERA MORALES
SECRETARIO

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONOMICAS
SECRETARIO

LIC. LUIS ANTONIO SUÁREZ ROLDÁN
DECANO

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONOMICAS
DECANO

m.ch

ACTO QUE DEDICO

A DIOS: Agradezco a Dios por haberme dado la vida, paciencia, perseverancia y la sabiduría para poder enfrentar este reto y sobre todo no dejarme desfallecer ante situaciones adversas.

A MIS PADRES: Luisa Hernández y Alfredo Velásquez, les agradezco mucho su cariño, consejos y apoyo incondicional.

A MIS HERMANOS: Odalis y Lenin, gracias por apoyarme.

A MIS SOBRINOS: Dianellyn y Hugo, espero que esto les sirva de motivación.

A MI NOVIA: Wendy, gracias por tu cariño y apoyo en todo y en especial en los momentos complicados de este proceso.

A MIS COMPAÑEROS: Especial dedicatoria a todos los compañeros de estudios que durante la carrera me apoyaron a seguir adelante, sin ustedes, esto no sería posible.

A LA UNIVERSIDAD: Gloriosa y tricentenaria Universidad de San Carlos de Guatemala, gracias por abrirme las puertas para realizar y culminar mis estudios universitarios.

AL LECTOR: Que este trabajo sea de utilidad para su desarrollo como profesional.

A todas aquellas personas que de una u otra forma me apoyaron poniendo su granito de arena para alcanzar esta meta, gracias.

ÍNDICE

Página

CAPÍTULO II
AUDITORÍA INTERNA Y CONTROL INTERNO

CAPÍTULO III
ISO 31000:2009 Y GESTIÓN DE RIESGOS

CAPÍTULO IV

EVALUACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS, EN UNA EMPRESA DE SERVICIOS ESPECIALIZADA EN EL PROCESAMIENTO DE DOCUMENTOS EN FORMA ELECTRÓNICA, UTILIZANDO LA NORMATIVA ISO 31000:2009

(CASO PRÁCTICO)

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La investigación de este tema es importante para el auditor y para los estudiantes de las ciencias económicas debido a que en la actualidad, el tema de la gestión del riesgo en las empresas guatemaltecas aún no es considerado dentro de los planes de continuidad del negocio, derivado que requiere inversión, esto ayudaría a identificar y evaluar el impacto que tendría la materialización de un riesgo, así como establecer controles que ayuden a minimizar la probabilidad que se materialice el evento, que en determinado momento, puede poner en riesgo la operación de la entidad.

Para el auditor interno es importante conocer los distintos modelos de control interno, dentro de los cuales se puede tomar en cuenta la norma ISO 31000:2009, herramienta que brinda un proceso para evaluar los riesgos y por ende, es de utilidad para que al elaborar el plan de auditoría, éste sea basado en riesgos, al realizarlo de esta forma, brindará una visión generalizada de la forma en que la empresa está tratando los riesgos y poder evaluar la efectividad de los controles aplicados.

El estudiante de las ciencias económicas, en su preparación para ser futuro profesional, debe conocer las distintas formas de control interno y evaluación de riesgos, ya que con el paso del tiempo, en las empresas, el tema de la gestión del riesgo será fundamental para la continuidad del negocio; por esta razón, el futuro profesional al conocer el tema, podrá ofrecer sus servicios de consultoría y aseguramiento de tal forma que sea reconocido por su trabajo y experiencia en el ramo.

Es por ello que la presente investigación tiene como objetivo principal proporcionar la evaluación del proceso de gestión de riesgos utilizando la normativa ISO 31000:2009, que permita externar una opinión sobre la efectividad del proceso de gestión de riesgos implementada en la empresa, por medio de la detección de oportunidades de mejora que, al ser atendidas, pueden reforzar la gestión de

riesgos, aportando de esta forma valor y ayudar al logro de los objetivos así como fortalecer el control interno de la empresa.

Derivado de lo anterior, el desarrollo de la presente investigación se encuentra dividido en cuatro capítulos, los cuales se detallan a continuación:

El Capítulo I, comprende los aspectos más relevantes de la empresa en Guatemala, los elementos que la constituyen, así como los aspectos que regulan la unidad de análisis.

En el Capítulo II se incluyen los aspectos de importancia relacionados con la auditoría interna, en los cuales se describen definiciones, objetivos, estructura organizacional, procedimientos, pruebas, planificación, programa y comunicación de resultados de la auditoría interna.

En el capítulo III se presentan los aspectos relacionados con la gestión del riesgo, su definición, el origen etimológico así como los tipos de riesgo, de igual forma se incluye el estándar ISO 31000:2009, aspectos generales, beneficios, alcance, principios, marco de trabajo, así como el proceso de gestión de riesgos incluyendo la definición de cada uno de sus componentes del proceso.

En el Capítulo IV, se presenta un caso práctico de una auditoría al proceso de gestión de riesgos, con un enfoque de aseguramiento de acuerdo a cada uno de los componentes del proceso de gestión de riesgos que indica el estándar ISO 31000:2009.

Por último, sobre la base de la investigación realizada, se presentan las conclusiones y recomendaciones a que se llegó, referencias bibliográficas consultadas.

CAPÍTULO I
EMPRESA DE SERVICIOS ESPECIALIZADA EN EL PROCESAMIENTO DE DOCUMENTOS EN FORMA ELECTRÓNICA

1.1 Definición de empresa

"Es la unidad económico-social en la que el capital, el trabajo y la dirección se coordinan para realizar una producción socialmente útil de acuerdo con las exigencias del bien común" (8:6).

"Empresa es el conjunto de trabajo, de elementos materiales y de valores incorpóreos coordinados, para ofrecer al público con propósito de lucro o de manera sistemática, bienes o servicios. Será reputada como un bien mueble" (19:104).

1.1.1 Elementos que constituyen una empresa

Los elementos necesarios para formar una empresa son: capital, trabajo y recursos materiales.

a. **Capital:** "total de recursos físicos y financieros que posee un ente económico, obtenidos mediante aportaciones de los socios o accionistas destinados a producir beneficios, utilidades o ganancias. Riqueza que se destina a la producción" (47).

b. **Trabajo:** "esfuerzo personal para la producción y comercialización de bienes y/o servicios con un fin económico, que origina un pago en dinero o cualquier otra forma de retribución. Es una parte o etapa de una obra de un proyecto para la formación de un bien de capital" (53).

c. **Recursos Materiales:** son todos aquellos bienes que posee la empresa, tanto los enterados como aportes de los propietarios, como los recibidos por adquisiciones a terceros a cualquier título: compra, trueque, dación en pago

o donaciones, siempre que sean susceptibles de ser valorizadas y que exista la documentación necesaria para registrarlas dentro del activo (52).

1.1.2 Factores que inciden en una empresa

Debe entenderse que una empresa no existe aislada, sino que la rodea un ambiente que a veces es hostil y que todas las acciones de éste hacia la empresa repercuten en el funcionamiento de la misma. De esta manera los factores que inciden en una empresa son:

a. **"Factor económico:** sus medios de producción pueden tener diferente enfoque, dependiendo el fin de la misma y el sistema económico en el que se desarrolle.

b. **Factores culturales:** la cultura en las sociedades modernas cambia a un ritmo muy acelerado, tanto en su aspecto material como en los valores e ideas, entendiéndose la cultura como todo complejo que comprende el saber, las creencias, el arte, la moralidad, el derecho, las costumbres y cualesquiera otras capacidades de hábitos adquiridos.

c. **Factores tecnológicos:** hoy en día la tecnología es la fuerza más importante que puede transformar y aumentar la capacidad humana.

d. **Factores políticos:** se refiere a la legislación que rige o afecta a una entidad y su forma de actuar, el empresario debe conocer perfectamente estas leyes, así como debe tomar en cuenta las políticas de otros países, que ejercen presión a la empresa" (8:7).

1.2 Diferencias entre las empresas lucrativas y no lucrativas

1.2.1 Empresas lucrativas

“Son las que persiguen la realización de una ganancia, por ejemplo tenemos a las fábricas, los hoteles, restaurantes, entre otros” (2:8).

1.2.2 Empresas no lucrativas

“Es una entidad cuyo fin no es la consecución de un beneficio económico sino que principalmente persigue una finalidad social y/o altruista y/o humanitaria y/o comunitaria. Este tipo de instituciones por lo general se financian gracias a ayudas y donaciones de personas, empresas, e instituciones y organizaciones de todo tipo, y en algunos casos también se reciben ayudas estatales puntuales o regulares (en forma de subsidios, exoneraciones fiscales, etc.)” (49).

1.3 Tipos y clasificación de las empresas

Existen variadas diferencias entre una empresa y otra. Sin embargo, según en qué aspecto nos fijemos, podemos clasificarlas de varias formas:

a. Sectores económicos
b. Por su tamaño
c. El origen de su capital
d. Constitución legal

1.3.1 Sectores económicos

a. **Extractivas:** dedicadas a explotar recursos naturales, ya sean renovables o no renovables, ejemplos de este tipo de empresas son las pesqueras, madereras, mineras, petroleras, entre otras.

b. **Servicios:** son aquellas que brindan o prestan servicio a la comunidad, puede ser: transporte, turismo, instituciones financieras, servicios públicos

(electricidad, agua potable) servicios privados (asesoría, ventas, publicidad, contable, administrativo), educación, finanzas, salud.

c. **Comercial:** son intermediarias entre productor y consumidor; su función primordial es la compra/venta de productos terminados, esta a su vez pueden clasificarse en:

    - **Mayoristas:** Venden a gran escala o al mayoreo.
    - **Minoristas (detallistas):** Venden al menudeo.
    - **Comisionistas:** Venden de lo que no es suyo, dan en consignación.
    - **Agropecuaria:** dedicadas a las actividades agrícolas, explotan los recursos del campo.

d. **Industrial:** la actividad primordial de este tipo de empresas es la producción de bienes mediante la transformación de la materia o extracción de materias primas, como es el caso de los ingenios.

1.3.2 Por su tamaño

Según el tamaño, se acostumbra a clasificar a las empresas en tres apartados: grandes, medianas y pequeñas. En la práctica existen distintos criterios para delimitar el tamaño de las empresas.

a. **Grande:** “se caracterizan por manejar capitales y financiamientos grandes, por lo general tienen instalaciones propias, sus ventas son de varios millones de dólares, tienen miles de empleados de confianza y sindicalizados, cuentan con un sistema de administración y operación muy avanzado y pueden obtener líneas de crédito y préstamos importantes con instituciones financieras nacionales e internacionales” (24:22).

b. **Mediana:** “en este tipo de empresas intervienen varios cientos de personas y en algunos casos hasta miles, generalmente tienen sindicato, hay áreas

bien definidas con responsabilidades y funciones, tienen sistemas y procedimientos automatizados" (24:23).

c. **Pequeñas:** "en términos generales, las pequeñas empresas son entidades independientes, creadas para ser rentables, que no predominan en la industria a la que pertenecen, cuya venta anual en valores no excede un determinado tope y el número de personas que las conforman no excede un determinado límite" (16:1).

d. **Micro:** "por lo general, la empresa y la propiedad son de propiedad individual, los sistemas de fabricación son prácticamente artesanales, la maquinaria y el equipo son elementales y reducidos, los asuntos relacionados con la administración, producción, ventas y finanzas son elementales y reducidos y el director o propietario puede atenderlos personalmente" (24:23).

1.3.3 Por el origen de su capital

a. **Publica:** es el tipo de empresa en la cual el capital es propiedad del estado, que puede ser nacional, o municipal, por ejemplo: el instituto guatemalteco del seguro social (IGSS).

b. **Privada:** se distinguen porque su capital proviene de inversionistas particulares y no reciben ningún apoyo económico del estado.

c. **Mixta:** es el tipo de empresa en la que la propiedad del capital es compartida entre el estado y los particulares.

1.3.4 Constitución legal

a. **Empresas Individuales:** se forma cuando una empresa mercantil posee solamente como propietario a una persona física.

b. **Empresas de sociedad:** se forma cuando una empresa mercantil tiene como propietario a una sociedad mercantil o persona jurídica, y posee como administrador a un representante legal denominado gerente, gestor, factor, administrador.

c. **Empresas en copropiedad:** se constituye cuando una empresa posee dos o más propietarios, pero sin establecer una sociedad u otro tipo de organización legal. Los propietarios obran de común acuerdo en todas sus operaciones mercantiles que se deriven de la misma.

d. **Empresas en participación:** es una empresa mercantil posee dos o más propietarios, que ante autoridad competente o notario público, han acordado unir esfuerzos para administrar y explotar dicha empresa.

1.4 Sociedades mercantiles

La sociedad mercantil regular es un sujeto autónomo de relaciones jurídicas constituidas por medio de un contrato que tiene notoriedad legal, entre dos o más personas, las cuales se proponen ejecutar, bajo una denominación social y con un fondo social, formado por las respectivas aportaciones, uno o más actos mercantiles, para repartir consiguientemente entre ellos los beneficios y las pérdidas de la empresa común en la proporción pactada o legal (44:44).

1.4.1 Sociedad colectiva

“Es la que existe bajo una razón social y en la cual todos los socios responden de modo subsidiario, ilimitado y solidariamente de las obligaciones sociales (19:19).

“Es una sociedad mercantil, de tipo personalista, que se identifica con una razón social, en la que los socios, por las obligaciones sociales, responden de modo subsidiario, ilimitada y solidariamente” (44:109).

a. **Ventajas**

- Su organización es fácil y económica
- La responsabilidad ilimitada de los socios es una garantía para los acreedores sociales
- El crédito personal del socio puede contribuir al éxito económico de la empresa;
- Tiene una administración flexible
- Su funcionamiento no es complicado

b. **Desventajas**

- La responsabilidad ilimitada no es atractiva para los socios
- Por su carácter personalista en el criterio social, crea dificultades y divergencias que hacen incierta e inefectiva su existencia.

c. **Razón social:** "se forma con el nombre y apellido de uno de los socios o con los apellidos de dos o más de ellos, con el agregado obligatorio de la leyenda; y compañía Sociedad Colectiva, leyenda que puede ser abreviada y Cía. S.C." (19:19).

1.4.2 Sociedad en comandita simple

"Es la compuesta por uno o varios socios comanditados que responden en forma subsidiara, ilimitada y solidaria de las obligaciones sociales; y por uno o varios socios comanditarios que tienen responsabilidad limitada al monto de su aportación" (19:21).

a. **Razón social:** "la razón social debe formarse con el nombre de uno de los socios comanditados o con los apellidos de dos o más de ellos si fueren varios y con el agregado obligatorio de la leyenda: "y Compañía, Sociedad en Comandita", la que podrá abreviarse: y Cía. S. en C." (19:21).

b. **Administración:** los socios comanditarios tendrán con exclusividad la administración de la sociedad y la representación legal de la misma, salvo que la escritura social permita que la administración la tengan extraños.

1.4.3 Sociedad de responsabilidad limitada

"Ésta sociedad está compuesta por varios socios que sólo están obligados al pago de sus aportaciones. Por las obligaciones sociales responde únicamente el patrimonio de la sociedad y, en su caso, la suma que a más de las aportaciones convenga la escritura social" (19:23).

El capital estará dividido en aportaciones que no podrán incorporarse a títulos de ninguna naturaleza ni denominarse acciones, no podrá otorgarse la escritura constitutiva de la sociedad, mientras no conste de manera fehaciente que el capital ha sido íntegra y efectivamente pagado.

La cantidad de socios para conformar la sociedad de responsabilidad limitada no podrá exceder de veinte.

a. **Razón o denominación social:** "la sociedad girará bajo una denominación o bajo una razón social. La denominación se formará libremente, pero siempre hará referencia a la actividad social principal. La razón social se formará con el nombre completo de uno de los socios o con el apellido de dos o más de ellos. En ambos casos es obligatorio agregar la palabra limitada o la leyenda: y Compañía Limitada, las que podrán abreviarse. Ltda. O Cía. Ltda., respectivamente" (19:23).

1.4.4 Sociedad en comandita por acciones

"Es aquella en la cual uno o varios socios comanditados responden en forma subsidiara, ilimitada y solidaria por las obligaciones sociales y uno o varios socios comanditarios tienen la responsabilidad limitada al monto de las acciones que han suscrito, en la misma forma que los accionistas de una sociedad anónima" (19:48).

a. **Razón social:** “la razón social se forma con el nombre de uno de los socios comanditados o con los apellidos de dos o más de ellos, si fueren varios, y con el agregado obligatorio de la leyenda: y Compañía Sociedad en Comandita por Acciones, la cual podrá abreviarse: y Cía., S.C.A.” (19:48).

Los socios comanditarios tienen a su cargo la administración de la sociedad y la representación legal de la misma y están sujetos a las obligaciones y responsabilidades de los administradores de la sociedad anónima.

1.4.5 Sociedad anónima

“Es la que tiene el capital dividido y representado por acciones. La responsabilidad de cada accionista está limitada al pago de las acciones que hubiere suscrito” (19:24).

La denominación social podrá formarse libremente, con el agregado obligatorio de la leyenda: Sociedad Anónima, que podrá abreviarse S.A.

“En cuanto a las características propias de la sociedad anónima la doctrina le asigna las siguientes:

- Es una sociedad capitalista
- El capital se divide y representa por títulos valores llamados acciones
- La responsabilidad del socio es limitada
- Hay libertad para transmitir la calidad de socio mediante la transferencia de las acciones; pero esta libertad se puede limitar contractualmente cuando se trata de títulos nominativos:
- Los órganos de la sociedad funcionan independientemente y cada uno tiene delimitadas sus funciones; y
- Se gobierna democráticamente, porque la voluntad de la mayoría es la que da fundamento a los acuerdos sociales sin perjuicio de los derechos de las minorías” (44:128).

a. **Capital autorizado:** “el capital autorizado de una sociedad anónima es la suma máxima que la sociedad puede emitir en acciones, sin necesidad de formalizar un aumento de capital. El capital autorizado podrá estar total o parcialmente suscrito al constituirse la sociedad y debe expresarse en la escritura constitutiva de la misma” (19:24).

Todas las acciones de una sociedad serán de igual valor y conferirán iguales derechos, en el momento de suscribir acciones es indispensable pagar por lo menos el veinticinco por ciento de su valor nominal, El capital pagado inicial de la sociedad anónima debe ser por lo menos de cinco mil quetzales.

1.5 Clasificación según su propósito

“Las sociedades empresariales pueden clasificarse por su actividad, su finalidad, por la naturaleza de su capital, por su tamaño o por su estructura legal”. (8:7) Según su propósito, las empresas se pueden clasificar de la siguiente forma:

- **Industrial:** La actividad primordial de este tipo de empresas es la producción de bienes mediante la transformación de la materia o extracción de materias primas, como es el caso de los ingenios.

- **Comercial:** Son intermediarias entre productor y consumidor; su función primordial es la compra/venta de productos terminados

- **Agrícola:** Son las entidades dedicadas a actividades tales como la ganadería, pesca o agricultura.

- **Servicios:** Son aquellas que tienen por función brindar una actividad que las personas necesitan para la satisfacción de sus necesidades a cambio de un precio. Pueden ser públicas o privadas.

1.6 Empresa de servicios

Son aquellas que tienen por función brindar una actividad que las personas necesitan para la satisfacción de sus necesidades, entre estos podemos mencionar servicios de recreación, asesoramiento, telecomunicaciones, transporte, entre otros. “El producto que ofrece una entidad de este tipo es intangible, aunque para cumplir su cometido debe crear una red de personal y equipamiento que le soporte el servicio que brinda” (48).

1.7 Organizaciones de negocio

“Las organizaciones de negocio existen por varias razones pero la más importante de ellas es que este tipo de empresas son organizaciones especializadas dedicadas a administrar el proceso de producción de un determinado giro de negocio. Entre sus funciones importantes está la organización para la explotación de economías de especialización, la obtención de recursos para la producción a gran escala y la administración del proceso de producción. Las empresas de negocio son organizaciones que se dedican a administrar el proceso de producción. La producción se organiza en empresas porque en general la eficiencia necesita producción a gran escala, la obtención de importantes recursos financieros, y la administración y supervisión cuidadosa de las actividades en curso” (41:121).

1.8 Procesamiento de información electrónica

“Es una serie de actividades mediante las cuales se ordenan, almacenan y preparan los archivos con la información captada, asegurando su congruencia con el fin de proceder a su explotación para la presentación de resultados” (54).

“Los avances en la captación, procesamiento y almacenamiento de datos han dado como resultado un crecimiento exponencial del volumen de datos, lo cual ha llevado a muchas organizaciones a establecer un enfoque estructurado para la gestión de la información que permita identificar el valor de esta, clasificarla en categorías por su importancia, y desarrollar procesos eficaces y adecuadas herramientas y métodos para la recogida, almacenamiento y distribución de los datos” (24:93).

1.9 Empresas de apoyo al sector bancario

Son organizaciones de negocio, cuya principal función es la explotación de economías por medio de la administración de los factores de producción. Dentro de estas organizaciones se observan aquellas empresas que brindan servicios de procesamiento de información para el sector bancario del país como empresas especializadas.

1.9.1 Principales actividades del negocio

Las actividades principales del giro de negocio de estas empresas, son las siguientes:

- Procesamiento de archivos electrónicos para la cámara de compensación bancaria.
- Procesamiento de archivos electrónicos para la cámara de compensación automatizada (CCA).
- Plataforma de negocios para la conectividad de los bancos al sistema internacional de pagos denominado SWIFT.
- Digitalización de giros del exterior
- Centro de almacenamiento de documentos.

1.9.2 Aspectos regulatorios que rigen la empresa

Estas empresas se ven obligadas a cumplir las leyes del país tanto comercial como fiscal; sin embargo, existe otro tipo de regulaciones aplicables derivado del giro del negocio, derivado de los servicios brindados al sector bancario, estas entidades se enfrentan a las normativas o regulaciones emitidas por aquellas instituciones o entes supervisores del sistema financiero regulado, de las cuales se mencionan las siguientes:

Aspectos legales y tributarios

- **Asamblea Nacional Constituyente, Constitución Política de la República de Guatemala y sus reformas:** también llamada Carta Magna, reconoce en su artículo 43 la libertad de industria, comercio y trabajo.

- **Congreso de la República de Guatemala, Decreto 27-92, "Ley del Impuesto al Valor Agregado" y sus reformas:** conocido como IVA es un impuesto generado por la venta o cambio de bienes o servicios, su pago es obligatorio para toda persona individual o jurídica incluyendo al estado.

- **Congreso de la República de Guatemala, Decreto 10-2012, "Ley de Actualización Tributaria":** en el Libro I, contiene el impuesto sobre la renta, conocido como ISR, la empresa está afecta al régimen de actividades lucrativas derivado de su actividad comercial.

- **Congreso de la República de Guatemala, Decreto 73-2008, "Ley del Impuesto de Solidaridad":** impuesto creado para dar cumplimiento a las obligaciones que le impone al estado la Constitución Política de la República de Guatemala en materia de inversión, a este impuesto están afectos todas las personas individuales o jurídicas.

- **Congreso de la República de Guatemala, Decreto 37-92, "Ley del Impuesto de Timbres Fiscales y Papel Sellado Especial para Protocolos" y sus reformas:** la empresa está afecta a este impuesto, debido a que anualmente realiza el pago de dividendos a los accionistas.

- **Congreso de la República de Guatemala, Decreto 15-98, "Ley del Impuesto Único Sobre Inmuebles":** establece un impuesto único anual, sobre el valor de los bienes inmuebles situados en la República de Guatemala, debido a que la empresa posee instalaciones para su funcionamiento, es afecta a esta ley.

- **Congreso de la República de Guatemala, Decreto 2-70, "Código de Comercio de Guatemala" y sus reformas:** es aplicable a los comerciantes, los negocios jurídicos mercantiles, también indica el tipo de sociedad mercantil en la que puede crearse una empresa.

Resoluciones de la Junta Monetaria

- **Resolución JM-51-2003 "Aprobación del Reglamento de la Cámara de Compensación Bancaria":** esta resolución tiene por objeto regular el funcionamiento de la cámara de compensación bancaria, por medio de la cual se compensarán los cheques recibidos por cada banco del sistema a cargo de los demás bancos, el documento también muestra el instructivo para la estandarización de cheques.

- **Resolución JM-189-2007 "Modificación del Reglamento de la Cámara de Compensación Bancaria":** la resolución indica la modificación en el monto de las operaciones en alto valor y bajo valor. Las operaciones de alto valor son todos los cheques de Q250,000.01 ó US$30,000.01 en adelante, y las operaciones de bajo valor, los cheques emitidos hasta un monto de Q250,000.00 ó US$30,000.00.

- **Resolución JM-140-2007 "Reglamento de la Cámara de Compensación Automatizada":** el reglamento regula la administración y funcionamiento de la cámara de compensación automatizada (CCA), por medio de la cual se compensarán las transacciones electrónicas.

- **Resolución JM-95-2011 "Reglamento para la Estandarización de Cuentas Bancarias":** este reglamento tiene por objeto establecer la estructura de la cuenta bancaria estandarizada para Guatemala, así como la metodología para su cálculo, con el propósito de facilitar el proceso automático de las transferencias de fondos que realicen las instituciones bancarias.

- **Resolución JM-102-2011 “Reglamento para la Administración del Riesgo Tecnológico”:** este reglamento tiene por objeto establecer los lineamientos mínimos que las entidades financieras deben cumplir para administrar el riesgo tecnológico; para la empresa objeto de estudio, es afectada por el capítulo VI, “Procesamiento de información y tercerización”, debido a que le presta servicio a los bancos, debe cumplir con este capítulo.

- **Resolución JM-4-2016 “Reglamento para la Administración del riesgo operacional”:** su objeto es proporcionar los lineamientos que la entidades financieras deben cumplir para administrar el riesgo del riesgo operacional.

Resoluciones del Banco de Guatemala

- **Resolución GG-02-2014:** esta resolución aprueba la modificación de los instrumentos normativos de la cámara de compensación bancaria.

- **Resolución GG-78-2013:** aprueba las modificaciones al instructivo para la estandarización de cheques en el sistema bancario Nacional.

- **Resolución GG-72-2010:** aprueba los instrumentos normativos y horarios de atención y de operación de la cámara de compensación bancaria.

- **Resolución GG-14-2009:** esta resolución determina el monto de las operaciones de alto y bajo valor y el procedimiento de liquidación de los cheques a compensar en la CCB y a liquidar en el sistema LBTR, en moneda nacional y moneda extranjera.

- **Resolución GG-37-2014:** aprueba las disposiciones administrativas y horarios de operación, de atención y de prestación de servicios de la cámara de compensación automatizada.

CAPÍTULO II
AUDITORÍA INTERNA Y CONTROL INTERNO

2.1 Definición

“La Auditoría Interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno” (29:17).

La auditoría interna es una de las piedras angulares del gobierno corporativo, junto con el consejo de administración, la alta dirección y la auditoría externa, La posición de privilegio que ocupa la auditoría interna dentro de la entidad le permite ser una valiosa ayuda para los miembros del comité de auditoría dado que ofrece un aseguramiento objetivo de los procesos de gobierno, riesgo y control.

2.1.1 Origen etimológico

“El origen etimológico de la palabra es el verbo inglés "Audit", que significa "comprobar", y es utilizado principalmente en el "Audit accounting", que es la traducción de auditoría.

El origen etimológico de la palabra es el verbo latino "Audire", que significa "oír", que a su vez tiene su origen en que los primeros auditores ejercían su función juzgando la verdad o falsedad de lo que les era sometido a su verificación principalmente oyendo” (50).

2.2 Principios

2.2.1 Integridad

La integridad de los auditores internos establece confianza y, consiguientemente, provee la base para confiar en su juicio.

2.2.2 Objetividad

Los auditores internos exhiben el más alto nivel de objetividad profesional al reunir, evaluar y comunicar información sobre la actividad o proceso a ser examinado. Los auditores internos hacen una evaluación equilibrada de todas las circunstancias relevantes y forman sus juicios sin dejarse influir, indebidamente, por sus propios intereses o por otras personas.

2.2.3 Confidencialidad

Respetan el valor y la propiedad de la información que reciben y no divulgan información sin la debida autorización, a menos que exista una obligación legal o profesional para hacerlo.

2.2.4 Competencia

Aplican el conocimiento, aptitudes y experiencia necesarios para desempeñar los servicios de auditoría interna.

2.3 Objetivos

Los objetivos del trabajo son declaraciones amplias desarrolladas, que definen los logros que se pretenden conseguir en el trabajo.

A nivel general, el objetivo primordial que persigue la auditoría interna es asistir a los miembros de la organización. Con lo anterior, se trata de explicar que la auditoría interna debe proporcionar análisis, valoraciones, recomendaciones y toda la información concerniente a las actividades revisadas. En consecuencia, se puede indicar que la auditoría interna persigue entre otros, cuatro objetivos principales:

a. **Garantizar información financiera confiable y oportuna:** deberá evaluar la efectividad de los controles internos existentes en la organización, que permitirá garantizar la autenticidad del registro de las transacciones, y por lo tanto la presentación razonable de los estados financieros de una manera oportuna y confiable.

b. **Salvaguarda de los activos:** Examinará, de manera adecuada y oportuna los activos de la organización, con el objetivo de determinar la propiedad de los activos, la adecuada salvaguarda contra riesgos y la existencia física de los mismos.
c. **Promover la eficiencia operativa de la entidad:** evaluará las actividades relacionadas con el uso adecuado y eficiente de los recursos de la organización, con el fin de promover la eficiencia de las operaciones de la entidad.
d. **Cumplimiento de objetivos, políticas, planes, procedimientos, leyes y reglamentos:** deberá conocer los objetivos, políticas, planes, procedimientos y reglamentos establecidos por la organización, así como leyes de carácter general aplicables, con el fin de verificar su cumplimiento y detectar mejoras que puedan ayudar a la organización a alcanzar los objetivos planteados.

De acuerdo a lo estipulado en el Marco para la Práctica Profesional de la Auditoría Interna, del Instituto de Auditores Internos, cada objetivo del auditor interno debe ser establecido. Los auditores internos deben realizar una evaluación preliminar de los riesgos pertinentes a la actividad bajo revisión. Los objetivos del trabajo deben reflejar los resultados de esta evaluación. Asimismo, debe considerar la probabilidad de errores, irregularidades, incumplimientos y otras exposiciones materiales al desarrollar los objetivos del trabajo.

2.3.1 Importancia de la auditoría interna

La auditoría interna constituye una herramienta gerencial para el control de gestión de las empresas, porque producen en su informe final, una especie de radiografía que revela la situación de la organización en ese momento, relacionada con los controles de calidad que debe realizar. Es la herramienta para saber dónde está la empresa con sus problemas y sistemas de información financiera.

El trabajo de los auditores internos también puede ser una función que puede realizar una firma de Contadores Públicos y Auditores; sin embargo, el auditor independiente debe considerar los procedimientos, si los hay, efectuados por los auditores internos para la determinación de la naturaleza, oportunidad y extensión de sus propios procedimientos de auditoría.

Tradicionalmente la auditoría interna se orienta hacia aquellos aspectos de tipo financiero, concentrando en la corrección de los registros contables y verificando que la corrección sea confiable; no obstante, ésta es sólo una de las áreas que se pueden considerar como básicas a cubrir por parte de la auditoría interna.

Con frecuencia realizan una serie de servicios para la gerencia, que incluyen evaluación y estudios del control interno, pero que no están limitados a éste; además, la revisión de prácticas operacionales para promover el incremento en la eficiencia y en la economía; y, el hacer investigaciones especiales en la dirección de la gerencia.

2.3.2 Responsabilidad de la auditoría interna

Todas las actividades dentro de una organización caen potencialmente dentro del ámbito de responsabilidad de los auditores internos. La auditoría interna es responsable de velar por la organización de una manera congruente con las normas profesionales de conducta. Esta responsabilidad incluye la coordinación de las actividades de auditoría interna con terceros, así como el mejor logro de los objetivos de auditoría y los de la organización.

Es importante que exista un documento donde se establezca claramente los propósitos de la auditoría interna, especificando el alcance no restringido de su trabajo y declarando que los auditores internos no tienen autoridad o responsabilidad sobre las actividades que auditan.

2.4 Normas Internacionales para el ejercicio profesional de la auditoría interna –NIEPAI-

Son normas indispensables que guardan relación con la independencia de la unidad, la integridad y capacidad profesional del auditor interno, el proceso de su trabajo y con la dirección de la unidad a su cargo.

“El propósito de las normas es:

- Definir principios básicos que representen el ejercicio de la auditoría interna tal como este debería ser.
- Proporcionar un marco para ejercer y promover un amplio rango de actividades de auditoría interna de valor añadido.
- Establecer las bases para evaluar el desempeño de la auditoría interna.
- Fomentar la mejora de los procesos y operaciones de la organización” (43:1).

La estructura de las normas está formada por las normas sobre atributos, las normas sobre desempeño y las normas de implantación.

Las normas sobre atributos tratan las características de las organizaciones y las personas que prestan servicios de auditoría interna.

Las normas sobre desempeño describen la naturaleza de los servicios de auditoría interna y proporcionan criterios de calidad con los cuales puede evaluarse el desempeño de estos servicios. Las normas de implantación amplían las normas sobre atributos y desempeño, proporcionando los requisitos aplicables a las actividades de aseguramiento y consultoría.

2.5 Código de ética

“El propósito del código de ética es promover una cultura ética en la profesión de la auditoría interna” (29:21), es necesario y apropiado contar con un código de ética

para la profesión, ya que en este se describen las normas de comportamiento que se espera sean observadas por los auditores internos.

En Guatemala existe una institución en la cual los contadores públicos y auditores pueden afiliarse, siendo esta la siguiente:

- Colegio de Contadores Públicos y Auditores de Guatemala

Esta institución cuenta con su código de ética, el cual resuelve adoptar en su totalidad del código de ética del IFAC (international federation of accountants).

La estructura del código de ética del IFAC se divide en tres secciones:

- **Aplicación general del código:** esta sección establece los principios fundamentales de ética profesional para los profesionales de la contabilidad.

- **Profesionales de la contabilidad en ejercicio:** esta sección del código describe la forma en que el marco conceptual es aplicable en determinadas situaciones a los profesionales de la contabilidad en ejercicio.

- **Profesionales de la contabilidad en la empresa:** esta sección describe la forma en que el marco conceptual es aplicable en determinadas situaciones a los profesionales de la contabilidad en la empresa.

2.6 Procedimientos de auditoría

2.6.1 Naturaleza de los procedimientos de auditoría

Los diferentes sistemas de organización, control, contabilidad y en general los detalles de operación de los negocios, hacen imposible establecer sistemas rígidos de prueba para el examen de los estados financieros. Por esta razón el auditor deberá, aplicando su criterio profesional, decidir cuál técnica o procedimiento de

auditoría o conjunto de ellos, serán aplicables en cada caso para obtener la evidencia que fundamente su opinión objetiva y profesional.

2.6.2 Extensión o alcance de los procedimientos de auditoría

Dado que las operaciones de las empresas son repetitivas y forman cantidades numerosas de operaciones individuales, generalmente no es posible realizar un examen detallado de todas las transacciones individuales que forman una partida global. Por esa razón, cuando se llenan los requisitos de multiplicidad de partidas y similitud entre ellas, se recurre al procedimiento de examinar una muestra representativa de las transacciones individuales, para derivar del resultado del examen de tal muestra, una opinión general sobre la partida global. Este procedimiento, no es exclusivo de la auditoría, sino que tiene aplicación en muchas otras disciplinas. En el campo de la auditoría se le conoce con el nombre de pruebas selectivas. La relación de las transacciones examinadas, respecto del total que forman el universo, es lo que se conoce como extensión o alcance de los procedimientos de auditoría y su determinación, es uno de los elementos más importantes en la planificación y ejecución de la auditoría.

2.6.3 Oportunidad de los procedimientos de auditoría

La época en que los procedimientos de auditoría se van a aplicar se le llama oportunidad. No es indispensable y a veces no es conveniente, realizar los procedimientos de auditoría relativos al examen de los estados financieros, a la fecha del examen de los estados financieros. Algunos procedimientos de auditoría son más útiles y se aplican mejor en una fecha anterior o posterior.

2.6.4 Técnicas de auditoría

Son los métodos de investigación y prueba que el contador público y auditor puede utilizar para comprobar la razonabilidad de la información, que le permita emitir su opinión profesional. Entre las técnicas de auditoría se pueden mencionar las siguientes:

a. **Estudio general:** consiste en la apreciación sobre las características generales de la empresa, de sus estados financieros y de las partes importantes, significativas o extraordinarias.

b. **Análisis:** “clasificación y agrupación de los distintos elementos individuales que forman una cuenta o una partida determinada, de tal manera que los grupos constituyan unidades homogéneas y significativas" (9:154).

c. **Inspección:** consiste en examinar los recursos materiales y registros de la compañía, los cuales pueden comprender desde los registros de actas de asamblea o comités, hasta registros auxiliares o documentos que tengan como fin respaldar la información financiera y administrativa que será utilizada como evidencia de auditoría

d. **“Confirmación:** obtención de una comunicación escrita de una persona independiente de la empresa examinada y que se encuentre en posibilidad de conocer la naturaleza y condiciones de la operación y por lo tanto, confirmar de una manera válida. Esta técnica se aplica solicitando a la empresa auditada, que se dirija a la persona a quien se pide la confirmación, para que conteste por escrito al auditor.

e. **Investigación:** obtención de información, datos y comentarios de los funcionarios y empleados de la propia empresa. Con esta técnica, el auditor puede obtener conocimiento y formarse un juicio sobre algunos saldos u operaciones realizadas por la empresa. Por ejemplo, el auditor puede formarse una opinión sobre la cobrabilidad de los saldos de deudores, mediante informaciones y comentarios que obtenga de los jefes de los departamentos de crédito y cobranzas de la empresa” (9:156).

f. **Declaración:** técnica en la cual se realiza una manifestación por escrito, con la firma de los interesados, del resultado de las investigaciones realizadas

con los funcionarios y empleados de la empresa. Esta técnica, se puede aplicar cuando la importancia de los datos o el resultado de las investigaciones realizadas lo ameritan.

g. **Certificación:** consiste en la obtención de cartas o documentos en el que se asegure la verdad de un hecho, legalizado por lo general, con la firma de funcionarios de la empresa.

h. **"Observación:** presencia física de cómo se realizan ciertas operaciones o hechos. El auditor se cerciora de la forma como se realizan ciertas operaciones, dándose cuenta ocularmente de la forma como el personal de la empresa las realiza. Por ejemplo, el auditor puede obtener la convicción de que los inventarios físicos fueron practicados de manera satisfactoria, observando cómo se desarrolla la labor de preparación y realización de los mismos" (9:157).

i. **Cálculo:** "verificación matemática de alguna partida. Hay partidas en la contabilidad que son resultado de cómputos realizados sobre bases predeterminadas. El auditor puede cerciorarse de la corrección matemática de estas partidas mediante el cálculo independiente de las mismas" (46).

2.7 Planificación de auditoría

Debido a la importancia del trabajo de auditoría, éste debe planearse adecuadamente con el fin de que se efectúe en el menor tiempo posible y con el mayor alcance.

La planificación de la auditoría interna constituye el desarrollo de una estrategia para el alcance y la conducción de la evaluación; implica prever los procedimientos de auditoría que van a emplearse, la extensión y oportunidad en que van a ser aplicados y el personal que debe intervenir en el trabajo.

La planificación de la Auditoría comprende los siguientes aspectos:

a. Delimitación de los objetivos de la auditoría.
b. Delimitación del alcance del trabajo de auditoría.
c. Obtención de la información necesaria que se relacione con las actividades y operaciones que se pretenden auditar.
d. Verificación de los controles que van a ser objeto de evaluación por parte de la auditoría.
e. Identificación de las áreas que por su importancia debe hacerse énfasis.
f. Preparación del programa de auditoría.
g. Determinación de la forma, oportunidad y destino de los resultados de la auditoría.

2.7.1 Clases de planificación

a. **Planificación técnica:** conocida como el plan de auditoría, el cual refleja el ámbito de acción de la entidad de una unidad de auditoría interna, orientado por las políticas y el establecimiento de los recursos necesarios que permitan su ejecución en forma eficiente.

b. **Planificación administrativa:** se fijan los objetivos a ser alcanzados, las prioridades, el tiempo y los recursos que se consideran necesarios para la realización de la evaluación; se concreta en un plan de acción para decidir de manera anticipada sobre su ejecución y la comunicación de resultados.

2.7.2 Planificación del trabajo de auditoría interna basado en riesgo

Se deben establecer planes basados en riesgos, a fin de determinar las prioridades de la actividad de auditoría interna. Dichos planes deben ser consistentes con las metas de la organización. “Los auditores internos deben elaborar y documentar un plan para cada trabajo, que incluya su alcance, objetivos, tiempo y asignación de recursos” (29:49).

“Al planificar el trabajo, los auditores internos deben considerar:

- Los objetivos de la actividad que está siendo revisada y los medios con los cuales la actividad controla su desempeño;
- Los riesgos significativos de la actividad, sus objetivos, recursos y operaciones y los medios con los cuales el impacto potencial del riesgo se mantiene a un nivel aceptable;
- La adecuación y eficacia de los procesos de gobierno, gestión de riesgos y control de la actividad comparados con un enfoque o modelo relevante; y
- Las oportunidades de introducir mejoras significativas en los procesos de gobierno, gestión de riesgos y control de la actividad” (29:49,50).

“La planificación de una auditoría implica el establecimiento de una estrategia global de auditoría, una planificación adecuada favorece la auditoría en varios aspectos, entre los cuales se puede mencionar los siguientes:

- Ayuda al auditor a prestar una atención adecuada a las áreas más importantes de la auditoría.
- Ayuda a identificar y resolver problemas potenciales oportunamente.
- Ayuda al auditor a organizar y dirigir adecuadamente la auditoría para que se realice de forma eficaz y eficiente.
- Facilita la selección de los miembros del equipo con niveles de capacidad y competencia adecuados para responder a los riesgos previstos.
- Facilita la dirección, supervisión y revisión del trabajo” (30:318).

El auditor interno debe “establecer planes basados en los riesgos, a fin de determinar las prioridades de la actividad de auditoría interna. Dichos planes deberán ser consistentes con las metas de la organización”, (29:44) el plan de trabajo de la actividad de auditoría interna debe estar basado en una evaluación de riesgos, realizada, al menos, anualmente.

2.8 Desempeño de la auditoría

“Los auditores internos deben identificar, analizar, evaluar y registrar suficiente información de manera tal que les permita cumplir con los objetivos del trabajo.

2.8.1 Identificación de la información: los auditores internos deben identificar información suficiente, fiable, relevante y útil de manera tal que les permita alcanzar los objetivos del trabajo.

2.8.2 Análisis y evaluación: los auditores internos deben basar sus conclusiones y los resultados del trabajo en análisis y evaluaciones adecuados” (43:16,17).

2.9 Comunicación de resultados

Los auditores internos deben comunicar los resultados del trabajo, cuando se emite una opinión o conclusión, debe considerar las expectativas de la alta dirección y debe estar soportada con información suficiente, relevante y útil.

2.9.1 Criterios para la comunicación

“Las comunicaciones deben incluir los objetivos y alcance del trabajo así como las conclusiones correspondientes, las recomendaciones, y los planes de acción” (27:162).

2.9.2 Calidad de la comunicación

“Las comunicaciones deben ser precisas, objetivas, claras, concisas, constructivas, completas y oportunas” (29:199).

2.9.3 Difusión de resultados

“El director ejecutivo de auditoría debe difundir los resultados a las partes apropiadas” (29:200).

El director ejecutivo de auditoría es responsable de comunicar los resultados finales a las partes, que puedan asegurar que se dé a los resultados obtenidos la debida consideración.

2.10 Modelo de las tres líneas de defensa

Es un marco alineado con el modelo del sistema de gobierno corporativo, clasifica las áreas funcionales y de responsabilidad de la organización que garantizan la gestión y supervisión de riesgos de forma eficaz.

Figura 1 Modelo de las tres líneas de defensa

Fuente: Instituto de Auditores Internos, las tres líneas de defensa para una efectiva gestión de riesgos y control

Las tres líneas de defensa que indica el modelo son:

- **Primera línea de defensa, la gestión operativa:** “las gerencias operativas son propietarias de los riesgos y los gestionan. Estas gerencias también son responsables de la implementación de acciones correctivas para hacer frente a deficiencias de proceso y control” (28:3).

- **Segunda línea de defensa, funciones de gestión de riesgos y cumplimiento:** “la gerencia establece diversas funciones de gestión de riesgos y cumplimiento para ayudar a crear y/o monitorear los controles de la primera línea de defensa” (28:4).

- **Tercera línea de defensa, auditoría interna:** “los auditores internos proveen aseguramiento sobre la efectividad del gobierno corporativo, la gestión de riesgos y el control interno, incluyendo la manera en que la primera y segunda línea de defensa alcanzan sus objetivos de gestión de riesgos y control” (28:5).

2.11 Control interno

“Es un proceso efectuado por el Consejo de Administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Fiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables” (23:16).

Para efectos de la presente tesis se mencionan las metodologías en lo que respecta la evaluación de control interno.

2.11.1 Control interno tradicional

“Comprende el plan de organización y el conjunto de métodos y procedimientos que aseguren que los activos están debidamente protegidos, que los registros contables son fidedignos y que la actividad de la entidad se desarrolla eficazmente según las directrices marcadas por la administración” (25:19).

2.11.2 Coso ERM

Es un marco para la administración del riesgo corporativo definido en ocho componentes interrelacionados entre sí, el cual expone que la administración de

riesgos “es un proceso efectuado por el directorio, gerencia y otros miembros del personal aplicado en el establecimiento de la estrategia y a través de la organización, diseñado para identificar riesgos y la respuesta al mismo” (15:29).

Los componentes de Coso ERM son:

- **Ambiente interno:** Abarca el entorno de la organización y establece la base de cómo el personal percibe y trata los riesgos, en este componente también se incluye la filosofía de administración de riesgo y el riesgo aceptado.

- **Establecimiento de objetivos:** se establecen los objetivos a nivel estratégico, siendo estos una base para los objetivos operativos, de información y de cumplimiento.

- **Identificación de eventos:** la administración identifica los eventos potenciales que, de ocurrir, pueden afectar negativamente a la empresa en la consecución de sus objetivos.

- **Evaluación de riesgos:** se analizan los riesgos considerando su probabilidad e impacto como base para determinar cómo deben ser administrados y se determinan los riesgos relevantes.

- **Respuesta a los riesgos:** la dirección determina cómo responder a los riesgos relevantes, las respuestas pueden ser las de evitar, reducir, compartir y aceptar el riesgo.

- **Actividades de control:** debe identificarse las actividades de control necesarias que ayuden a asegurar que se llevan a cabo efectivamente las respuestas a los riesgos.

- **Información y comunicación:** la información se identifica, y se comunica en forma y plazo adecuado, que permita a las personas involucradas afrontar sus responsabilidades.

- **Supervisión:** la gestión de riesgos debe supervisarse, observando el funcionamiento de sus componentes a lo largo del tiempo y deben realizarse las modificaciones necesarias para su funcionamiento óptimo.

2.11.3 Normas ISO

Son normas elaboradas por la organización internacional para la estandarización, ISO por sus siglas en inglés, es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.

Por ser fundamental estas normas en la elaboración de la presente tesis, se ampliará en el capítulo III.

CAPÍTULO III
ISO 31000:2009 Y GESTIÓN DE RIESGOS

3.1 Definición de riesgo

Es la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad.

“Aunque la incertidumbre está presente en el largo plazo, se puede manifestar aún en el corto plazo. Con la incertidumbre se asocia el riesgo, al resultar imposible determinar los eventos que puedan presentarse y sus consecuencias” (39:21).

3.1.1 Origen etimológico

“La palabra “riesgo” viene del italiano Risicare, que significa desafiar, retar, enfrentar, atreverse. En el nuevo diccionario español-latino etimológico, se define como: peligro, prueba, tentativa, exponerse a un peligro, poner en peligro a uno, suscitarle algún peligro, lanzarse, arrojarse al peligro” (39:30).

3.2 Tipos de riesgo

“Desde el punto de vista empresarial, existen innumerables riesgos generados tanto por el entorno que influye sobre la empresa, como por el desarrollo normal de sus actividades” (39:35).

3.2.1 Riesgo inherente

“El riesgo inherente es aquél al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto” (16:64).

3.2.2 Riesgo de control

“Influye de manera muy importante los sistemas de control interno que estén implementados en la empresa y que en circunstancias lleguen a ser insuficientes o inadecuados para la aplicación y detección oportuna de irregularidades. Es por esto

la necesidad y relevancia que una administración tenga en constante revisión, verificación y ajustes los procesos de control interno” (51).

3.2.3 Riesgo de detección

“Este tipo de riesgo está directamente relacionado con los procedimientos de auditoría, por lo que se trata de la no detección de la existencia de error en el proceso realizado” (51).

3.2.4 Riesgo residual

“Es el que permanece después de que la dirección desarrolle sus respuestas a los riesgos” (16:64).

3.2.5 Riesgos de entorno

“El entorno de una organización consta de muchos elementos: desde el país donde está ubicada, la naturaleza que la rodea, la región y ciudad donde está situada, el sector y la industria a la cual pertenece, las condiciones económicas, políticas, sociales y culturales donde opera” (39:35).

3.2.6 Riesgos generados en la empresa

“Las organizaciones, al ejecutar sus procesos en busca del cumplimiento de sus objetivos, pueden verse abocadas a un sinnúmero de riesgos propios, específicos e individuales: estos riesgos son llamados riesgos no sistemáticos y pueden afectar sus procesos, recursos humanos, físicos, tecnológicos, financieros y organizacionales, a los clientes y hasta su imagen.

“El objetivo primordial de la administración de riesgos es maximizar las oportunidades y minimizar las pérdidas asociadas a los riesgos, es decir, buscar un equilibrio entre riesgo y oportunidad, de acuerdo con la tolerancia al riesgo de la organización” (39:37,44).

3.2.7 Riesgo empresarial

Definidos los diferentes tipos de riesgo generados por el entorno o por la misma organización, se dispone de los elementos necesarios para tratar el concepto riesgo empresarial, que implica un análisis integral del manejo del riesgo dentro de las compañías.

3.3 Gestión del riesgo

“Todas las actividades de una organización implican riesgo. Las organizaciones gestionan el riesgo mediante su identificación y análisis y luego evaluando si el riesgo se debería modificar por medio del tratamiento del riesgo con el fin de satisfacer los criterios del riesgo. A través de este proceso, las organizaciones se comunican y consultan con las partes involucradas, monitorean y revisan el riesgo y los controles que lo están modificando, con el fin de garantizar que no se requiere tratamiento adicional del riesgo” (30:1).

“Al evaluar los riesgos, la dirección considera los eventos esperados e inesperados. Muchos de éstos son rutinarios y recurrentes y ya se contemplan en los programas de gestión y presupuestos operativos, pero otros son inesperados. La dirección evalúa el riesgo de los eventos potenciales inesperados y, si todavía no lo ha hecho, los eventos esperados que puedan tener un impacto significativo en la entidad.

La administración de riesgos es el conjunto de acciones llevadas a cabo en forma estructurada e integral, que permite a las organizaciones identificar y evaluar los riesgos que pueden afectar el cumplimiento, con el fin de emprender en forma efectiva las medidas necesarias para responder ante ellos” (16:64,41).

“Ésta administración del riesgo es necesaria debido a la incertidumbre y a la posibilidad que tienen las empresas de verse enfrentadas a circunstancias, tanto internas como externas, que puedan afectar el logro de sus objetivos organizacionales” (39:42).

3.3.1 Importancia de la gestión del riesgo

La importancia que tiene en estos tiempos, para las empresas, la gestión de riesgos y a la vez saber el porqué del auge y el surgimiento de esta gestión, para obtener un proceso adecuado para la empresa; esto quiere decir, reducción de los niveles de riesgo existentes para la entidad, también dará a conocer la definición de gestión de riesgos, cuyo objetivo es la buena aplicación de esta medida, y conocer además definiciones de los principios básicos de la gestión de riesgos, procesos y ejemplos de modelos de gestión de riesgos para implementar dentro de la empresa.

3.3.2 Objetivos de la gestión del riesgo

El objetivo primordial de la gestión de riesgos es maximizar las oportunidades y minimizar las pérdidas asociadas a los riesgos, es decir, buscar un equilibrio entre riesgo y oportunidad, de acuerdo con la tolerancia al riesgo de la organización.

Por medio de la implementación de la gestión de riesgos en la empresa, se logran diferentes objetivos, entre ellos:

- Asegurar la supervivencia de la empresa, preservando la continuidad de su operación, de tal forma que no se interrumpa la prestación de sus servicios o la producción y comercialización de sus bienes, y se eviten pérdidas financieras catastróficas que puedan llevarla a la quiebra, afectar su participación en el mercado o sus planes de desarrollo.

- Proteger a los empleados y a quienes estén relacionados con las operaciones de la empresa, mejorando y haciendo más seguras, las condiciones de trabajo del personal e implementando medidas de prevención y protección.

- Evitar que las operaciones de la empresa produzcan daños al ambiente, al controlar la emisión de contaminantes que degraden la calidad del agua, aire, suelo, etc.

- Utilizar los recursos humanos, físicos y financieros en forma eficaz, para que contribuyan al logro de los objetivos propuestos por la organización.

- Prevenir o mitigar cualquier pérdida económica que pueda ocasionar la ocurrencia de los riesgos, al disminuir el grado de inseguridad de las operaciones de la empresa hasta límites considerados tolerables.

3.3.3 Responsabilidades

"El Consejo de Administración, la dirección, los directores financieros y de riesgos, los auditores internos y, de hecho, toda persona de la entidad, contribuyen a una gestión eficaz de riesgos" (16:101).

Dentro de los roles y responsabilidades de cada persona de la entidad se pueden mencionar los siguientes:

a. **Consejo de Administración:** forma parte del componente del ambiente interno de la gestión del riesgo y debe tener la composición y enfoque necesario para conseguir que ésta sea efectiva.

b. **Dirección:** el gerente general tiene la responsabilidad última sobre la gestión del riesgo, su mayor responsabilidad es establecer un ambiente interno positivo, proporcionar liderazgo y orientación a los directivos.

c. **Auditoría Interna:** una de las responsabilidades de la auditoría interna es evaluar la efectividad de la gestión; sin embargo, existen roles principales como respecto a la gestión del riesgo como las siguientes:

    - Revisión del manejo de los riesgos claves
    - Evaluación de reportes de riesgos claves
    - Aseguramiento de que los riesgos son correctamente evaluados
    - Brindar aseguramiento sobre procesos de gestión de riesgo.

d. **Oficial de riesgo:** establece las políticas de la gestión del riesgo incluyendo la definición de roles y responsabilidades y participa en la formulación para su implementación.

e. **Directivos financieros:** La labor importante es la prevención y detección de la información fraudulenta y ayuda a establecer el tono de la conducta ética.

La gestión de riesgos es, hasta cierto punto, responsabilidad de toda persona en una empresa y, por esto, debería ser una parte explícita o implícita de su descripción de funciones, los roles y responsabilidades de cada empleado deberían comunicarse efectivamente.

3.4 ISO 31000:2009

Esta norma forma parte del grupo de normas sobre gestión del riesgo en normas codificadas por la organización internacional de estandarización ISO. El propósito de la norma es proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo.

3.4.1 Alcance

La norma internacional proporciona principios y directrices genéricas sobre la aplicación de la gestión de riesgos, se puede aplicar a cualquier empresa pública, privada o comunitaria, asociación, a un grupo o de manera individual.

Es genérica y no específica una industria o sector. Puede aplicarse en toda la vida de una organización, y para una amplia gama de actividades, procesos, funciones, proyectos, productos, servicios, activos, operaciones y decisiones.

Aunque esta norma internacional proporciona directrices genéricas, no es la intención de imponer la uniformidad de gestión del riesgo a las organizaciones, el diseño e implementación de planes de gestión de riesgos y marcos deberán tener

en cuenta las diversas necesidades de una organización específica, sus objetivos particulares, el contexto, estructura, operaciones, procesos específicos.

La norma se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, ya que tiene consecuencias positivas o negativas.

La norma ISO 31000:2009 no está prevista para fines de certificación, ya que únicamente proporciona guías y no establece requisitos para la implementación de la gestión de riesgos.

3.4.2 Beneficios de la norma

La norma ISO 31000 está diseñada para ayudar a las organizaciones a:

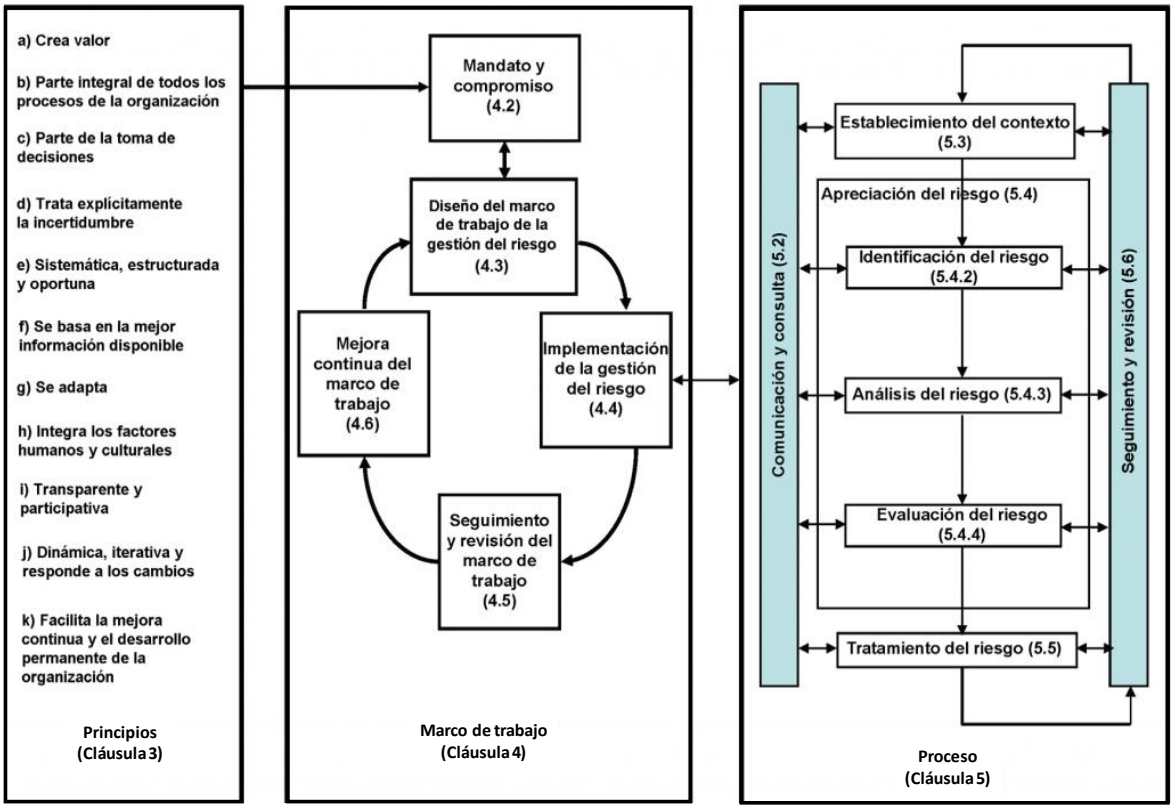
- Aumentar la probabilidad de lograr los objetivos
- Fomentar la gestión proactiva
- Ser conscientes de la necesidad de identificar y tratar el riesgo en toda la organización
- Mejorar en la identificación de oportunidades y amenazas
- Cumplir con las exigencias legales y reglamentarias pertinentes, así como las normas internacionales
- Mejorar la información financiera
- Mejorar la gobernabilidad
- Mejorar la confianza de los grupos de interés
- Establecer una base confiable para la toma de decisiones y la planificación
- Mejorar los controles
- Asignar y utilizar con eficacia los recursos para el tratamiento del riesgo
- Mejorar la eficacia y eficiencia operacional
- Mejorar la salud y seguridad, así como la protección del medio ambiente.
- Mejorar la prevención de pérdidas, así como la gestión de incidentes
- Minimizar las pérdidas económicas
- Mejorar el aprendizaje organizacional

- Mejorar la capacidad de recuperación de la organización.

El estándar está estructurado en tres elementos relacionados entre sí que son:

- Principios para la gestión de riesgos
- Marco de trabajo para la gestión de riesgos
- Proceso de gestión de riesgos

Figura 2 Relación entre los principios, marco de trabajo y proceso de gestión de riesgos



Fuente: ISO 31000:2009

3.4.3 Principios de gestión de riesgos

Los principios bajos los cuales está regida el estándar ISO 31000:2009 se definen de la siguiente forma:

- **Crea Valor:** la gestión del riesgo, tangiblemente, contribuye al logro de los objetivos y mejorar el desempeño de la organización, a través de la revisión de su sistema de gestión y sus procesos.

- **Está integrada en los procesos de la organización:** la gestión del riesgo debe integrarse en el sistema de gestión existente tanto a nivel estratégico y operativo.

- **Forma parte de la toma de decisiones:** la gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.

- **Trata explícitamente la incertidumbre:** mediante la identificación de riesgos potenciales, la organización puede aplicar reducción de herramientas y el riesgo de financiamiento, con el objetivo de maximizar las posibilidades de éxito y minimizar la pérdida de oportunidades.

- **Es sistemática, estructurada adecuada:** los procesos de gestión de riesgo deben ser coherentes en toda la organización para asegurar la efectividad, relevancia, consistencia y fiabilidad de los resultados.

- **Está basada en la mejor información disponible:** eficaz de gestión de riesgos, es importante considerar y entender toda la información disponible y relevante para una actividad, reconociendo las limitaciones de los datos y los modelos utilizados.

- **Está hecha a la medida:** la gestión del riesgo está alineada con el contexto externo e interno de la organización y con su perfil de riesgo.

- **Tiene en cuenta factores humanos y culturales:** la gestión del riesgo debe reconocer la contribución de los individuos y los factores culturales para el logro de los objetivos de la organización.

- **Es transparente y participativa:** al involucrar a las partes interesadas pertinentes, interna y externa, durante el proceso de gestión del riesgo, la organización reconoce la importancia de la comunicación y consulta en las etapas de identificación, evaluación y tratamiento de riesgos.

- **Es dinámica, iterativa y sensible al cambio:** la gestión del riesgo debe ser flexible. El entorno competitivo requiere la organización para adaptarse al contexto interno y externo, especialmente cuando nuevos riesgos aparecen, ciertos riesgos se cambian, mientras que otros desaparecen.

- **Facilita la mejora continua de la organización:** las organizaciones con una madurez en la gestión de riesgo, son aquellos que invierten a largo plazo y demuestran la normal realización de sus objetivos.

3.4.4 Marco de trabajo para la gestión del riesgo

El éxito de la gestión del riesgo dependerá de la eficacia del marco de gestión que proporciona las bases y arreglos para aplicarla en toda la organización a todos los niveles. El marco ayuda en la gestión de riesgos de manera efectiva a través de la aplicación del proceso de gestión de riesgos a diferentes niveles y dentro de contextos específicos de la organización. El marco garantiza que la información sobre el riesgo derivado del proceso de gestión del riesgo está adecuadamente informado y utilizado como base para la toma de decisiones y la rendición de cuentas en todos los niveles de la organización relevante.

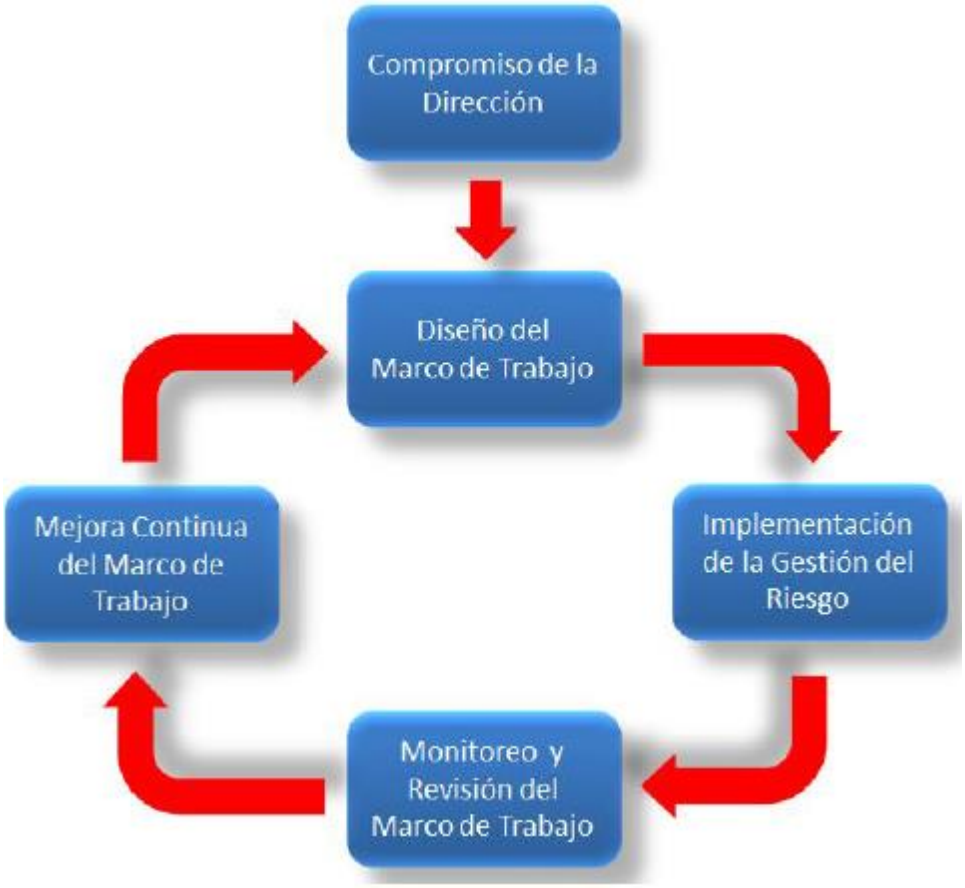
Esta cláusula describe los componentes necesarios del marco para la gestión de riesgos y la forma en que se relacionan entre sí de manera iterativa, como se muestra en la Figura 3.

La variedad, complejidad y naturaleza de los riesgos puede ser de muy diversa índole, por lo que éste estándar propone unas pautas genéricas sobre cómo gestionar los riesgos de forma sistemática y transparente.

El diseño y la implementación de la gestión de riesgos dependerán de las diversas necesidades de cada organización, de sus objetivos concretos, contexto, estructura, operaciones, procesos operativos, proyectos, servicios, etc.

La interpretación de estas pautas para realizar el diseño e implantación de la gestión de riesgos dependerá de las necesidades que tenga la organización, de sus objetivos, contexto, estructura, procesos operativos, proyectos, servicios, etc.

Figura 3 Marco de trabajo para la gestión de riesgos



Fuente: ISO 31000:2009

a. Compromiso de la dirección

Para asegurar la eficacia de la gestión de riesgos, se requiere un compromiso firme y sostenido por la dirección de la organización, así como la planificación estratégica para lograr el compromiso a todos los niveles, en esta fase la dirección debería:

- Definir y aprobar la política de gestión de riesgos
- Asegurar de que la política de la cultura y la gestión de riesgos de la organización están alineados
- Determinar los indicadores de rendimiento de gestión de riesgos que se alinean con los indicadores de desempeño de la organización
- Alinear los objetivos de gestión de riesgos con los objetivos y estrategias de la organización
- Asegurar el cumplimiento legal y regulatorio
- Asignar responsables y responsabilidades en los niveles apropiados dentro de la organización
- Asegurar de que los recursos necesarios se asignan a la gestión de riesgos
- Comunicar los beneficios de la gestión de riesgos a todas las partes interesadas; y
- Asegurar de que el marco para la gestión del riesgo sigue siendo apropiada.

b. Diseño del marco de trabajo

El diseñar un marco de trabajo, previo a iniciar la gestión de riesgos, ayuda de la siguiente forma:

- **Comprender la organización y su contexto:** Es importante evaluar y comprender tanto el contexto externo e interno de la organización, ya que éstos pueden influir significativamente en el diseño de la estructura.

- **Política de gestión de riesgos:** La política de gestión de riesgos debe establecer claramente los objetivos de la organización para, y el compromiso con la gestión del riesgo.

- **Rendición de cuentas:** La organización debe asegurarse que existe rendición de cuentas, la autoridad y la competencia adecuada para la gestión de riesgos, incluyendo la implementación y mantenimiento del proceso de gestión de riesgos y garantizar la eficacia y la eficiencia de adecuación de los controles.

- **La integración en los procesos de organización:** La gestión de riesgos debe formar parte de todas las prácticas y procesos de la organización de una manera que es pertinente, eficaz y eficiente.

- **Recursos:** La organización debe asignar recursos adecuados para la gestión de riesgos.

- **Establecimiento de la comunicación interna y los mecanismos de presentación de informes:** La organización debe establecer la comunicación interna y los mecanismos de información con el fin de apoyar y fomentar la rendición de cuentas y la propiedad de riesgo.

- **El establecimiento de la comunicación externa y la presentación de informes mecanismos:** La organización debe desarrollar e implementar un plan sobre cómo va a comunicarse con las partes interesadas externas.

c. Implementación de la gestión del riesgo

La gestión del riesgo se lleva a cabo, asegurando que el proceso de gestión de riesgos sea aplicado a todos los niveles y funciones pertinentes de la organización, como parte de las prácticas de la organización y procesos de negocio

d. Monitoreo y revisión del plan de trabajo

Para garantizar que la gestión de riesgos es eficaz y sigue apoyando el desempeño organizacional, la organización debe:

- Establecer medidas de desempeño
- Medir periódicamente el progreso y las desviaciones respecto al plan de gestión de riesgos
- Revisar periódicamente si el marco de gestión de riesgos, la política y el plan siguen siendo adecuados, dado el contexto interno y externo de las organizaciones
- Informar sobre los riesgos, los avances en el plan de gestión de riesgos y garantizar lo bien que la política de gestión de riesgos se está siguiendo
- Controlar la eficacia del marco de gestión de riesgos

e. Mejora continua del plan de trabajo

Con base a la revisión del plan de trabajo, se deben tomar decisiones acerca de cómo puede mejorarse el marco de gestión de riesgos, la política y el plan. Las decisiones deben conducir a mejoras en la cultura y gestión de riesgos de la organización.

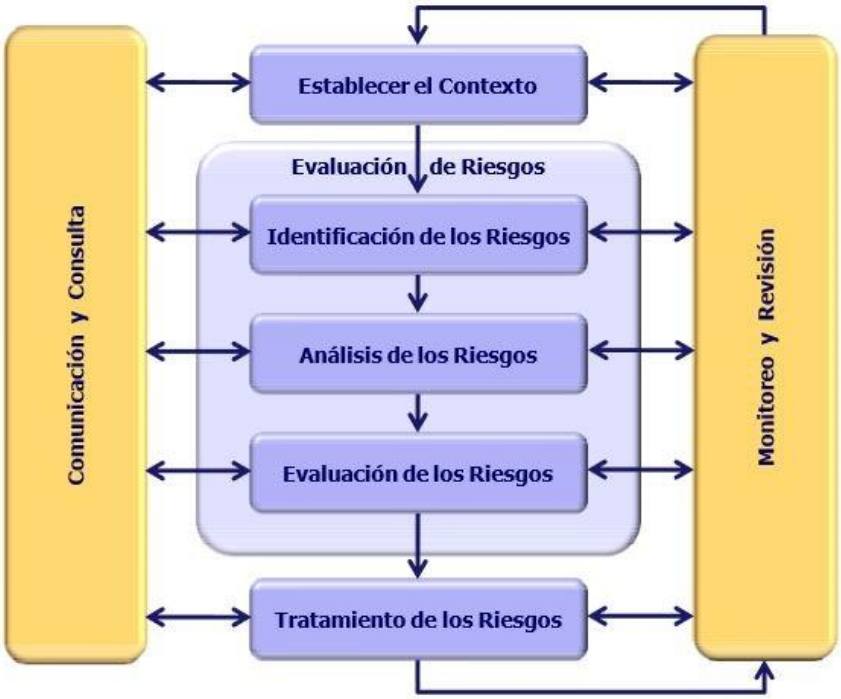
3.4.5 Proceso de gestión de riesgos

El proceso de gestión de riesgos consiste en aplicar métodos lógicos y sistemáticos para:

- Comunicación y consulta en todo el proceso
- Establecer el contexto
- Identificar, analizar, evaluar y tratar los riesgos
- Seguimiento y revisión del riesgo
- Registro y notificación de los resultados

El proceso de gestión de riesgos debe ser una parte integral de la gestión, se incorpora en la cultura, los procesos y las prácticas de gobierno y gestión de la organización.

Figura 4 Proceso de gestión de riesgos



Fuente: ISO 31000:2009

a. Comunicación y consulta

La Norma ISO 31000:2009 considera la comunicación y consulta como el primer punto del proceso, mostrando la gran relevancia del mismo e indicando que las comunicaciones y las consultas con las partes interesadas, tanto externas como internas a la organización, deben realizarse en todas las etapas del proceso de gestión de riesgos.

En esta fase del proceso, la información se identifica, capta y comunica de una forma y en un marco de tiempo, que permita a las personas llevar a cabo sus responsabilidades. Los sistemas de información facilitan la gestión de riesgos y la toma de decisiones y con ellos existe una comunicación eficaz fluyendo en todas las direcciones dentro de la organización.

Cabe mencionar que de nada sirve tener todo un proceso, políticas y procedimientos bien establecidos si no se comunican. La información se necesita a todos los niveles de la organización para identificar, evaluar y responder a los riesgos y por otra parte dirigir la entidad y conseguir sus objetivos.

b. Establecer el contexto

Al establecer el contexto, la organización lo alinea a sus objetivos, se definen los parámetros externos e internos que deben tenerse en cuenta en la gestión del riesgo, y establece los criterios de aplicación y de riesgo para el resto del proceso.

Mientras que muchos de estos parámetros son similares a los considerados en el diseño del marco de gestión de riesgos, al establecer el contexto para el proceso de gestión de riesgos, que deben ser considerados en mayor detalle y en particular la forma en que se relacionan con el ámbito de aplicación del proceso de gestión del riesgo en particular.

El contexto debe incluir parámetros internos y externos relevantes para la organización:

- **Establecimiento del contexto externo:** La comprensión del contexto externo es importante con el fin de garantizar que los objetivos y preocupaciones de los grupos de interés externos son considerados en el desarrollo de criterios de riesgo. Se basa en el contexto de toda la organización, pero con detalles específicos de los requisitos legales y reglamentarios, percepciones de los usuarios y otros aspectos de los riesgos específicos para el ámbito de aplicación del proceso de gestión de riesgos.

- **Establecimiento del contexto interno**: Es el ambiente interno, en el que la organización busca alcanzar sus objetivos, el proceso de gestión de riesgos debe estar alineada con la cultura, procesos, estructura y estrategia de la organización. contexto interno es cualquier cosa dentro de la organización

que pueden influir en la manera en que una organización va a gestionar el riesgo.

- **Establecimiento del contexto del proceso de gestión de riesgos:** Los objetivos, las estrategias, el alcance y los parámetros de las actividades de la organización, o las partes de la organización en la que se está aplicando el proceso de gestión de riesgos, deben establecerse.

- **Definición de los criterios de riesgo:** La organización debería definir los criterios que se utilizarán para evaluar la importancia del riesgo. Los criterios deben reflejar los valores de la organización, objetivos y recursos. Algunos criterios pueden ser impuestas por, o deriva de los requisitos legales y reglamentarios y otros requisitos que la organización suscriba. Los criterios de riesgo deben ser coherentes con la política de gestión de riesgos de la organización, se definen al comienzo de cualquier proceso de gestión de riesgos y se revisan continuamente.

c. Identificación de los riesgos

En esta fase del proceso, la organización debe identificar las fuentes de riesgo, áreas de impacto, eventos (incluyendo cambios en las circunstancias), causas y sus posibles consecuencias. El objetivo de este paso es generar una lista completa de los riesgos sobre la base de esos eventos que podrían crear, mejorar, prevenir, degradar, acelerar o retardar la consecución de objetivos. Es importante identificar los riesgos asociados a no perseguir una oportunidad. La identificación integral es fundamental, porque el riesgo de que no se identifica en esta etapa no se incluirá en el análisis adicional.

La identificación debe incluir riesgos aunque si su fuente está bajo el control de la organización o no, a pesar de que la fuente de riesgo o causa pueden no ser evidentes. La identificación de riesgos debe incluir el examen de los efectos reacción en cadena de consecuencias particulares, incluidas en cascada y los

efectos acumulativos. También se debe tener en cuenta una amplia gama de consecuencias, incluso si la fuente o causa del riesgo pueden no ser evidentes. Así como la identificación de lo que podría suceder, es necesario tener en cuenta las posibles causas y escenarios que muestran lo que pueden producirse consecuencias. Todas las causas y consecuencias significativas deben ser consideradas.

La organización debe aplicar herramientas de identificación de riesgos y técnicas que se adapten a sus objetivos y capacidades, así como a los riesgos que enfrentan. La información relevante y actualizada es importante en la identificación de riesgos, esto debe incluir información de antecedentes adecuada siempre que sea posible, las personas con conocimientos adecuados deben estar involucrados en la identificación de riesgos.

d. Análisis de los riesgos

El análisis de riesgos es un proceso que se utiliza para comprender la naturaleza, las fuentes y las causas de los riesgos identificados para estimar el nivel de riesgo, también se utiliza para estudiar los impactos y consecuencias y para examinar los controles que existen a la fecha.

El análisis del riesgo se puede realizar con diversos grados de detalle, dependiendo del riesgo, el propósito del análisis y la información, datos y recursos disponibles. El análisis puede ser cualitativo o cuantitativo, o una combinación de ellos, dependiendo de las circunstancias.

Las consecuencias y su posibilidad se pueden determinar modelando los resultados de un evento o grupo de eventos, o mediante extrapolación a partir de estudios experimentales o de los datos disponibles. Las consecuencias se pueden expresar en términos de impactos tangibles e intangibles. En algunos casos, se requiere más de un valor numérico o descriptor para especificar las consecuencias y su posibilidad en diferentes momentos, lugares, grupos o situaciones.

e. Evaluación de los riesgos

El propósito de la evaluación del riesgo es facilitar la toma de decisiones, basado en los resultados de dicho análisis, acerca de que riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento.

La evaluación del riesgo implica la comparación del nivel de riesgo observado durante el proceso de análisis y de los criterios del riesgo establecidos al considerar el contexto. Con base en esta comparación, se puede considerar la necesidad de tratamiento.

Las decisiones se deberían tomar de acuerdo con los requisitos legales, reglamentarios y otros. La evaluación del riesgo también puede tener como resultado la decisión de no tratar el riesgo de ninguna manera diferente del mantenimiento de los controles existentes.

Figura 5 Flujo del riesgo inherente y residual

Fuente: Elaboración propia con base al trabajo realizado

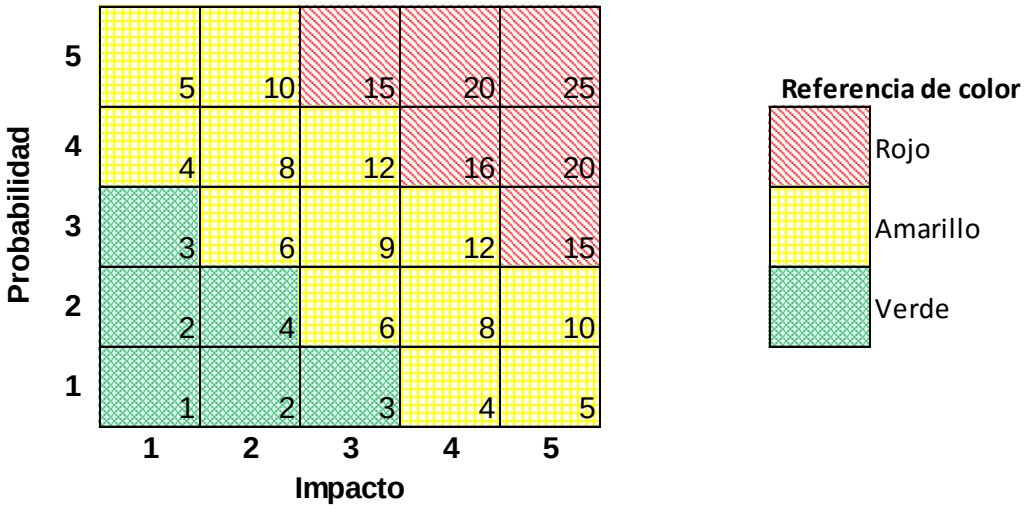
Luego de la evaluación de cada riesgo con sus respectivos controles, se obtiene una matriz la cual muestra la evaluación en cada uno de los criterios definidos.

Un medio que se utiliza para representar gráficamente los resultados obtenidos en la matriz de riesgos es el mapa de calor, esta representación gráfica está ordenada por cuadrantes que ayudan a la visualización del nivel de exposición de cada uno de los riesgos identificados y evaluados.

El siguiente modelo está basado con probabilidades e impacto en cinco niveles, donde los niveles de riesgo están presentados por un código de color, donde el rojo

representa un riesgo elevado, el amarillo un riesgo moderado y el verde un riesgo reducido.

Figura 6 Mapa de calor



Fuente: Elaboración propia con base al trabajo realizado

El mapa de calor descrito en la figura anterior se basa en cinco niveles siendo 1 muy bajo y 5 muy alto, para darle una valoración a los riesgos se multiplica probabilidad por impacto y el resultado se grafica en el mapa. Los criterios de parametrización deben ser elaborados por expertos y con experiencia para obtener los resultados deseados.

f. Tratamiento de los riesgos

Son las medidas que se toman en torno a un riesgo identificado y analizado, y está relacionado con las acciones preventivas o correctivas que se toman en torno a un riesgo. El tratamiento de los riesgos involucra una o más opciones para modificar los riesgos y la implementación de tales opciones para el caso en que los niveles de riesgo residual superen los límites del nivel de riesgo definido.

Para los riesgos significativos, una entidad deberá considerar típicamente las respuestas posibles dentro de una gama de opciones de respuesta, las cuales podrían ser:

- **Evitar:** para evitar un riesgo, se debe eliminar su probabilidad de ocurrencia o disminuir totalmente su impacto, es la decisión de no involucrarse o de retirarse de una actividad, con la finalidad de no quedar expuesto a ningún riesgo.
- **Mitigar:** es colocar puntos de control que ayuden a eficientar los procesos del negocio, así como aumentar la implicación de la dirección en la toma de decisiones y el seguimiento.
- **Compartir:** consiste en involucrar a un tercero en su manejo, quien en algunas ocasiones, puede absorber parte de las pérdidas ocasionadas por su ocurrencia e incluso responsabilizarse de la aplicación de las medidas de control para reducirlo, se puede mencionar los seguros o bien terciarizar los procesos de negocio.
- **Aceptar:** significa que no es necesario desarrollar medidas adicionales de prevención o protección del riesgo analizado, es aceptar el factor de riesgo, en torno a que se adapte a las tolerancias al riesgo establecidas.

Este componente del proceso tiene relación con la tolerancia al riesgo y costo beneficio; todo tipo de tratamiento implica un costo ya sea directo o indirecto y el mismo debe evaluarse bajo el criterio de costo beneficio, tomando en consideración el costo inicial del diseño e implementación, así como el costo que implica el mantenimiento del control o respuesta. Al evaluar controles que dan respuesta a un riesgo, se debe tener en mente que es lo que mitigan, si la probabilidad o el impacto.

g. Monitoreo y revisión

El proceso de administración de riesgos no tiene fin. Debe implementarse, monitorearse y mejorarse permanentemente, para monitorear el comportamiento de los riesgos en los procesos y determinar qué tan efectivas han sido las medidas de

tratamiento, los responsables de su manejo utilizan los indicadores de riesgo, para establecer cómo se aplica el proceso de administración de riesgos en toda la empresa, se puede efectuar un proceso de autoevaluación o realizar una evaluación con personal ajeno a la administración, una mirada independiente que garantiza un análisis crítico sobre lo acertado del proceso de administración de riesgos y su efectividad.

Con el fin de asegurar que la gestión integral de riesgo es eficaz y continúa siendo vigente para las necesidades particulares de la empresa, la organización mide el desempeño de la gestión de riesgo mediante el uso de indicadores, tales como los mapas de calor generados, los cuales deben ser revisados periódicamente, analizando los cambios que puedan observarse, analizando y dando respuesta a las variaciones presentadas. Igualmente, se debe realizar un monitoreo a la implementación y efectividad de los planes de tratamiento a los riesgos que no contaban con controles que lo mitigan o que no eran efectivos.

Tomando en cuenta el resultado de la supervisión permanente, periódica y de apoyo, la organización deberá tomar decisiones sobre la mejora continua que deba realizarse al marco y proceso de gestión de riesgos, con la finalidad de alcanzar un mayor grado de madurez y mejorar la cultura de la organización en cuanto a la administración del riesgo.

3.5 Relación con otros estándares ISO

El estándar ISO 31000:2009 por ser una norma que brinda principios guías genéricas para la gestión de riesgos se soporta en otras normas que permiten reforzar la implementación de la norma, de igual forma sirve como referencia a otros estándares que basan su enfoque en gestión de riesgos, una característica importante de todas las normas es que pretenden ser aplicables a cualquier organización, independientemente de su tipo o tamaño, o los productos y servicios que ofrece.

3.5.1 ISO 27005:2011, “Gestión de riesgos de seguridad de la información”

Es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de la información, la norma proporciona directrices para la implementación en la empresa basada en los principios de integridad, confidencialidad y disponibilidad. Para un una mejor comprensión del estándar, se requiere el conocimiento de los conceptos, modelos, procesos y terminologías descritas en la ISO 27001 “Seguridad de la información”

3.5.2 ISO 9001:2015 “Sistemas de gestión de calidad – requisitos”

Esta norma indica los requisitos para un sistema de gestión de calidad cuando una organización necesita demostrar su capacidad para proporcionar de forma coherente productos y servicios que satisfagan al cliente, en esta norma la gestión de riesgos se vuelve fundamental ya que el objetivo es alcanzar un perfeccionamiento continuo de la calidad de sus productos o servicios.

3.5.3 Guía ISO 73:2009, “Gestión de riesgos – vocabulario”

Proporciona las definiciones de los términos genéricos relacionados con la gestión de riesgos. Su objetivo es fomentar una comprensión mutua y constante con un enfoque coherente de la descripción de las actividades relacionadas con la gestión del riesgo, y el uso de una terminología uniforme en los procesos y marcos que se ocupan de la gestión de riesgos.

3.5.4 ISO 31010:2009, “Técnicas de evaluación de riesgos”

La norma está directamente relacionada con ISO 31000:2009, debido a que proporciona orientación sobre la selección de técnicas sistemáticas para la evaluación de riesgos, incluye 31 técnicas y/o herramientas que pueden ser utilizadas en las fases de identificación, análisis y evaluación de riesgos, estás técnicas se detallan en la figura 7 donde se indica su nivel de aplicabilidad en cada fase.

Figura 7 Aplicabilidad de las herramientas utilizadas para la evaluación de riesgos

No.	Herramienta/técnica	Identificación de riesgos	Análisis de riesgos			Evaluación de riesgos
			Consecuencia	Probabilidad	Nivel de riesgo	
1	Lluvia de ideas	M	N	N	N	N
2	Entrevistas esetructuradas o semi-estructuradas	M	N	N	N	N
3	Delphi	M	N	N	N	N
4	Listas de verificación	M	N	N	N	N
5	Análisis preliminar de peligro	M	N	N	N	N
6	Estudios de peligro y operabilidad (HAZOP)	M	M	A	A	A
7	Análisis DE peligro y puntos de control crítico (HACCP)	M	M	N	N	M
8	Evaluación de riesgo ambiental	M	M	M	M	M
9	¿Qué si? Estructurado (SWIFT)	M	M	M	M	M
10	Análisis de escenario	M	M	A	A	A
11	Análisis de impacto al negocio	A	M	A	A	A
12	Análisis de causa raíz	N	M	M	M	M
13	Análisis de efecto en modo de falla	M	M	M	M	M
14	Análisis de arbol de fallas	A	N	M	A	A
15	Análisis de árbol de eventos	A	M	A	A	N
16	Análisis causa y consecuencia	A	M	M	A	A
17	Análisis causa y efecto	M	M	N	N	N
18	Análisis de capas de protección (LOPA)	A	M	A	A	N
19	Árbol de decisión	N	M	M	A	A
20	Análisis de confiabilidad humana	M	M	M	M	A
21	Análisis de "corbata"	N	A	M	M	A
22	Análisis centrado en la confiabilidad	M	M	M	M	M
23	Análisis de circuito	A	N	N	N	N
24	Análisis Markov	A	M	N	N	N
25	Simulación Monte Carlo	N	N	N	N	M
26	Estadísticas y redes Bayesianas	N	M	N	N	M
27	Curvas FN	A	M	M	A	M
28	Índices de riesgo	A	M	M	A	M
29	Matriz de consecuencia / probabilidad	M	M	M	M	A
30	Análisis costo / beneficio	A	M	A	A	A
31	Análisis de decisión multi criterio (MCDA)	A	M	A	M	A

M = Muy aplicable

A = Aplicable

N = No aplica

Fuente: ISO 31010:2009

CAPÍTULO IV
EVALUACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS, EN UNA EMPRESA DE SERVICIOS ESPECIALIZADA EN EL PROCESAMIENTO DE DOCUMENTOS EN FORMA ELECTRÓNICA, UTILIZANDO LA NORMATIVA ISO 31000:2009
(CASO PRÁCTICO)

4.1 Antecedentes

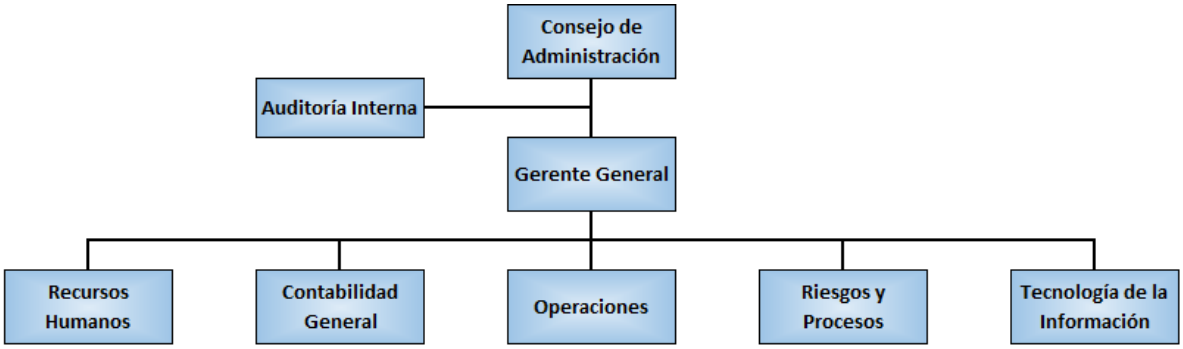
La empresa La Digital S.A, fue creada en octubre de 1995 iniciando sus operaciones el mismo año, las oficinas se encuentran ubicadas en la 20 avenida 10-50 Edificio el Negociador en la zona 10 de la ciudad capital. Su objetivo principal es brindar el servicio de procesamiento de documentos de forma electrónica al sistema bancario nacional para la compensación bancaria, su visión es establecerse como eje estratégico para el sector financiero en el procesamiento de documentos, para así ofrecer servicios innovadores y confiables a sus clientes.

La Digital S.A. es una empresa guatemalteca que brinda servicios al sistema bancario nacional y su misión es promover a través de servicios especializados en el procesamiento de documentos en forma electrónica, la generación y preparación de información para la compensación bancaria, incorporando innovación tecnológica para beneficio de sus clientes y a su vez generando bienestar para los colaboradores que en ella laboran. Los valores que la identifican y que están plasmados como parte de su cultura son la integridad, servicio al cliente, calidad en el servicio e innovación.

Esta empresa está conformada por una asamblea general de accionistas, un consejo de administración, un gerente general y un gerente en cada una de las áreas; actualmente laboran en la empresa 125 empleados, distribuidos de la forma siguiente: 45 personas de administración, y 80 personas en el área de operaciones.

Su estructura organizacional es la siguiente:

Figura 8 Estructura organizacional de "La Digital, S.A."



Fuente: Elaboración propia con base al trabajo realizado

Dentro de la organización existe un departamento de auditoría interna, el cual está integrado por cuatro personas y estructurado de la siguiente forma:

- Auditor Interno
- Auditor de sistemas
- Auditor de riesgos y operaciones
- Auditor administrativo

Figura 9 Estructura del departamento de auditoría interna

Fuente: Elaboración propia con base al trabajo realizado

Derivado que los procesos del negocio son directamente para el sistema bancario nacional, en julio de 2011 se inició con el proceso de la implementación del sistema de gestión del riesgo, por lo cual la gerencia de riesgos y procesos trabaja desde

esa fecha impartiendo capacitaciones, talleres entre otras actividades para concientizar a los colaboradores de la empresa para que el proyecto sea exitoso.

Como parte del plan de trabajo del departamento de auditoría interna, se tiene planificada una evaluación a la gestión de riesgos, tomando como base la norma ISO 31000:2009, debido a que la norma se divide en tres secciones se decidió realizar la auditoría en tres fases, el trabajo consistirá en auditar específicamente el proceso de gestión de riesgos, el cual deberá brindar un informe donde se demuestren los hallazgos detectados dicha auditoría será ejecutada en el tercer trimestre del año 2016.

ÍNDICE DE PAPELES DE TRABAJO

PT.	M	
Hecho por:	Sv	29/07/2016
Revisado:	Wp	01/08/2016

La Digital, S.A.

Auditoría interna

Cédula de marcas de auditoría

Marca	Descripción
✔	Verificado conforme
✘	Verificado Inconforme
■	No verificado
⊘	No aplica
●	En seguimiento de implementación
⊖	No implementado
↻	Cotejado con
ⓘ	Informado

4.2 Nombramiento del auditor interno

PT.	N	
Hecho por:	Sv	29/07/2016
Revisado:	Wp	01/08/2016

NOMBRAMIENTO No. 04/2016

PARA: **Sender Alfredo Velásquez Hernández – auxiliar de auditoría**

DE: **Wendy Paredes – Auditora interna**

ASUNTO: **Auditoría al proceso de gestión de Riesgos**

FECHA: **29/07/2016**

I **ÁREA A AUDITAR: GERENCIA DE RIESGOS Y PROCESOS**

II **ACTIVIDAD:**
Revisar, analizar y validar la gestión de riesgos, basado en las disposiciones que indica el estándar ISO 31000:2009 enfocando esta evaluación únicamente al proceso de gestión de riesgos.

III **OBJETIVO:**
Desarrollar apropiadamente las pruebas para validar la eficiencia y efectividad del proceso de gestión de riesgos, para asegurar que todos los componentes del proceso están identificados y apropiadamente administrados.

IV **PERÍODO DE REVISIÓN:**
Tercer trimestre 2016

V **ESPECIFICACIÓN:**
Este proyecto debe iniciarse el día lunes 1 de agosto del presente año y entregar resultados el día 16 de agosto del presente año.

Muy atentamente,

Licda. Wendy Paredes
Auditora Interna

4.3 Planificación de la auditoría

PT.	P	
Hecho por:	Sv	01/08/2016
Revisado:	Wp	03/08/2016

Para el trabajo de evaluación al proceso de gestión de riesgos tomando como referencia el estándar ISO 31000:2009, se requiere la inversión de 118 horas hombre distribuidas entre el auditor designado y el jefe de auditoría.

Período: del 1 al 16 de agosto de 2016

Descripción	Fecha	Auxiliar de auditoría	Auditora interna	Total
Planificación administrativa	29 de julio	8	1	9
Evaluación del control interno	1 y 2 de agosto	16	1	17
Ejecución de la auditoría	3 al 11 de agosto	56	0	56
Elaboración del borrador del informe	12 de agosto	8	0	8
Discusión del informe	16 de agosto	8	4	12
Informe Final y recomendaciones	17 de agosto	8	8	16
Total de horas invertidas		**104**	**14**	**118**

La Digital, S.A.
Programa de auditoría
Proceso de Gestión de Riesgos
Gerencia de Riesgos y Procesos

PT.	A 1 de 3	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

Objetivo: Verificar la conformidad del proceso de gestión de riesgos implementado de acuerdo con el estándar ISO 31000:2009.

Alcance: Revisar cada uno de los componentes del proceso de gestión de riesgos, verificando la eficiencia y efectividad de la información y ejecución del proceso

Los siguientes procedimientos deberán ser aplicados de forma sistemática, analítica y objetivamente, con el fin de lograr el objetivo del mismo.

No.	Procedimiento	Ref.	Pág.
Comunicación y consulta			
1.	Analice los procesos de comunicación y consulta que deben de tenerse dentro de la gestión de riesgos.	C1-1	76
2.	Verifique la periodicidad de los reportes de la gerencia de riesgos y procesos al comité de riesgos	C1-1	76
3.	Verifique la periodicidad de los reportes del comité de riesgos al consejo de administración	C1-2	77
Establecimiento del contexto			
4.	Verifique que se tenga establecido el nivel de tolerancia al riesgo	C2-1	79
5.	Verifique que se tenga establecido niveles de impacto	C2-2	80
6.	Verifique que se tenga establecido niveles de probabilidad	C2-3	81
7.	Evalúe las metas y objetivos de las actividades del proceso de gestión de riesgos	C2-6	84

PT.	A 2 de 3	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

No.	Procedimientos	Ref.	Pág.
8.	Verifique los responsables del proceso de gestión de riesgos	C2-6	84
9.	Verifique que se cuente con un alcance definido para el proceso de gestión de riesgos	C2-6	84
Identificación de riesgos			
10.	Verifique que se cuente con categorías de riesgo operacional	C3-1	86
11.	Verifique que se cuente con listado de eventos, causas y posibles consecuencias	C3-2	87
12.	Verifique las técnicas utilizadas en la identificación de riesgos	C3-3	88
Análisis de riesgos			
13.	Verifique que se cuente con listado de niveles de categorías de riesgos	C4-1	90
14.	Verifique la técnica utilizada en el análisis de riesgos	C3-3	88
Evaluación de riesgos			
15.	Verifique que se cuente con una matriz de riesgos	C5-1	92
16.	Verifique el cuales son los aspectos que deben considerarse para considerar riesgos que requieren tratamiento y su identificación en la matriz	C5-1	92
17.	Verifique que se cuente con mapas de calor de riesgos	C5-2	93
Tratamiento de riesgos			
18.	Verifique que se cuente con planes de tratamiento del riesgo y que cumpla con lo siguiente: • riesgo asociado	C6-1	95

PT.	A 3de 3	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

No.	Procedimientos	Ref.	Pág.
	• Servicio asociado • Responsable • Fecha propuesta • Pasos para la implementación (plan de acción)	C6-1	95
19.	Verifique si se cuenta con otras opciones de tratamiento	C6-2	96
Monitoreo y revisión			
20.	Verifique que tipo de actividades de monitoreo y revisión se realizan en la empresa	C7-1	98
21.	Verifique las actas del comité de riesgos y valide los puntos relacionados al monitoreo de eventos de riesgo	C7-1	98
22.	Verifique las actas del comité de riesgos y valide si existen puntos que relacionados a la identificación de riesgos nuevos.	C7-1	98
Comité de riesgos			
23.	Verifique que exista acta de constitución del comité de riesgos de la empresa	D1	100
24.	Verifique que exista acta de aprobación del comité de riesgos de la empresa por parte del consejo de administración	D2	101
Otros procedimientos			
25.	Realice un análisis de brechas del proceso de gestión de riesgos, en base a la evidencia observada	E1	103
26.	Genere una cédula de aspectos a mejorar	E2	105

La Digital, S.A.

Cuestionario de Control Interno

Proceso de: gestión de riesgos

Gerencia de riesgos y procesos

Gerente: Lic. Víctor García

PT.	B 1 de 6	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

Objetivo:

- Asegurar que todas las exposiciones materiales de riesgo están identificadas y apropiadamente administradas a través de sus controles relacionados.

- Desarrollar apropiadamente las pruebas para validar la eficiencia y efectividad del control vigente.

Favor de contestar el presente cuestionario de evaluación de control interno de una forma objetiva. Marque con una "X" la respuesta y donde corresponda aplique un pequeño comentario para ampliar la respuesta.

No.	Cuestionamiento	SI	No	Comentario
1.	¿Qué entiende por riesgo?	X		**Posibilidad que una amenaza se materialice**
2.	¿Existe actualmente una gestión de riesgos?	X		
3.	¿Qué entiende por gestión o administración de riesgos?	X		**La evaluación y análisis de riesgos que pueden impactar en la empresa.**
4.	¿Se cuenta con un manual para la gestión del riesgo?	X		**Manual de normas y políticas para la gestión de riesgos**

PT.	B 2 de 6	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

No.	Cuestionamiento	SI	No	Comentario
5.	¿Cuál es el marco de referencia utilizado para la gestión del riesgo de la empresa?	X		**El marco de referencia para construir la estructura de gestión de riesgos en la empresa, fue el estándar ISO 31000:2009**
6.	¿Se cuenta actualmente con Matrices de Riesgo?	X		**Se tiene una matriz de riesgo operativo y una de riesgo tecnológico**
7.	¿Se lleva periódicamente retroalimentación respecto a temas de riesgos al personal de la organización?	X		**Se tiene un plan de capacitaciones dentro del cual se consideran temas de riesgos**
8.	¿Quién es el ente encargado de velar por la capacitación en temas de riesgos para el personal de la empresa?	X		**La gerencia de riesgos y procesos, apoyándose en la gerencia de recursos humanos**
9.	¿Se tiene definido cuales son los riesgos a los cuales puede afrontarse la empresa dado el giro del negocio?	X		**Se pueden visualizar en la matriz de riesgos**
10.	¿Se cuenta con una adecuada segregación de funciones dentro de la gestión de riesgos?	X		

PT.	B 3 de 6	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

No.	Cuestionamiento	SI	No	Comentario
11.	¿Se tiene establecido los parámetros para la gestión de riesgos y están estos debidamente aprobados?	X		**Se cuenta con la declaración de los parámetros de riesgos donde se observa como está establecido.**
12.	¿Se tiene definido cuál es el alcance de la gestión de riesgos?	X		**Los procesos críticos que resulten del análisis de impacto al negocio**
13.	¿Se tiene definido el nivel de tolerancia al riesgo y está debidamente aprobado?	X		**Se observa dentro de la declaración de parámetros de riesgo.**
14.	¿Quién es el encargado de establecer y autorizar el nivel de tolerancia al riesgo?	X		**El Consejo de administración**
15.	¿Se ha procedido a determinar y analizar el nivel de cultura de riesgos que existe en la organización?	X		
16.	¿Cuenta la gerencia de riesgos y procesos con indicadores para monitorear el desempeño de la gestión de riesgos?		X	**Únicamente se mide el desempeño de la gestión de riesgo mediante el uso de los mapas de calor generados para cada servicio de misión crítica para evaluar variaciones en los riesgos, también se monitorea la implementación de los planes de tratamiento.**

PT.	B 4 de 6	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

No.	Cuestionamiento	SI	No	Comentario
17.	¿Se cuenta con mapas de calor por cada servicio de misión crítica?	X		
18.	¿Cuántas fases contempla el modelo de gestión de riesgos para la empresa?	X		**7 fases**
19.	¿Se tiene establecido los procesos de comunicación y consulta que deben darse dentro de la gestión de riesgos?	X		**Se cuentan con reportes que se presentan al comité de riesgos**
20.	¿Se tiene definido cuales son los criterios de evaluación de frecuencia, impacto, criticidad y sensibilidad de los riesgos identificados?	X		**Se observa dentro de la declaración de parámetros de riesgo.**
21.	¿Cuál fue el criterio para establecer los niveles de frecuencia, impacto, criticidad y sensibilidad para los riesgos asociados a los servicios críticos de la empresa?	X		**La frecuencia y el impacto se establecieron en base al juicio de expertos (gerencia general y gerentes), además de la asesoría de un experto en el tema**
22.	¿Se cuenta con un catálogo sobre fuentes de riesgo para la gestión de riesgos?	X		**Para riesgo operacional, se tomaron de base las categorías de riesgo de Basilea II**

PT.	B 5 de 6	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

No.	Cuestionamiento	SI	No	Comentario
23.	¿Se cuenta con un listado de amenazas y vulnerabilidades para el riesgo operativo?		X	**Para el riesgo operativo no se utilizó, sin embargo para riesgo tecnológico si se cuenta.**
24.	¿Se cuenta con planes de tratamiento para los riesgos con nivel de impacto medio y alto?	X		**Se cuenta con un formato donde están debidamente identificados los riesgos que requieren tratamiento.**
25.	¿Se tienen identificados en la matriz los riesgos que están aplicando tratamiento de riesgo?		X	**En la matriz no, únicamente en el formato**
26.	¿Se tiene definido que debe de contemplar un plan de tratamiento a riesgos?	X		**Riesgo y servicio asociado, responsable, fecha de resolución y descripción del plan de acción**
27.	¿Se cuenta con líneas de comunicación que permitan de forma oportuna comunicar sobre los planes de tratamiento y el resultado de los mismos?	X		**Se realiza en el comité de riesgos**
28.	¿Queda registro del monitoreo que se hace a la gestión de riesgos?	X		**En las actas de comité de riesgos**

PT.	B 6 de 6	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

No.	Cuestionamiento	SI	No	Comentario
29.	¿Con que periodicidad se informa al comité de riesgos sobre cambios en los riesgos?	X		**Cada 3 meses**
30.	¿Con que periodicidad se informa al consejo de administración sobre cambios en los riesgos?	X		**Cada 6 meses**
31.	¿Cada cuánto tiempo se realiza la actualización y mejora a la matriz del riesgo operativo?	X		**Una vez al año**
32.	¿Cuenta con registro formal de identificación de riesgos nuevos?		X	**Únicamente queda en punto de acta**
33.	¿Cuenta con registro de revisión de la efectividad controles?		X	**No se cuenta con registro formal**
34.	¿Se cuenta con acta de constitución para el comité de riesgos?	X		
35.	¿Se llevan reuniones periódicas del comité de riesgos?	X		**Una vez al mes**
36.	¿Se realiza acta de comité de riesgos en cada reunión que es llevada a cabo?	X		

PT.	B1 1 de 2	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

La Digital, S.A.

Auditoría interna

Cédula narrativa del cuestionario de control interno

El día miércoles 03 de agosto siendo las 09:00 horas se realizó una entrevista con el Licenciado Víctor García, quien ocupa el cargo de gerente de riesgos y procesos, para dar respuesta a un cuestionario de control interno, mismo que acepto realizar sin ningún inconveniente.

El motivo de la entrevista corresponde a la ejecución de la auditoría al proceso de gestión de riesgos.

El cuestionario se compone de treinta y seis interrogantes, partiendo de preguntas de carácter general, continuando con preguntas más específicas con la gestión de riesgos, las respuestas obtenidas se detallan de la siguiente manera:

- Indicó que la posibilidad que una amenaza se materialice lo considera como un riesgo, asimismo indicó que la gestión o administración de riesgos comprende la evaluación y análisis de riesgos que puedan impactar a la empresa.
- Actualmente existe si una gestión de riesgos dentro de la empresa, iniciando en el año 2011, gestión que se mejora con el paso del tiempo, actualmente cuenta con un manual de normas y políticas para el conocimiento del personal.
- El marco de referencia utilizado desde sus inicios es el estándar ISO 31000:2009, modelo que cuenta con 7 fases, también cuenta con la declaración de parámetros de la gestión de riesgos debidamente aprobado

PT.	B1 2 de 2	
Hecho por:	Sv	03/08/2016
Revisado:	Wp	05/08/2016

- por el Consejo de Administración y comunicado por el gerente general, documento donde se puede observar los criterios de evaluación de la gestión y cuentan con matrices donde se observan los riesgos que puede afrontar la empresa y se actualizan una vez al año, enfocado en los procesos críticos del negocio.
- Cuenta con planes de capacitación relacionados con riesgos y se apoya en la gerencia de recursos humanos para su realización.
- Para identificar los planes de tratamiento cuentan con un formato establecido para ubicarlos de forma más rápida.
- Para comunicar los resultados cuentan con reportes que se presentan al comité de riesgos debidamente constituido, estos quedan registrados en las actas de comité de riesgos, la periodicidad de comunicación de resultados es cada 3 meses, sin embargo el comité se reúne de forma mensual para tratar otros temas relacionados. Para comunicar los resultados al Consejo de Administración se realiza cada 6 meses

El gerente de riesgos y procesos indicó que no cuentan con indicadores para monitorear el desempeño de la gestión, únicamente utilizan los mapas de calor para ver el comportamiento de los riesgos, adicional indicó que no hay registro formal de identificación de riesgos nuevos y revisión de efectividad de controles, únicamente son tratados en reunión de comité.

La entrevista finalizó el mismo día, siendo las 11:30 horas, firmando de conformidad con lo descrito en la presente narrativa.

Lic. Víctor García
Gerente de riesgos procesos

Sender Velásquez
Auxiliar de auditoría

PT.	C	
Hecho por:	Sv	08/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.

Auditoría interna

Proceso de Gestión de Riesgos, según ISO 31000:2009

PT.	C1	
Hecho por:	Sv	08/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.

Auditoría interna

Comunicación y consulta

No.	Descripción	Ref.	Pág.
1	Reportes del comité de riesgos	C1-1	76
2	Reportes de la gerencia de riesgos	C1-2	77

PT.	C1-1	
Hecho por:	Sv	08/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.

Auditoría interna

Reportes del comité de riesgos

No.	Nombre de reporte	Periodicidad	Reporta a
1	Matriz de riesgos y sus cambios	Semestral	Consejo de administración
2	Mapa de calor de riesgos		
3	Efectividad de los planes de tratamiento		
4	Mejoras realizadas a la administración de riesgos		
5	Cumplimiento de políticas y procedimientos de riesgos		

Conclusión: Se verificó la información y comunicación de la misma al ente competente, no observándose inconsistencia alguna.

PT.	C1-2	
Hecho por:	Sv	08/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.

Auditoría interna

Reportes de la gerencia de riesgos

No.	Nombre de reporte	Periodicidad	Reporta a
1	Matriz de riesgos y sus cambios	Trimestral	Comité de Riesgos
2	Monitoreo de la efectividad de los planes de tratamiento		
3	Mejoras realizadas a la administración de riesgos		
4	Efectividad de capacitación y sensibilización en temas relacionados a riesgos		

Conclusión: Se verificó la información y comunicación de la misma al ente competente, no observándose inconsistencia alguna.

PT.	C2	
Hecho por:	Sv	08/08/2016
Revisado:	Wp	12/08/2013

La Digital, S.A.

Auditoría interna

Establecimiento del contexto

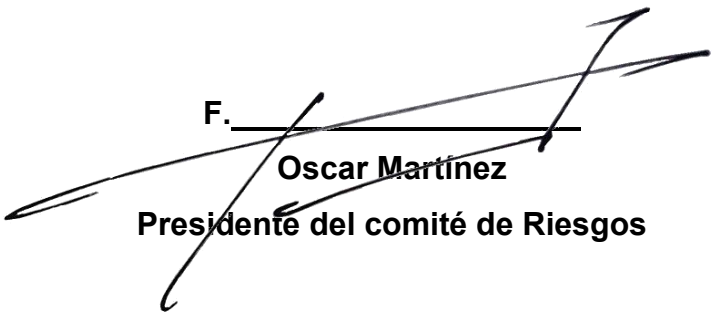
La Digital, S.A.

Declaración de parámetros de riesgo

PT.	C2-1	
Hecho por:	Sv	09/08/2016
Revisado:	Wp	12/08/2016

Declaración:

La empresa denominada La Digital, S.A. definió como nivel de tolerancia al riesgo, un impacto de hasta Q25,000.00, mismo que es el máximo que cubre nuestra póliza de seguro ante cualquier eventualidad. Para el efecto, los criterios de impacto de acuerdo a los eventos que puedan generarse y materializarse, están con base a las siguientes consideraciones aprobadas por el Consejo de Administración: hasta Q10,000.00 impacto bajo, hasta Q20,000.00 impacto medio, y por arriba de Q20,000.00, como un impacto alto, también se establece como punto de referencia la probabilidad de eventos de uno a tres en un mes, siendo uno bajo y tres alto. Los niveles de criticidad de la información son dos, crítico y no crítico, siendo crítico cuando está relacionado con los procesos del negocio. Los niveles de sensibilidad son tres: público, interno, y confidencial. Para la determinación de los eventos, así como la frecuencia de su ocurrencia se llevan bitácoras de registros que se proceden a evaluar cada tres meses para la evaluación correspondiente y actualización de la matriz de riesgos.



F._____

Oscar Martínez

Presidente del comité de Riesgos

PT.	C2-2	
Hecho por:	Sv	09/08/2016
Revisado por:	Wp	12/08/2016

La Digital, S.A.

Auditoría interna

Niveles de impacto

Niveles de impacto		
Código	**Criterio**	**Descripción**
1	Bajo	Aplica si las pérdidas financieras o si el cambio adverso o si al materializarse el riesgo, los impactos son hasta Q10,000.00.
2	Medio	Aplica si las pérdidas financieras o si el cambio adverso o si al materializarse el riesgo, los impactos son hasta Q20,000.00.
3	Alto	Aplica si las pérdidas financieras o si el cambio adverso o si al materializarse el riesgo, los impactos son mayores a Q20,000.00.

Conclusión: En la evaluación de los niveles de impacto, no se observó inconsistencia alguna debido a que son consistentes con la declaración de parámetros de riesgo (C2-1).

PT.	C2-3	
Hecho:	Sv	09/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.

Auditoría interna

Niveles de probabilidad

Niveles de probabilidad		
Código	**Criterio**	**Descripción**
1	Bajo	Aplica cuando el evento se registra una vez en un mes
2	Medio	Aplica cuando el evento se registra dos veces en un mes
3	Alto	Aplica cuando el evento se registra tres o más en un mes

Conclusión: En la evaluación de los niveles de probabilidad no se observó inconsistencia alguna debido a que son consistentes con la declaración de parámetros de riesgo (C2-1).

PT.	C2-4	
Hecho por:	Sv	09/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.

Auditoría interna

Niveles de criticidad

Categoría de criticidad		
Código	**Criticidad**	**Descripción**
1	Critica	Información relacionada con los procesos críticos del negocio
2	No critica	Información no relacionada con los procesos críticos del negocio

Conclusión: En la evaluación de las categorías de criticidad no se observó inconsistencia alguna debido a que son consistentes con la declaración de parámetros de riesgo (C2-1).

PT.	C2-5	
Hecho:	Sv	09/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Niveles de sensibilidad

Categoría de sensibilidad		
Código	**Criterio**	**Descripción**
1	Pública	Información destinada para el conocimiento del público en general.
2	Interna	Información destinada para el conocimiento de los colaboradores en el desarrollo diario de sus funciones
3	Confidencial	Información relacionada con estrategias del negocio.

Conclusión: En la evaluación de las categorías de sensibilidad no se observó inconsistencia alguna debido a que son consistentes con la declaración de parámetros de riesgo (C2-1).

PT.	C2-6	
Hecho por:	Sv	09/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Contexto del proceso de gestión de riesgo operativo

Contexto del proceso de gestión de riesgos	
Metas y objetivos:	- Identificar escenarios de riesgos que pudieran afectar los procesos críticos de la empresa - Analizar los diferentes riesgos identificados y valorar su nivel de riesgo para la empresa - Evaluar la aceptación de los riesgos analizados e identificar si requieren tratamiento o no - Establecer el tipo de tratamiento para los riesgos que lo requieren
Responsables del proceso:	Gerencia de riesgos y procesos
Alcance:	Procesos críticos resultantes del análisis por parte de los expertos en el proceso
Período de tiempo del análisis y evaluación:	1 año
Período de tiempo de vigencia de las estimaciones de riesgo:	1 año
Metodología de análisis y evaluación de riesgos	Se multiplicará probabilidad por impacto, el resultado será el nivel de exposición
Identificar y especificar las decisiones que se deberán tomar	Se deben identificar los riesgos que requieren tratamiento, con especial énfasis en los riesgos con exposición 3 en adelante

Conclusión: En la evaluación del contexto del proceso de gestión de riesgo operativo, no se observó inconsistencia alguna.

PT.	C3	
Hecho por:	Sv	09/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.

Auditoría interna

Identificación de riesgos

PT.	C3-1	
Hecho por:	Sv	09/08/2016
Revisado por:	Wp	12/08/2016

La Digital, S.A.

Auditoría Interna

Categorías para identificación de riesgos

Categorización de Riesgo	Descripción
Fraude interno	Apropiación indebida de activos de la entidad o incumplir leyes o políticas para beneficio propio.
Fraude externo	Actos realizados por una persona externa a la entidad, que buscan defraudar, o apropiarse indebidamente de activos.
Relaciones laborales y seguridad en el puesto de trabajo	Actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y en general la legislación vigente sobre la materia.
Clientes, productos y prácticas empresariales	Incumplimiento negligente o involuntario de una obligación frente a los clientes y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos materiales	Pérdidas derivadas de daños sufridos en activos materiales, como consecuencia de desastres naturales u otros acontecimientos.
Incidencias en el negocio y fallo en los sistemas	Pérdidas derivadas de incidentes por fallas en los sistemas (problemas de hardware, software y telecomunicaciones).
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones.

Conclusión: En la evaluación de las categorías para identificación de riesgos no se observó inconsistencia alguna debido a que son consistentes con la clasificación de Basilea II.

PT.	C3-2	
Hecho por:	Sv	09/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Listado de eventos, causas y posibles consecuencias

Evento	Fraude interno
	Fraude externo
	Relaciones laborales y seguridad en el trabajo
	Clientes, productos y prácticas empresariales
	Daños en activos materiales
	Fallo en sistemas
	Ejecución, entrega y gestión de procesos
	Interrupción de servicios
Causa	Maliciosa
	Accidental
	Error
	Falla
	Natural
	Requerimiento externo
Posible consecuencia	Asignación incorrecta de roles o perfiles de usuarios
	Denegación de servicios por ataques informáticos
	Desastres naturales o siniestros causados por el hombre
	Falla de software en la transmisión de los archivos hacia los clientes
	Fallas y/o errores en la aplicación de parches y/o actualizaciones
	Fallo en hardware
	Fallo en software
	Interrupción de los servicios que impidan la configuración de los sistemas
	Interrupción del negocio en el proceso
	Pérdida total de manuales y documentos que soportan la administración
	Procesos incorrectos de mantenimiento en hardware o software
	Requerimientos no atendidos en forma oportuna y/o de forma incorrecta

PT.	C3-3	
Hecho por:	Sv	09/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Técnicas utilizadas para la identificación de riesgos

No.	Técnica	Descripción
1	Índices de riesgo	Técnica con enfoque cualitativo para priorizar y comparar riesgos.
2	Matriz de consecuencia/probabilidad	Técnica utilizada para priorizar riesgos a través de una combinación de calificaciones cualitativas de consecuencias y probabilidades para producir un nivel de riesgo o calificación de riesgo.

Conclusión: En la evaluación de las categorías para identificación de riesgos no se observó inconsistencia alguna debido a que son consistentes con las técnicas para la evaluación de riesgos de ISO 31010:2009.

PT.	C4	
Hecho por:	Sv	10/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Análisis de riesgos

No.	Descripción	Ref.	Pág.
1	Categorías de riesgo por niveles	C4-1	90

La Digital, S.A.
Auditoría interna
Categoría de riesgos por niveles

PT.	C4-1	
Hecho:	Sv	10/08/2016
Revisado:	Wp	12/08/2016

Categoría Nivel 1	Categoría Nivel 2
Fraude interno	Operaciones no autorizadas
	Abuso de Información privilegiada
	Apropiación indebida de fondos
Fraude externo	Daños por ataques informáticos
	Robo de información
Relaciones laborales y seguridad en el puesto de trabajo	Remuneración, contratación, despidos, prestaciones
	Accidentes laborales, seguridad
	Todo tipo de discriminación
Clientes, productos y prácticas empresariales	Divulgación de información del cliente
	Defecto en los productos/servicios
	Litigios sobre resultados de actividades de asesoramiento
Daños a activos materiales	Pérdidas por desastres naturales
Incidencias en el negocio y fallo en los sistemas	Hardware, software, telecomunicaciones
Ejecución, entrega y gestión de procesos	Errores, introducción de datos, mantenimiento o descarga
	Inexactitud de informes externos
	Inexistencia de autorizaciones, rechazos de clientes
	Pérdida o daño de activos del cliente por negligencia
	Litigios con distribuidores

PT.	C5	
Hecho por:	Sv	10/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Evaluación de los riesgos

La Digital, S.A.
Auditoría interna
Matriz de Riesgos

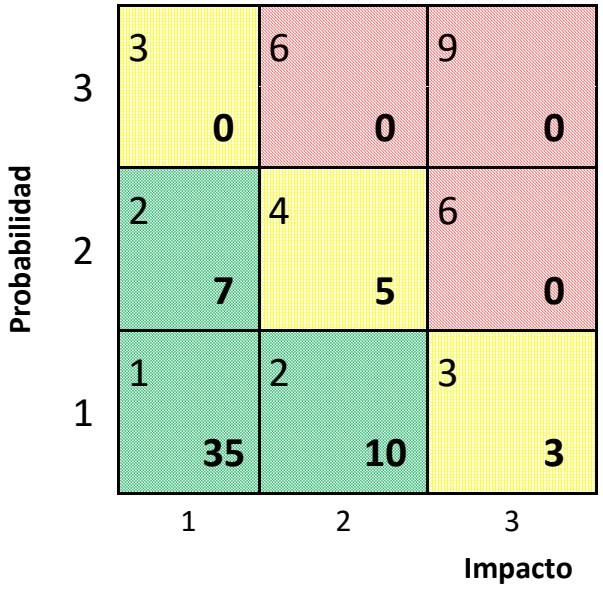
PT.	C5-1	
Hecho por:	Sv	10/08/2016
Revisado:	Wp	12/08/2016

						RIESGO RESIDUAL SEGÚN LA ADMINISTRACIÓN				
No.	**Nombre Actividad**	**Descripción Riesgo Operativo**	**Categorización de Riesgo**	**Control Establecido**	**Gerencia responsable**	**Frecuencia**	**Ponderación Frecuencia**	**Impacto**	**Ponderación Impacto**	**Nivel de Exposición**
1	Operaciones administrativas	Los Oficiales de seguridad de la empresa, crean un usuario ficticio, para efectuar transacciones fraudulentas	Fraude Interno	cámaras de circuito cerrado	Riesgos y procesos	Bajo	1	Bajo	1	**1**
2	Operaciones administrativas	Personal Insuficiente de tecnología afectando las operaciones administrativas.	Relaciones Laborales y Seguridad en el Trabajo	Politica de vacaciones para que no coincidan en la misma fecha	Operaciones	Medio	2	Bajo	1	**2**
3	Operaciones administrativas	Concentracion de conocimientos del personal de tecnología	Relaciones Laborales y Seguridad en el Trabajo	Sensibilizaciones para compartir el conocimiento	Tecnología de información	Bajo	1	Bajo	1	**1**
4	Operaciones administrativas	Incumplimiento en los tiempos requeridos/acordados para la contratacion de personal.	Relaciones Laborales y Seguridad en el Trabajo	Procedimiento de reclutamiento y selección de personal	Recursos Humanos	Medio	2	Medio	2	**4**
5	Operaciones administrativas	Reclamos por no atender solicitudes de mantenimiento y/o configuraciones en el sistema	Clientes, Productos y Prácticas Empresariales	Mesa de ayuda	Tecnología de información	Medio	2	Bajo	1	**2**
6	Operaciones administrativas	Pérdidas materiales por desastres naturales o causados por el hombre	Daños en Activos Materiales	Póliza de seguro	Riesgos y procesos	Bajo	1	Alto	3	**3**
7	Operaciones administrativas	Fallas del hardware, software y comunicaciones	Fallo en Sistemas	Plan de continuidad de Negocio	Tecnología de información	Bajo	1	Bajo	1	**1**
8	Operaciones administrativas	Enviar transacciones fraudulentas	Fraude Interno	Autorización del mensaje por parte del banco	Tecnología de información	Bajo	1	Bajo	1	**1**
9	Digitalización de datos CCB	Divulgar información confidencial del cliente	Clientes, Productos y Prácticas Empresariales	Bitácoras manuales de asignación de actividades, equipo y personas	Operaciones	Bajo	1	Medio	2	**2**
10	Generación de datos para compensación	Fallas en hardware o software que soporta servicios de la Cámara de CCA	Fallo en Sistemas	Estrategias de disponibilidad	Tecnología de información	Bajo	1	Bajo	1	**1**

Conclusión: La matríz fue evaluada con base a los criterios establecidos por la administración, sin embargo no es posible identificar los riesgos que requieren tratamiento.

PT.	C5-2	
Hecho por:	Sv	10/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Mapa de calor de riesgo operativo



Conclusión: El mapa de calor fue evaluado con base a los criterios definidos por la administración, sin embargo solo se cuenta con un mapa consolidado y no por servicio crítico de acuerdo a lo indicado en el cuestionario de control interno (B 3 de 6)

PT.	C6	
Hecho por:	Sv	10/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Tratamiento de los riesgos

PT.	C6-1	
Hecho por:	Sv	10/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.

Auditoría Interna

Planes de tratamiento 2015

Proceso	Correlativo del riesgo	Riesgo	Plan de acción	Responsable	Fecha
Operaciones administrativas	**4**	**Incumplimiento en los tiempos requeridos para la contratación de personal**	Identificación de puestos claves en cada proceso, para dar prioridad al proceso de reclutamiento y selección	Gerente de recursos humanos	30 de diciembre de 2015
Operaciones administrativas	**6**	**Pérdidas materiales por desastres naturales o causados por el hombre**	Evaluación de la póliza de seguro de todo riesgo para determinar si se adecúa a las necesidades de la empresa	Gestor de riesgos y procesos	31 de julio de 2015

PT.	C6-2	
Hecho por:	Sv	10/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.

Auditoría Interna

Evaluación de planes de tratamiento

No.	Plan de Tratamiento	Riesgo Asociado	Servicio Asociado	Nivel de Riesgo	Responsable	Fecha de Cumplimiento	Comunicado
1	Identificación de puestos claves en cada proceso, para dar prioridad al proceso de reclutamiento y selección	✔	✘	✔	✔	✔	✔
2	Evaluación de la póliza de seguro de todo riesgo para determinar si se adecúa a las necesidades de la empresa	✔	✘	✔	✔	✔	✔

Conclusión: De acuerdo a lo observado se puede determinar que el formato de los planes de tratamiento presenta inconsistencia conforme a lo indicado por el gerente de riesgos y procesos en el cuestionario de control interno (B 5 de 6) y el formato proporcionado (C6-1).

PT.	C7	
Hecho por:	Sv	11/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Monitoreo y revisión

No.	Descripción	Ref.	Página
1	Acta del comité de riesgos	C7-1	98

ACTA 01-2015
COMITÉ DE RIESGOS
LA DIGITAL, S.A.

PT.	C7-1	
Hecho por:	Sv	10/08/2016
Revisado:	Wp	12/08/2016

En la ciudad de Guatemala, siendo las catorce horas con treinta minutos del siete de julio del año 2015, en la sala de sesiones de la empresa La Digital, S.A. se encuentra reunido el comité de riesgos, para hacer constar lo siguiente: **PRIMERO: Agenda de Reunión.** El secretario del comité informa sobre la agenda de la reunión, la cual contiene los puntos siguientes: 1) Lectura de la agenda; 2) Ajuste y aprobación del Reglamento del comité de Riesgos; 3) Aprobación del Manual de Gestión Integral de Riesgos; 4) Identificación de riesgos nuevos; 5) Planes de Acción propuestos derivados del análisis de riesgo; 6) Puntos varios. A continuación se sometió a consenso la aprobación de la Agenda. El pleno del comité de riesgos aprueba todos los puntos de la agenda a tratar. **SEGUNDA: del funcionamiento.** Se pone a discusión del pleno el Reglamento del comité de Riesgos de la Digital, S.A. y lo indicado en el manual de normas y políticas de la gestión integral de riesgos. Quedó establecido que se tomarán las decisiones del comité por consenso. Quedó establecido que se realizara la programación en forma semestral. El comité de riesgos por consenso aprobó los documentos indicados. **TERCERA:** Se realizó la presentación de riesgos nuevos identificados por la gerencia de riesgos y procesos, luego de una amplia deliberación se decide que estos deben ser integrados a la matriz de riesgo operativo al finalizar el año. **CUARTA:** Se realizó la propuesta de los planes de acción elaborados para mitigar los riesgos según el análisis que se hizo, se discutieron las inquietudes del pleno quedando de acuerdo con los planes de acción elaborados. **QUINTA:** No habiendo más que hacer constar se da por finalizada la presente acta en el mismo lugar y fecha, siendo las diecisiete horas en punto.

Oscar Martínez
Presidente del Comité

Edgardo Soto
Secretario

PT.	D	
Hecho por:	Sv	11/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Comité de riesgos

ACTA DE CONSTITUCION
COMITÉ DE RIESGOS
LA DIGITAL, S.A.

PT.	D1	
Hecho por:	Sv	11/08/2016
Revisado:	Wp	12/08/2016

En la ciudad de Guatemala, siendo las diez horas en punto del día dieciocho de junio del año dos mil once, en la sala de sesiones de La Digital, S.A. se encuentran reunidos los representantes de la empresa: Oscar Martínez, Edgardo Soto, Andrés González, Saúl Pineda, María Contreras, Karla Alves, José Pinto y Leticia Rodríguez, para hacer constar lo siguiente: **PRIMERO: de su integración**. Son miembros del Comité de Riesgos las personas descritas anteriormente. Estas personas no recibirán remuneración por formar dicho comité. El mismo será presidido por el Gerente General o la persona que éste designe, en caso de ausencia. **SEGUNDO: de su objetivo principal**. El Comité de Riesgos tiene como objetivo fundamental definir las estrategias para medir y mitigar la exposición del riesgo Tecnológico y Operativo y velar por la implementación de los acuerdos adoptados, relacionados con la Gestión del Riesgo. **TERCERO: Son deberes y derechos de los integrantes del Comité**: participar en forma directa y continua en el desenvolvimiento de las actividades del Comité; todos sus miembros a ejercer el derecho de voz y voto, con excepción del Auditor Interno que únicamente tiene derecho a voz pero sin voto. **CUARTO: de las reuniones**. El Comité de Riesgos podrá reunirse por los menos cada dos semanas los primeros tres meses a partir de la fecha y después una vez al mes en forma ordinaria y en forma extraordinaria cuando uno de sus miembros lo solicite. Habrá quórum cuando a una reunión asistan más de la mitad de sus miembros. En caso que se considere oportuno, se podrán invitar a las reuniones a otros funcionarios, los cuales asistirán con voz pero sin voto. De cada reunión se levantará una minuta correspondiente por la persona que sea nombrada como Secretario (a). **QUINTO:** No habiendo más que hacer constar se da por finalizada la presente Acta Constitutiva en el mismo lugar y fecha, siendo las doce horas en punto.

Oscar Martínez
Presidente del Comité

Edgardo Soto
Secretario

PT.	E	
Hecho por:	Sv	11/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Comité de riesgos

PT.	E1 1 de 2	
Hecho por:	Sv	11/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Análisis de brechas del proceso de gestión de riesgos

Cláusula	Descripción	Implementado	Comentarios
5.2	**Comunicación y consulta**		
1	Existe comunicación y consulta con partes interesadas internas y en cada etapa del proceso de gestión de riesgos	Si	
2	Existe un plan de comunicación y consulta	Si	
5.3	**Estableciendo el contexto**		
1	Definir las metas y objetivos de las actividades de gestión de riesgos	Si	
2	Definir responsabilidades para el proceso de gestión de riesgos	Si	
3	Definir el alcance	Si	
4	Definir la actividad, proceso, función, proyecto, producto, servicio o activo en términos de tiempo y ubicación	Si	
5	Definir la metodología de análisis y evaluación de riesgos	Si	
6	Definir la forma en la que se evaluará el desempeño y efectividad en la gestión de riesgos	No	No se cuenta con indicadores de desempeño en la gestión de riesgos
5.4.2	**Identificación de riesgos**		
1	Se identifican las fuentes de riesgo	Si	
2	áreas de impacto	Si	
3	eventos y sus causas	Si	
4	consecuencias potenciales	Si	
5.4.3	**Análisis de riesgos**		
1	Consideración de las causas y fuentes de riesgo	Si	
5.4.4	**Evaluación de riesgos**		
1	Se realiza la comparación del nivel de riesgo encontrado durante el proceso de análisis con el criterio establecido en el contexto	Si	

PT.	E1 2 de 2	
Hecho por:	Sv	11/08/2016
Revisado:	Wp	12/08/2016

5.5	**Tratamiento de riesgos**		
1	Se han definido las opciones de tratamiento de riesgos	Parcial	Se cuenta con planes de tratamiento, sin embargo no se identifican en la matriz de riesgos
2	Se establecen planes de tratamiento de riesgos	Si	
3	Las razones de la selección de opciones de tratamiento, incluyendo el beneficio esperado.	No	
4	Responsables de implementar el plan	Si	
5	Acciones propuestas	Si	
6	Requerimientos de recursos incluyendo contingencias	No	
7	Tiempos y programación de actividades	Parcial	Solo cuenta con una fecha estimada
5.6	**Monitoreo y revisión**		
1	El monitoreo y revisión forma parte del proceso de gestión de riesgos	Si	
2	Las responsabilidades sobre el monitoreo y revisión se encuentran claramente definidas	Si	
3	Asegurar que los controles son efectivos y eficientes tanto en su diseño como en su operación	Parcial	
4	Identificar riesgos emergentes	Parcial	Registro únicamente en acta de comité de riesgos

Conclusión: Como resultado del análisis de brechas, se puede determinar que existen puntos que no son consistentes con lo que recomienda la norma, por lo que deben ser atendidos para estar de conformidad a lo establecido.

PT.	E2	
Hecho por:	Sv	11/08/2016
Revisado:	Wp	12/08/2016

La Digital, S.A.
Auditoría interna
Cédula de aspectos a mejorar

No.	Oportunidad de mejora	Acciones a tomar	Criticidad	Ref.	Pág.
1	No se cuenta con un registro de aseguramiento de la efectividad de controles, sin embargo estos son considerados en la matriz de riesgos	Establecer un registro de aseguramiento de efectividad de controles para validar su correcta evaluación	Media	B	77
2	No se cuenta con un registro formal de riesgos emergentes, estos se quedan registrados únicamente en actas de comité de riesgos	Establecer un registro de riesgos emergentes para reforzar el control por parte de la gerencia de riesgos y procesos	Media	B	77
3	En la matriz de riesgo operativo, no es posible identificar los riesgos que requieren tratamiento	Identificar los riesgos que requieren tratamiento para mayor facilidad de identificación en la matriz	Baja	C5-1	96
4	La administración cuenta únicamente con un mapa de calor unificado donde se observa la distribución de todos los riesgos, sin embargo indicaron que contaban con un mapa por cada servicio	Establecer mapas de calor por cada servicio de misión crítica para identificar la cantidad de riesgos que corresponde a cada servicio	Media	C5-2	97
5	En los planes de tratamiento, se observa inconsistencia con la información que debe contener	Cumplir con el formato establecido por la administración	Baja	C6-2	100
6	No se cuentan con indicadores para monitorear la efectividad de la gestión de riesgos	Establecer indicadores de desempeño que permitan monitorear la efectividad de la gestión de riesgos	Alta	E2	107

LA DIGITAL, S.A.
INFORME DE AUDITORÍA INTERNA

Guatemala 16 de agosto de 2016

Dirigido a:
Lic. Oscar Martínez
Presidente del comité de riesgos
Presente.

Estimado Lic. Martínez

De conformidad a nuestro programa de auditoría, hemos concluido con la evaluación de la gestión de riesgos, la revisión cubrió el período del tercer trimestre de 2016, dicha actividad fue realizada por el auditor Sender Velásquez durante el período comprendido del 15 al 31 de marzo del año en curso.

Nuestro trabajo fue efectuado de conformidad con las Normas Internacionales para el Ejercicio Profesional de Auditoría Interna y limitada a lo que requiere el estándar ISO 31000:2009 “Gestión de Riesgos”, específicamente en el proceso de gestión de riesgos.

De acuerdo a los resultados obtenidos en eta auditoría, se concluye que cada uno de los componentes del proceso se aplica de manera adecuada, no obstante se observaron situaciones que afectan en cierta manera el proceso; dichas situaciones encontradas se presentan a continuación con su nivel de criticidad.

OPORTUNIDADES DE MEJORA Y ACCIONES A TOMAR

OPORTUNIDAD DE MEJORA 1

Nivel de criticidad: Media

No se cuenta con un registro de aseguramiento de la efectividad de controles, sin embargo estos son considerados en la matriz de riesgos para reducir la probabilidad o el impacto y obtener un nivel de exposición residual.

Causa

Falta de control en el registro

Efecto

Ausencia de registros históricos para evaluaciones posteriores.

ACCIONES A TOMAR

Establecer un registro de aseguramiento de efectividad de controles para validar su correcta evaluación.

OPORTUNIDAD DE MEJORA 2

Nivel de criticidad: Media

No se cuenta con un registro formal de riesgos emergentes, estos riesgos quedan registrados únicamente en actas de comité de riesgos.

Causa

Deficiencia en el control

Efecto

Ausencia de registro de riesgos emergentes para su análisis

ACCIONES A TOMAR

Documentar a través de un registro de riesgos emergentes para reforzar el control por parte de la gerencia de riesgos y procesos.

OPORTUNIDAD DE MEJORA 3

Nivel de criticidad: Baja

En la matriz de riesgo operativo, no es posible identificar los riesgos que requieren tratamiento.

Causa

Deficiencia en el control

Efecto

Limitación en identificar riesgos que requieren tratamiento

ACCIONES A TOMAR

Identificar los riesgos que requieren tratamiento para mayor facilidad de interpretación en la matriz de riesgos.

OPORTUNIDAD DE MEJORA 4

Nivel de criticidad: Media

La administración cuenta únicamente con un mapa de calor unificado donde se observa la distribución de todos los riesgos, sin embargo el gerente de riesgos y procesos indicó que contaban con un mapa por cada servicio.

Causa

Falta de comunicación en la gerencia

Efecto

Entrega de información incorrecta

ACCIONES A TOMAR

Establecer mapas de calor por cada servicio de misión crítica para identificar la cantidad de riesgos que corresponde a cada servicio.

OPORTUNIDAD DE MEJORA 5

Nivel de criticidad: Baja

En los planes de tratamiento, se observa inconsistencia con la información que debe contener de acuerdo a lo indicado por el gerente de riesgos y procesos.

Causa

Deficiencia en el control

Efecto

Incumplimiento a lo establecido por la administración

ACCIONES A TOMAR

Cumplir con el formato establecido por la administración.

OPORTUNIDAD DE MEJORA 6

Nivel de criticidad: Alta

Se determinó que no se cuentan con indicadores para monitorear la efectividad de la gestión de riesgos.

Causa

Deficiencia en el control

Efecto

Inconsistencia con lo establecido en la norma ISO 31000:2009

ACCIONES A TOMAR

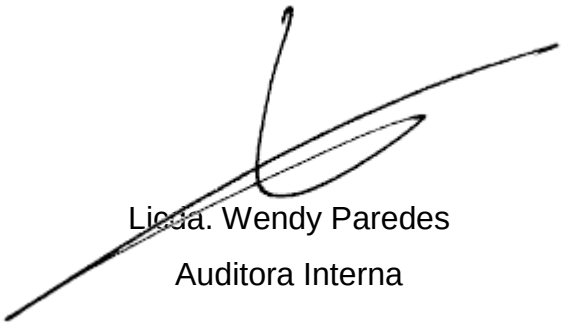
Establecer indicadores de desempeño que permitan monitorear la efectividad de la gestión de riesgos.

COMENTARIOS DEL AUDITADO

El gerente de riesgos y procesos está de acuerdo con las oportunidades de mejora y con las acciones a tomar, e iniciarán con las medidas correctivas.

El departamento de auditoría interna desea expresar su agradecimiento por la cooperación recibida durante la revisión por parte del personal de riesgos y procesos y a los colaboradores de la empresa.

Atentamente,



Licda. Wendy Paredes

Auditora Interna

CONCLUSIONES

1. Se puede confirmar que la gestión de riesgos es importante para el funcionamiento efectivo de la empresa, porque ayuda a minimizar el impacto en caso de materializarse un evento que pueda afectar la operación, es por eso que la auditoría interna debe evaluar los controles establecidos, para poder verificar la eficiencia del proceso, la evaluación periódica de los controles podrá indicar la capacidad de respuesta que tienen los mismos al presentarse un riesgo.

2. La empresa debe reconocer que puede sufrir pérdidas monetarias significativas, si no le da la importancia debida, al cumplimiento de los controles y políticas establecidas, para reducir la posibilidad de ocurrencia de un riesgo.

3. La importancia en la adaptación y aplicación de los modelos de control interno o estándar de gestión de riesgos en la empresa, deben ser debidamente analizados y adoptados a la naturaleza de la misma; sin embargo, para que los sistemas de control interno sean efectivos, deben ser debidamente transmitidos a todos los niveles de la entidad, para tener una base sólida sobre el conocimiento de la gestión del riesgo.

4. La ISO 31000:2009 se presenta como un marco de referencia que puede contribuir significativamente a la gestión de riesgos y a la estrategia de aseguramiento de la gestión de riesgos por parte del auditor interno, ya que lo toma como marco de referencia para realizar sus evaluaciones correspondientes que tiendan a fortalecer el control interno.

RECOMENDACIONES

1. La empresa debe considerar la mejora continua en la gestión de riesgos, ya que de esta forma, se logra madurar el proceso de gestión, obteniendo con esto un resultado que impacta de forma positiva para realizar sus procesos con mayor certeza y ayudando al logro de los objetivos trazados.

2. Auditoría interna debe participar activamente y en forma periódica en la verificación de los controles establecidos, estos deben ser evaluados a través de auditorías basadas en riesgos, para que puedan encaminarse al desarrollo del proceso de prevención, y deben realizarse en su totalidad y no parcialmente, para poder alcanzar eficiencia en las empresas para minimizar los riesgos.

3. La auditoría interna debe conocer el sistema de gestión de riesgos implantado en la empresa para que pueda aportar ideas que generen valor agregado; sin embargo, no debe participar en la gestión como tal, ya que esto limitaría la objetividad de la auditoría interna como departamento dentro de la empresa. Adicionalmente se debe tener presente la norma que rige la carrera de contador público y auditor.

4. La gestión de riesgos no debe limitarse únicamente a la normativa ISO 31000:2009, ya que estos son algunos requisitos que debe cumplir la empresa para poder dar respuesta a los riesgos; la empresa para la mejora continua, debe buscar otros modelos que puedan adaptarse para reforzar de esta forma la gestión.

REFERENCIAS BIBLIOGRÁFICAS

1. Asamblea Nacional Constituyente, Constitución Política de la República de Guatemala, promulgada en el año de 1,985.

2. Banco de Guatemala, El sistema de pagos de Guatemala: Evaluación y propuesta de modernización, Guatemala, octubre 2004.

3. Banco de Guatemala, Resolución GG-02-2014 "Modificación y aprobación de los instrumentos normativos de la Cámara de Compensación Bancaria", año 2014.

4. Banco de Guatemala, Resolución GG-14-2009 "Determinación del monto de las operaciones de alto valor y de bajo valor y el procedimiento de liquidación de los cheques a compensar en la CCB y a liquidar en el Sistema LBTR, en moneda nacional y en moneda extranjera", año 2009.

5. "Banco de Guatemala, Resolución GG-37-2014 ""Aprobación de las disposiciones administrativas y Horarios de Operación, de Atención y de Prestación de Servicios de la Cámara de Compensación Automatizada"", año 2014".

6. Banco de Guatemala, Resolución GG-72-2010 "Aprobación de los instrumentos normativos y Horarios de Atención y de Operación de la Cámara de Compensación Bancaria", año 2010.

7. Banco de Guatemala, Resolución GG-78-2013 "Modificaciones al Instructivo para la Estandarización de Cheques en el Sistema Bancario Nacional", año 2013.

8. Benavides Pañeda, Javier. ”Administración”. McGraw-Hill Interamericana editores, S.A. de C.V. México D.F. Año 2004.

9. Blanco Luna Yanel. Normas y procedimientos de la auditoría integral, Bogotá marzo 2004.

10. BSI British Standards, ISO 31000:2009 "Risk management - Principles and Guidelines", edición 2009.

11. BSI British Standards, ISO 31010:2009 "Risk Management - Risk Assessment Techniques", edición 2009.

12. BSI British Standards, ISO 9001:2015 "Quality Management Systems Requirements", edición 2015.

13. BSI British Standards, ISO Guide 73:2009 "Risk Management - Vocabulary", edición 2009.

14. BSI British Standards, ISO/IEC 27005:2011 "Information Technology - Security techniques - Information security risk management", edición 2011.

15. Committee of Sponsoring Organizations of the Treadway Commission, Gestión de Riesgos Corporativos, Técnicas de Aplicación, Año 2013.

16. Committee of Sponsoring Organizations of the Treadway Commission, Gestión de Riesgos Corporativos, Marco Integrado, Año 2013.

17. Congreso de la República de Guatemala, Decreto 10-2012, Ley de Actualización Tributaria.

18. Congreso de la República de Guatemala, Decreto 15-98, Ley del Impuesto Único Sobre Inmuebles.

19. Congreso de la República de Guatemala, Decreto 2-70, Código de Comercio y sus reformas.

20. Congreso de la República de Guatemala, Decreto 27-92, Ley del Impuesto al Valor Agregado y sus reformas.

21. Congreso de la República de Guatemala, Decreto 37-92, Ley del Impuesto de Timbres Fiscales y de Papel Sellado Especial para Protocolos y sus reformas.

22. Congreso de la República de Guatemala, Decreto 73-2008, Ley del Impuesto de Solidaridad.

23. Coopers & Lybrand, Los Nuevos Conceptos del Control Interno, edición 1997.

24. De Zuani Elio Rafael. "Introducción a la Administración de Organizaciones", Segunda Edición, Editorial Maktub, 2003.

25. Estupiñan Gaitán Rodrigo, Control interno y fraudes con base los ciclos transaccionales: Análisis del Informe COSO I y II, segunda edición, ECOE Ediciones, Bogotá Colombia, año 2006

26. Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), Norma Técnica Colombiana NTC-ISO 31000 Gestión del Riesgo y Directrices. Año 2011.

27. Instituto de Auditores Internos, Consejo para la Práctica 2210.A1-1, edición 2016.

28. Instituto de Auditores Internos, Declaración de posición, Las tres líneas de defensa para una efectiva gestión de riesgos y control, enero 2013.

29. Instituto de Auditores Internos, Marco Internacional para la Práctica profesional. Edición 2016.

30. Instituto Mexicano de Contadores Públicos, Normas Internacionales de Auditoría y Control de Calidad, Edición 2011.

31. ISO Tools Excellence, Norma ISO 31000: El valor de la gestión de riesgos en las organizaciones.

32. Junta Monetaria, JM-056-2011 "Reglamento para la Administración Integral de Riesgos", Año 2011.

33. Junta Monetaria, Resolución JM 102-2011 "Reglamento para la Administración del Riesgo Tecnológico", año 2011.

34. Junta Monetaria, Resolución JM 140-2007 "Reglamento de la Cámara de Compensación Automatizada", año 2007.

35. Junta Monetaria, Resolución JM 189-2007 "Modificación del Reglamento de la Cámara de Compensación Bancaria", año 2007.

36. Junta Monetaria, Resolución JM 4-2016 "Reglamento para la Administración del riesgo operacional", año 2016.

37. Junta Monetaria, Resolución JM 51-2003 "Aprobación del Reglamento de la Cámara de Compensación Bancaria", año 2003.

38. Junta Monetaria, Resolución JM 95-2011 "Reglamento para la Estandarización de Cuentas Bancarias", año 2011.

39. Mejía Quijano Rubí Consuelo. Administración de Riesgos, Un enfoque integral. Universidad EAFIT. Medellín, Colombia. Año 2010.

40. Ramos Leonardo. Norma ISO 27000, Seguridad de la Información. Gerencia General de Tecnologías de la Información. Año 2009.

41. Samuelson Paul A. & William D. Nordhaus, "Economía, con aplicaciones a Latinoamerica", 19 Edición. Mcgraw-Hill Interamericana editores, S.A. de C.V., Año 2010.

42. Serra, Carlos ISO 31000:2009 Herramienta para evaluar la gestión de riesgos, Datasec Uruguay.

43. The Institute of Internal Auditors, Normas Internacionales para el Ejercicio profesional de la Auditoría Interna, Florida USA, edición 2010.

44. Villegas Lara, René Arturo. Derecho mercantil guatemalteco, tomo 1 sexta edición 2004.

Web grafía

45. Definición de Auditoria Externa
Recuperado en: http://www.mailxmail.com/auditoria-interna-externa-definicion-caracteristicas_h.html
el 27/03/2016 a las 15:10

46. Definición de cálculo
Recuperado en: http://secretosenred.com/articles/3305/1/objetivos-y-procedimientos-de-auditoría-para-las-obligaciones--financieras/paacutegina1.html
el 27/03/2016 a la 15:15

47. Definición de capital
Recuperado en: http://www.definicion.org/capital.html
el 27/03/2016 a las 15:20

48. Definición de empresa de servicios
Recuperado en: http://deconceptos.com/ciencias-sociales/empresa-de-servicio.html
el 27/03/2016 a las 15:20

49. Definición de empresa no lucrativa
Recuperado en: http://es.wikipedia.org/wiki/Organizaci%C3%B3n_sin_%C3%A1nimo_de_lucro.html
el 27/03/2016 a las 15:30

50. Etimología de la palabra Auditoría
Recuperado en: http://es.wikipedia.org/wiki/Auditor%C3%ADa.html
el 27/03/2016 a las 15:40

51. Tipos de riesgo de auditoría
Recuperado en: http://www.gerencie.com/tipos-de-riesgos-de-auditoria.html
el 27/03/2016 a las 15:45

52. Definición de recursos materiales
Recuperado en: http://www.ecas.cl/index.php/comunidad/45-contable/209-glosario-de-terminos.html
el 27/03/2016 a las 16:05

53. Definición de trabajo
Recuperado en: http://www.definicion.org/trabajo.html
el 27/03/2016 a las 16:00

54. Norma técnica para la generación de estadística básica.
Recuperado en: http://www.inegi.org.mx/est/contenidos/proyectos/aspectos metodologicos/documentostecnicos/doc/norma_tecnica_para_la_generacion_de_estadistica_basica.pdf
el 27/03/2016 a las 15:55

ANEXOS

ANEXO 1
TÉRMINOS Y DEFINICIONES

Actitud del riesgo: la aproximación de una organización para evaluar y, eventualmente, perseguir, retener, tomar o huir del riesgo.

Análisis del riesgo: proceso que comprende la naturaleza del riesgo y determina el nivel del riesgo.

Comunicación y consulta: procesos continuos e iterativos que una organización conduce para proveer, compartir u obtener información, y establecer un diálogo con las partes interesadas, con respecto a la gestión de riesgos.

Consecuencia: resultado de un evento que afecta los objetivos.

Contexto externo: entorno externo en el que la organización busca alcanzar sus objetivos.

Contexto interno: entorno interno en el que la organización busca alcanzar sus objetivos.

Control: medida que modifica el riesgo.

Criterios del riesgo: términos de referencia con los cuales se evalúa el significado del riesgo.

Establecimiento del contexto: se trata de definir los parámetros externos e internos que deben ser tomados en cuenta para gestionar el riesgo, establecer el alcance y los criterios del riesgo para la política de gestión de riesgos.

Evaluación del riesgo: proceso general de identificación, análisis y evaluación del riesgo.

Evaluación del riesgo: procesos en el que se comparan los resultados del análisis de riesgos con los criterios del riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

Evento: ocurrencia o cambio en un conjunto particular de circunstancias.

Fuente del riesgo: elemento que, ya sea individual o en conjunto, tiene el potencial intrínseco de aumentar riesgos.

Gestión de riesgos: actividades coordinadas que dirigen y controlan una organización con relación al riesgo.

Identificación del riesgo: procesos de encontrar, reconocer y describir riesgos.

Marco de referencia de la gestión de riesgos: conjunto de componentes que provee los fundamentos y los arreglos organizacionales para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión de riesgos.

Monitoreo: supervisión continua, observación crítica o determinación del estatus para identificar cambios en el nivel de rendimiento requerido o esperado.

Niveles del riesgo: magnitud de un riesgo o una combinación de riesgos, expresados en términos de la combinación de consecuencias y su probabilidad.

Parte Interesada: persona u organización que puede afectar, ser afectada, o percibirse como afectada por una decisión o actividad.

Perfil del riesgo: descripción de cualquier conjunto de riesgos.

Plan de gestión de riesgos: esquema dentro del marco de referencia de gestión de riesgos, que especifica la aproximación, los componentes y los recursos de gestión que se aplicarán a la gestión de riesgos.

Política de la gestión de riesgos: declaración de las intenciones generales y la dirección de una organización relativa al riesgo.

Probabilidad: posibilidad de que algo ocurra.

Proceso de gestión de riesgos: aplicación sistemática de políticas, procedimientos y prácticas de gestión para las actividades de comunicación, consulta, establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo.

Propietario del riesgo: persona o entidad con la responsabilidad y autoridad de gestionar un riesgo.

Revisión: actividad realizada para determinar la idoneidad y efectividad para alcanzar los objetivos establecidos.

Riesgo residual: el riesgo que permanece luego del tratamiento del riesgo.

Riesgo: efecto de incertidumbre en los objetivos.

Tratamiento del riesgo: proceso que modifica el riesgo.

SESIÓN DE CONSEJO 07-2011

ACTA No. 140-2011

PT.	D2	
Hecho:	Sv	11/08/2016
Revisado:	Wp	12/08/2016

En la ciudad de Guatemala, a las siete horas con treinta y cinco minutos del veintitrés de julio de dos mil once, reunidos en las instalaciones del Hotel el Caminante, salón La Roya, los señores Directores: José López, Ricardo Pérez, Lucero Mijares, quien funge como secretario de esta sesión, Silvia Rodríguez, Carlos Pérez y Giovanno Conrado; y el Gerente General de la sociedad señor Oscar Martínez, para hacer constar lo siguiente: **PRIMERA:** El Ingeniero López, pone a consideración de los señores Directores la agenda, la cual contiene los puntos siguientes: 1) Lectura y aprobación de la agenda; 2) Lectura y aprobación del acta anterior; 3) Institucionalización de la gestión de riesgos. Luego de discutida, se aprueba por unanimidad la agenda propuesta. **SEGUNDA:** El Ingeniero López, solicita a los señores Directores la ratificación del acta 138-2011 correspondiente a la sesión del 18 de junio de 2011, la cual es aprobada. **TERCERA:** El Licenciado Martínez, hace del conocimiento del Consejo de Administración, que se procedió a la formación del Comité de Riesgos de la entidad, informando que el objetivo del mismo será establecer una cultura de gestión de riesgo institucional, así como velar por la implementación de los acuerdos adoptados, relacionados con la de Gestión de Riesgo y determinar la exposición al riesgo tecnológico y operativo a la que se encuentra expuesta la empresa. Adicionalmente, informa que los miembros del equipo gerencial serán los integrantes del mismo y que, recaerá sobre la Gerencia General la responsabilidad de informar al Consejo de Administración, sobre los resultados de la gestión integral del riesgo, así como sobre la Auditoría Interna recae la responsabilidad de informar al mismo órgano de los resultados de los procesos de fiscalización correspondientes. Los señores directores se dan por enterados. **NOVENA:** No habiendo nada más que hacer constar, se da por terminada la presente acta, en el mismo lugar y fecha siendo las nueve horas con veinte minutos.

José López
Presidente

Lucero Mijares
Secretario