**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**

**FACULTAD DE CIENCIAS ECONÓMICAS**

# "LA FUNCIÓN DE LA AUDITORÍA INTERNA, EN LA ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO CON BASE A LA REGULACIÓN DE LA JUNTA MONETARIA APLICABLE A LAS EMPRESAS QUE SE ESPECIALIZAN EN EL PROCESAMIENTO MASIVO DE DOCUMENTOS DE FORMA ELECTRÓNICA, EN LA COMPENSACIÓN DE CHEQUES PARA EL SISTEMA BANCARIO DEL PAÍS"

**TESIS:**

**PRESENTADA A LA HONORABLE JUNTA DIRECTIVA**

**DE LA FACULTAD DE CIENCIAS ECÓNOMICAS**

**POR:**

**JOSUÉ FERNANDO CHETE ORTÍZ**

**PREVIO A CONFERÍRSELE EL TÍTULO DE**

**CONTADOR PÚBLICO Y AUDITOR**

**EN EL GRADO ACADÉMICO DE**

**LICENCIADO**

**GUATEMALA, JUNIO DE 2015**

**MIEMBROS DE LA JUNTA DIRECTIVA**
**FACULTAD DE CIENCIAS ECONÓMICAS**

| | |
|---|---|
| Decano Interino | Lic. Luis Antonio Suárez Roldán |
| Secretario | Lic. Carlos Roberto Cabrera Morales |
| Vocal Segundo | Lic. Carlos Alberto Hernández Gálvez |
| Vocal Tercero | Lic. Juan Antonio Gómez Monterroso |
| Vocal Cuarto | P.C. Oliver Augusto Carrera Leal |
| Vocal Quinto | P.C. Walter Obdulio Chigüichón Boror |

**EXONERADO DE LOS EXÁMENES DE ÁREAS PRÁCTICAS BÁSICAS**

De conformidad con los requisitos establecidos en el capítulo III, artículo 15 y 16 del Reglamento para la Evaluación Final de Exámenes de Áreas Prácticas Básicas y Examen Privado de Tesis y al inciso 5.3 del punto Quinto, del acta 13-2013 de la sesión celebrada por Junta Directiva el 20 de septiembre de 2013.

**PROFESIONALES QUE REALIZARON EL EXAMEN PRIVADO DE TESIS**

| | |
|---|---|
| Presidente: | Lic. Oscar Noé López Cordón |
| Secretario: | Lic. Mibzar Amós Castañón Orozco |
| Examinador: | Lic. Carlos Vicente Solórzano Soto |

Guatemala, 28 de Enero de 2,014

Licenciado
José Rolando Secaida Morales
Decano de la Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala
Ciudad Universitaria

Estimado Señor Decano:

En atención a la designación efectuada por medio del Dictamen Auditoria No. 003-2014, procedí a revisar y asesorar el trabajo de Tesis denominado **"LA FUNCIÓN DE LA AUDITORÍA INTERNA, EN LA ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO, CON BASE A LA REGULACIÓN DE LA JUNTA MONETARIA, APLICABLE A LAS EMPRESAS QUE SE ESPECIALIZAN EN EL PROCESAMIENTO MASIVO DE DOCUMENTOS DE FORMA ELECTRÓNICA, EN LA COMPENSACIÓN DE CHEQUES PARA EL SISTEMA BANCARIO DEL PAÍS"**, preparado por el estudiante Josué Fernando Chete Ortiz.

El trabajo efectuado, es el resultado de la investigación y experiencia que el estudiante sustenta, quien de esta manera hace un valioso aporte que enriquece el material de consulta para los profesionales de la Contaduría Pública y Auditoría, así como de personas relacionadas a la profesión.

Por lo anterior, ante mi opinión el trabajo realizado reúne los requisitos necesarios de tesis, por lo que recomiendo su aprobación para ser presentado por el estudiante Josué Fernando Chete Ortiz en su Examen Privado de Tesis, previo a conferírsele el título de Contador Público y Auditor en el grado de Licenciado.

Atentamente,

Licda. Blanca Miriam Camey Gómez
Colegiado No. 1643

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE
CIENCIAS ECONOMICAS
Edificio "S-8"
Ciudad Universitaria, Zona 12
Guatemala, Centroamérica

**DECANATO DE LA FACULTAD DE CIENCIAS ECONOMICAS. GUATEMALA, OCHO DE ABRIL DE DOS MIL QUINCE.**

Con base en el Punto cuarto, inciso 5.1, subinciso 5.1.1 del Acta 09-2015 de la sesión celebrada por la Junta Directiva de la Facultad el 10 de marzo de 2015, se conoció el Acta AUDITORÍA 446-2014 de aprobación del Examen Privado de Tesis, de fecha 21 de noviembre de 2014 y el trabajo de Tesis denominado: "LA FUNCIÓN DE LA AUDITORÍA INTERNA, EN LA ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO CON BASE A LA REGULACIÒN DE LA JUNTA MONETARIA APLICABLE A LAS EMPRESAS QUE SE ESPECIALIZAN EN EL PROCESAMIENTO MASIVO DE DOCUMENTOS DE FORMA ELECTRÓNICA, EN LA COMPENSACIÓN DE CHEQUES PARA EL SISTEMA BANCARIO DEL PAÍS", que para su graduación profesional presentó el estudiante **JOSUÉ FERNANDO CHETE ORTIZ**, autorizándose su impresión.

Atentamente,

*"ID Y ENSEÑAD A TODOS"*

LIC. CARLOS ROBERTO CABRERA MORALES
SECRETARIO

EL SECRETARIO

LIC. JOSE ROLANDO SECAIDA MORALES
DECANO

EL DECANO

Ingrid
REVISADO

Smp.

## DEDICATORIA

| | |
|---|---|
| A DIOS: | Padre, Hijo y Espíritu Santo, por brindarme la sabiduría para obtener el conocimiento y alcanzar este éxito. |
| A MIS PADRES: | Por su incondicional apoyo, en especial a mi señora Madre por sus constantes consejos y atenciones. |
| A MI HIJA: | Aylin Urvashi Chete Cifuentes, inspiración de mi vida y bendición más grande que el cielo me ha otorgado. |
| A MI ESPOSA: | Por brindarme su apoyo incondicional y cuidar de mi hija durante el tiempo que permanecí en este recorrido. |
| A MI FAMILIA: | A mis hermanos, cuñadas, sobrinos, primos y demás, que depositaron en mí su confianza y su granito de apoyo en cada momento. |
| A MIS AMIGOS: | Que me acompañaron en este largo viaje y que me apoyaron en cada etapa transcurrida. |
| A LA USAC: | Tricentenaria casa de estudios y voz de los sin voz. |
| A LOS LECTORES: | Que en sus manos tienen este preciado trabajo, esperando les apoye en su crecimiento profesional. |

# ÍNDICE

**CONTENIDO** **PÁG**

**CAPÍTULO III**

**REGLAMENTO PARA LA ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO, SEGÚN RESOLUCIÓN DE LA JUNTA MONETARIA JM-102-2011 CON VIGENCIA A PARTIR DEL 01 DE SEPTIEMBRE DE 2011**

## CAPÍTULO IV
## ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO

**CAPÍTULO V**

**LA FUNCIÓN DE LA AUDITORÍA INTERNA, EN LA ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO CON BASE A LA REGULACIÓN DE LA JUNTA MONETARIA APLICABLE A LAS EMPRESAS QUE SE ESPECIALIZAN EN EL PROCESAMIENTO MASIVO DE DOCUMENTOS DE FORMA ELECTRÓNICA, EN LA COMPENSACIÓN DE CHEQUES PARA EL SISTEMA BANCARIO DEL PAÍS**

**(CASO PRÁCTICO)**

# ÍNDICE DE CUADROS Y GRÁFICAS

## ÍNDICE DE CUADROS

## ÍNDICE DE GRÁFICAS

# INTRODUCCIÓN

La tecnología actualmente es una herramienta de gestión que toda organización utiliza, avanzando de forma acelerada brindando nuevas soluciones a las empresas que buscan hacer más eficientes sus procesos y mejorar la calidad de sus servicios, sin embargo este avance ha traído una serie de amenazas que emergen de la tecnologías de la información y que al no ser gestionadas adecuadamente pueden ocasionar pérdidas graves a las organizaciones, dando lugar así a la necesidad de poder administrar todos estos riesgos relacionados de una forma ordenada, sistemática y metodológicamente. En el año 2011 la Junta Monetaria emite la resolución JM-102-2011 “Reglamento para la Administración del Riesgo Tecnológico”, cuya aplicación es de observancia general para todo el sistema bancario del país, sin embargo, por medio de su artículo 25 todas las empresas que brindan servicios terciarizados en el procesamiento de información al sistema bancario, se ven  afectas a las disposiciones de este reglamento.

El presente trabajo está contenido en cinco capítulos que tienen como finalidad brindar el conocimiento necesario para poder tener una adecuada gestión en la administración del riesgo tecnológico y conocer así también las funciones de auditoría interna en este campo, siendo la base principal para su desarrollo la regulación de la Junta Monetaria apoyada en mejores prácticas para Tecnología de Información y administración de riesgos tecnológicos.

El Capítulo I, presenta generalidades de la empresa, factores que influyen en ella, su clasificación y composición como una organización de negocio, su estructura organizacional funcional, principales servicios que brinda al sector bancario y los aspectos regulatorios a los que se ve afecta.

En el Capítulo II, se desarrolla lo relacionado a la función de auditoría interna brindando conceptos y categorías respecto a la auditoría y la reestructuración de la visión dado los procesos especiales que desarrolla la organización, define las

funciones de la auditoría interna, establece lo que es una auditoría de cumplimiento la cual debe de ejecutarse en base a la planificación del trabajo de la auditoría basado en riesgos y brinda algunas técnicas que pueden apoyar en el desarrollo del trabajo de la auditoría de TI.

El Capítulo III, desarrolla lo relacionado a la regulación JM-102-2011 “Reglamento para la Administración del Riesgo Tecnológico”, iniciando con un análisis sobre las disposiciones generales determinando la estructura general que conlleva la regulación, así mismo la presentación de cada tema requerido dentro del reglamento acompañado de conceptos relacionados tomados de buenas prácticas para tecnología de la información con la finalidad de brindar un conocimiento mayor sobre el tema que se trata.

En el Capítulo IV, se presenta los conocimientos básicos a considerar en la implementación de la gestión del riesgo tecnológico, metodologías para su administración y desarrolla el proceso para la administración del riesgo tecnológico basado principalmente en el marco de referencia COSO ERM. Además de brindar, puntos de referencia para la implementación del comité de riesgos, las funciones y responsabilidades dentro de la administración del riesgo tecnológico, la documentación de los procesos de TI, los cambios en las estructuras administrativas, de infraestructura y control, como la implementación de un Gestor de Seguridad de la Información, derivado de la implementación de la regulación, así como modelos de nivel de efectividad y madurez del control de TI.

Por último, en el Capítulo V se presenta un caso práctico de una auditoría de cumplimiento para la administración del riesgo tecnológico, con un enfoque de aseguramiento a los requerimientos de la regulación JM-102-2011 “Reglamento para la Administración del Riesgo Tecnológico” y desarrollado bajo el marco de referencia para el proceso de la gestión del riesgo tecnológico. Se incluye al final de este trabajo como anexo un glosario de términos para apoyar a la comprensión de conceptos relacionados con las tecnologías de la información.

# CAPÍTULO I

# EMPRESAS ESPECIALIZADAS EN EL PROCESAMIENTO DE INFORMACIÓN MASIVA

## 1.1 Empresa

“Es una unidad económica-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. Los elementos necesarios para formar una empresa son: capital, trabajo y recursos materiales”. (6:6)

### 1.1.1 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”. (6:7) De esta manera los factores que inciden en una empresa son:

- **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.
- **Factores culturales:** se entiende por cultura todo aquello que comprende el saber, las creencias, el arte, la moralidad, el derecho, las costumbres y cualesquiera otras capacidades de hábitos adquiridos.
- **Factores tecnológicos:** hoy en día la tecnología se ha vuelto en la fuerza más importante que puede transformar y aumentar la capacidad humana.
- **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.

## 1.2 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”. (6:7) A continuación se presenta una clasificación básica de las empresas:

- **Empresa Industrial:** Son todas aquellas que llevan a cabo en su proceso de producción la transformación de materia prima o insumos.
- **Empresa Comercial:** Son las entidades que llevan a cabo la compra venta de mercancías, sin transformarlas, realizando únicamente actividades de intercambio.
- **Empresa Agrícola:** Son las entidades dedicadas a actividades tales como la ganadería, pesca o silvícolas.
- **Empresa de servicios:** Son entidades que comercializan servicios profesionales o de cualquier otro tipo; estos servicios pueden ser de negociación, comunicación, asesorías, entre otros.

## 1.3 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, de asesoramiento, de telecomunicaciones, de transporte, entre otros. “El producto que ofrece una entidad de este tipo es intangible, aunque para cumplir su cometido debe crear toda una red de personal y equipamiento que le soporte el servicio que brinda”. (31)

Estas son empresas u organizaciones independientes, que pueden ser un segmento o una parte relacionada, que “proporciona servicios a usuarios de la entidad, como parte de los propios sistemas de información relevantes para la información financiera”. (24:25)

## 1.4 Tercerización de servicios

La tercerización es cada vez más reconocida como una solución eficiente, experta y eficaz en relación a su costo, diseñada para satisfacer las demandas de implementación, mantenimiento, seguridad y operaciones de los sistemas. “El acceso a personal capacitado, infraestructuras de tecnología avanzada, flexibilidad y ahorro en los costos son los componentes que impulsan la tercerización, en especial la de Tecnología de la Información”. (18:2)

La tercerización se ha convertido en una herramienta básica para lograr eficiencias, en tiempos de crisis o de prosperidad, la tercerización “puede permitir a una empresa centrarse en las competencias básica, mejorar los procesos y aumentar la flexibilidad. La tercerización de servicios puede ayudar a una empresa a reducir costos, generar flujos de caja, y/o reducir o eliminar las operaciones de bajo valor”. (28:11,13)

## 1.5 Ventajas y desventajas de la tercerización

Ventajas:

- Reducción de costos en los procesos productivos.
- Mejor calidad del servicio.
- Eliminación de los costos de selección del personal.
- Ayuda a redefinir la empresa y apoya a enfrentar cambios de negocios.
- Constituye una larga ventaja competitiva sostenida.
- La inversión en planta y equipo se reduce. (29:10)

Desventajas:

- Estancamiento en la innovación
- El costo de ahorro en la tercerización puede ser el no esperado

- Reducción de beneficios
- Pérdida de control sobre la producción (29:10)

### 1.6 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 especializadas 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”. (26:121)

### 1.7 Procesamiento de información masiva

El procesamiento de la información se define como la “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”. (37)

“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”. (16:93)

## 1.8 Empresas especializadas para el sector bancario

Son organizaciones de negocio, cuya principal función es la explotación de economías en escala por medio de la administración de los factores de producción, “bajo una adecuada administración y supervisión cuidadosa de las actividades en curso”. (26:121) Dentro de estas organizaciones podemos localizar aquellas empresas que brindan servicios de digitalización de imágenes y procesamiento de información para el sector bancario del país como empresas especializadas.

Son sociedades organizadas bajo forma mercantil, como una sociedad anónima, entendiéndose esta como la “que tiene el capital dividido y representado por acciones, representadas por títulos que servirán para acreditar y transmitir la calidad y los derechos del socio”. (7:85,99) Estas empresas se ven obligadas a cumplir las leyes del país tanto comerciales como fiscales, sin embargo existen otro tipo de regulaciones aplicables derivado del giro del negocio, mismas que se detallaran en el transcurso del trabajo.

### 1.8.1 Organización de la empresa

La estructura organizacional de este tipo de empresas puede variar dependiendo del tamaño y complejidad de los servicios que pueda brindar, sin embargo, bajo un esquema básico de operación estas entidades cuentan con una asamblea de accionistas y presentan la siguiente estructura organizacional:

- Consejo de Administración
- Gerencia General
- Gerencia de Operaciones
- Gerencia de Tecnología de la Información
- Gerencia de Riesgos
- Gerencia de Recursos Humanos

- Gerencia Financiera
- Auditoría Interna

Debe entenderse que como empresas mercantiles organizadas como sociedad anónima, tienen un capital “dividido y representado por acciones” (7:85), por lo cual existe una Asamblea General de Accionistas la cual está formada por los accionistas y “es el órgano supremo de la sociedad y expresa su voluntad social en las materias de su competencia”. (7:132)

Algunas entidades cuentan además con comités sobre aspectos importantes a gestionarse dentro de la organización y que apoyan al gobierno corporativo, estos comités pueden ser:

- Comité de Cumplimiento
- Comité de Auditoría
- Comité de Riesgos
- Comité de Tecnología de la Información
- Comité de Ética

### 1.8.2 Principales actividades de negocio

Las actividades principales del giro de negocio de estas empresas especializadas para el sector bancario, son las siguientes:

- Digitalización de imágenes de cheques para la cámara de compensación bancaria (CCB).
- Procesamiento de archivos electrónicos para la cámara de compensación bancaria por medio de la captura remota en agencia de imágenes.
- 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 para procesos de check 21.
- Procesamiento y digitalización de cheques propios de ventanilla.
- Centro de almacenamiento de documentos.

### 1.8.3 Aspectos regulatorios que rigen la empresa

Derivado de los servicios especializados y 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 la cuales podemos mencionar las siguientes:

Resoluciones de la Junta Monetaria

- Resolución JM-51-2003 “Reglamento de la Cámara de Compensación Bancaria”.
- Resolución JM-189-2007 “Modificación del Reglamento de la Cámara de Compensación Bancaria”.
- Resolución JM-140-2007 “Reglamento de la Cámara de Compensación Automatizada”.
- Resolución JM-95-2011 “Reglamento para la Estandarización de Cuentas Bancarias”.
- Resolución JM-102-2011 “Reglamento para la Administración del Riesgo Tecnológico”. (38)

Resoluciones del Banco de Guatemala

- Resolución GG-02-2014 “Modificación y aprobación de los instrumentos normativos de la Cámara de Compensación Bancaria”.

- Resolución GG-78-2013 “Modificaciones al instructivo para la Estandarización de Cheques en el Sistema Bancario Nacional”.
- Resolución GG-72-2010 “Aprobación de los instrumentos normativos y horarios de atención y de operación de la Cámara de Compensación Bancaria”.
- Resolución GG-14-2009 “Determinación del 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 “Aprobación de las disposiciones administrativas y horarios de Operación, de Atención y de Prestación de Servicios de la Cámara de Compensación Automatizada”. (38)

# CAPÍTULO II

# LA FUNCIÓN DE AUDITORÍA INTERNA

## 2.1 Auditoría

“Es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización y lograr los objetivos propuestos.” (13:2)

“La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo, son de carácter indudable. La auditoría requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben de seguirse y estimar los resultados obtenidos”. (Ídem)

## 2.2 Auditoría Interna

La definición de auditoría interna establece el propósito fundamental, la naturaleza y el alcance de la actividad de auditoría interna y se define de la forma siguiente:

“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”. (23:5)

“La definición de auditoría interna enfatiza que esta es una actividad independiente, la cual debe reportar al nivel más alto en la estructura organizativa. Para justificar este importante rol, la auditoría interna debe realizar actividades que

ayuden a la organización a cumplir con la misión de alcanzar sus objetivos en todas las áreas de la estructura organizativa". (23:3)

### 2.3 Reestructuración de la visión de auditoría interna

La visión de auditoría interna debe ser apoyar a la administración, a través de las evaluaciones de las transacciones, asesoría y consultoría especializada, con el fin de brindar seguridad razonable de que los objetivos propuestos por la administración están siendo alcanzados. Esto implica que los miembros del departamento de auditoría interna deben de prepararse en relación a los proyectos estratégicos que lleve adelante la organización, actuando en principio bajo aquellas prácticas que definen su actuar, tal como el Marco de Referencia para la Práctica de Auditoría Interna, cuyo documento proporciona un esquema estructurado sobre los principios en que descansa la actuación de la auditoría interna, estos son "requisitos básicos para el ejercicio de la auditoría interna y para evaluar la eficacia de su desempeño". (23:10)

La actividad de auditoría interna debe ser independiente y los auditores internos deben ser objetivos en el cumplimiento de su trabajo, deben estar libre de injerencias al determinar el alcance de la auditoría, el desempeño de su trabajo y al comunicar sus resultados, evitando todo tipo de conflicto de intereses en su accionar y ejecución de su trabajo. "Los trabajos deben de cumplirse con aptitud y cuidado profesional, la actividad de auditoría interna, colectivamente debe reunir u obtener los conocimientos, las aptitudes y otras competencias necesarias para cumplir con sus responsabilidades. Los auditores internos deben cumplir su trabajo con el cuidado y la aptitud que se esperan de un auditor interno razonablemente prudente y competente. El cuidado profesional adecuado no implica infalibilidad". (23:17,18)

Es importante que se desarrolle un programa de aseguramiento y mejora de la calidad que cubra todos los aspectos de la actividad de la auditoría interna, esto

incluye programas de evaluaciones a nivel interno como externo, siendo esta ultimas ejecutadas por lo menos una vez cada cinco años, por medio del Instituto de Auditores Internos en relación al cumplimiento del Marco de Referencia para la Práctica de Auditoría Interna.

Por el último, la actividad de la auditoría interna fue diseñada con el fin de agregar valor a las organizaciones, por medio de sus evaluaciones a los procesos, detectando aquellos puntos de mejora en los mismos que permitan eficientar los recursos y mejorar los resultados obtenidos, por tanto el director de auditoría interna debe gestionar eficazmente la actividad de auditoría interna para asegurar que por medio de esta actividad realmente se añada valor a la organización.

### 2.4 Marco Internacional para la Práctica Profesional

Es un documento emitido por el Instituto de Auditores Internos (IIA), principal promotor del modelo COSO ERM, estas normas tienen como propósito “definir principios básicos que representen el ejercicio de la auditoría interna tal como debería ser, proporcionar un marco para ejercer y promover un amplio rango de actividades de auditoría interna de valor añadido, establecer bases para evaluar el desempeño de la auditoría interna y fomentar la mejora de los procesos y operaciones de la organización”. (23:10)

#### 2.4.1 Declaración de Auditoría Interna

“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”. (23:5)

### 2.4.2 Código de ética

“Tiene como objetivo principal promover la cultura ética en el ejercicio de la profesión de la auditoría interna, basándose en los principios y reglas de conducta contenidas en el marco, y cuyo propósito es guiar la conducta ética de los auditores para realizar un trabajo profesional”. (23:3)

El código de ética se aplica tanto a individuos como a las entidades que proveen servicios de auditoría interna, y se espera que los auditores internos apliquen y cumplan los siguientes principios:

- **Integridad:** Establece confianza y, consiguientemente, provee la base para confiar en su juicio.
- **Objetividad:** Los auditores internos realizan una evaluación equilibrada de todas las circunstancias relevantes y forman sus juicios sin dejarse influir indebidamente por sus propios intereses o por otras personas.
- **Confidencialidad:** Es respetar 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.
- **Competencia:** Los auditores internos aplican el conocimiento, aptitudes y experiencia necesarios al desempeñar los servicios de auditoría interna.

“Contar con un código de ética para la profesión de auditoría interna es necesario y apropiado, ya que ésta se basa en la confianza que se imparte a su aseguramiento objetivo sobre la gestión de riesgos, control y dirección”. (23:7)

### 2.4.3 Normas sobre atributos y desempeño

La estructura de las normas está formada por las normas sobre atributos y las normas sobre desempeño. “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". (23:11)

### 2.4.4 Servicios de aseguramiento y consultoría

Los servicios de aseguramiento que brinda la auditoría interna son "un examen objetivo de evidencias con el propósito de proveer una evaluación independiente de los procesos de gestión de riesgos, control y gobierno de una organización" y los servicios de consultoría "son actividades de asesoramiento y servicios relacionados, proporcionadas a los clientes, cuya naturaleza y alcance estén acordados con los mimos y estén dirigidos a añadir valor y a mejorar los procesos de gobierno, gestión de riesgos y control de una organización, sin que el auditor interno asuma responsabilidades de gestión". (23:193)

## 2.5 Funciones de la auditoría interna

"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". (23:5)

"Actividad de evaluación establecida o proporcionada como un servicio a la entidad. Sus funciones incluyen entre otras cosas el examen, evaluación y monitoreo de lo adecuado del control interno y su efectividad". (24:30)

## 2.6 Planificación del trabajo de Auditoría Interna de TI basado en riesgo

Se deben de 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”. (23: 28)

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 gestión de riesgos y control de la actividad comparados con un enfoque o modelo de control relevante.
- Las oportunidades de introducir mejoras significativas en los procesos de gestión de riesgos y control de la actividad. (23:29)

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 mencionan 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. (24:318)

El objetivo del auditor es planificar la auditoría con el fin de que sea realizada de manera eficaz. 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",(23:23,24) el plan de trabajo de la actividad de auditoría interna debe estar basado en una evaluación de riesgos documentada, realizada al menos anualmente.

## 2.7 Detección de necesidades de capacitación de la auditoría interna

El departamento o área de auditoría interna debe de capacitarse constantemente a fin que le permita ser proactiva en su actividad y apoyar a la alta dirección en el logro de sus objetivos.

Ante este fin la auditoría interna debe realizar periódicamente un DNC (detector de necesidades de capacitación) que le permita detectar sus necesidades de fortalecimiento a fin de poder llevar a cabo un plan de capacitación constante y efectivo que dé respuesta y soporte a su plan de trabajo anual, con lo cual podrá enfocar adecuadamente sus esfuerzos a los puntos reales donde debe de brindar servicios de aseguramiento.

## 2.8 Auditoría de cumplimiento

Una auditoría de cumplimiento consiste en el examen y evaluación que se realiza con el objetivo de verificar el cumplimiento de las leyes, decretos y demás disposiciones jurídicas inherentes a la organización. Según las normas internacionales de auditoría para una auditoría de cumplimiento las disposiciones legales y reglamentarias a las que una entidad está sujeta constituyen el marco normativo, y los objetivos del auditor son:

- La obtención de evidencia de auditoría suficiente y adecuada del cumplimiento de las disposiciones legales y reglamentarias.
- La aplicación de procedimientos de auditoría específicos que ayuden a identificar casos de incumplimiento que puedan tener un efecto material.

- Responder adecuadamente al incumplimiento o a la existencia de indicios de incumplimiento de las disposiciones legales y reglamentarias identificados durante la realización de la auditoría. (24:263)

Así mismo, se especifica que el incumplimiento son acciones u omisiones de la entidad, intencionadas o no, que son contrarias a las disposiciones de la ley.

### 2.9 Otras técnicas a considerar por la auditoría interna

En la actividad de auditoría interna existen un sin fin de técnicas o herramientas que pueden ser utilizadas como parte de su alcance, las cuales ayudan a obtener evidencia de la adecuada gestión de las tecnologías de la información, a continuación se presentan un listado de las mismas.

#### 2.9.1 Técnicas de auditoría asistidas por computadora (TAAC)

Esta técnica consiste en “cualquier herramienta automatizada de auditoría, tal como el software generalizado de auditoría, los generadores de datos de prueba, programas de auditoría computarizados y elementos de auditoría de especialización”. (23:194)

Como se ha dicho esta técnica basada en herramientas informáticas permite seleccionar y procesar información para fines de auditoría, facilitando técnicas de muestreo y mejorando el alcance de las pruebas de cumplimiento y sustantivas; lo cual requiere que el auditor al aplicarlas posea los conocimientos y destrezas especiales en dichas técnicas. Entre los procedimientos que soporta están:

- Prueba a controles de aplicaciones
- Selección y monitoreo de transacciones
- Verificación de datos (integridad y disponibilidad)
- Análisis de programas de aplicación.

### 2.9.2 Hackeo ético (Ethical Hacking)

Es una actividad que puede ser utilizada en ambientes controlados para realizar intrusiones a los sistemas informáticos de una organización, donde los responsables de los sistemas a atacar han sido informados de forma previa y han autorizado los mismos con el fin de establecer el estado de inseguridad de los sistemas, así como conocer detalles de sus vulnerabilidades.

Un proceso de análisis de seguridad, se concentra en llevar a cabo evaluaciones que permita reflejar los niveles de seguridad actuales en una infraestructura de TI, considerando las siguientes características: visibilidad, accesos, confianza, autenticación, confidencialidad, privacidad, autorización, integridad, seguridad y alarmas. El auditor de sistemas debe tener en cuenta algunas consideraciones, tales como las siguientes:

- No actuar en ninguna forma que podría resultar en la ruptura de la confidencialidad o la contravención de cualquier ley o contrato.
- Debe conseguir el consentimiento por escrito previo a la realización de una prueba de seguridad.
- Se debe poner a disposición del cliente la información detallada asociada a las acciones que se tomarán como parte de la prueba de seguridad.
- Los auditores deben concientizar a sus clientes en sus responsabilidades de resguardar su información por medios seguros.

### 2.9.3 Implementación de un servidor de auditoría (audit server)

Es una herramienta que brinda apoyo de forma automática para los procesos de fiscalización, el cual genera eventos por excepciones. Esta herramienta está basada en sentencias de SQL y requiere que se tenga conocimientos básicos de programación para poder llevar a cabo la ejecución de sentencias que brinden resultados satisfactorios. El SQL es un lenguaje de consulta estructurado que

permite realizar consultas en bases de datos. Al implementar un servidor de Auditoría se podrá monitorear eventos o grupos de eventos de manera automatizada, a nivel de servidor o base de datos.

- A nivel de servidor, las acciones incluyen las operaciones dentro del servidor, como cambios de administración y operaciones de inicio o cierre de sesión.
- A nivel de base de datos, comprenden operaciones de lenguaje de manipulación de datos o definición de datos.
- A nivel de auditoría, son las sentencias relacionadas con el proceso tal de auditoría.

El cuadro siguiente muestra las funciones básicas de programación que deben conocerse, así como el porcentaje de uso en las consultas que se realizan.

**Cuadro1**

**Funciones básicas de programación**

| Funciones Básicas de Programación | | |
|---|---|---|
| **Función** | **Descripción** | **% de Uso** |
| Select | Consultar información | 46% de los casos |
| Insert | Registrar información | 31% de los casos |
| Update | Actualizar información | 16% de los casos |
| Delete | Eliminar información | 7% de los casos |

| Ejemplo de una consulta simple: | |
|---|---|
| ***Select*** | Columnas |
| ***from*** | tabla |
| ***where*** | condiciones |

Fuente: Elaboración propia en base al trabajo realizado.

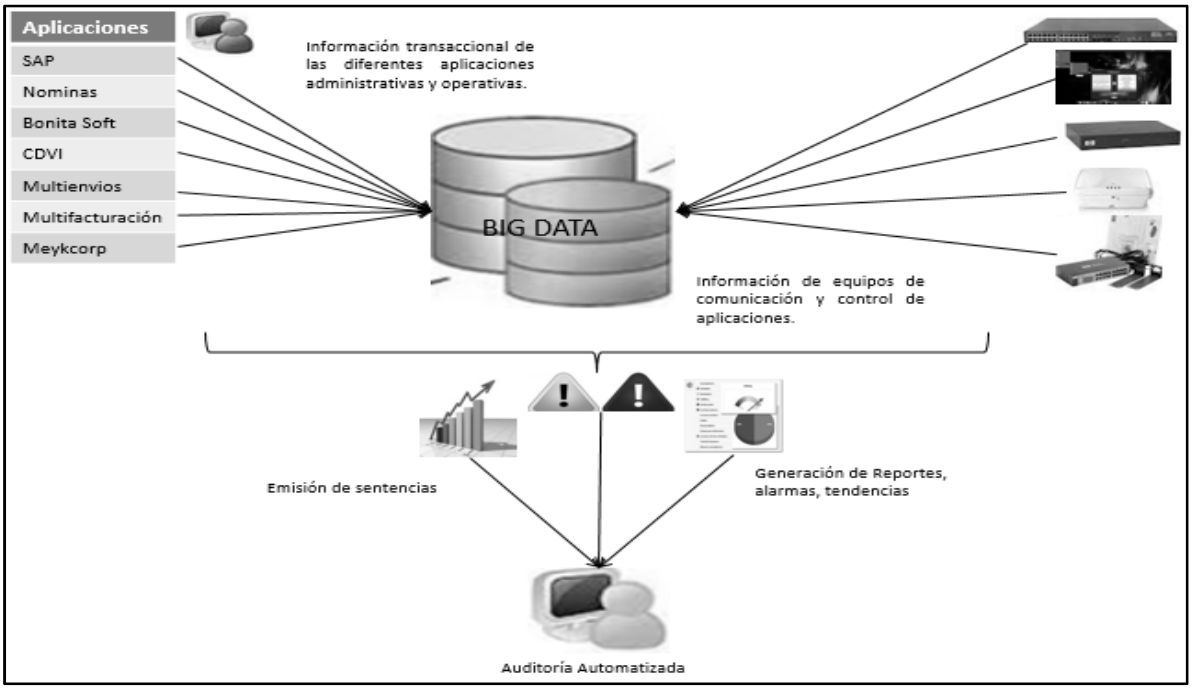
Esta herramienta se utiliza para poder tener en línea consultas a gran nivel transaccional y de varios aplicativos o sistemas al mismo tiempo, a continuación se presentan los pasos a seguir en la implementación del mismo:

- Definir con el área de tecnología, como generar una big data.
- Definición de matriz de controles.
- Definir las sentencias de SQL para implementar los controles.
- Llevar a cabo estudio de factibilidad de los controles y sus sentencias.
- Definir capacidades del servidor con el área de tecnología.
- Pruebas de implementación, consulta y resultados.

Al definir la big data, se debe establecer que información se requiere de cada sistema, bases de datos, servidores y otros programas para que se pueda realizar el consolidado en un solo servidor, el cual debe de guardar todas las medidas de seguridad de la información, con la finalidad de mantener la integridad, confidencialidad y disponibilidad que se requiere. El modelo siguiente muestra un ejemplo de cómo funciona un servidor de auditoría en la compilación de la información y la realización de las consultas.

**Gráfica 1**

**Diagrama de un servidor de auditoría (Audit Server)**




Fuente: Elaboración propia en base al trabajo realizado.

Los resultados de una auditoría especifica o la ejecución de sentencias programadas para ejecutarse cada cierto tiempo, tendrán un destino y un formato de salida, lo cual permite tener un seguimiento oportuno de los eventos que se dan y determinar de forma eficiente la generación de riesgos que puedan impactar a la organización y a la seguridad de la información.

Como bien se indicó se debe de generar una matriz de controles que permita llevar a cabo el monitoreo sobre los aspectos que se desean auditar de forma automática, en esta matriz se debe de establecer el proceso a auditar, el objetivo, periodicidad, tipo de salida de la información, el análisis a realizar, parámetros a cumplir y los campos mínimos propuestos que deben de cumplirse al ejecutarse una sentencia. El anexo 4 presenta una matriz detallada como soporte que puede ser desarrollada para así poder implementarla.

## 2.10 El auditor de sistemas de información y sus funciones

La auditoría de sistemas es la actividad que permite garantizar el nivel de control y salvaguardar los activos tecnológicos y la información en ellos contenidos, por medio de la integridad, confidencialidad y disponibilidad de los datos, apoyando a que las organizaciones alcancen sus objetivos propuestos. Por tanto, la auditoría de sistemas es el conjunto de métodos y técnicas que se aplican a los procesos, estructuras de TI y personal, para verificar como se están llevando a cabo los lineamientos dictados para el área de tecnología con base a buenas prácticas adoptadas por la organización, generando un informe final con el resultado del estado de los procesos auditados.

Los campos de acción de la auditoría en sistemas son:

- La evaluación administrativa del área de tecnología.
- La evaluación de los sistemas y procedimientos.
- La evaluación de la infraestructura tecnológica de TI.

- Evaluación de la seguridad de la información.
- Evaluación de las regulaciones legales que deben de cumplirse.

Algunos objetivos que la auditoría de sistemas debe de cumplir, son:

- Salvaguardar los activos (hardware, software y recurso humano).
- Integridad de los datos.
- Efectividad y eficiencia de los sistemas.
- Asegurar la seguridad de la información.

Al planificar una auditoría al área de TI el auditor de sistemas debe de contar con los conocimientos técnicos requeridos y tener capacidad profesional para llevar a cabo la auditoría a realizar, debiendo considerar en su planificación el entorno en que se desenvuelve la empresa, el ambiente a auditar, las personas críticas dentro del proceso, tener un conocimiento general sobre las líneas de negocio de la organización, así como los tipos de aplicativos que utiliza y en caso de entidades que se ven afectas a normativas, debe de conocer las mismas.

Algunas características que debe de guardar el perfil del auditor en sistemas, son:

- Tener conocimiento de buenas prácticas relacionadas al área de TI.
- Tener pericia en los diferentes procesos de Tecnología.
- Tener organización para llevar de forma controlada el proceso de auditoría.
- Tener independencia y objetividad en la verificación del cumplimiento de los estándares que aplican a la empresa.
- Tener conocimientos básicos en gestión empresarial, tecnológica, base de datos, seguridad de la información, sistemas de información, entre otros.
- Guardar la confidencialidad de los datos observados.

# CAPÍTULO III

# REGLAMENTO PARA LA ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO, SEGÚN RESOLUCIÓN DE LA JUNTA MONETARIA JM-102-2011 CON VIGENCIA A PARTIR DEL 01 DE SEPTIEMBRE DE 2011

## 3.1 Alcance del reglamento y disposiciones generales

La normativa JM-102-2011 fue elevada a consideración de la Junta Monetaria en agosto del 2011 en cumplimiento a lo establecido por el artículo 55 de la ley de bancos y grupos financieros. Este artículo establece que los bancos y las empresas que integran grupos financieros deberán contar con procesos integrales que incluyan, entre otros, la administración del riesgo operacional, del cual forma parte el riesgo tecnológico, todo ello con el propósito de identificar, medir, controlar, monitorear y prevenir los riesgos.

El reglamento considera estar acorde a buenas prácticas observadas a nivel internacional, por lo tanto indica que las organizaciones afectas al mismo, deben de contar con lineamientos mínimos a fin de llevar a cabo una adecuada administración del riesgo tecnológico, con el objetivo de mitigar el riesgo de pérdidas financieras ocasionadas por la materialización de dicho riesgo.

El reglamento define que el riesgo tecnológico “es la contingencia de que la interrupción, alteración, o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, provoque pérdidas financieras a la institución” (27:2) y como administración de riesgo tecnológico “el proceso que consiste en identificar, medir, monitorear, controlar, prevenir y mitigar el riesgo tecnológico.” (Ídem)

El objeto de este reglamento es establecer los lineamientos mínimos que los bancos, las sociedades financieras, las entidades fuera de plaza o entidades off

shore y las empresas especializadas en servicios financieros que forman parte de un grupo financiero, deberán cumplir para administrar el riesgo tecnológico. Sin embargo, de acuerdo al artículo 25 el alcance de aplicación del presente reglamento va más allá del sistema bancario, al indicársele a los afectados que "cuando se contraten servicios de terceros para el procesamiento de su información, las instituciones serán las responsables de cumplir con lo establecido en este reglamento". (27:25)

Entre sus definiciones hay dos conceptos importantes en relación a la clasificación de la información, a decir, criticidad y sensibilidad de la información, el primero se refiere a la "clasificación de la información en diferentes niveles considerando la importancia que ésta tiene para la operación del negocio" y la segunda como "clasificación de la información según el perjuicio que ocasione a la institución su alteración, destrucción, pérdida o divulgación no autorizada". (27:2)

### 3.1.1 Objeto del reglamento

El reglamento tiene como objeto "establecer los lineamientos mínimos que los bancos, las sociedades financieras, las entidades fuera de plaza o entidades off shore y las empresas especializadas en servicios financieros que forman parte de un grupo financiero, deberán cumplir para administrar el riesgo tecnológico". (27:1) No obstante, el artículo 25 de dicho reglamento establece: "cuando se contraten servicios de terceros pare el procesamiento de su información, las instituciones serán las responsables de cumplir con lo establecido en este reglamento. (27:25)

### 3.1.2 Gestión de riesgos

Riesgo es la contingencia numérica (cualitativa o cuantitativa) de que una amenaza se materialice por falta de control. Otra definición que se nos brinda en relación a riesgos indica que es la "posibilidad de ocurrencia de cualquier evento (interno y externo) que puede afectar a una empresa, ocasionándole pérdidas que

disminuyen la capacidad para lograr sus objetivos y generar valor para sus accionistas, dueños, grupos de interés y beneficiarios". (2:3)Por ende la gestión 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 de sus objetivos, con el fin de emprender en forma efectiva las medidas necesarias para responder ante ellos.

Otra definición acorde seria que la gestión de riesgos es "un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos". (15:16)

### 3.1.3 Riesgo tecnológico

El riesgo tecnológico se puede indicar que es el potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daños a la organización, en el ámbito regulatorio nacional la Junta Monetaria en su resolución JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico lo define como "La contingencia de que la interrupción, alteración o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, provoquen pérdidas financieras a la institución". (27:2)

El Riesgo Tecnológico "puede materializarse cuando no hay adecuados planes de gerencia, contingencia, monitoreo del rendimiento tecnológico relacionado a proyectos, productos o servicios. También cuando las organizaciones invierten tarde y, en algunas ocasiones, sin probar adecuadamente las tecnologías". (10:5)

La administración del riesgo tecnológico "es el proceso que consiste en identificar, medir, monitorear, controlar, prevenir y mitigar el riesgo tecnológico." (27:2)

### 3.1.4 Estructura general de la regulación JM-102-2011

La regulación JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico está construida en siete capítulos, el primero de ellos define las disposiciones generales, así como definiciones relacionadas al riesgo tecnológico, los siguientes cinco capítulos representan todo el modelo de la administración del riesgo tecnológico como las actividades de control que deben de disponerse como medidas mínimas, y el último capítulo son las disposiciones transitorias y finales que deben observar las instituciones afectas al mismo.

A continuación se presente la estructura básica de la regulación para una mejor apreciación:

- Organización para la administración del riesgo tecnológico (Capítulo II del Reglamento).
- Infraestructura de TI, sistemas de información, bases de datos y servicios de TI (Capítulo III del reglamento).
- Seguridad de tecnología de la información (Capítulo IV del reglamento).
- Continuidad de operaciones de tecnología de la información (Capítulo V del reglamento).
- Procesamiento de información y tercerización (Capítulo VI del reglamento).

## 3.2 Organización para la administración del riesgo tecnológico

Entre los puntos que deben de considerarse en la organización para la administración del riesgo tecnológico están, las políticas y procedimientos, definición de responsabilidades, creación de un comité de gestión de riesgos, unidad de administración de riesgos, elaboración de un plan estratégico de TI, estructura organizacional de TI y la formalización del manual de administración del riesgo tecnológico, que permitan a una institución “realizar permanentemente una

adecuada administración del riesgo tecnológico, considerando la naturaleza, complejidad y volumen de sus operaciones” .(27:3)

### 3.2.1 Políticas y procedimientos

“Las instituciones deberán establecer e implementar políticas y procedimientos que les permitan realizar permanentemente una adecuada administración del riesgo tecnológico, de la institución, considerando naturaleza, complejidad y volumen de las operaciones. Dichas políticas y procedimientos deberán comprender, como mínimo, las metodologías, herramientas o modelos de medición del riesgo tecnológico”. (27:3)

“Una política es una decisión unitaria que se aplica a todas las situaciones similares, una orientación clara hacia donde deben dirigirse todas las actividades de un mismo tipo, el propósito real de las políticas en una organización, es simplificar la burocracia administrativa y ayudar a la organización a obtener utilidades. Así mismo, una política tiene razón de ser, cuando contribuye directamente a que las actividades y procesos de la organización logren sus propósitos”. (5:27,28)

Los procedimientos por su parte “son la acción que consiste en proceder, así mismo está vinculado a un método o una manera de ejecutar algo. Es un documento escrito que describe secuencialmente, la forma de realizar una actividad para lograr un objetivo dado, dentro de un alcance establecido. Un procedimiento es una forma sistemática de hacer las cosas”. (5:24)

### 3.2.2 Consejo de administración

“El consejo de administración o quien haga sus veces, en lo sucesivo el consejo, sin prejuicio de las responsabilidades que le asignan otras disposiciones legales aplicables, es el responsable de velar porque se implemente e instruir para que se

mantenga en adecuado funcionamiento y ejecución la administración del riesgo tecnológico". (27:4)

### 3.2.3 Comité de gestión de riesgos

"Es el encargado de garantizar que la capacidad de identificar, evaluar y gestionar los riesgos sigue evolucionando con relación al riesgo aceptado por la organización". (16:117) Centrándose principalmente en la eficiencia de la gestión de riesgos corporativos y debe revisar aquellos riesgos que puedan considerarse materiales, la meta del comité consiste en fomentar una reflexión más amplia por parte de la dirección con relación a los riesgos, de tal manera que "se aplique un enfoque más amplio para seguir transformando las competencias de la organización y su visión de gestión de riesgos". (Ídem)

"Estará integrado como mínimo por un miembro del Consejo y por las autoridades y funcionarios que dicho Consejo designe. El comité estará a cargo de la dirección de la administración del riesgo tecnológico, entre otros riesgos, para lo cual deberá encargarse de la implementación, adecuado funcionamiento y ejecución de las políticas y procedimientos aprobados para dicho propósito. Las sesiones y acuerdos del Comité deberán constar en acta suscrita por quienes intervinieron en la sesión". (27:5)

Entre las responsabilidades del comité se pueden definir:

- Supervisar el desarrollo y el análisis anual de las estrategias de riesgos.
- Desarrollar y perfeccionar el riesgo aceptado y la tolerancia al riesgo.
- Proponer al consejo de administración para su aprobación, las políticas y procedimientos para la administración del riesgo tecnológico.
- Reportar al consejo de administración periódicamente y cuando la situación lo amerite sobre la exposición al riesgo tecnológico de la organización. (16:117)

- Analizar los reportes que remita la unidad de administración de riesgos sobre el cumplimiento de las políticas establecidas y “sobre la exposición del riesgo tecnológico de la institución, los cambios sustanciales de tal exposición y su evolución en el tiempo, así como adoptar las medidas correctivas correspondientes”. (27:5)
- Otras funciones que el consejo de administración le asigne.

### 3.2.4 Unidad de administración de riesgos

Es la responsable de realizar las actividades operativas respecto a la administración integral de riesgos, es el ente encargado “de apoyar al Comité en la administración del riesgo tecnológico, para lo cual tendrá las funciones tales como proponer políticas, procedimientos y sistemas para la administración del riesgo tecnológico, revisar al menos anualmente las políticas y procedimientos, el plan estratégico de TI y el plan de continuidad de operaciones de TI, también monitorear la exposición al riesgo y mantener registros históricos del mismo, analizar los riegos nuevos que puedan generarse derivado de la implementación de las innovaciones tecnológicas; reportar sobre la exposición al riesgo tecnológico y su evolución en el tiempo, así como del cumplimiento de las políticas y procedimientos aprobados por el Comité de Gestión de Riesgos”. (27:6)

La unidad debe de ser independiente de las unidades de negocios, a fin de evitar conflictos de intereses y asegurar una adecuada segregación de funciones, la regulación establece “que el consejo debe de asegurarse que la estructura organizacional de TI permita apoyar a la Unidad en los aspectos relacionados con el riesgo tecnológico”. (Ídem)

### 3.2.5 Plan estratégico de TI

“Las instituciones, como parte de su plan estratégico general, deberán tener un plan estratégico de TI alineado con la estrategia de negocios, para gestionar la

infraestructura de TI, los sistemas de información, la base de datos y al recurso humano de TI". (27:7)

El plan estratégico de TI debe incluir, como mínimo, los aspectos siguientes:

- Objetivos de TI alineados a la estrategia de negocios en función del análisis e impacto de factores internos y externos en esta materia;
- Estrategias de TI, para la consecución de los objetivos;
- Proyectos y actividades específicas; y,
- El presupuesto financiero para su ejecución. (Ídem)

El plan estratégico de TI es un plan a largo plazo con un horizonte de tres a cinco años, en el cual la gerencia del negocio y de TI, describen de forma cooperativa como los recursos de TI contribuirán a los objetivos estratégicos empresariales, así como los costos y riesgos relacionados.

"El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI los cuales deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y como el uso de los recursos y el logro de los beneficios serán monitoreados y administrados". (21:30)

### 3.2.6 Organización de TI

"Las organizaciones deberán contar con una estructura organizacional de TI que esté alineada con el plan estratégico, asegurándose que el recurso humano de TI tenga las capacidades necesarias mediante programas de entrenamiento y capacitación, una adecuada segregación de funciones, delegación de autoridad, definición de roles y asignación de responsabilidades, todo esto soportado en un

marco de trabajo estructurado de procesos, los cuales deberán estar debidamente identificados". (27:8)

La organización debe estar enmarcada en un "marco de trabajo de procesos de TI que asegure la trasparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Deben de existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas, y la segregación de funciones. Para garantizar el soporte oportuno a los requerimientos del negocio". (21:41) La definición de los procesos, organización y relaciones de TI, debe estar enfocado en "el establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y en la definición e implementación de procesos de TI con dueños, y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión". (Ídem)

### 3.2.7 Manual de administración del riesgo tecnológico

"Las políticas y procedimientos deberán constar por escrito en un manual de administración del riesgo tecnológico que será aprobado por el Consejo, el cual conocerá y resolverá sobre las propuestas de actualización y modificación al mismo". (27:9) Entiéndase entonces que es un documento escrito formalmente donde se hace constar las políticas y procedimientos establecidos para la administración del riesgo tecnológico.

## 3.3 Infraestructura, sistemas, base de datos y servicios de TI

La tecnología de la información se puede definir como un conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizada de la información. Se podría definir como:

“Tecnologías para el almacenamiento, recuperación, proceso y comunicación de la información”. (33) En su defecto infraestructura de tecnología de la información, es “el hardware, software, redes, instalaciones y otros elementos que se requieren para desarrollar, probar, entregar, monitorear, controlar o dar soporte a los servicios de tecnología de la información. La infraestructura de TI excluye el recurso humano, los procesos y la documentación”. (27:2)

Sistemas de información se denomina al “conjunto organizado de datos, procesos y personas para obtener, procesar, almacenar, transmitir, comunicar y disponer de la información en la institución para un objetivo específico y se conoce como tecnología de la información o TI, al uso de la tecnología para obtener, procesar, almacenar, transmitir, comunicar y disponer de la información, para dar viabilidad a los procesos del negocio”. (Ídem)

Una base de datos es “la organización sistemática de archivos de datos para facilitar su acceso, recuperación y actualización, los cuales están relacionados unos con otros y son tratados como una entidad. Puede decirse que una base de datos es un banco de datos organizado como un tipo estructurado de datos”. (13:99)

El conjunto de programas que permite manejar cómodamente una base de datos o el conjunto de facilidades y herramientas de actualización y recuperación de una base de datos se denomina DBMS, que quiere decir, sistema de información de base de datos (Data Base Management System). (Ídem)

Y los servicios de TI son un conjunto de actividades que buscan responder a las necesidades de un cliente por medio de un cambio de condición en los activos tecnológicos potenciando el valor de estos y reduciendo el riesgo inherente por medio de “una adecuada gestión de los servicios de TI de acuerdo con las prioridades del negocio”. (27:15)

### 3.3.1 Esquema de la información del negocio

“Las instituciones deberán contar con un esquema actualizado de la información del negocio que represente la interrelación entre la infraestructura de TI, los sistemas de información, los servicios de TI y los procesos de las principales líneas de negocio”. (27:10)

### 3.3.2 Inventario de infraestructura, sistemas y base de datos

“Las instituciones deberán mantener inventarios actualizados de su infraestructura de TI, de sus sistemas de información y de sus bases de datos”. (27:11)

Los inventarios de infraestructura de TI, deberán contar, como mínimo, con lo siguiente:

- Especificaciones técnicas de sus elementos (tipo, nombre, función y mantenimiento).
- Ubicación física de sus elementos. (Ídem)

Los inventarios de sistemas de información, deben contar mínimo con lo siguiente:

- Características de los sistemas de información.
- Documentación técnica
- Documentación para el usuario final. (Ídem)

Los inventarios de bases de datos, deben contener como mínimo lo siguiente:

- Nombre
- Descripción general de la información que contiene
- Manejador de base de datos o sistemas de gestión de archivos y su versión.

- Nombre de los servidores en que reside
- Diccionario de datos
- Diagramas de relación; y
- Nombre del administrador de la base de datos (Ídem)

### 3.3.3 Administrador de base de datos

“Las instituciones deberán designar uno o más administradores de base de datos para gestionar los controles de accesos, la integridad, disponibilidad y confidencialidad de los datos, así como los procesos de creación, actualización o eliminación de estructuras en las bases de datos, entre otros”. (27:12)

### 3.3.4 Diagrama de relación

“Es la representación gráfica que describe la distribución de datos almacenados en las bases de datos de la institución y la relación entre éstos, tales como los diagramas de entidad-relación para el caso de bases de datos del tipo relacional”. (27:2)

### 3.3.5 Diccionario de datos

“Es la documentación relativa a las especificaciones de los datos, tales como su identificación, descripción, atributos, el dominio de valores, restricciones de integridad y ubicación dentro de una base de datos”. (Ídem)

### 3.3.6 Monitoreo de la infraestructura, sistemas y base de datos

“Las instituciones deberán realizar evaluaciones periódicas de la capacidad y desempeño de la infraestructura de TI, de los sistemas de información y de las bases de datos, con el objeto de determinar necesidades de ampliación de capacidades o actualizaciones. Las instituciones deberán documentar y llevar

registro de las evaluaciones periódicas y realizar análisis de tendencias para determinar capacidades futuras". (27:13)

### 3.3.7 Adquisición, mantenimiento e implementación de TI

"Las instituciones deberán contar con procesos documentados y planes operativos para la adquisición, mantenimiento e implementación de la infraestructura de TI, de los sistemas de información y de las bases de datos" (27:14)

En lo referente a adquisición y mantenimiento, deberán incluirse como mínimo los siguientes aspectos:

- Selección de proveedores, considerando factibilidad tecnológica y económica.
- Contratación, considerando la suscripción y ejecución. (Ídem)

En lo referente a implementación, deberán incluirse como mínimo lo siguiente:

- Realización de pruebas.
- Registro y monitoreo de la implementación. (Ídem)

La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. "Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio para garantizar que las mismas sigan satisfaciendo los objetivos del negocio". (21:12,13)

"Las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica, esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio". (21:81) Como parte de la

adquisición, implementación y mantenimiento de los recursos de TI adquiridos, se deben de tomar en consideración aspectos como:

- Generación de documentación y manuales de usuarios y para TI.
- Transferencia de conocimientos a los usuarios involucrados.
- Desarrollar y seguir un conjunto de procedimientos y estándares consistente en el proceso general de adquisiciones de la organización.
- Administración de contratos con proveedores.
- Contar con un control de cambios relacionado con la infraestructura y las aplicaciones dentro del ambiente de producción.
- Contar con ambientes de prueba y de producción. (21:86, 90, 93, 98)

### 3.3.8 Gestión de servicios de TI

"Se debe de contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, que hagan posible una comunicación efectiva entre la gerencia de TI y los clientes del negocio respecto a los servicios requeridos". "El marco de trabajo para la gestión de servicios de TI debe incluir procesos para la creación de requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLAs), acuerdos de niveles de operación (OLAs) y las fuentes de financiamiento". (21:101,102)Las instituciones deberán realizar una adecuada gestión de los servicios de TI de acuerdo con las prioridades del negocio estableciendo, como mínimo, los aspectos siguientes:

- Un catálogo que comprenda la definición de cada servicio de TI.
- Acuerdos de niveles de servicio de TI establecidos entre las áreas del negocio y las áreas de TI.
- Procesos de gestión de incidentes y problemas.
- Procesos de gestión de cambios en infraestructura de TI, sistemas de información y bases de datos. (27:15)

“Los servicios deben implantarse con un enfoque de catálogo/portafolio de servicios. Un servicio entregado por TI es una meta de TI, pero es un indicador de desempeño y una capacidad para el negocio”. (21:22)

### 3.3.9 Ciclo de vida de los sistemas de información

“Las instituciones deberán implementar metodologías adecuadamente documentadas para el análisis, diseño, desarrollo, pruebas, puesta en producción, mantenimiento, control de versiones y control de calidad de los sistemas de información. Las actividades de desarrollo y producción deberán realizarse en ambientes distintos”. (27:16)

## 3.4 Seguridad de tecnología de la información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

Debe entenderse que “la seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos”. (25:16)

### 3.4.1 Gestión de la seguridad de la información

“Las instituciones deberán gestionar la seguridad de su información con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos, así como

mitigar los riesgos de pérdida, extracción indebida y corrupción de la información". (27:17) Su orientación será siempre en función de confidencialidad, integridad, disponibilidad, y cumplimiento. Debe hacerse conocer lo que se debe hacer y lo que no, estos acuerdos deben estar en función de la variabilidad de las tecnologías, naturaleza de los interesados, alcance de las sanciones y cambios en los procedimientos. La gestión de seguridad de tecnología de la información debe considerar como mínimo, los aspectos siguientes:

- Identificación y clasificación de la información de acuerdo a criterios de sensibilidad y criticidad.
- Roles y responsabilidades para la gestión de la seguridad de la información.
- Monitoreo de la seguridad de la información.
- Seguridad física que incluya controles y medidas de prevención para resguardar adecuadamente la infraestructura de TI.
- Seguridad lógica que incluya controles y medidas de prevención para resguardar la integridad y seguridad de los sistemas de información y de los datos. (27:17)

Estas políticas deberán ser un marco de referencia, que orientan al gobierno corporativo para la realización de procedimientos correctos. Su orientación será siempre, el cumplimiento de la misión y la visión. "Debe entenderse que serán un marco de referencia basado en reglas, que orientan al gobierno de la TI para la realización de procedimientos tecnológicos correctos". (14:3)

Se debe administrar la seguridad de TI "al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio". (21:118) Así también, deberá garantizarse que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria, lo que busca es "mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad". (21:120)

### 3.4.2 Criticidad y sensibilidad de la información

La criticidad “se refiere a la clasificación de la información en diferentes niveles considerando la importancia que ésta tiene para la operación del negocio”. (27:2) Mientras que la sensibilidad se define en la normativa como la “clasificación de la información según el prejuicio que ocasione a la institución su alteración, destrucción, pérdida o divulgación no autorizada”. (Ídem)

### 3.4.3 Copias de respaldo

Es realizar regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo a una política adecuada de recuperación, con el objetivo de mantener la integridad y disponibilidad de los servicios de tratamiento de información y comunicación. “Se debe de decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de soportes”. (35)

“Las instituciones deberán tener copias de la información de la infraestructura de TI, sistemas de información y bases de datos, para lo cual deberán considerar como mínimo la información a respaldar, periodicidad y validación de las copias, procedimientos de restauración, congruencia con la estrategia institucional para la continuidad de operaciones y ubicación de las copias de respaldo y de la documentación de los procedimientos de restauración.” (27:18)

### 3.4.4 Operaciones y servicios a través de canales electrónicos

Un canal electrónico es un medio para comunicarse por internet o por red de telecomunicaciones abiertas que abarca desde conexiones directas, el world wide web público, cable y redes privadas virtuales. Otro contexto sobre el tema indica “que es una herramienta desarrollada en ambiente gráfico HTML (Lenguaje de Marcas de Hipertexto), que permite acceder a través de la red mundial de

información (Internet) a toda la información, productos y servicios de la relación que se mantiene con las filiales de un banco y se emplea cuando no es necesario un contacto humano. Por ejemplo, hacer transacciones bancarias o hacer consultas en Internet". (17:259)

El sistema bancario ha utilizado cada vez más los canales electrónicos para recibir instrucciones y entregar sus productos y servicios a sus clientes. Es entonces "la provisión de transacciones de productos o servicios bancarios en línea por un banco. Desde el punto de vista del sistema bancario este servicio puede ser categorizado en tres niveles, sitios web de información básica, sitios web de transacciones simples y sitios web de transacciones avanzadas". (3:2,5) Las instituciones que realicen operaciones y presten servicios financieros a través de canales electrónicos deberán implementar, como mínimo, lo siguiente:

- Mecanismos para la protección y control de la infraestructura de TI, los sistemas de información y las bases de datos.
- Medidas de seguridad en el intercambio de información a través de los canales electrónicos. Cualquier intercambio de información sensible debe estar respaldado por un certificado digital, cifrado de datos u otro mecanismo que permita garantizar la trasferencia de información.
- Programas de educación y divulgación de información para clientes; y
- Registro y bitácoras de las transacciones efectuadas. (27:19)

### 3.4.5 Controles aplicativos en tecnología de la información

Se entiende por controles de aplicación los "procedimientos manuales o automatizados que operan típicamente a nivel del proceso del negocio. Los controles aplicativos pueden ser de naturaleza preventiva o de detección y están diseñados para asegurar la integridad de los registros. En consecuencia, los controles aplicativos se refieren a procedimientos utilizados para iniciar, registrar, procesar y reportar transacciones u otros datos". (24:23)

### 3.4.6 Buenas prácticas en tecnología de la información

“Los marcos de referencia con herramientas sólidas son esenciales para asegurar que los recursos de TI estén alineados con los objetivos del negocio, y que los servicios y la información satisfagan los requisitos de calidad, financieros y de seguridad… COBIT e ITIL no son mutuamente excluyentes y pueden ser combinados para obtener un poderoso marco de referencia de mejores prácticas, control y gobierno en la gestión de servicios de TI. Las empresas que quieren ubicar sus programas ITIL en el contexto de un amplio marco de referencia de gobierno y control deberían utilizar COBIT”. (4:8)

Incrementalmente hoy en día, el uso de “estándares y mejores prácticas tales como ITIL, COBIT e ISO/IEC 27002, está siendo conducido por requerimientos de negocio para mejoras de desempeño, transparencia y control sobre actividades de TI”. (4:10)

- **COBIT:** “Es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales. COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas”. (4:13) “COSO es generalmente aceptado como el marco de trabajo de control interno para las empresas. COBIT es el marco de trabajo de control interno generalmente aceptado para TI”. (21:7)

- **ITIL V3:** Las siglas de ITIL significan Information Technology Infrastructure Library o bien Librería de Infraestructura de Tecnología de Información. Esta metodología es la aproximación más globalmente aceptada para la gestión de servicios de tecnologías de información en todo el mundo, ya

que es una recopilación de las mejores prácticas tanto del sector público como del sector privado. Estas mejores prácticas se dan en base a toda la experiencia adquirida con el tiempo en determinada actividad y son soportadas bajo esquema organizacionales complejos, pero a su vez bien definidos y que se apoyan en herramientas de evaluación e implementación. “La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI”. (4:14)

- **ISO/IEC 27002:** “El objetivo del estándar ISO/IEC 27002:2005 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para mejorar la fiabilidad en la seguridad de la información en las relaciones inter organizacionales”. (4:17) Los principios rectores en la norma ISO/IEC 27002:2005 son los puntos de partida para la implementación de seguridad de la información. Se basan en cualquiera de los requisitos legales o en las mejores prácticas generalmente aceptadas.

### 3.5 Continuidad de operaciones de tecnología de la información

“La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio”. (21:113)

Se debe desarrollar un marco de trabajo para la continuidad de TI para soportar la continuidad del negocio como un proceso consistente y largo a través de toda la organización, este marco debe de tomar en cuenta la estructura organizacional, la cobertura de roles, las tareas y responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes. “El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación”. (21:114)

### 3.5.1 Plan de continuidad de operaciones de TI

Un plan de contingencia se define como “la identificación y protección de los procesos críticos de la organización y los recursos requeridos para mantener un aceptable nivel de transacciones y de ejecución, protegiendo estos recursos y preparando procedimientos para asegurar la sobrevivencia de la organización en caso de desastre. En la elaboración del plan de contingencia deben de intervenir los niveles ejecutivos de la organización y el personal usuario y técnico de los procesos”. (13:252,253)

“Las instituciones deberán contar con un plan de continuidad de operaciones de TI, que esté alineado a las necesidades de la institución, para recuperar los procesos críticos de las principales líneas de negocio soportados por TI, así como la información asociada en caso de una interrupción”. (27:20) El plan de continuidad de operaciones de TI deberá incluir, como mínimo, los aspectos siguientes:

- Objetivo y alcance del plan.
- Identificación de los procesos críticos de las principales líneas de negocio.
- Identificación de los proceso de TI que soportan los procesos de negocio.
- Procedimientos y canales de comunicación.
- Procedimientos de recuperación y restauración procesos críticos.

- Identificación y descripción de responsabilidades del personal clave para la continuidad de operaciones de TI y listado de proveedores.
- Recursos necesarios para la recuperación.
- Convenios documentados con terceros; e
- Identificación de factores de dependencia interna y externa de la institución, tales como proveedores, personal de la entidad u otros, y las acciones para mitigar el riesgo de dicha dependencia. (27:20)

### 3.5.2 Pruebas al plan de continuidad de operaciones de TI

"Las instituciones deberán elaborar como parte del plan de continuidad de TI un plan de pruebas que incluya, como mínimo: alcance, escenarios y periodicidad. Los resultados de las pruebas realizadas deberán documentarse y, cuando corresponda, adecuar el plan de continuidad de operaciones de TI en función de los resultados obtenidos". (27:21)

### 3.5.3 Capacitación del personal clave para la continuidad de operaciones

"Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información, estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran"."La organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión". (21:12,41)

Se debe de "implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia debe asegurar también de que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas, así como evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente de negocios, operativo o de TI para garantizar que la

función de TI cuente con un número suficiente de recursos para soportar adecuadamente y apropiadamente a las metas y objetivos del negocio". (21:42)

"Las instituciones deberán mantener capacitado al personal clave, para activar o probar el plan de continuidad de operaciones de TI y sus modificaciones". (27:22) En este aspecto, debe definirse e identificarse al personal clave de TI y "minimizarla exposición a dependencias sobre individuos claves por medio de la captura de conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal, verificando de forma periódica que el personal tenga las habilidades para cumplir con sus roles con base a su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les de mantenimiento, usando programas de calificación y certificación según sea el caso". (21:56)

### 3.5.4 Centro de cómputo alterno

"Las instituciones deberán contar con un centro de cómputo alterno con las características físicas y lógicas necesarias para dar continuidad a las operaciones y los procesos críticos de negocios, cumpliendo con los requisitos establecidos referentes a seguridad de tecnología de la información, infraestructura de TI, sistemas de información y bases de datos". (27:23)

El centro de cómputo alterno deberá estar en una ubicación distinta del centro de cómputo principal, de tal forma que no se vean expuestos a un mismo nivel de riesgo ante la ocurrencia de un mismo desastre. Se entenderá por desastre todo evento que interrumpa las operaciones normales de un negocio". (Ídem)

El centro de cómputo alterno es parte del plan de continuidad de las operaciones y cubre "la necesidad de brindar continuidad en los servicios de TI, un proceso efectivo de continuidad de servicios, minimiza la probabilidad e impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves

del negocio". (21:113) Un centro de cómputo alterno busca "garantizar la continuidad del servicio y asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI". (Ídem)

"La administración del sitio de almacenamiento externo a las instalaciones, debe de apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de la empresa. La gerencia de TI debe asegurar que existan acuerdos para evaluaciones periódicas, al menos una vez por año, respecto al contenido, la protección ambiental y la seguridad. Como también asegurar la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados". (21:114)

### 3.6 Procesamiento de información y tercerización

El procesamiento de la información es la "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". (37)

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 tercerizar su información.

#### 3.6.1 Procesamiento de información

"Las instituciones podrán procesar su información dentro o fuera del territorio nacional debiendo contar para el efecto con la infraestructura de TI, sistemas de información, bases de datos y personal técnico capacitado con el propósito de asegurar la disponibilidad, integridad, confidencialidad y accesibilidad de la información". (27:24)

En el caso de procesamiento fuera del territorio nacional, las instituciones previamente deberán contar con autorización de la Superintendencia de Bancos y cumplir con los requisitos siguientes:

- Contar con un centro de cómputo alterno ubicado en el territorio nacional.
- Disponer de personal técnico y uno o más administradores de bases de datos, en el territorio nacional, capacitados para operar el centro de cómputo alterno.
- Replicación en tiempo real hacia servidores locales de su información procesada fuera del territorio nacional; y
- Permitir a la Superintendencia de Bancos el libre acceso a su infraestructura de TI, sistemas de información, bases de datos e instalaciones ubicadas fuera del territorio nacional, y proporcionar a ésta la información que le requiera. (27:24)

### 3.6.2 Tercerización

“Cuando se contraten servicios de terceros para el procesamiento de su información, las instituciones serán las responsables de cumplir con lo establecido en el reglamento”. (27:25) En los contratos que se suscriban las instituciones deberán incluir, como mínimo, lo siguiente:

- Que la Superintendencia de Bancos tendrá libre acceso a las instalaciones de los contratados, infraestructura de TI, sistemas de información y bases de datos, relacionadas con el servicio contratado por la institución.
- Que el contratado tiene obligación de proporcionarle a la Superintendencia de Bancos, cuando ésta se lo requiera, toda la información y/o documentos relacionados con las operaciones y servicios de tercerización prestados.
- Que el contratado guardará la confidencialidad de las operaciones y servicios que realizare y demás información a que tenga acceso con motivo de su relación con la institución contratante.

- Que el contratado se compromete a cumplir con la institución lo establecido en el reglamento, relativo a la infraestructura de TI, sistemas de información, bases de datos, servicios de TI, seguridad de la tecnología de la información y continuidad de operaciones de tecnología de la información.
- Acuerdos de niveles de servicio. (27:25)

### 3.7 Junta Monetaria

Es la autoridad máxima del Sistema Financiero. Sus funciones son determinadas por la Constitución Política de la República de Guatemala y la Ley Orgánica del Banco de Guatemala. Tiene a su cargo “la determinación de la política monetaria, cambiaria y crediticia del país y velar por la liquidez y solvencia del sistema bancario nacional, asegurando la estabilidad y el fortalecimiento del ahorro nacional”. (8:133)

### 3.8 Banco de Guatemala

“Es una entidad descentralizada autónoma, con personalidad jurídica, patrimonio propio, con plena capacidad para adquirir derechos y contraer obligaciones, de duración indefinida y con domicilio en el departamento de Guatemala, así mismo tiene como objetivo principal contribuir a la creación y mantenimiento de las condiciones más favorables al desarrollo ordenado de la economía nacional, propiciando las condiciones monetarias, cambiarias y crediticias que promueven la estabilidad en el nivel general de precios”. (19:2,3)

Entre sus principales funciones están:

- Ser el único emisor de la moneda nacional.
- Procurar que se mantenga un nivel adecuado de liquidez en el sistema bancario mediante la utilización de instrumentos para este fin.

- Procurar el buen funcionamiento del sistema de pagos.
- Recibir en depósito los encajes bancarios y los depósitos legales.
- Administrar las reservas monetarias internacionales, de acuerdo a los lineamientos que dicte la Junta Monetaria.
- Otras funciones compatibles con la naturaleza de Banco Central que le sean asignadas por mandato legal.

### 3.9 Superintendencia de Bancos

La Superintendencia de Bancos (SIB), organizada conforme a la Constitución Política de la República de Guatemala, Ley de Supervisión Financiera, Ley Orgánica del Banco de Guatemala, La Ley Monetaria y las demás leyes, “es el órgano que ejerce la vigilancia e inspección de bancos, instituciones de crédito, empresas financieras, empresas de seguros y las demás que la ley disponga. La Superintendencia de Bancos es un órgano de la Banca Central y la dirección de la misma está ejercida por la Junta Monetaria”. (20:1,2)

La Superintendencia de Bancos está organizada de acuerdo a la Ley de Supervisión Financiera, decreto 18-2002 del Congreso de la República de Guatemala y sus reglamentos, aprobados por la Junta Monetaria.

### 3.10 Sistema financiero del país

Es el conjunto de instituciones públicas y privadas que generan, captan, administran y canalizan tanto el ahorro como la inversión dentro de una actividad financiera, política y económica del país; por lo que constituyen el eje o la base fundamental en que descansa la estabilidad financiera y el desarrollo económico del país.

El sistema financiero en general comprende la oferta y la demanda de dinero y de valores de toda clase, en moneda nacional y extranjera. Se difiere entonces en

que “es el sistema circulatorio que liga los bienes, los servicios y finanzas en los mercados domésticos e internacionales”, también se dice que “el sistema financiero administra el riesgo de la economía”. (26:464,465)

El sistema financiero representa un papel muy importante para el crecimiento económico de un país, por ello “se coincide en afirmar que su función principal es contribuir con el logro de los objetivos de estabilización y crecimiento económico de un país. Al mismo tiempo, se le atribuyen ciertas funciones específicas como la creación, intercambio, transferencia y distribución de activos y pasivos financieros.” Y su función principal la podemos definir como “contribuir con el logro de los objetivos de estabilización y crecimiento económico de un país”. (32)

### 3.11 Sistema bancario de Guatemala

“Conjunto de entidades o instituciones que dentro de la economía de un país presentan el servicio de banca, es decir de intermediación financiera”. (1:44) Está conformado por las instituciones bancarias legalmente establecidas en el país y que prestan sus servicios a las personas, empresas y organizaciones que impliquen el uso de dinero.

### 3.12 Sistema de pagos

El banco de Guatemala define los sistemas de pago como “un sistema que consta de una serie de instrumentos, procedimientos bancarios y, por lo general, sistemas interbancarios de transferencia de fondos que aseguran la circulación del dinero” y también como “un conjunto de instrumentos, procedimientos y normas para la transferencia de fondos entre los participantes del sistema. Esto suele implicar que existe un acuerdo entre un grupo definido de participantes en el sistema y el operador del mismo, y que la transferencia de fondos se realiza utilizando una infraestructura técnica acordada de antemano”. (11:2)

### 3.13 Compensación bancaria

Es un procedimiento utilizado por las instituciones de crédito para simplificar las operaciones acreedoras y deudoras que tengan entre sí, a través de tramitar diariamente en un lugar común y mediante un reglamento, aquellos documentos en los que se reúna previamente las calidades de deudor y acreedor, respecto de instituciones que operan en una misma plaza, inclusive en una región o en todo el territorio de la República. “Este procedimiento se realiza tanto de títulos de crédito, como de aquellos que les presentan sus clientes para sus cobros realizando las operaciones respectivas, liquidando los saldos en la cuenta corriente que cada institución tiene en el Banco Central”. (12:56)

### 3.14 Cheque

Es un documento que “constituye el medio normal o regular de disponer total o parcialmente del saldo acreedor de una cuenta corriente bancaria, revistiendo la forma de una orden escrita, extendida en formularios que suministra la institución en la cual se tiene la cuenta corriente con saldo favorable y se concreta en la entrega de la cantidad mencionada, o en el acreditamiento de dicha cantidad en otra cuenta por el mismo banco”. (22:680)

Otro concepto referente al cheque como título valor es que “incorpora el derecho literal y autónomo de pagar una suma de dinero, cuyo ejercicio o transferencia es imposible independientemente del título, se libra contra un banco, en formularios impresos y suministrados y aprobados por el mismo”. (7:385,494)

Las características generales de impresión, color y diseños, son variables; más no así las medidas, las áreas de distribución de zonas en el cuerpo de los cheques, las cuales están establecidas en el documento denominado “Instructivo para la Estandarización de Cheques en el Sistema Bancario Nacional”, anexo al Reglamento de la Cámara de Compensación Bancaria, Resolución JM-51- 2003.

# CAPÍTULO IV

# ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO

## 4.1 Implementación de la gestión del riesgo tecnológico

La gestión del riesgo tecnológico debe de ser establecido bajo criterios de buenas prácticas, considerando en el mismo lineamientos mínimos que coadyuven en primer lugar a la administración en el logro de sus objetivos estratégicos, segundo gestionar adecuadamente aquellos riesgos que de materializarse puedan ocasionar pérdidas graves o irreparables a la entidad y tercero dar cumplimiento a disposiciones establecidas por entes reguladores.

Como primer paso para la implementación de una gestión de riesgos, debe de entenderse que la misma impulsa la credibilidad y la transparencia, facilitando el incremento de ingresos, reducción de gastos y ayuda a manejar intangibles como reputación y marca.

Los pasos a seguir en el establecimiento de la metodología para la administración del riesgo tecnológico debiese ser:

a. Definir el contexto para la administración del riesgo.
b. Establecer el marco de referencia para gestionar los riesgos.
c. Definir el proceso para la administración del riesgo tecnológico.

El contexto se refiere al todo el ambiente tanto interno como externo en que opera la organización, normas jurídicas, leyes y normativas internas a las que está expuesta, cultura organizacional, estructura organizacional y de tecnología, relación con proveedores y clientes. Comprende además el establecer los objetivos, metas y alcance del proyecto, definición de responsabilidades, entre otros aspectos que se consideren necesarios.

El marco es la adopción o consulta de mejores prácticas para definir las políticas y procedimientos que regirán la administración del riesgo tecnológico, el mismo requiere dirección y compromiso por parte de todos los involucrados para el diseño adecuado, implementación, seguimiento y revisión del marco de trabajo, por medio de la mejora continua al mismo.

El proceso para la administración de riesgos se refiere al cómo llevar a cabo la identificación, análisis, evaluación, tratamiento, supervisión y comunicación relacionada a la administración del riesgo tecnológico. El proceso como tal debe ser parte integral de la gestión de la organización, debe de considerarse como parte de una cultura y sobre todo, la administración del riesgo tecnológico debe estar en contexto a los procesos del negocio.

Durante la implementación de la administración del riesgo tecnológico debe de establecerse un equipo de trabajo multidisciplinario que tenga los conocimientos necesarios en metodologías de riesgos, control, tecnología de la información y de los servicios o procesos críticos del negocio, el cual en base a su conocimiento y experiencia aporten al enriquecimiento y madurez a la administración del riesgo tecnológico.

### 4.2 Metodologías para la administración de riesgos

Los marcos de referencia son esenciales para asegurar que los recursos de TI estén alineados con los objetivos del negocio, estos marcos o metodologías, brindan a la vez herramientas sólidas para una adecuada administración del riesgo, es preciso aclarar que la administración de riesgo tecnológico es un proceso que involucra una mejora continua y que no termina con la implementación del mismo. Por varios años se han creado marcos de trabajo, metodologías y estándares destinados al gobierno de TI y a la administración de los riesgos de tecnología, “hoy como cada organización, trata de entregar valor a través de TI, a la vez que gestiona un complejo rango de riesgos relacionados a

TI, el uso efectivo de las mejores prácticas puede ayudar a evitar la reinvención de sus propias políticas y procedimientos, optimizando el uso de escasos recursos de TI y reduciendo la incidencia de los mayores riesgos de TI". (4:10)

A continuación se presentan las características principales de algunas de estas mejores prácticas con la finalidad de tener una orientación para su aplicación, según las necesidades que tenga la empresa.

### 4.2.1 Marco de trabajo 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)

Este marco de trabajo es un proceso dinámico basado en un conjunto de actividades, realizado por las personas, aplicado como estrategia de negocio y diseñado y enfocado a identificar eventos y no solo riesgos. Entre sus conceptos claves podemos definir:

a. Toda entidad debe dar valor al accionista
b. Toda entidad tiene incertidumbre
c. La incertidumbre puede ser un riesgo o una oportunidad

Los componentes principales de COSO ERM, son:

- Ambiente interno
- Establecimiento de objetivos
- Identificación de eventos
- Evaluación de riesgos

- Respuesta a los riesgos
- Actividades de control
- Información y comunicación
- Supervisión (16:6)

### 4.2.2 Estándar ISO 31000:2009 Gestión de Riesgos

Es un estándar que “proporciona los principios y las directrices genéricas sobre la gestión de riesgo, que puede utilizarse por cualquier empresa, pública, privada o social, asociación, grupo o individuo. Por tanto, no es específica de una industria o sector concreto”. (36)

El enfoque está estructurado en tres elementos claves que son:

- Principios para la gestión del riesgos
- Estructura para la gestión del riesgo
- Proceso de gestión del riesgos

Este estándar define el riesgo como “el efecto de la incertidumbre en la consecución de los objetivos”. (Ídem)Indica además que la gestión del riesgo y el aseguramiento de su eficacia continua, requiere un compromiso fuerte y sostenido por parte de la alta dirección de la organización y planes de acción que permitan que el personal a todo nivel tenga compromiso con el proceso.

### 4.2.3 Estándar AS/NZS 4360:2004

Es un documento que brinda directrices de cómo establecer e implementar un proceso de gestión de riesgos, basado en un conjunto de etapas que inician con el establecimiento del contexto del riesgo y continúa con las etapas subsiguientes, identificación, análisis, evaluación y tratamiento de riesgos. Esta metodología tuvo su origen en Australia y Nueva Zelanda.

Algunas de sus características principales son:

- Requiere establecer directrices de forma descendente, que van desde la parte superior en la estructura organizacional hasta el personal operativo.
- Provee un modelo de proceso detallado.
- Identifica y gestiona los riesgos a nivel corporativo.
- Se alinea a los objetivos del negocio.

### 4.2.4 Marco de trabajo RISK IT

Es un marco de trabajo diseñado y creado por la Asociación de Auditoría y Control de Sistemas de Información, ISACA, principalmente diseñado como un recurso educativo para los oficiales de información, la alta dirección y administración de TI.

El marco de los riesgos de TI, RISK IT, se complementa con COBIT el cual proporciona un conjunto de controles para mitigar los riesgos de TI. RISK IT establece las mejores prácticas con el fin de establecer un marco para las organizaciones para identificar, gobernar y administrar los riesgos asociados a su negocio. Por lo tanto RISK IT, es un marco de trabajo con enfoque práctico que tiene como base un conjunto de principios para guiar la gestión integral de los riesgos de TI.

### 4.2.5 Marco de trabajo COBIT

Es un marco de trabajo creado por ISACA, cuyo enfoque está basado en las tecnologías de información y el gobierno de TI y cuenta con una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, brinda “buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica”. (21:5) La misión de COBIT es investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI aceptado a nivel internacional, para la adopción por parte de las empresas y

el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.

Este marco establece siete criterios de control para la información, siendo estos, efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Así mismo, ofrece mecanismos para la medición de las capacidades de los procesos con objeto de conseguir una mejora continua. Este marco se “ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI”. (21:8)

Actualmente COBIT 4.1 es la versión de mayor referencia el cual cuenta con 4 dominios, 34 procesos y 210 objetivos de control, sin embargo, en el año 2012 se publicó la nueva versión COBIT 5 para la seguridad de la información, mismo que proporciona una visión empresarial del Gobierno de TI, el cual por medio de la tecnología y la información crean valor a las empresas.

### 4.2.6 Estándar ISO/IEC 27005:2011 Seguridad de la Información

Es un estándar basado en la seguridad de la información, provee directrices para la gestión de los riesgos, el cual requiere que se tengan conocimientos previos de otros estándares como lo son la ISO/IEC 27001 e ISO/IEC 27002 los cuales proveen información sobre conceptos, modelos, procesos y terminología utilizados en la seguridad de la información.

Esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información, e indica que corresponde a cada organización definir su enfoque para la gestión del riesgo, dependiendo de su sistema de gestión de seguridad de la información.

Entre sus objetivos podemos mencionar:

- Enfoque de gestión de riegos tecnológicos, relacionado con la seguridad de la información.
- Alineación con los objetivos de negocio, relacionados con la protección e integridad de la información.
- Provee un modelo de proceso detallado, que soporta la gestión de riesgos.
- Requiere la participación de todo el personal desde la alta dirección hasta el personal operativo, por medio de directrices.

### 4.2.7 Metodología MAGERIT

Metodología de análisis y gestión de riesgos para los sistemas de información cuyo objetivo es minimizar los riesgos en la implantación y uso de las tecnologías de la información. Fue elaborada por el Consejo Superior de Administración Electrónica de España y actualmente existe en su versión tres.

Magerit está compuesto por tres libros, el primero establece el método que debe de seguirse, el segundo brinda un catálogo de elementos a considerarse y el tercero es la guía técnica de aplicación. Algunas características de esta metodología son:

- Su enfoque con los objetivos de los negocios es parcial ya que tiene enfoques muy particulares.
- La perspectiva de aplicación se adhiere únicamente a los riesgos de sistemas de información de TI y su entorno.
- Es una metodología de acceso libre a todo el público.

## 4.3 Fases para la gestión de riesgos de TI en base a COSO ERM

El proceso de la gestión de riesgos consiste en dirigir todas las actividades necesarias para asistir a la organización en busca de mayores beneficios, reduciendo la incertidumbre a un nivel aceptado por el negocio cuando se utilizan

los recursos de tecnología. La administración del riesgo tecnológico, hace parte de la actividad empresarial y por lo tanto debe de formar parte de la gestión de riesgos corporativos, asegurando una estructura uniforme, lógica, repetitiva y comparable con el desarrollo y administración de los riesgos de la organización. A continuación se presentan las fases para la administración del riesgo tecnológico en base a COSO ERM.

### 4.3.1 Ambiente de control

Es la base en que se sustenta toda la organización e influye en la conciencia de sus empleados respecto al riego tecnológico, los factores que deben ser considerados son la filosofía de la gestión de riesgos, la tolerancia al riesgo, valores éticos y competencia del personal, así como la definición de autoridad, responsabilidades y estructura organizacional que soportara la administración.

Este componente es el punto inicial de todo el proceso para la administración del riesgo tecnológico y conlleva la definición de los parámetros internos y externos que han de considerarse en la administración del riesgo, estableciendo el alcance que tendrá y los criterios que soportaran dicha gestión. Lo que se debe de establecer de forma clara es lo siguiente:

- **Filosofía de la Gestión de Riesgos:** Es el compendio de “creencias y actitudes compartidas que caracterizan el modo en que la organización contempla el riesgo en todas sus actuaciones. Esta filosofía se plasma en las declaraciones sobre las políticas, procedimientos, las comunicaciones verbales y escritas, y la toma de decisiones”.(16:10)

- **Declaración de Administración de Riesgo Tecnológico:** “Es un proceso efectuado por el consejo de administración, su dirección y restante personal, aplicado en la definición de la estrategia y en toda la entidad;

diseñado para identificar eventos potenciales que puedan afectar a la organización y gestionar así los riesgos dentro del riesgo aceptado".(15:7)

- **Declaración de Riesgo Tecnológico:** "Es la contingencia potencial de que la interrupción, alteración o fallas derivadas del uso o dependencia del hardware, software, sistemas de información, aplicaciones, base de datos, redes y cualquier otro medio de distribución y manejo de información, dentro de la organización, provoque pérdidas financieras a la empresa".(27:2)

- **Nivel de Apetito al Riesgo Tecnológico:** Es la definición del nivel máximo de riesgo o valor cuantitativo, el cual la organización está dispuesta a asumir en busca de valor por medio de sus procesos. El Consejo de Administración es el encargado de aprobar los límites del apetito en los factores del riesgo tecnológico. "El riesgo aceptado puede expresarse en términos cualitativos o cuantitativos" (16:23). Por ejemplo, una entidad pude definir que su máximo de apetito al riesgo es hasta el monto máximo que le cubre una póliza de seguro de todo riesgo, la cual está en un monto de hasta Q250,000.00, siendo este valor el apetito al riesgo que asume.

- **Niveles de Criticidad:** "Se refiere a la clasificación de la información en diferentes niveles, considerando la importancia que esta tiene para la operación del negocio". (27:2) Este factor aplica a los activos de TI (infraestructura, información y personal) y a la información, cuando estos ponen en peligro la continuidad del negocio o de la operación de la entidad.

- **Niveles de Sensibilidad:** Es la "clasificación de la información según el perjuicio que ocasione a la institución su alteración, destrucción, pérdida o divulgación no autorizada". (27:2) Este factor aplica únicamente a la información, siempre y cuando se vea en riesgo los criterios de la información (confidencialidad, integridad, disponibilidad). Los niveles a

utilizar se identifican al igual que en el nivel de criticidad, la información puede ser: pública, interna, privada, confidencial.

- **Niveles de Probabilidad:** Es la posibilidad de ocurrencia de un evento, en un tiempo determinado y que como consecuencia altera los resultados esperados. Por lo cual se marcan rangos que analizados permitirán definir los niveles sobre los cuales se analizara un riesgo materializado, este puede ser bajo, medio, alto y grave.

- **Niveles de Impacto:** Es la pérdida que ocasiona la materialización de una amenaza y el efecto o consecuencias en los objetivos de la organización.

- **Exposición al Riesgo:** También denominado como nivel de riesgo y es la magnitud de un riesgo o la combinación de varios riesgos. Su resultado se obtiene de la de la evaluación de los criterios expuestos anteriormente, probabilidad por impacto y criticidad más sensibilidad.

### 4.3.2 Establecimiento de objetivos

Los objetivos se establecen a escala estratégica, estableciendo con ellos una base para los objetivos operativos, de información y de cumplimiento. “Cada entidad se enfrenta a una gama de riesgos procedentes de fuentes externas e internas y una condición previa para una adecuada identificación, evaluación y respuesta a los riesgos es fijar los objetivos, los cuales tienen que estar alineados con el riesgo aceptado por la entidad, lo cual orienta a su vez los niveles de tolerancia al riesgo de la misma”. (16:19)Los objetivos al nivel de empresa están vinculados y se integran con otros objetivos más específicos, que repercuten en cascada en la organización hasta llegar a sub objetivos establecidos. “Estos objetivos deben de estar vinculados con la misión, visión y objetivos estratégicos y otros objetivos relacionados”. (16:21)

### 4.3.3Identificación de riesgos

La identificación de riesgos puede “comprender una combinación de técnicas y herramientas de apoyo, las cuales se basan tanto en el pasado como en el futuro, esta identificación se realiza con la finalidad de identificar posibles acontecimientos que afecten el logro de los objetivos”. (16:30) Se busca con ello llegar a obtener un portafolio de riesgos tecnológicos que deben ser analizados periódicamente basados en listados “elaborados por el personal de la entidad o bien pueden ser listas externas genéricas, las cuales deben ser revisadas y sometidas a mejoras, adaptando su contenido a las circunstancias de la entidad”. (Ídem)

La identificación dentro del contexto de la administración del riesgo tecnológico consiste en poder identificar el activo tecnológico y determinar sus amenazas y vulnerabilidades, ya que el riesgo tecnológico se genera cuando una amenaza explota las vulnerabilidades en un activo para causar daños o pérdidas en los procesos de negocio.

Riesgo = Activo * Amenaza * Vulnerabilidad

Los activos tecnológicos son todos aquellos recursos de tecnología necesarios para que los procesos de TI funcionen adecuadamente, estos se pueden dividir en tres grandes rubros que son Infraestructura, Información y Personal. También se debe de elaborar un catálogo de amenazas y vulnerabilidades, siendo una amenaza una circunstancia o agente que puede explotar una vulnerabilidad accidental o voluntariamente, y una vulnerabilidad es una debilidad en el diseño de los controles que soportan la seguridad en las tecnologías de la información.

También debiese de identificar las fuentes generadoras de los riesgos, es decir, identificar aquel elemento que solo o en combinación tiene el potencial intrínseco de originar una amenaza.

**Cuadro 2**

**Fuentes de riesgo**

| Fuentes de Riesgo | |
|---|---|
| 1 | Hardware |
| 2 | Software |
| 3 | Seguridad de Sistemas |
| 4 | Controles y Politicas |
| 5 | Recurso Humano |
| 6 | Factores Externos |
| 7 | Regulatorio o Legal |

Fuente: Elaboración propia en base al trabajo realizado.

### 4.3.4 Evaluación de riesgos

La evaluación de riesgos tecnológicos “permite a una entidad considerar la amplitud con que los eventos potenciales impactan en la consecución de los objetivos, desde una doble perspectiva que es probabilidad e impacto, usando normalmente una combinación de métodos cualitativos y cuantitativos”, (16:45) en función a la categorización o portafolio elaborado de eventos de riesgos, tomando en consideración los criterios de criticidad y sensibilidad en el análisis.

La evaluación puede realizarse por medio de la técnica cualitativa o cuantitativa, la primera se basa en cualidades y la segunda en importes monetarios. El proceso consiste en clasificar el riesgo según el impacto que tenga en los procesos de TI y la probabilidad de ocurrencia del mismo, proveyendo así el nivel de riesgo que tienen los procesos de TI, esta actividad permite poder identificar las fortalezas y debilidades del área de tecnología.

La probabilidad se mide por cantidad de veces de ocurrencia de un evento en un determinado tiempo y el impacto por el daño ocasionado por la materialización de una amenaza. A continuación se presenta un esquema de cómo poder evaluar un

activo de tecnología, en este caso se tomara como ejemplo el servidor de correo electrónico y tomando como referencia únicamente la probabilidad y el impacto.

**Cuadro 3**

**Evaluación de un Activo Tecnológico**

| Activo Evaluado: Servidor de Correo Electrónico | |
|---|---|
| **Punto de evaluación** | **Detalle** |
| Amenaza / Riesgo | Ataques externos |
| Vulnerabilidades | Incorrecta aplicación de patches<br>Falta de capacidad del personal |
| Probabilidad | Alta (99%) |
| Impacto | Alto |
| Calificacion Cualitativa | Riesgo Alto |
| Calificación Cuantitativa | 990,000 |

| Valor Activo | Probabilidad | Calificación Cuantitativa |
|---|---|---|
| 1,000,000 | 0.99 | 990,000 |

Fuente: Elaboración propia en base al trabajo realizado.

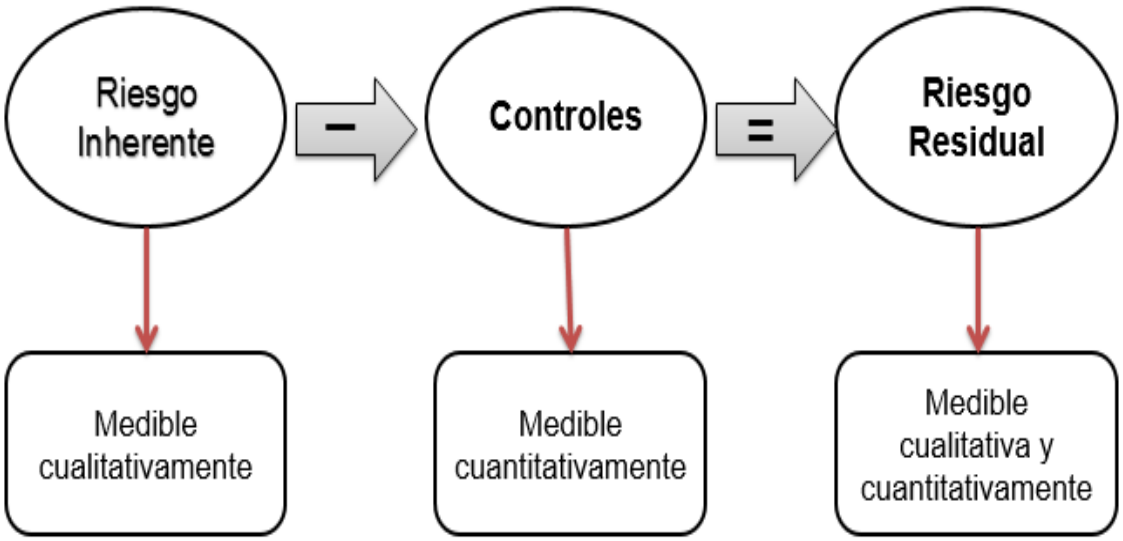
Como se observa en el Cuadro 2 el nivel de impacto monetario (cuantitativo) de materializarse esta amenaza seria de Q990,000.00 ya que su probabilidad de ocurrencia está en un 99%.

Lo anterior nos lleva a identificar y definir dos conceptos que deben de tomarse en cuenta el riesgo inherente y residual; definiendo el riesgo inherente como “aquél al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto” (16:45), y el riesgo residual, como “aquél que permanece después de que la dirección desarrolle sus respuestas a los riesgos. (16:46)Así mismo, debe de considerarse la materialidad de llegarse a concretar una amenaza, lo cual significa el impacto potencial que tendrá en los Estados Financieros de la empresa.

La evaluación de un riesgo tecnológico debe llevar consigo la comprensión y entendimiento del mismo, causas y fuentes del riesgo, así también otros atributos que se consideren a fin de determinar el nivel de riesgo de una forma adecuada y objetiva, considerándose los controles que le dan respuesta y su efectividad.

**Gráfica2**

**Flujo del riesgo inherente y residual**




Fuente: Guía de aplicación, COSO ERM.

La evaluación del riesgo permite facilitar la toma de decisiones en base a los resultados obtenidos, estableciendo así planes de tratamiento para los riesgos más altos, a la par de definir la prioridad para su implementación.

Luego de la evaluación de cada activo tecnológico con sus respectivas amenazas y vulnerabilidades, se obtiene una matriz la cual muestra la evaluación en cada uno de los cuatro criterios definidos por cada activo o control evaluado, misma que debe estar en contexto con la regulaciónJM-102-2011 Reglamento para la Administración del Riesgo Tecnológico. El anexo 2 muestra una matriz de riesgos que ayuda a visualizar como queda representado cada criterio bajo una evaluación realizada.

Un medio que se utiliza para representar gráficamente los resultaos obtenidos en la matriz del riesgo tecnológico es el mapa de riesgos, “en el cual los riesgos se representan de manera tal que los más significativos resalten, diferenciándolos de los menos significativos”, (16:60) esta representación gráfica esta ordenada por cuadrantes que ayudan a la visualización del nivel de exposición de cada uno los riesgos tecnológicos identificados y evaluados. El modelo siguiente 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”. (Ídem)

**Cuadro 4**

**Mapa de calor**

| PROBABILIDAD | | | | | |
|---|---|---|---|---|---|
| 1 | 5 | 10 | 15 | 20 | 25 |
| 2 | 4 | 8 | 12 | 16 | 20 |
| 3 | 3 | 6 | 9 | 12 | 15 |
| 4 | 2 | 4 | 6 | 8 | 10 |
| 5 | 1 | 2 | 3 | 4 | 5 |
| | 1 | 2 | 3 | 4 | 5 |
| | IMPACTO | | | | |

Fuente: Guía de aplicación, COSO ERM.

### 4.3.5Respuesta al riesgo

La respuesta al riesgo 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. La respuesta al riesgo, también denominada en algunas buenas prácticas como tratamiento al riesgo 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”, (16:69) las cuales podrían ser:

- **Evitar:** es la decisión de no involucrarse en una actividad o de retirarse de ella 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:** implica protegerse de los riesgos utilizando instrumentos del mercado de capital a largo plazo, tales como los seguros, o bien externalizar los procesos de negocio.
- **Aceptar:** es aceptar el factor de riesgo, en torno a que se adapte a las tolerancias al riesgo establecidas. (16:70)

Este componente del proceso tiene relación con la tolerancia al riesgo y costo beneficio; debe de entenderse que la respuesta al riesgo lo define el consejo de administración. Todo tipo de respuesta implica un costo ya sea directo o indirecto y el mismo debe de 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 debemos tener en mente que es lo que mitigan, si la probabilidad o el impacto.

### 4.3.6 Actividades de control

“Después de haber seleccionado las respuesta a los riesgos, se debe de identificar las actividades de control necesarias que ayuden a asegurar que la respuestas seleccionadas se lleven a cabo adecuadamente y oportunamente”. (16:79) Es necesario resaltar que las actividades de control se establecen para velar porque se “lleven a cabo de manera adecuada la respuesta a los riesgos, sin embargo, en

el caso de ciertos objetivos las propias actividades de control constituyen la respuesta al riesgo". (16:80)

Los controles son las medidas que se toman para mitigar el impacto de una amenaza, y estos pueden ser correctivos, preventivos o detectivos. Los controles tal como lo dicen las buenas prácticas deben ser suficientes, comprensibles y oportunos, para que puedan apoyar en la administración del riesgo tecnológico.

Un control no formalizado es débil, un control documentado es fuerte, cuando un control no está formalizado se cae en dependencia del personal y una organización debiese de depender de sus procesos no del personal. A los controles aplicables para dar respuesta a los riesgos tecnológicos se les realiza una evaluación para determinar qué tan efectivos son y si realmente aportan a la mitigación de los riesgos identificados. A continuación se ofrece un ejemplo de cómo poder evaluar los atributos del control.

**Cuadro 5**

**Evaluación de atributos del control interno**

**Atributos de Control Interno**

**Amenaza:** Tormenta Electrica

**Tipo de Amenaza:** Natural

**Controles Asociados**

| No. | Nombre del Control | Tipo | Auto | Docto Formal | Implem | Evaluado |
|---|---|---|---|---|---|---|
| 1. | Tierra física instalada | Preventivo | Si | No | Si | N/A |
| 2. | Planta Electrica | Preventivo | Si | No | Si | Si |
| 3. | UPS | Preventivo | Si | Si | Si | Si |
| 4. | Sitio Alterno de Operaciones | Preventivo | No | Si | Si | Si |
| 5. | Seguro médico (personal) | Preventivo | No | Si | Si | Si |

Fuente: Elaboración propia en base al trabajo realizado.

Al momento de establecer y evaluar las actividades de control se debe de verificar la segregación de funciones en torno al proceso, roles y responsabilidades y el control interno, dando respuesta a las interrogantes ¿Qué? ¿Quiénes? ¿Cómo?

En la segregación de funciones existen cuatro funciones que deben de considerase estas son operador, administrador, supervisor y evaluador. El que opera puede administrar mas no puede supervisar, el que administra puede supervisar mas no puede operar, cuando se da una mezcla de estas funciones deben de existir controles compensatorios, el cual puede ser cumplido por un rol independiente que queda de los anteriormente indicados. A continuación se presenta un cuadro que permite visualizar lo indicado en el párrafo anterior.

**Cuadro 6**

**Segregación de funciones**

| Proceso | Roles y Responsabilidades | Evidencia de lo que hace |
|---|---|---|
| A 1 | Operación | Bitácora de operación |
| A 2 | Administrador | Bitácora de administración |
| A 3 | Supervisor | Supervisión de lo establecido |
| | Evaluador | Evalua lo establecido |

Políticas
Procedimientos
Estándar
Metodología

Fuente: Guía de Aplicación COSO ERM.

“Las actividades de control tienen lugar a través de toda la organización, a todos los niveles y en todas las funciones, esto incluye una gama tan diversa de actividades tales como aprobaciones, autorizaciones, conciliaciones, revisiones, seguridad de los activos y segregación de las funciones”. (16:79)

### 4.3.7 Información y comunicación

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”. (16:85)

Los informes generados en el proceso de la administración del riesgo tecnológico facilita la administración de los mismos. Entre los reportes que pueden generarse están:

- Reportes del nivel de riesgo
- Reporte de vulnerabilidades y amenazas asociadas a los activos
- Alertas de exposición al riesgo
- Registro de eventos
- Tendencia del riesgo tecnológico

Cabe mencionar que de nada sirve tener todo un proceso, políticas y procedimientos bien establecidos sino se informan y comunican. La información debe de ser clasificada de acorde a los criterios de integridad, confidencialidad y disponibilidad, lo cual apoyara en la definición de que debe contener cada informe y quien debe tener acceso al mismo, así también debe de establecerse mecanismos que la resguarden. La información puede ser: Pública, Interna, Privada, Confidencial.

“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”, (16:85) es aquí donde la aplicación de la tecnología ayuda a mejorar la eficacia y eficiencia de los proceso de información.

Algunas consideraciones que se deben de tomar en cuenta para determinar los requisitos de información, pueden ser:

- Que datos se precisan para obtener métricas de rendimiento
- Qué nivel de detalle se necesita en la información
- Con que frecuencia ha de recogerse la información
- Cuáles son los criterios que debe de cumplir la información
- Donde y como debe de recogerse la información
- Qué mecanismos de recuperación de datos son necesarios.
- Otros que se consideren.

Por ende la comunicación es muy importante ya que por medio de ella la dirección realiza comunicados específicos y orientados a las expectativas de comportamiento y responsabilidades del personal. “La comunicación sobre procesos y procedimientos debería de alinearse con la cultura deseada y reforzarla continuamente”. (16:97)

La comunicación es muy importante ya que ella es clave para apoyar a crear el entorno adecuado para la administración del riesgo tecnológico y apoya a gestionar adecuadamente todo el proceso por cada uno de sus componentes.

### 4.3.8 Supervisión

“Durante el transcurso normal de las actividades de la gestión, tiene lugar una supervisión permanente. El alcance y frecuencia de las evaluaciones independientes dependerá fundamentalmente de la evaluación de riesgos y la eficacia de los procedimientos de supervisión permanente. Las deficiencias en la gestión del riesgo tecnológico deben comunicarse”. (16:103) La Auditoría Interna en este aspecto debe de evaluar como el área de tecnología ha evaluado sus riesgos y si el nivel de riesgo es el adecuado de acorde a las directrices de la alta dirección. Entendiéndose que asegurar es ver que el sistema está funcionando

eficaz y eficientemente, permeándose de esta forma su función dentro de la gestión del riesgo tecnológico.

Con el fin de asegurar que la gestión integral de riesgo es eficaz y continua siendo vigente para las necesidades particulares de la empresa, la organización mide el desempeño de la gestión de riesgo tecnológico 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 de realizar un monitoreo a la implementación y efectividad de los planes de tratamiento a los riesgos que no contaban con controles que lo mitigaran o que no eran efectivos.

Teniendo en cuenta el resultado de la supervisión permanente, periódica y de apoyo, la organización deberá de tomar decisiones sobre la mejora continua que deba de 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.

### 4.4 Implementación del comité de gestión de riesgos

El comité para la gestión de riesgos, es un grupo de profesionales delegados por la junta directiva de una organización para garantizar la gestión estratégica de los riegos, debe estar conformado por miembros conocedores del negocio y de la administración de riesgos para mejorar el alcance del mismo. Algunos factores que deben de considerarse en su implementación son:

- Las necesidades de los grupos de interés.
- Alineación con las estrategias de la organización.
- Vigilancia del proceso de gestión de riesgos.
- Alcance de las responsabilidades del comité de riesgos.
- Comunicación con otros entes fiscalizadores.

El comité debe encargarse de “garantizar que la capacidad de identificar, evaluar y gestionar los riesgos sigue evolucionando con relación al riesgo aceptado por la organización. Para ello, se centrará principalmente en la eficacia de la gestión de riesgos tecnológicos”. (16:117)

La implementación debe de realizarse de la forma siguiente:

- Debe de constituirse mediante acta del consejo de administración.
- Estar conformado por personal no ejecutivo y un delegado del consejo de administración.
- Elaborar y rectificar el reglamento bajo el cual se regirá, instrumento que servirá para garantizar su alcance, funciones y responsabilidades.
- Elegir un presidente, el cual no podrá ser el delegado del consejo de administración.
- Definición de la periodicidad de las reuniones.
- Elegir un secretario, quien deberá levantar un acta de todas las reuniones que realice el comité.

En algunas organizaciones, se establece el comité de riesgos con los altos directivos de la organización, incluyendo directores funcionales tales como el Gerente de Riesgos, Gerente de Tecnología, Gerente Financiero, Gerente de Operaciones, Gerente General, Auditoría Interna, entre otros. Donde la auditoría interna participa con voz pero no con voto.

### 4.5 Roles y responsabilidades en la gestión del riesgo tecnológico

Para que la administración del riesgo tecnológico sea adecuada y de forma transparente debe de establecerse las responsabilidades de cada uno de los entes involucrados en el desarrollo, mantenimiento, mejora y supervisión de la administración del riesgo tecnológico. La regulación de la Junta Monetaria JM-102-2011 Reglamento para la administración del riesgo tecnológico, delimita algunas

responsabilidades que deben de considerarse en la administración del riesgo tecnológico, sin embargo, para serlo más integral deben de considerarse las responsabilidades de aquellos interesados, de acorde a las funciones que llevan dentro de una organización.

A continuación se detalla las responsabilidades por cada ente involucrado:

### 4.5.1 Consejo de administración

Es el responsable de velar porque se implemente un adecuado sistema de gestión de riesgos, así como instruir para que se mantenga en adecuado funcionamiento y ejecución de la administración del riesgo tecnológico.

Para cumplir con lo indicado en el párrafo anterior el Consejo de Administración, como mínimo deberá:

- Aprobar las políticas y procedimientos requeridos, el plan estratégico de TI, el plan de continuidad de operaciones de TI, así como conocer y resolver sobre las propuestas de actualización y autorizar las modificaciones respectivas.
- Conocer los reportes que le remita el Comité de Riesgos sobre la exposición al riesgo tecnológico, los cambios sustanciales de tal exposición y su evolución en el tiempo, así como las medidas correctivas adoptadas.
- Conocer los reportes sobre el nivel de cumplimiento de las políticas y procedimientos aprobados, así como las propuestas sobre acciones a adoptar con relación a los incumplimientos. Asimismo, en caso de incumplimiento el Consejo debe adoptar las medidas que correspondan, sin perjuicio de las sanciones legales que el caso amerite.
- Asegurar que la estructura organizacional para administrar TI, permita asesorar al comité de gestión de riesgos y a la unidad de administración de riesgos en los aspectos relacionados con el riesgo tecnológico. (27:4)

### 4.5.2 Comité de gestión de riesgos

Debe estar integrado por un miembro del consejo de administración y por las autoridades y funcionarios que el consejo designe. “El comité estará a cargo de la dirección de la administración del riesgo tecnológico, para lo cual deberá encargarse de la implementación, adecuado funcionamiento y ejecución de las políticas y procedimientos aprobados”. (27:5) Sus funciones y responsabilidades son:

- Proponer al Consejo, para su aprobación, las políticas y procedimientos para la administración del riesgo tecnológico, así como el plan estratégico de TI y el plan de continuidad de operaciones de TI.
- Proponer al Consejo el manual de administración del riesgo tecnológico y sus actualizaciones.
- Analizar las propuestas sobre actualización de las políticas, procedimientos, plan estratégico de TI, plan de continuidad de operaciones de TI y su plan de pruebas, y proponer al Consejo las actualizaciones que procedan.
- Definir la estrategia para la implementación de las políticas y procedimientos aprobados para la administración del riesgo tecnológico y su adecuado cumplimiento.
- Revisar, al menos anualmente, las políticas y procedimientos y proponer la actualización, cuando proceda.
- Analizar los reportes que le remita la Unidad de Administración de Riesgos, sobre la exposición del riesgo tecnológico en la institución, los cambios sustanciales de tal exposición y su evolución en el tiempo, así como adoptar las medidas correctivas correspondientes.
- Analizar la información que le remita la Unidad de Administración de Riesgos sobre el cumplimiento de las políticas y procedimientos aprobados, así como evaluar las causas de los incumplimientos que hubieren, y proponer al Consejo acciones a adoptar con relación a dichos incumplimientos.

- Reportar al Consejo, al menos semestralmente y cuando la situación lo amerite, sobre la exposición al riesgo tecnológico de la institución, los cambios sustanciales de tal exposición; su evolución en el tiempo, las principales medidas correctivas adoptadas y el cumplimiento de las políticas y procedimientos aprobados.
- Así como otras funciones relacionadas que le asigne el Consejo. (27:5)

Todas las reuniones que lleve adelante el comité de riesgos deberán constar en acta suscrita por quienes intervinieron en la sesión.

### 4.5.3 Unidad de administración de riesgos

Es el ente que ayuda al comité en la administración del riesgo tecnológico, para lo cual debe de cumplir con las siguientes funciones:

- Proponer al Comité políticas y procedimientos para la administración del riesgo tecnológico, así como el plan estratégico de TI, el plan de continuidad de operaciones de TI y su plan de pruebas.
- Revisar, al menos anualmente y cuando la situación lo amerite, las políticas, los procedimientos, el plan estratégico de TI, y para los procesos críticos, el plan de continuidad de operaciones de TI y su plan de pruebas, y proponer su actualización al Comité.
- Monitorear a través de la herramienta establecida, la exposición al riesgo tecnológico y mantener registros históricos sobre dicho monitoreo, así como medir el riesgo tecnológico.
- Analizar el riesgo tecnológico inherente de las innovaciones en TI que se implementen en la institución y el que se derive de los nuevos productos y servicios propuestos por las unidades de negocios.
- Reportar al Comité, al menos trimestralmente y cuando la situación lo amerite, sobre la exposición al riesgo tecnológico de la institución, los

cambios sustanciales de tal exposición y su evolución en el tiempo, así como proponer al Comité las medidas correctivas correspondientes.

- Verificar e informar al Comité, al menos trimestralmente y cuando la situación lo amerite, sobre el nivel de cumplimiento de las políticas y procedimientos aprobados.
- Identificar las causas del incumplimiento de las políticas y procedimientos aprobados, determinar si los mismos se presentan en forma reiterada e incluir sus resultados en el informe respectivo y proponer las medidas correctivas, debiendo mantener registros históricos sobre tales incumplimientos.
- Otras funciones relacionadas que le asigne el Comité. (27:6)

### 4.5.4 Gerencia de la tecnología de la información

Es el ente responsable de apoyar en la gestión de las tecnologías de la información, manteniendo activos los servicios que brinda a las unidades del negocio y así como a los clientes externos de la institución. Sus responsabilidades las podemos delimitar como las siguientes:

- Generar periódicamente cuando el Gestor de Seguridad de la Información lo requiera, los insumos necesarios para la cualificación de la probabilidad e impacto en las amenazas y vulnerabilidades definidas en el respectivo catálogo, así como toda información que requiera a fin de ejecutar su rol dentro de la gestión del riesgo tecnológico.
- Debe proveer los insumos necesarios a Auditoría Interna para pueda ejecutar sus evaluaciones y verificaciones en cuanto a la gestión del riesgo tecnológico.
- Debe proveer los insumos necesarios para que la Unidad de Administración de Riesgos pueda llevar a cabo sus responsabilidades definidas dentro de la gestión del riesgo tecnológico.

- Debe velar para que los niveles de servicio esperados por los usuarios de la información (clientes internos y externo), estén siempre de acuerdo a sus expectativas operativas y de uso.
- Velar por que los niveles del riesgo tecnológico se mantengan dentro de los criterios aceptados por la institución.
- Otras de acuerdo a su gestión.

### 4.5.5 Gestor de la seguridad de la información

Es el responsable de planear, coordinar y administrar los procesos de la seguridad de la información en la organización, así como contribuir a la difusión de la cultura en este tema entre los colaboradores de la entidad. Entre sus principales funciones y responsabilidades podemos mencionar:

- Definir la estrategia de seguridad de la información, en conjunto con la alta dirección, implementando las acciones definidas.
- Administrar los requerimientos de seguridad lógica y física.
- Detectar necesidades y vulnerabilidades de la seguridad de la información, y proponer las respectivas soluciones de acuerdo al criterio de costo beneficio.
- Documentar las políticas, procedimientos y estándares de seguridad, velando por el cumplimiento de estándares y regulaciones que sean aplicables a la institución.
- Aplicar una metodología de análisis de riesgo que permita evaluar la efectividad de los controles, la respuesta a los eventos, nivel de cumplimiento a las políticas de seguridad.
- Apoyar al comité de riesgos y a la unidad de administración de riesgos, en el proceso de identificación y evaluación de riesgos, así como la mejora a los procesos y políticas de tecnología de la información.
- Gestionar con el departamento de tecnología el cumplimiento de las mejoras señalas por entes supervisores, auditoría interna, auditoría externa.

### 4.5.6 Auditoría Interna

“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 proceso de gestión de riesgos, control y gobierno”. (23:5)

La función de la auditoría interna debe ser “evaluar la eficacia y contribuir a la mejora de los procesos de gestión de riesgos”; (23:26) La actividad de auditoría interna debe determinar si los procesos de riesgos son eficaces en base a un juicio que resulta de la evaluación de lo siguiente:

- Los objetivos de la organización apoyan a la misión de la organización y están alineados con la misma,
- Los riesgos significativos están identificados y evaluados,
- Selección de respuestas apropiadas al riesgo que alinean los riesgos con la aceptación de riesgos por parte de la organización, y
- Captación de información sobre riesgos relevantes, permitiendo al personal, la dirección y el Consejo cumplir con sus responsabilidades, y se comunica dicha información oportunamente a través de la organización. (23:27)
- Diseño y funciones del proceso de gestión de riesgos.
- Eficacia y eficiencia de las respuestas al riesgo y actividades de control relacionadas.
- Integridad y exactitud de la información generada sobre la gestión de riesgos. (16:123)

Por ende, en la administración del riesgo tecnológico su función es verificar y controlar a través de su plan de trabajo anual que los servicios de la Gerencia de Tecnología de la Información, las actividades de control del Gestor de Seguridad de la Información y las propuestas emitidas por la Unidad de Administración de

Riesgos, sean adecuados, convenientes y oportunos según los requerimientos de la institución, recomendando a quien corresponda las acciones de mejora continua para el proceso de la administración del riesgo tecnológico.

### 4.6 Definición de controles para TI, según la resolución JM-102-2011

Para la identificación de los controles que solicita la resolución JM-102-2011 Administración del Riesgo Tecnológico emitida por la Junta Monetaria en septiembre del año 2011, se debe iniciar con identificar la estructura de la regulación, la cual consta de cinco dominios (capítulos), veintitrés procesos (artículos) y un total de 93 controles o actividades de control (requisitos), esto a partir del capítulo segundo de la resolución, esta estructura permite gestionar los riesgos tecnológicos en cumplimiento a la normativa.

Los requisitos o actividades de control deben entrar en un proceso de análisis y verificación a fin de establecer su aplicabilidad para la empresa, lo cual dependerá del giro del negocio, estructura, tamaño y complejidad de sus procesos. A continuación se presenta un esquema de los dominios, sin embargo los procesos y controles (requisitos) se pueden observar en el anexo 3.

**Cuadro7**

**Dominios de la regulaciónJM-102-2011**

| Dominios de la Resolución JM-102-2011 | | |
|---|---|---|
| **No.** | **Nombre** | **Ubicación** |
| 1 | Organización para la administración del Riesgo Tecnologico | Capítulo II |
| 2 | Infraestructura de TI, sistemas de información, bases de datos y servicios de TI | Capítulo III |
| 3 | Seguridad de Tecnología de la Información | Capítulo IV |
| 4 | Continuidad de operaciones de tecnología de la información | Capítulo V |
| 5 | Procesamiento de información y tercerización | Capítulo VI |

Fuente: JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico.

## 4.7 Documentación de procesos

La documentación de los procesos permite fácilmente comprender los riegos de la unidad, proceso o servicio de TI y la respuesta que se da a ellos, un objetivo importante que tiene la documentación de procesos es transmitir información y compartir conocimientos dentro de la organización. La documentación por ende es una forma de poder gestionar y controlar cómo las personas en una empresa realizan los procesos establecidos.

“El nivel de documentación de la administración del riesgo tecnológico varía entre una organización y otra, esto a menudo por el tamaño, complejidad y estilo de gestión. Además de la amplitud y profundidad de la documentación, las consideraciones al respecto incluyen si estarán en soporte papel o electrónico, si estará centralizada o distribuida y cuáles son los medios de acceso para actualización y revisión”. (16:109)

Las políticas y procedimientos ayudan a realizar permanentemente una adecuada administración del riesgo tecnológico, estas deben de comprender como mínimo, las metodologías, herramientas o modelos de medición del riesgo tecnológico. También debe de considerarse establecer políticas para elaborar, implementar y actualizar el plan estratégico de TI. La documentación debe considerar:

- Organigramas.
- Descripción de papeles, autoridad y responsabilidades claves.
- Manuales de políticas.
- Procedimientos operativos.
- Diagramas de flujo de procesos.
- Controles relevantes y sus responsabilidades asociadas.
- Indicadores clave de rendimiento.
- Riesgos claves identificados.
- Mediciones claves del riesgo. (Ídem)

Todo documento creado y puesto en producción debe ser ingresado a un sistema de administración de documentos, el cual ayude a controlar el periodo de vida de los documentos, facilitar el acceso a los documentos, niveles claros de comunicación y debe de ser integral para toda la organización.

A continuación se presenta un ejemplo de un control manual que puede apoyar en la administración de los documentos de TI.

**Cuadro 8**

**Lista maestra de documentos de TI**

**Documentación de Tecnología de la Información**

**Año 2013**

| Codigo | Tipo | Vr | Nombre | Formato | Estado |
|---|---|---|---|---|---|
| TI-MN-001 | Manual | 1 | Administración del Riesgo de TI | Digital | Aprobado |
| GTI-PRO-001 | Procedimiento | 1 | Administración de usuarios de Red | Digital | En Revisión |
| GTI-PRO-024 | Procedimiento | 2 | Cambios a las BD y Sistemas Operativos | Digital | En Eleboración |
| GTI-POL-001 | Politica | 1 | Seguridad de la información | Digital | Implementado |
| GTI-INS-001 | Instructivo | 1 | Buen uso del recurso informatico | Manual | Aprobado |
| GTI-INS-005 | Instructivo | 2 | Gestión de incidentes de TI | Manual | Descontinuado |

Fuente: Elaboración propia en base al trabajo realizado.

La documentación puede ser identificada por un código donde los primeros tres dígitos representa la gerencia o área, los siguientes el tipo de documento el cual podría ser un manual, una política, un procedimiento, un instructivo, acuerdos de nivel de servicio, otra documentación; los últimos reflejan el correlativo.

Los estados de la documentación se pueden estandarizar bajo los criterios siguientes: Elaboración, Revisión, Implementado, Aprobado y Descontinuado.

## 4.8 Cambios en las estructuras administrativas de TI (Gobierno de TI)

De igual forma que el gobierno corporativo es crítico para asegurar que las decisiones claves sean coherentes con los valores, la visión y la estrategia de la empresa, el gobierno de TI “es fundamental para garantizar que las decisiones relacionadas con las tecnologías de la información encajan, con los objetivos de la organización”. (35)

El gobierno de TI consiste en el liderazgo, los procesos y las estructuras que aseguran que las tecnologías de la organización apoyan los objetivos y estrategias de la empresa; su objetivo debe de ser asegurar que las tecnologías utilizadas aportan valor a los procesos de la empresa y que el riesgo asociado a ellas está controlado. Los enfoques que debe de cumplir el gobierno de TI, deben ser:

- **Alineación Estratégica:** esto implica alinearse a los objetivos de la organización y construir capacidades necesarias para brindar valor agregado.
- **Entrega de Valor:** es ejecutar sus procesos y servicios con la propuesta de valor agregado.
- **Administración de Riesgos:** identificar y administrar los riesgos para preservar el valor.
- **Administración de Recursos:** optimizar el desarrollo y uso de los recursos disponibles.
- **Monitoreo del Desempeño:** significa evaluar los resultados para aplicar acciones correctivas y redirigir sus servicios.

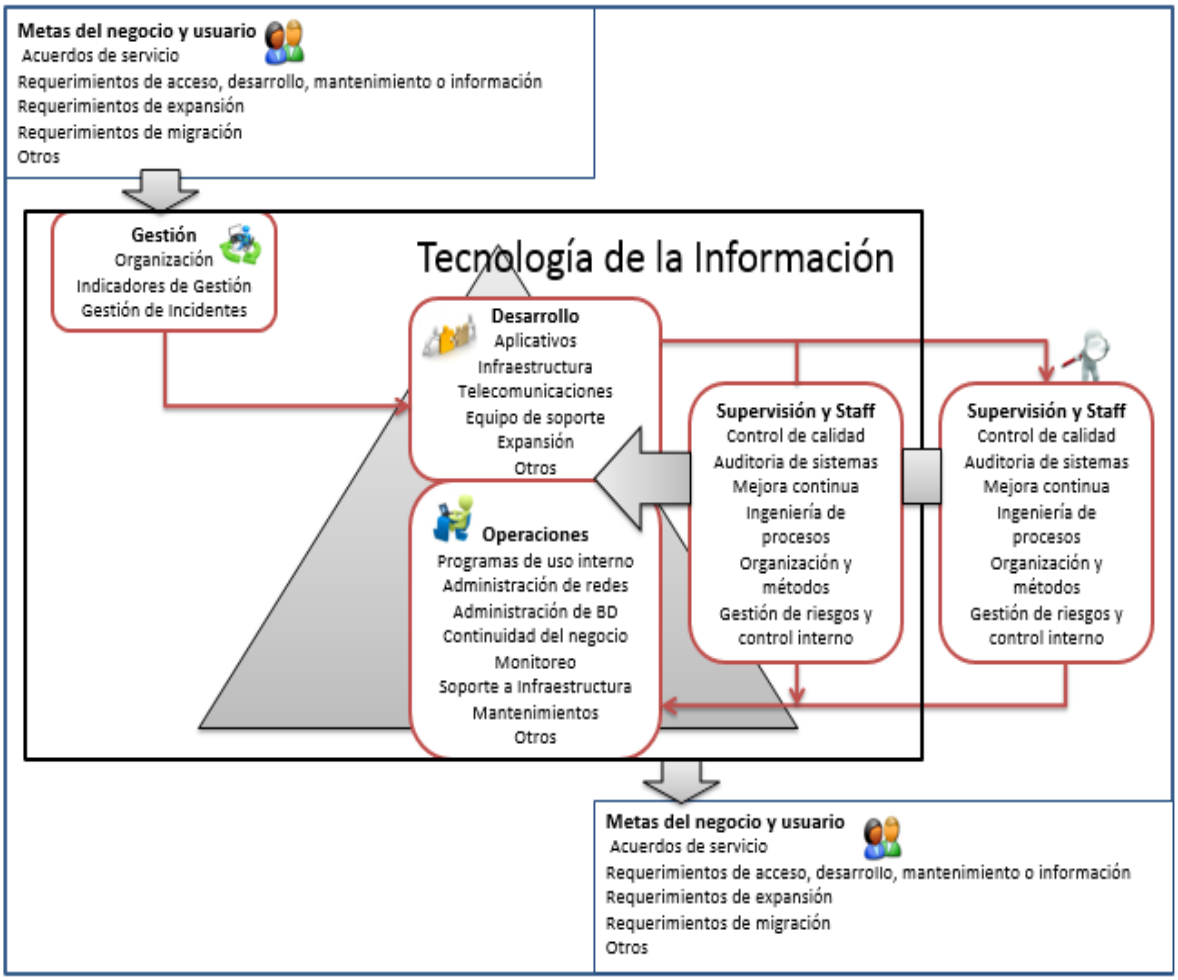
La segregación de funciones y el análisis de los puestos de trabajo actual, así como los requeridos realmente para dar respuesta a los riesgos detectados son parte integral de los cambios que deben de considerarse, así como las implicaciones que esto puede suponer. Las estructuras fundamentales de TI, deben de contar con las siguientes especificaciones:

- Área de Gestión
- Área de Desarrollo
- Área de Operaciones
- Área de Supervisión y Staff

A continuación se presenta un modelo de la estructura de TI que es fundamental exista en las empresas, sin embargo cabe mencionar que dependerá mucho de la complejidad de TI y el tamaño de la organización lo que determinara dicha estructura organizacional.

**Gráfica 3**

**Estructura fundamental de TI**




Fuente: ISO/IEC 27002:2005.

Este tipo de estructura muestra como dentro de la estructura de tecnología se han separado las funciones en Gestión, Desarrollo y Operaciones, así también, se cuenta con un grupo de supervisión y control de calidad totalmente separado de las últimas dos áreas mencionadas pero como parte de la estructura de TI, existiendo aun así un equipo totalmente independiente que abarca todas las revisiones a TI tal es el caso de Auditoría Interna, el Gestor de Seguridad de la Información y entes supervisores.

### 4.9 Cambios en las estructuras de infraestructura y control

La administración del riesgo tecnológico busca evitar que la "interrupción, alteración, o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, provoquen pérdidas financieras a la institución". (27:2) Es ahí donde nace la necesidad de contar con una infraestructura que dé respuesta a los requerimientos del negocio con el fin de alcanzar los objetivos planteados por la organización.

La infraestructura es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que brinda TI que en conjunto dan soporte a las aplicaciones o sistemas de información de una organización. A continuación se brinda un cuadro, donde se puede apreciar un ejemplo de lo que puede comprender cada una de las ramas descritas anteriormente:

**Cuadro 9**

**Infraestructura Tecnológica**

| Infraestructura Tecnológica | | |
|---|---|---|
| **Hardware** | **Software** | **Servicios TI** |
| Servidores<br>Computadoras<br>Redes<br>Enlaces | Sistemas operativos<br>Bases de datos<br>lenguajes de programacion<br>Herramientas de administracion | Soporte técnico<br>seguros<br>Comunicaciones |

Fuente: Elaboración propia en base al trabajo realizado.

Al considerar los cambios en el diseño de una infraestructura tecnológica debe de tomarse en cuenta lo siguiente:

- **Fase 1:** Diagnostico, se debe diagnosticar el estado actual de TI.
- **Fase 2:** Estudio de factibilidad, debe de establecerse los criterios que permitan asegurar el uso óptimo de los recursos empleados, determinando la factibilidad operativa, técnica y económica de implementar una infraestructura de TI que permita alta disponibilidad de los recursos.
- **Fase 3:** Diseño del proyecto, es donde se genera una propuesta de diseño de Infraestructura Tecnológica que permita alta disponibilidad de los recursos.

Actualmente las organizaciones se basan cada día más en redes y comunicaciones para su operación y por ende requieren asegurar que sus sistemas y aplicaciones siempre estén disponibles, en organizaciones que brinda servicios de procesamiento masivo de información por medio de tecnología de punta, TI siempre debe ofrecer un nivel continuo de disponibilidad de sus servicios, para apoyar los procesos de negocio.

La alta disponibilidad se refiere a herramientas y tecnologías, incluyendo recursos de hardware de respaldo, que permiten a un sistema recuperarse rápidamente de una caída.

### 4.10 Implementación de un gestor de seguridad de la información

Un Gestor de seguridad de la información, es un ente independiente del área de tecnología pero relacionada con la misma, que brinda servicios de aseguramiento, control y aprovisionamiento en relación a la seguridad de la información. Es la persona responsable de planear, coordinar y administrar los procesos de seguridad informática en una organización. El gestor de seguridad de la información también llamado Oficial de Seguridad de la Información OSI, tiene la

función de brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática. Dentro de una estructura organizacional se puede requerir que pueda quedar bajo responsabilidad de algunas de las siguientes áreas, de acuerdo a la estructura funcional de la organización:

- Debajo de la responsabilidad directa del consejo de administración
- Debajo de la responsabilidad de la alta dirección
- Debajo de la responsabilidad de la Unidad de Riesgos
- Debajo de la responsabilidad de la auditoría interna

La implementación de un gestor de seguridad debe de considerarse en base al tamaño de la organización y el efecto de la tecnología en los servicios de misión crítica que lleva adelante. Para su implementación debe de considerarse los conocimientos y experiencia que debe poseer. A continuación se presente un modelo que puede considerarse.

**Cuadro 10**

**Conocimientos y experiencia del Gestor de Seguridad de la Información**

| Conocimientos y experiencia en Seguridad Informática | |
|---|---|
| **Conocimientos y Experiencias Minimas** | **Conocimmiento y Experiencia Deseable** |
| Sistemas Operativos a nivel de usuario (Windows, Linux, UNIX) | Sistemas Operativos a nivel de administrador (Windows, Linux, UNIX) |
| Stack de TCP/IP | Protocolos de seguridad (IPSec) |
| Protocolos de seguridad (RPC, TCP, UDP) | Herramientas de Seguridad (scanners, firewalls, IDS) |
| Lenguajes de Programación | Criptografías |
| Legislación | Mecanismos de seguridad (Firmas digitales, certificados) |
| | Conocimientos de estandares |
| | Computo Forense |

Fuente: Perfiles Profesionales para Seguridad Informática, Universidad de Perú.

### 4.10.1 Perfil de puesto

Luego de definida la figura del gestor de seguridad de la información, se debe de proceder a establecer el perfil posible o ideal del mismo, esto dependerá en gran manera de la organización donde se implemente, ya que cada una tendrá sus propias expectativas y necesidades sobre la seguridad de la información y la manera en que se gestione, sin embargo, debe de tomarse en cuenta como mínimo en sus conocimientos lo referenciado en el cuadro 10.

La adecuación del perfil así como el desarrollo del mismo es una responsabilidad de Recursos Humanos, sin embargo, para el mismo pueden ser considerados las opiniones del gerente de tecnología y de auditoría interna, quienes podrán aportar gran valor al perfil del Gestor de Seguridad de la Información, el cual debe ser conocido y aprobado por el consejo de administración.

## 4.11 Inventario de eventos

Un evento es un incidente que se presenta en un proceso y cuya consecuencia es que el resultado final del mismo difiere de lo que se había planeado, este se puede dar a falta de adecuación o un fallo de los procesos, el personal y los sistemas internos o bien por acontecimientos externo.

La metodología de identificación de eventos en una entidad puede comprender una combinación de técnicas y herramientas de apoyo, “las direcciones utilizan listados de eventos posibles comunes que se elaboran por el personal de la entidad o bien son listas externas genéricas. Cuando se trata de listados genéricos externos, el inventario se revisa y se somete a mejoras, adaptando su contenido a las circunstancias de la entidad, para presentar una mejor relación con los riesgos de la organización y consecuentes con el lenguaje común de gestión de riesgos corporativos de la entidad”. (16:31) “Mediante la agrupación de posibles eventos de características similares, la dirección puede determinar con más precisión las

oportunidades y riesgos, esta clasificación de eventos posibles, ayuda a asegurar que los esfuerzos para su identificación sean completos y ayuda a desarrollar posteriormente una perspectiva de cartera". (16:44)

A continuación se presenta un modelo de control que puede apoyar en el registro de eventos dados en una secuencia natural de un proceso.

**Cuadro 11**

**Inventario de eventos**

Inventario de Eventos

Gerencia de Tecnología de la Información

Año 2013

| No. | Fecha | H.Inicial | H.Final | Categoria | Evento | Descripción | Estatus | Seguimiento | Asignado a |
|---|---|---|---|---|---|---|---|---|---|
| 01 | 01/07/2013 | 9:40 | 10:01 | Sistemas | Caida Sistema | Programa APPX no levanta | Pendiente | - | Soporte Tecnico I |
| 02 | 05/07/2013 | 14:30 | 14:35 | Accesos | Error Operativo | Bloqueo de contraseña | Cerrado | Reseteo de contraseña | Mesa de Ayuda |
| 03 | 13/07/2013 | 16:01 | 16:10 | Accesos | Fallo en Comunicaciones | Sin acceso a la red | Pendiente | Se esta revisando | Admin Redes |

Fuente: Elaboración propia en base al trabajo realizado.

Los eventos pueden ser clasificados según la naturaleza de la empresa, giro del negocio y procesos que lleva adelante, a continuación se presenta un listado de eventos típicos que pueden generarse:

- Errores operativos
- Actividad no autorizada
- Fallos en comunicaciones
- Caída de sistemas
- Fallos de programación
- Accesos no autorizados a sistemas
- Incumplimiento de proveedores

Así también, un evento puede ser simple o múltiple, simple es aquel que genera un solo impacto y por consiguiente el evento múltiple genera varios impactos a los procesos de TI y/o de la organización.

### 4.12 Medición del nivel de control en tecnología de la información (TI)

Debe de entenderse en primer lugar que 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”. (9:4) Si bien el control interno es un proceso, su eficacia es el estado o la situación del proceso en un momento dado.

La documentación de los procesos también ayuda en la determinación del nivel de efectividad del control, dependiendo de la criticidad del proceso; La ficha técnica que se presenta a continuación puede brindar apoyo en la determinación de la efectividad del control, el cual puede establecerse bajo tres criterios generales que son en proceso, implementado o mejorado.

**Cuadro 12**

**Establecimiento del nivel de control**

**Nivel de Control en TI**

| | | | | En Proceso (No Implementado) | | | Efectivo En 90% | Efectivo 100% |
|---|---|---|---|---|---|---|---|---|
| **P** | **SP** | **Control** | **No existente** | **Inicial** | **En Proceso** | **Implementado** | **Mejorado** |
| **Base de Datos** | | | **0** | **0** | **0** | **2** | **1** |
| | **Administración de BD** | | 0 | 0 | 0 | 2 | 1 |
| | | Administrador de Base de Datos | 0 | 0 | 0 | 0 | 1 |
| | | Atribuciones del DBA | 0 | 0 | 0 | 1 | 0 |
| | | Inventario de Bases de Datos | 0 | 0 | 0 | 1 | 0 |
| **Seguridad de Sistemas Operativos** | | | **1** | **0** | **0** | **0** | **0** |
| | **Gestión de Usuarios** | | 1 | 0 | 0 | 0 | 0 |
| | | Inhabilitación del grupo Everyone en los servidores | 1 | | | | |

Fuente: Elaboración propia en base al trabajo realizado.

El primer paso es enlistar los procesos y subprocesos que puedan existir, así como los controles o actividades de control relacionados a cada uno de estos, definido esto se pasa a la parte de evaluación del control para determinar su nivel de efectividad, con base a cinco criterios que brindaran el estatus del control interno en un proceso y en el área de forma global.

**Cuadro 13**

**Criterios de efectividad del control de TI**

| Efectividad del Control en TI | | |
|---|---|---|
| **Criterio** | **%** | **Estatus** |
| No Existente | 20 | En Proceso |
| Inicial | 40 | En Proceso |
| En Proceso | 60 | En Proceso |
| Implementado | 90 | Implementado |
| Mejorado | 100 | Mejorado |

Fuente: Elaboración propia en base al trabajo realizado.

La evaluación del control ira en dos fases, primero evaluar criterios de existencia, implementación, documentación y la segunda se centrara en las características que un control debe de guardar, para así definir si es efectivo o no. El criterio de efectividad puede variar de acuerdo a la administración o criterios de evaluación que se utilicen, sin embargo, en los criterios que se exponen en el presente trabajo se toma que todo control con un porcentaje menor al noventa por ciento, es no efectivo. A continuación se presenta un modelo de cómo medir la efectividad con datos supuestos.

**Cuadro 14**

**Criterios del control interno**

| Nota: Si el control en revisión posee el criterio coloque 1 en la columna "SI", caso contrario colo que 0 en la columan "NO" | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Existe** | | **Implementado** | | **Documentado** | | **Caracteristicas C.I** | | **Efectivo** | | |
| **Si** | **No** | **Si** | **No** | **Si** | **No** | **Si** | **No** | **Si** | **No** | $\overline{X}$ |
| 1 | | 1 | | 1 | | | 0.6 | | 0 | 0.7 |

Fuente: Elaboración propia en base al trabajo realizado.

Las características del control interno se evaluaran bajo cinco criterios cuyo resultado cuando sea mayor al 90% se indicara que es efectivo, caso contrario será colocado como no efectivo.

Las características del control indicadas en el cuadro anterior, se evalúan bajo cinco criterios:

- **Suficiente:** Que no es mucho ni poco, sino lo necesario para alcanzar el objetivo del mismo.
- **Oportuno:** Actúa de inmediato para detectar desviaciones.
- **Comprensible:** Se tiene claridad del porque se aplica.
- **Eficaz:** Cumple el objetivo de minimizar riesgos.
- **Eficiente:** Provee el uso adecuado de los recursos.

En el modelo siguiente se muestran la evaluación de las características del control interno, cuyo resultado promedio, es colocado en la columna indicada en el cuadro 14, para determinar la efectividad del control.

**Cuadro 15**

**Características del control interno**

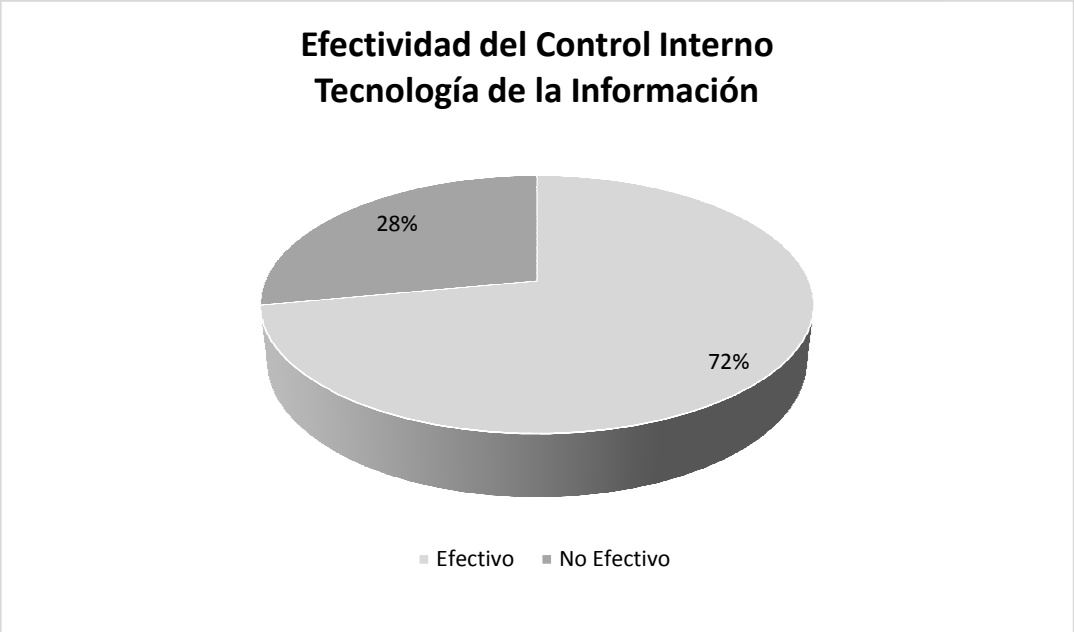
| Caracteristicas del Control | | | | | |
|---|---|---|---|---|---|
| **Suficiente** | **Oportuno** | **Comprensible** | **Eficaz** | **Eficiente** | $\overline{X}$ |
| 0 | 1 | 0 | 1 | 1 | 0.6 |

Fuente: Elaboración propia en base al trabajo realizado.

Al finalizar la evaluación permitirá definir el nivel de efectividad en cada control, lo cual permite ubicar por medio de las operaciones geométricas el estatus de cada control según corresponda y generar gráficos que permitan una mejor visualización. En el presente caso es no efectivo ya que es menor al 90%.

**Gráfica 4**

**Efectividad del control interno en TI**




Fuente: Elaboración propia en base al trabajo realizado.

### 4.13 Modelo de madurez para la gestión de riesgos de TI

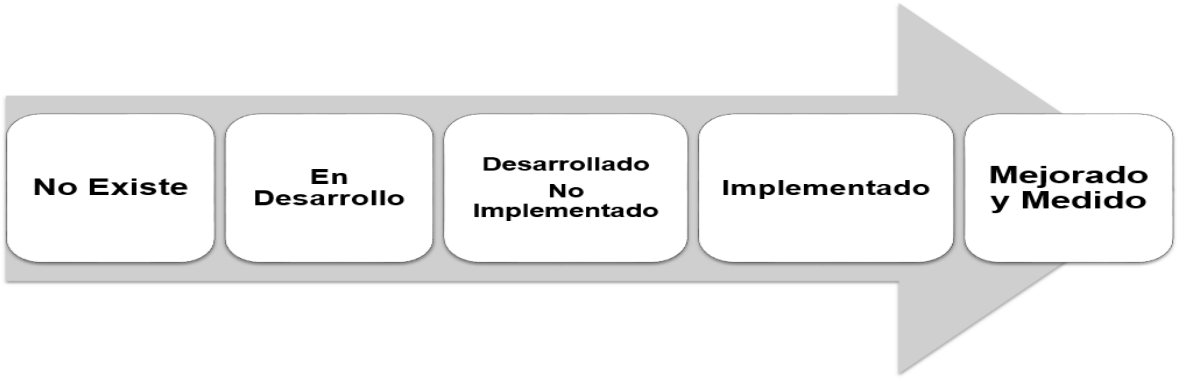
"El modelo de madurez para la administración y control de los procesos de TI, se basa en un método de evaluación definido por la organización, de tal forma que esta área pueda evaluarse a sí misma desde un nivel de no existente (0) hasta un nivel optimizado (5); los niveles de madurez están diseñados como perfiles de los procesos de TI, que una empresa reconocería como descripciones de estados posibles actuales y futuros". (21:17) Utilizando los modelos de madurez desarrollados una organización podrá identificar lo siguiente:

- El desempeño real de los procesos de tecnología de la información, es decir donde se encuentra hoy.
- El objetivo de mejora en relación a los procesos de tecnología, es decir donde desea estar la empresa.
- El crecimiento requerido, entre "como es" y "como será". (21:18)

El nivel de madurez se mide en cinco estados de cumplimiento y gestión documental de los controles y su objetivo, como bien se ha dicho es la mejora continua en el gobierno de TI, las escalas secuenciales son: (1) El control no existe, (2) El control está en proceso de desarrollo, (3) El control está desarrollado pero no implementado, (4) El control esta implementado y, (5) El control esta mejorado y medido.

**Gráfica 5**

**Nivel de madurez de TI**




Fuente: Elaboración propia en base a COBIT 4.1

### 4.14Computación en la Nube (Cloud Computing)

La computación en la nube comúnmente llamada Cloud Computing representa un gran cambio en lo forma de almacenar la información y ejecutar aplicaciones, ya que todo esto se encuentra en la web, es decir, en vez de tener todo alojado en un ordenador de escritorio, todo se encuentra ubicado en la nube, lo cual no es más que un conjunto de servidores y redes de acceso a través de internet.

“Se entiende como la tendencia de disponer de archivos y aplicaciones directamente desde la web, lo cual permite acceder a servicios y aplicaciones mediante cualquier navegador convencional, en este tipo de tecnología un usuario puede ingresar a todo tipo de servicios sin necesidad de instalar un software en un ordenador”. (39)

### 4.14.1 Ventajas y desventajas

Las ventajas que podemos observar en el Cloud Computing, son las siguientes:

- Acceso a la información y los servicios desde cualquier lugar.
- Disponibilidad del servicio y/o aplicación web 24/7 los 365dias.
- Accesibilidad mediante diferentes tecnologías compatibles, tales como: ipads, móviles, portátiles, blackberrys, netbooks, etc.
- Servicios gratuitos y de pago según las necesidades del usuario.
- No saturación del uso del disco duro en el ordenador o aplicación que se usa, debido a que solo se necesita un navegador web, e internet.
- Empresas con facilidad de escalabilidad.
- Capacidad de procesamiento y almacenamiento sin instalar máquinas localmente. (39)

Las desventajas que pueden observarse en este tipo de tecnología son:

- Acceso de toda la información a terceras empresas.
- Dependencia de los servicios en línea.
- Descontrol del manejo, almacenamiento y uso de esta información.
- Dependiendo de la tecnología sobre la que se desarrolle, ciertos tipos de dispositivos podrían no acceder al servicio.
- Mayor dependencia de proveedores de internet, fibra óptica u otras tecnologías.
- Posibilidad de que delincuentes cibernéticos revienten la seguridad del servicio y se hagan con datos privados.
- En ocasiones, puede que debido a una catástrofe natural o error humano, dicho servicio quede fuera de servicio, con las malas repercusiones a los clientes. (39)

### 4.14.2 Riesgos asociados al Cloud Computing

Los riesgos en este tipo de tecnología pueden ser varios, sin embargo se identifican siete riesgos principales que deben ser considerados en el área del Cloud Computing, los cuales se presentan a continuación:

- **La confianza del proveedor:** externalizar las aplicaciones y datos corporativos, conlleva que se asegure la calidad del servicio, términos contractuales basado en los principios de confidencialidad, integridad y disponibilidad.
- **Conformidad legal:** un aspecto a resaltar es que el responsable de la información es el propietario de la misma. Por ellos los proveedores de este tipo de tecnología deben permitir cualquier tipo de auditoría externa y cumplir cualquier medida que se necesaria para garantizar la seguridad de sus clientes.
- **Localización de los datos:** es uno de los puntos fuertes de esta tecnología pero también uno de sus mayores riesgos, ya que debe de permitirse el ingreso a los datos en cualquier momento, independientemente donde estén localizados.
- **Protección de la información:** se corre el riesgo de que otros puedan acceder a nuestra información, derivado a que se comparten recursos por ende no puede ir en menoscabo la confidencialidad de la información.
- **Recuperación:** desconocer la ubicación de la información no puede implicar jamás que no existan las medidas necesarias de seguridad y replicación para garantizar su recuperación en caso de desastre o pérdida de la misma.
- **Colaboración con la justicia:** puede no existir acatamiento de leyes o regulaciones respecto a la protección y seguridad de la información, independientemente de las normas propias del país donde se localicen los datos y aplicaciones del usuario.

- **Una relación "para toda la vida":** La sostenibilidad del proveedor tiene que estar garantizada. Fusiones, quiebras, cualquier cambio en su negocio no puede dejar 'indefenso' al cliente y, por ello, se establecerá un compromiso de continuidad a largo plazo en la relación en los propios términos del contrato. (39)

### 4.15 Cibercrimen

Un cibercrimen es "cualquier acto ilegal que se comete a través de computadoras, como robo de identidad, acceso no autorizado a sistemas, cambio de información, estafas, robo de dinero; hasta crimen organizado que utiliza medios electrónicos para delinquir (pornografía infantil, trasiego de personas, etc.)".(30)

El más común es el uso de los virus que pueden borrar, desaparecer, descomponer y/o facilitar el acceso de los criminales a la información personal. También podemos definir que son un conjunto de actividades ilegales asociadas con el grupo de tecnologías de la información, especialmente en Internet. Está definido como un acto ilegal que involucra una computadora, sus sistemas o sus aplicaciones.

#### 4.15.1 Cibercrimen en Guatemala

"4054 es el número de registro que tiene la iniciativa de ley contra el Cibercrimen, con fecha de ingreso 11 de mayo de 2009 al congreso de la república de Guatemala, la misma está compuesta por 31 folios. Desde el año indicado se discute la iniciativa de ley y fue propuesta por varios diputados entre ellos Sr. Mariano Rayo y Francisco Contreras, la ley ha pasado por los respectivos procesos dentro del Congreso de la República de Guatemala y actualmente se encuentra dentro de la comisión de legislación. Por lo que no está emitida y se encuentra en su fase de discusión y divulgación, procesos iniciados desde septiembre 2009". (34)

# CAPÍTULO V

# LA FUNCIÓN DE LA AUDITORÍA INTERNA, EN LA ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO, CON BASE A LA REGULACIÓN DE LA JUNTA MONETARIA, APLICABLE A LAS EMPRESAS QUE SE ESPECIALIZAN EN EL PROCESAMIENTO MASIVO DE DOCUMENTOS DE FORMA ELECTRÓNICA, EN LA COMPENSACIÓN DE CHEQUES PARA EL SISTEMA BANCARIO DEL PAÍS
# (CASO PRÁCTICO)

## 5.1 Antecedentes de la empresa

La empresa Imagen S.A, fue fundada en mayo del año 1999 e inicio sus operaciones en ese mismo año, sus oficinas se encuentran en la 4ta avenida 16-65 Edificio Los Platinos en la zona 10. Su propósito es brindar soporte al sistema bancario del país por medio del procesamiento masivo de documentos de forma electrónica para la compensación de cheques, su visión es establecerse como eje estratégico para el sector financiero en el procesamiento de documentos, evolucionando conforme a las tendencias mundiales, para así ofrecer servicios innovadores y confiables a sus clientes.

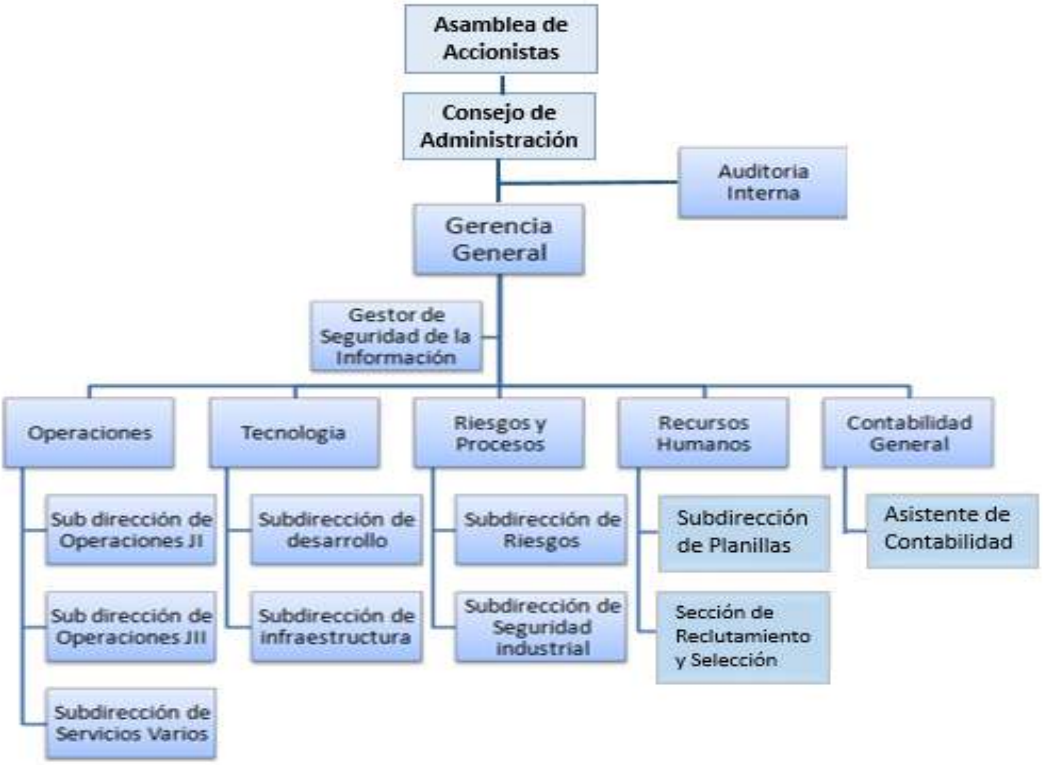
La empresa Imagen, S.A. es una empresa de capital guatemalteco de apoyo al sector financiero y su misión es promover economía de escala, a través de servicios especializados en el procesamiento masivo de documentos en forma electrónica, incorporando innovación tecnológica para beneficio de sus clientes y accionistas y a la vez generando bienestar para sus colaboradores. Los valores que la identifican y que están plasmados como parte de su cultura son la integridad, servicio al cliente y superación personal.

Esta empresa es dirigida por una asamblea general de accionistas, un consejo de administración, una gerencia general y gerentes en cada una de las áreas; cuenta

además con un departamento de auditoría interna. Actualmente laboran en la entidad 131 empleados, distribuidos de la forma siguiente:35 Personal de Administración, 27 Personal de Operaciones JI, 38 Personal de Operaciones JII y 31 Personal de Servicios Varios. Su estructura organizacional es la siguiente:

**Organigrama 1**

**Estructura Organizacional**




Fuente: Elaboración propia en base al trabajo realizado.

Dentro de la estructura existe un departamento de auditoría interna, mismo que rinde sus informes al consejo de administración, el cual está organizado de la forma siguiente:

- Auditor Interno
- Asistente de auditoría financiero administrativo
- Asistente de auditoría de operaciones y riesgos
- Asistente de auditoría de sistemas

Sus principales líneas de negocio están integradas por los siguientes servicios:

- Cámara de Compensación Bancaria
- Cámara de Compensación Automatizada
- Plataforma de Negocios Swift
- Remesas al Exterior
- Digitalización de cheques de ventanilla

Derivado a que sus procesos de negocio son directamente para el sistema bancario del país, en septiembre del 2011 con la publicación de la regulación de la Junta Monetaria para la Administración del Riesgo Tecnológico (JM-102-2011), la entidad se vio afecta a la misma por medio del artículo 25 del citado reglamento, por lo cual inicio un proceso de implementación de la gestión del riesgo tecnológico con el fin de darle cumplimiento a lo establecido, por medio de una asesoría con una empresa especializada.

Como parte integral de su plan de trabajo el departamento de Auditoría Interna, tiene contemplado realizar una evaluación, tomando como base la regulación JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico y el proceso para la administración que se ha definido para tal caso por la dirección en base a COSO ERM, dicha auditoria será ejecutada en el tercer trimestre del año 2014.

Ante lo anterior expuesto, se le nombra como el auditor para la ejecución de la misma, y se requiere que realice los papeles de trabajo que considere necesarios a fin de brindar una seguridad razonable sobre la administración del riesgo tecnológico.

El plan de trabajo para el año 2014 de auditoría interna para el área de tecnología de la información, se observa a continuación:

| *PLAN DE TRABAJO AI_2014* | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | ACTIVIDAD | Septiembre | | | | Octubre | | | |
| | | | | | | | | | |
| | GERENCIA GENERAL | | | | | | | | |
| | GERENCIA DE RECURSOS HUMANOS | | | | | | | | |
| | GERENCIA CONTABILIDAD GENERAL | | | | | | | | |
| | GERENCIA DE OPERACIONES | | | | | | | | |
| | GERENCIA DE TECNOLOGIA Y SOPORTE | | | | | | | | |
| 1 | Auditoria de Seguridad de la informacion 1ra fase | | | | | | | | |
| 2 | Auditoria de cumplimiento al Plan Estrategico de IT (1) | | | | | | | | |
| 3 | Auditoria Soporte al Hardward | | | | | | | | |
| 4 | Auditoria de Base de datos e implantacion del desarrollo de proyectos 1ra. Fase | | | | | | | | |
| 5 | Auditoria de Redes y comunicaciones 1ra fase | | | | | | | | |
| 6 | Auditoria de restriccion y perfilamiento de usuarios * | | | | | | | | |
| 7 | Auditoria de procesamiento de informacion y Tercerizacion | | | | | | | | |
| 8 | Auditoria Relacion con Proveedores y servicios de IT | | | | | | | | |
| 9 | Auditoria Planeacion continuidad del negocio | | | | | | | | |
| 10 | Auditoría de accesos a los sistemas no administrados por IT | | | | | | | | |
| 11 | Auditoria a la Administracion del Riesgo Tecnologico según JM-102-2011 - cumplimiento regulatorio | | | | | | | | |
| 12 | Auditoria de Seguridad de la informacion 2da fase | | | | | | | | |
| 13 | Auditoria de Base de datos e implantacion del desarrollo de proyectos 2da. Fase | | | | | | | | |
| | GERENCIA DE RIESGOS Y PROCESOS | | | | | | | | |
| | ACTIVIDADES ADMINISTRATIVAS Y OTROS | | | | | | | | |

**5.2 Nombramiento del auditor**

**IMAGEN, S.A.**

**NOMBRAMIENTOAI-10-2014**

DE: Auditor Interno

PARA: Auditor de Operaciones y Riesgos

ASUNTO: Auditoría a la Administración del Riesgo Tecnológico

FECHA: 10/09/2014

**I ÁREA A AUDITAR:**

Gerencia de Tecnología de la Información.

**II ACTIVIDAD:**

Evaluación del adecuado proceso para la administración del riesgo tecnológico y el cumplimiento regulatorio de la JM-102-2011.

**III OBJETIVO:**

Desarrollar apropiadamente las pruebas para validar la eficiencia y efectividad de la administración del riesgo tecnológico, así como del cumplimiento en todos los aspectos que se establecen en la regulación JM-102-2011

**IV PERIODO DE REVISIÓN:**

Tercer trimestre del 2014

**V ESPECIFICACIÓN:**

Este proyecto debe iniciarse el día lunes 10 de Septiembre y entregar resultados el día 08 de octubre del 2014.

Proceder a ejecutarla el procedimiento ya fue revisado.

Muy atentamente,

Lic. Miriam Camey

Auditora Interna

## 5.3 Planificación de la auditoría

Para el trabajo de evaluación a la administración del riesgo tecnológico en base a la regulación JM-102-2011, se requiere la inversión de 194 horas hombre distribuidas entre el auditor asignado y el gerente de auditoría.

**Periodo: del 09 de septiembre al 08 de octubre del 2014**

| Descripción | Fecha | Auditor Asignado | Gerente de Auditoria | Total Horas Hombre |
|---|---|---|---|---|
| Planificación administrativa | 09 de septiembre | 8 | 1 | 9 |
| Conocimiento del proceso a auditar | 10, 11 de septiembre | 16 | 1 | 17 |
| Evaluación del control interno | 12, 13 de septiembre | 16 | 2 | 18 |
| Planificación para la ejecución | 16, 17 de septiembre | 16 | 2 | 18 |
| Ejecución de la auditoria | 18 de septiembre al 01 de octubre | 80 | 0 | 80 |
| Revisión de papales de trabajo | 02, 03 de octubre | 16 | 0 | 16 |
| Elaboración del borrador del informe | 04 de octubre | 8 | 0 | 8 |
| Discusión del informe | 07 de octubre | 8 | 4 | 12 |
| Informe final y recomendaciones | 08 de octubre | 8 | 8 | 16 |
| | Horas Hombre | 176 | 18 | 194 |
| | Costo Hora Hombre | 27.33 | 77.11 | |
| | **Costo Total** | **Q4,810.08** | **Q1,387.98** | **Q6,198.06** |

Los costos hora hombre están definidos en base a los salarios mensuales devengados por cada uno de los involucrados en la auditoría a realizar. Los recursos físicos y tecnológicos para la realización de este trabajo de auditoría se definen a continuación:

| Descripción | Cantidad |
|---|---|
| Laptop | 1 |
| Impresora | 1 |
| Tabla shanon | 1 |
| Hojas en blanco | indefinido |
| Utiles de Oficina | indefinido |

## 5.4 Índice de papeles de trabajo

**Imagen, S.A.**

**Auditoría Interna -2014**

**Índice de Papeles de Trabajo**



**Imagen, S.A.**

**Auditoria Interna -2014**

**Marcas de Auditoría**

| P/T | MC | |
|---|---|---|
| Elaboro: | Jfco | 12/09/2014 |
| Reviso: | Bmc | 12/09/2014 |

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

**IMAGEN, S.A.**

**PROGRAMA DE AUDITORÍA INTERNA**

**ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO**

| P/T | A | |
|---|---|---|
| Elaboro: | Jfco | 11/09/2014 |
| Reviso: | Bmc | 12/09/2014 |

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

| No. | PROCEDIMIENTOS | REF. | PÁG. |
|---|---|---|---|
| 01. | Verifique la existencia del comité de riesgos, acta de constitución y el nivel de conocimiento respecto a metodologías y herramientas para la gestión de riesgos. | AA-1 | 114 |
| 02. | Verifique actas de reunión del comité de riesgos, así como la periodicidad de sus reuniones. | AA-2 | 115 |
| 03. | Verifique que se tenga un adecuado proceso integral de documentación de los procesos de TI, observando metodología, codificación, control de documentos, tipo, estatus, otros. | AA-3 | 117 |
| 04. | Tenga a la vista y analice el plan estratégico de TI y verifique que estén alineados a los objetivos estratégicos de la organización. | AA-4 | 118 |
| 05. | Evalué que se cuente con una adecuada estructura organizacional de TI dentro de la empresa. | AA-5 | 119 |
| 06. | Evalué que se tengan una adecuada segregación de funciones, observando que se tengan adecuadamente definidas las responsabilidades de cada uno de los involucrados en el proceso. | AA-6 | 120 |
| 07. | Observe que se cuente con un presupuesto directamente para la gerencia de tecnología y su adecuada administración | AA-7 | 121 |

| No. | PROCEDIMIENTOS | REF. | PÁG. |
|---|---|---|---|
| 08. | Observe que se cuente con una declaración en relación al riesgo tecnológico, así como la determinación de una filosofía para la administración del riesgo tecnológico. | BB-1-1 | 124 |
| 09. | Evalué que se tenga establecido los niveles de criticidad, sensibilidad, probabilidad e impacto para la administración del riesgo tecnológico, definiendo si son adecuadas y están aprobadas por el consejo de administración. | BB-1-1 al BB-1-5 | 124 a la 126 |
| 10. | Verifique el establecimiento de objetivos para la administración del riesgo tecnológico tanto a nivel general como específicos. | BB-2-1 AL BB-2-2 | 128 |
| 11. | Verifique que tenga establecido y actualizado el inventario de activos de TI. | BB-3-1 | 130 |
| 12. | Verifique que se tenga un catálogo de riesgos identificados que puedan afectar a los activos de TI. | BB-3-2 | 131 |
| 13. | Evalué la matriz de riesgos de TI, así como su adecuada gestión y representación. Observando la adecuada aplicación de los criterios establecidos y aprobados por el consejo de administración. | BB-4-1 | 133 |
| 14. | Verifique la existencia de planes de tratamientos para aquellos riesgos bajo calificación Alto o Grave. | BB-4-2 | 134 |
| 15. | Revise que se cuente con un inventario de infraestructura de Tecnología de la Información y que se esté gestionando adecuada y oportunamente. | BB-3-1 | 130 |
| 16. | Revise que se tenga un inventario de los sistemas de información en el área de TI y que este actualizado. | BB-3-1 | 130 |
| 17. | Verifique la existencia de un inventario de bases de datos, el cual debe de estar actualizado y contar con la información adecuada para su gestión. | BB-3-1 CC-1-4 | 130 139 |

| No. | PROCEDIMIENTOS | REF. | PÁG. |
|---|---|---|---|
| 18. | Verifique que se realicen monitoreos al rendimiento de la infraestructura, bases de datos y sistemas de información. | C-1-1 | 136 |
| 19. | Verifique el inventario de los servicios de TI, observando que este actualizado. | CC-1-2 | 137 |
| 20. | Verifique y analice la administración de los incidentes de TI. | CC-1-3 | 138 |
| 21. | Evalué el perfil del Administrador de Bases de Datos, verificando que sea adecuado y que cumpla con los requisitos mínimos o requerimientos del negocio. | CC-1-5 | 140 |
| 22. | Verifique que se cuente con un proceso de clasificación de la información. | CC-2-1 | 144 |
| 23. | Verifique que se cuente con medidas de seguridad física para el área del Data Center. | CC-2-2 | 145 |
| 24. | Evalué la matriz de acceso llevada por TI, verificando usuarios de alta y baja, actualización, revisiones y otros. | CC-2-3 | 146 |
| 25. | Evalué que se cuente con un inventario de copias de respaldo y otras medidas para asegurar la información. | CC-2-4 | 147 |
| 26. | Verifique que se tenga un plan de continuidad para las operaciones de TI y que esté debidamente probado. | CC-3-1 al CC-3-4 | 149 a la 152 |
| 27. | Verifique que se tenga un plan de capacitaciones integral para el área de tecnología y que esté de acuerdo a los planes estratégicos del negocio. | CC-3-5 | 153 |
| 28. | Evalué que se cuente con un control de proveedores de TI y su adecuada gestión. | CC-4-1 | 155 |
| 29. | Evalué que se cuente con un Gestor de Seguridad de la Información y el cumplimiento de sus funciones | CC-4-2 | 156 |

**IMAGEN, S.A.**

**CUESTIONARIO DE CONTROL INTERNO**

**ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO**

**REALIZADO A: GERENTE DE TECNOLOGÍA DE LA INFORMACIÓN**

| P/T | B | |
|---|---|---|
| Elaboro: | Jfco | 12/09/2014 |
| Reviso: | Bmc | 13/09/2014 |

**Objetivos:**

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

b. 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 |
|---|---|---|---|---|
| 01. | ¿Se ha completado la implementación de la administración del riesgo tecnológico? | | X | Esta implementado en un 90% |
| 02. | ¿Se tienen documentados todos los procesos de TI? | X | | Están totalmente documentados. |
| 03. | ¿Se cuenta con un proceso de administración de documentos, para la documentación de TI? | X | | Si, existe un control de gestión documental en efecto. |
| 04. | ¿Se cuenta con un manual para la administración del riesgo tecnológico? | X | | MNP para la Administración del Riesgo Tecnológico. |
| 05. | ¿Se cuenta con una unidad para la administración de riesgos, que apoyo en la identificación y evaluación de los mimos? | X | | Esta es totalmente independiente del área de tecnología. |

| No. | Cuestionamiento | Si | No | Comentario |
|---|---|---|---|---|
| 06. | ¿Se tiene establecido un comité de riesgos y está debidamente formalizado con su acta de constitución? | X | | Su constitución se puede observar en el acta de constitución. |
| 07. | ¿Se reúnen periódicamente los miembros del comité a fin de poder filtrar y evaluar los eventos generados de riesgo tecnológico? | X | | Las reuniones se tienen mensualmente. |
| 08. | ¿Se cuenta con un plan estratégico de TI, alineado a los objetivos estratégicos del negocio? | X | | Este es conocido por la Gerencia General y aprobado por el C.A. |
| 09. | ¿Se cuenta con una estructura organizacional de TI, donde se delimite las áreas de gestión, desarrollo y operaciones? | X | | Este ya está desarrollado, sin embargo se trabaja en su implementación. |
| 10. | ¿Se ha implementado la gestión del proceso de la administración de riesgo tecnológico en base a la JM-102-2011? | X | | La base ha sido la JM-102-2011 apoyado en otros marcos de buenas prácticas. |
| 11. | ¿Se tiene definido los niveles de criticidad y sensibilidad, en la administración del riesgo tecnológico? | X | | Estos fueron aprobados por el Consejo de Administración |
| 12 | ¿Se tienen definido los niveles de probabilidad e impacto? | X | | Aprobados por el Consejo. |

| No. | Cuestionamiento | Si | No | Comentario |
|---|---|---|---|---|
| 13. | ¿Se ha establecido el nivel de apetito al riesgo? | X | | Está definido hasta un monto de $25,000 |
| 14. | ¿Se cuenta con un catálogo de los activos de TI, considerando los niveles de criticidad y sensibilidad? | X | | Está debidamente actualizado. |
| 15. | ¿Se tiene definida la matriz de riesgos y la forma de evaluar cada proceso? | X | | En el MNP de la Administración del Riesgo Tecnológico |
| 16. | ¿Se cuentan con mapas de calor que permitan visualizar los riesgos de mayor impacto? | X | | Estos son generados automáticamente por medio de la matriz. |
| 17. | ¿Se evalúa periódicamente los riesgos identificados verificando su situación actual? | X | | Trimestral o semestralmente. |
| 18. | ¿Se tiene inventario de la infraestructura de TI y se encuentra actualizado? | X | | Este sirvió para definir las amenazas y vulnerabilidades. |
| 19. | ¿Se tiene inventario de las bases de datos de los sistemas de información, con sus diccionarios de datos y diagramas de relación? | X | | Está actualizado y es revisado de forma periódica por el DBA. |
| 20. | ¿Se cuenta con un perfil definido para el administrador de bases y se evalúa periódicamente sus resultados? | X | | Aparte de él, existe un auxiliar de DBA que lo apoya. |
| 21. | ¿Se cuenta con informes de rendimiento de los sistemas de información, bases de datos e infraestructura de TI? | X | | Estos son generados trimestralmente. |

| No. | Cuestionamiento | Si | No | Comentario |
|---|---|---|---|---|
| 22. | ¿Se cuenta con un inventario de los servicios que brinda TI? | X | | Aunque están en proceso de formalización con los usuarios. |
| 23. | ¿Se cuenta con procesos que permitan gestionar adecuadamente los incidentes de TI? | X | | Se cuenta con una mesa de ayuda para el efecto. |
| 24. | ¿Se cuenta con procedimientos para el escalonamiento de respuesta a los incidentes de TI? | X | | Están presentes en el MNP para la Administración del Riesgo Tecnológico. |
| 25. | ¿Se cuenta con un procedimiento para la clasificación de la información? | X | | Existe un diagrama de apoyo para el entendimiento de los propietarios de la información. |
| 26. | ¿Se tienen establecidos medidas de seguridad física para el Data Center? | X | | Sin embargo, estas son administradas por la subdirección de seguridad industrial |
| 27. | ¿Se cuenta con una adecuada matriz de accesos, que permita gestionar los usuarios de forma oportuna y clara? | X | | Está debidamente actualizada al 30 de septiembre. |
| 28. | ¿Se realizan copias de respaldo para la información de la organización, clasificada según su criticidad y sensibilidad? | X | | Están gestionadas por medio de un control de back ups, resguardadas de forma adecuada. |

| No. | Cuestionamiento | Si | No | Comentario |
|---|---|---|---|---|
| 29. | ¿Se cuenta con un plan de continuidad de operaciones de TI, ante cualquier eventualidad? | X | | Está documentado y probado. |
| 30. | ¿Se han realizado pruebas que permitan garantizar la oportunidad y eficacia del plan de continuidad de operaciones de TI? | X | | Existen informes de las pruebas realizadas |
| 31. | ¿Se tiene establecido quienes son el personal crítico en TI? | X | | Se está trabajando en un plan de sucesión de puestos. |
| 32. | ¿Se capacita al personal de forma adecuada para dar respuesta a los objetivos del área de TI y a los objetivos de la organización? | X | | Se realiza un DNC anualmente con la gerencia de RRHH para definir las capacitaciones. |
| 33. | ¿Se cuenta con un sitio alterno de operaciones? | X | | Está ubicado en zona 7 y cuenta con los requisitos mínimos de operación. |
| 34. | ¿Se cuenta con una gestión de proveedores para el área de TI? | | X | Actualmente se está trabajando en ello. |

**NOTA:** El presente cuestionario de control interno está basado en la regulación de la Junta Monetaria JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico.

**CONCLUSIÓN:** El cuestionario fue finalizado con éxito y adecuadamente, observándose que la mayoría de cuestionamientos fueron respondidos de forma afirmativamente. Los resultados obtenidos serán cotejados con los resultados de los procedimientos a evaluar para un mejor alcance del trabajo.

**Imagen S.A.**
**Auditoría Interna**
**Organización para la Administración del Riesgo Tecnológico**

| P/T | AA | |
|---|---|---|
| Elaboro: | Jfco | 18/09/2014 |
| Reviso: | Bmc | 19/09/2014 |

**Imagen, S.A.**

**Acta de Constitución** ✔

**Comité de Riesgos** ✔

| P/T | AA-1 | |
|---|---|---|
| Elaboro: | Jfco | 18/09/2014 |
| Reviso: | Bmc | 19/09/2014 |

En la ciudad de Guatemala, siendo las nueve horas en punto del día once del mes de octubre del 2011, en la sala de sesiones de la empresa Imagen, S.A. se encuentran reunidos las personas, Faustino López, Ambrosio Shell, Lucrecia Pineda, Azucena Carrillo, José Artemis, Miriam Camey y Rafael Buenavista, para hacer constar lo siguiente: **PRIMERO: De su integración.** Los descritos anteriormente pasaran a formar parte del comité de riesgos a partir de la presente fecha, Estas personas no recibirán remuneración por formar parte de dicho comité. El mismo será presidido por el Gerente General o la persona que el designe, en caso de su ausencia. **SEGUNDO: De su objetivo principal.** El comité de riesgos tiene como objetivo fundamental definir las estrategias para medir y mitigar la exposición al riesgo tecnológico y operativo, así como velar por la implementación de los acuerdos adoptados en cuestión de la gestión de riesgos. **TERCERO: Son derechos y obligaciones de los miembros del comité.** Participar en forma activa y continua en el desenvolvimiento de las actividades del comité; todos sus integrantes ejercerán voz y voto, a excepción de la Auditoría Interna, quien solo tendrá voz, mas no voto. **CUARTO: De las reuniones.** El comité de riesgos deberá reunirse como mínimo 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 se considere oportuno se podrá invitar a las reuniones a otros funcionarios, quienes asistirán con voz pero sin voto. De cada reunión se levantara un acta. **QUINTO: Plazos de los nombramientos.** Los miembros del comité permanecerán en sus funciones por tiempo indefinido. **SEXTO:** No habiendo nada más que constar se da por finalizada la presente Acta Constitutiva en el mismo lugar y fecha, siendo las doce horas en punto.

**Faustino López**
**Presidente del Comité**

**Ambrosio Shell**
**Secretario**

| | |
|---|---|
| ✔ | Verificado conforme |
| X | Verificado Inconforme |

**IMAGEN, S.A.**

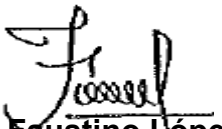
**CR-ACTA 01-2013** ✔

**COMITÉ DE RIESGOS** ✔

| P/T | AA-2 | |
|---|---|---|
| Elaboro: | Jfco | 18/09/2014 |
| Reviso: | Bmc | 19/09/2014 |

En la ciudad de Guatemala, siendo las once horas del dieciocho de julio del año dos mil trece, en la sala de sesiones de la empresa Imagen, S.A. se encuentra reunido el Comité de Riesgos, para hacer constar lo siguiente: **PRIMERA: 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) Lectura y aprobación del acta del Comité de Riesgos de fecha siete de abril de dos mil trece; 3) Documento formal que se redactara en cada sesión del Comité de Riesgos y el código que se utilizara para identificación del documento; 4) Validez del documento de cada reunión; 4) Rotación de Secretaría; 5) 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: Lectura y aprobación del acta del Comité de Riesgos de fecha siete de abril de dos mil trece**. Se dio lectura al acta que contiene la sesión del Comité de Riesgos de fecha siete de abril del dos mil trece. Después de leída el pleno del Comité de Riesgos aprueba el contenido del documento, haciendo la enmienda que a esta acta debe adjuntársele físicamente: el Reglamento del Comité de Riesgos, el Manual de la Gestión Integral de Riesgos y los mapas de calor. **TERCERA: Documento formal que se redactara en cada sesión del Comité de Riesgos y el código que se utilizara para identificación del documento**. Se presentó al pleno del comité para su discusión si el documento que debe redactarse en cada sesión del Comité de Riesgos debe ser un acta o una minuta. El pleno del comité de Riesgos por consenso aprobó que se deba redactar un acta en cada sesión que se realice. Se propone que la codificación del acta de cada sesión sea de la siguiente manera las letras en mayúscula CR guión ACTA espacio No. seguido del correlativo del acta guion año (CR-ACTA No. 01-2013). El pleno del Comité de Riesgos por consenso aprobó la codificación a utilizar para cada acta de reunión. **CUARTA: Validez del acta de cada reunión.** Se presentó

al pleno del Comité de Riesgos para su discusión que para la validez de un acta de reunión del Comité de Riesgos sean necesarias únicamente las firmas del Secretario y Presidente en funciones del Comité indicado pudiendo firmar los demás integrantes si así lo desean. El pleno del Comité de Riesgos por consenso aprobó este punto. **QUINTA:** Rotación de Secretaría: Se presentó la iniciativa al pleno del Comité de Riesgos de que la secretaría sea rotativa entre los miembros del Comité. El pleno del Comité de Riesgos por consenso aprobó este punto. **SEXTA:** Puntos varios: Se presentó la iniciativa de que en las sesiones del Comité de Riesgos se tratara lo relacionado con los siguientes temas: Riesgos, Riesgo Tecnológico y Continuidad del Negocio y que en cada acta de sesión del Comité de Riesgos quede establecido todo lo tratado sobre los temas indicados. El pleno del Comité de Riesgos por consenso aprobó este punto. **SEPTIMA:** Finalización de la Reunión: No habiendo más que hacer constar se da por finalizada la presente Acta en el mismo lugar, el día dieciocho de julio del dos mil trece, siendo las doce horas en punto.



**Faustino López**
**Presidente del Comité**

**Ambrosio Shell**
**Secretario**

| | |
|---|---|
| ✓ | Verificado conforme |
| X | Verificado Inconforme |

**Imagen, S.A.**

**Gerencia de TI -2014**

**Lista Maestra de Documentos de los Procesos de Tecnología de la Información**

| P/T | AA.3 | |
|---|---|---|
| Elaboro: | Jfco | 18/09/2014 |
| Reviso: | Bmc | 20/09/2014 |

| DUEÑO DEL PROCESO | TIPO DOCUMENTO | CÓDIGO DOCUMENTO | NOMBRE DEL DOCUMENTO | Ver | Formato | ESTADO DOCUMENTO | |
|---|---|---|---|---|---|---|---|
| GERENCIA DE TI | INSTRUCTIVO | GTI-INS-GTI-001 | Instructivo para definir tablas de sensibilidad y criticidad de la información y probabilidad e impacto del riesgo tecnológico | 1 | Digital | Aprobado (listo para implementar) | ✓ |
| GERENCIA DE TI | INSTRUCTIVO | GTI-INS-GTI-002 | Instructivo para identificar los principales activos de tecnología con su nivel de criticidad y sensibilidad | 1 | Digital | Aprobado (listo para implementar) | ✓ |
| SUBDIRECCION DE INFRAESTRUCTURA | INSTRUCTIVO | SDI-INS-GTI-004 | Instructivo para la actualización del diagrama de red y diagrama de infraestructura | 1 | Digital | Aprobado (listo para implementar) | ✓ |
| SUBDIRECCION DE TI | INSTRUCTIVO | SDT-INS-GTI-006 | Instructivo para realizar respaldos y su restauración – de las bases de datos | 1 | Digital | Aprobado (listo para implementar) | ● |
| GERENCIA DE TI | INSTRUCTIVO | GTI-INS-GTI-016 | Instructivo para la gestión del riesgo tecnológico | 1 | Digital | Implementado (vigente) | ● |
| GERENCIA DE TI | POLITICA | GTI-POL-GTI-001 | Politicas de Seguridad de la Información | 1 | Digital | Implementado (vigente) | ✓ |
| GERENCIA DE TI | MANUAL | GTI-MAN-GTI-001 | Manual de gestión del riesgo tecnológico | 1 | Digital | Aprobado (listo para implementar) | ⊖ |
| ✓ | ✓ | | ✓ | | ✓ | ✓ | ) Z-5 |

**Observación:** En la revisión realizada se observó que el Manual que rige la Administración del Riesgo Tecnologico no ha sido implementado, por lo cual no se puede brindar seguridad razonable en todo el proceso como tal.

| | |
|---|---|
| ✓ | Verificado conforme |
| ● | En seguimiento |
| ⊖ | No implementado |
| ) | Va para |

**Imagen S.A.**
**Gerencia de Tecnología**
**Plan Estrategico de TI** ✔

| P/T | AA.4 | |
|---|---|---|
| Elaboro: | Jlco | 20/09/2014 |
| Reviso: | Umc | 21/09/2014 |

| | Nombre de tarea | Duration |
|---|---|---|
| 1 | **Estratégicos** | **231 days?** |
| 2 | PLAN DE TRABAJO CREA ... | 231 days? |
| 3 | DESARROLLO IIC | 204 days |
| 28 | PREPARACIÓN TÉCNICA BANCOS E ICG | 211 days? |
| 39 | ACUERDOS INTERBANCARIOS Y PROCEDIMIENTOS OPERATIVOS INTERNOS | 86 days? |
| 45 | PRUEBAS Y CERTIFICACIÓN | 89 days? |
| 48 | PREPARACIÓN PARA EL PASE A PRODUCCIÓN | 21 days? |
| 63 | CAPACITACIONES ICG | 1 day? |
| 71 | ANALISIS FINANCIERO | 1 day? |
| 76 | **PLATAFORMA DE MERCADO SWIFT** | 99.75 days? |
| 77 | Asesoramiento | 1 day |
| 78 | Procesos x Banco y forma de operación | 5 days |
| 79 | Instalación de Servidores | 7 days |
| 80 | Instalación SW | 72.75 days |
| 91 | Fin del Proyecto | 0 days |
| 92 | Capacitación del personal asignado | 5 days |
| 93 | Documentar procesos | 1 day? |
| 94 | **Renovación del Sitio Alterno** | 94 days? |
| 95 | Planificación del Proyecto | 1 day? |
| 96 | Desarrollo del Proyecto | 1 day? |
| 97 | TI | 7 days |
| 106 | **Regulatorios** | **239 days?** |
| 107 | JM-102-2011 REGLAMENTO RIESGO TECNOLÓGICO Y SU GESTIÓN | 239 days |
| 115 | JM-86-2011 ESTANDARIZACIÓN DE LA CUENTA BANCARIA IBAN | 86 days? |
| 147 | | |
| 148 | **Mejora Continua** | **230.75 days** |
| 149 | Renovación SAN / Servidores | 29 days |
| 163 | Integración Remesas Optimus | 127 days? |
| 171 | Concientización Políticas | 135 days |
| 178 | DRP – DR Entorno Virtual | 65 days |
| 183 | Monitor Servicios Optimus (Compensación) | 60 days |
| 186 | Seguimiento a la gestión por competencias | 1 day? |

✔

**Observación:** Se observó el cronograma de actividades del plan estrategico de TI, el cual esta alineado a los objetivos del negocio; se observó que para la implementación de la administración del riesgo tecnológico se asignaron 239 días.

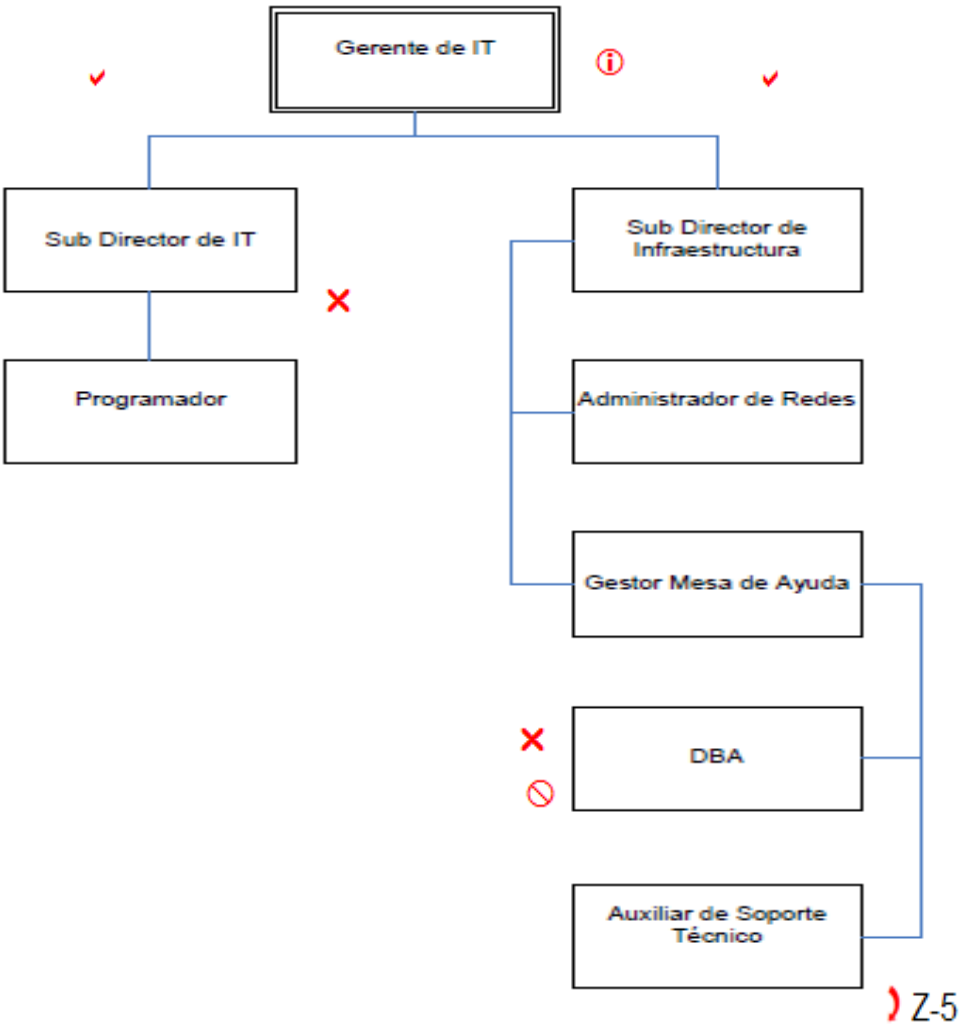
| | |
|---|---|
| ✔ | Verificado conforme |

**Imagen, S.A.**

**Gerencia de TI**

**Estructura Organizacional de TI** ✔

| P/T | AA-5 | |
|---|---|---|
| Elaboro: | Jfco | 19/09/2014 |
| Reviso: | Bmc | 20/09/2014 |




**Observación:** Se detectó concentración de conocimiento en el Subdirector de TI, ya que no ha delegado las funciones que debe desempeñar el administrador de Base de Datos (DBA); El colaborador que tiene este perfil se encuentra dentro de la estructura organizacional bajo responsabilidad del Subdirector de Infraestructura, dando lugar a que este no cuente con el conocimiento necesario para el puesto requerido y tampoco cumple con los requisitos mínimos esperados.

| | |
|---|---|
| ✔ | Verificado conforme |
| ✘ | Verificado Inconforme |
| ⊘ | No aplica |
| ⓘ | Informado |
| ) | Va para |

**Imagen S.A.**
**Auditoría Interna**
**Definición de Responsabilidades -Riesgo Tecnologico-**

| P/T | AA-6 | |
|---|---|---|
| Elaboro: | Jfco | 19/09/2014 |
| Reviso: | Bmc | 20/09/2014 |

| Actividad | C.A. | Comité | Riesgo | TI | GSI | AI | |
|---|---|---|---|---|---|---|---|
| Aprobación de politicas y procedimientos | ✓ | | | | | | ✓ |
| Conocer y aprobar medidas correctivas | ✓ | | | | | | ✓ |
| Acciones sobre incumplimientos a las politicas | ✓ | | | | | | ✓ |
| Asegurar la estructura para administrar TI | ✓ | | | | | | ✓ |
| Proponer la politicas y procedimientos | | ✓ | | | | | ✓ |
| Proponer el manual de adminstración de riesgo de TI | | ✓ | | | | | ✓ |
| Definir estrategias de administración de riesgos de TI | | ✓ | | | | | ✓ |
| Revisión anual de politicas y procedimientos | | ✓ | | | | | ✓ |
| Analizar reportes remitidos por la unidad de riesgos | | ✓ | | | | | ✓ |
| Reportar al consejo de administración sobre la exposición al riesgo | | ✓ | | | | | ✓ |
| Proporner al comité las politicas y procedimientos del Riesgo de TI | | | ✓ | | | | ✓ |
| Monitorear la exposición al riesgo tecnologico | | | ✗ | | | | ✓ |
| Analizar el riesgo tecnologico inherente de las innovaciones en TI | | | ✓ | | | | ✓ |
| Reportar trimestralmente al comité sobre la exposición al riesgo tecnologico | | | ✓ | | | | ✓ |
| Verificar e informar al comité sobre el incumplimiento de politicas y procedimientos | | | ✗ | | | | ✓ |
| Generar periodicamente reportes para el analisis de la probabilidad e impacto de los riesgo tecnologicos | | | | ✓ | | | ✓ |
| Proveer los reportes a todas las áres fiscalizadores en cuanto a requerimientos del riesgo tecnologico | | | | ✓ | | | ✓ |
| Velar por que el nivel de servicio a usuarios este siempre de acuerdo a las expectativas esperadas | | | | ✓ | | | ✓ |
| Velar porque los niveles de riesgo se mantengan dentro del criterio de riesgo aceptado | | | | ✓ | | | ✓ |
| Definir estrategia de la seguridad de la información | | | | | ✓ | | ✓ |
| Administrar la seguridad física y lógica | | | | | ✓ | | ✓ |
| Detectar vulnerabilidades en la seguridad de la Info | | | | | ✓ | | ✓ |
| Documentar las politicas y procedimientos en la gestión del riesgo tecnologico | | | | | ✓ | | ✓ |
| Aplicar metodología para el analisis de riesgo de TI | | | | | ✓ | | ✓ |
| Apoyar al comité y unidad de riesgos en la identificación y evalución de riesgos | | | | | ✗ | | ✓ |
| Gestionar con TI, las mejoras señaladas para el área | | | | | ✗ | | ✓ |
| Evaluar el proceso de administración de riesgo tecnologico, proveyendo oportunidades de mejora continua | | | Z-5 | | | ✓ | ✓ |

**Observación:** Se observó que algunas actividades o responsabilidades definidas para la unidad de riesgos y para el gestor de seguridad de la información, no estan siendo ejecutadas de conformidad a lo establecido.

| | |
|---|---|
| ✓ | Verificado conforme |
| ✗ | Verificado Inconforme |

**Imagen S.A.**
**Gerencia de Tecnología**
**Prespuesto 2014**
**Al: 31 de Agosto del 2014**

| P/T | AA-7 | |
|---|---|---|
| Elaboro: | Jfco | 23/09/2014 |
| Reviso: | Bmc | 24/09/2014 |

| CUENTA/NOMBRE | Presupuesto | Ejecutado | Variación | |
|---|---|---|---|---|
| **(50102) MANTENIMIENTOS** | **2,495,808.00** | | | |
| **(50102001) MANTENIMIENTO EQUIPO DE COMPUTO** | **535,700.00** | **540,391.00** | **0.88%** | ✓ |
| (00-10000032) Mantenimiento Ips Intrushield | 74,400.00 | 73,500.00 | **-1.21%** | ✓ |
| (00-10000033) Mantenimiento Vmware | 168,000.00 | 169,800.00 | **1.07%** | ✓ |
| (00-10000035) Mant. Impresor hp 4250 | 500.00 | 455.00 | **-9.00%** | ✓ |
| (00-10000038) Mant. Ups | 84,000.00 | 83,489.00 | **-0.61%** | ✓ |
| (00-10000039) Mant. Servidores | 48,000.00 | 48,001.00 | **0.00%** | ✓ |
| (00-10000205) Mantenimiento de swicht | 23,200.00 | 23,567.00 | **1.58%** | ✓ |
| (00-10000207) Mantenimiento Solucion NAC | 49,600.00 | 47,500.00 | **-4.23%** | ✓ |
| (00-10000208) Firewalls | 64,000.00 | 68,901.00 | **7.66%** | ✓ |
| (00-10000222) Mantenimiento impresoras | 4,000.00 | 3,500.00 | **-12.50%** | ✓ |
| (00-10000226) Mant. de Discos | 20,000.00 | 21,678.00 | **8.39%** | ✓ |
| **(50102005001) SOFTWARE** | **1,813,720.00** | **1,820,172.00** | **0.36%** | ✓ |
| (00-10000002) Mantenimiento Licencia Antivirus | 80,000.00 | 79,875.00 | **-0.16%** | ✓ |
| (00-10000070) Optimus | 303,360.00 | 304,567.00 | **0.40%** | ✓ |
| (00-10000071) Licenciamientos | 18,160.00 | 17,945.00 | **-1.18%** | ✓ |
| (00-10000074) Mantenimiento Tarificador | 9,600.00 | 10,345.00 | **7.76%** | ✓ |
| (00-10000075) Mysql | 40,000.00 | 39,999.00 | **0.00%** | ✓ |
| (00-10000076) Silver Bullet | 7,600.00 | 8,603.00 | **13.20%** | ✓ |
| (00-10000077) Licenciamiento Microsoft | 240,000.00 | 239,178.00 | **-0.34%** | ✓ |
| (00-10000079) Mantenimiento Backup Exec | 8,000.00 | 7,350.00 | **-8.13%** | ✓ |
| (00-10000080) Sysaid | 17,400.00 | 19,300.00 | **10.92%** | ✓ |
| (00-10000081) Mantenimiento Peiset | 1,048,000.00 | 1,054,002.00 | **0.57%** | ✓ |
| (00-10000206) Antispam | 17,600.00 | 15,600.00 | **-11.36%** | ✓ |
| (00-10000213) Remesas + | 24,000.00 | 23,408.00 | **-2.47%** | ✓ |
| **(50103001) SERVICIOS GENERALES** | **172,032.00** | **171,456.00** | **-0.33%** | ✓ |
| **(50103001005) TELEFONÍA Y COMUNICACIONES** | **172,032.00** | **171,456.00** | **-0.33%** | ✓ |
| (00-10000010) Enlace Fibra Optica Oscura Optel | 172,032.00 | 171,456.00 | -0.33% | ✓ |
| | | () | | |

**Observación:** Se observó una adecuada gestón del presupuesto de TI ya que lo ejecutado ha estado dentro de los parametros de lo presupuestado.

| | |
|---|---|
| ✓ | Verificado conforme |
| () | Cotejado con Contabilidad |

**Imagen S.A.**

**Auditoría Interna**

**Proceso para la Administración del Riesgo Tecnológico**

| P/T | BB | |
|---|---|---|
| Elaboro: | Jfco | 23/09/2014 |
| Reviso: | Bmc | 24/09/2014 |

**Imagen S.A.**
**Auditoría Interna**
**Ambiente de Control**

| P/T | BB-1 | |
|---|---|---|
| Elaboro: | Jfco | 23/09/2014 |
| Reviso: | Bmc | 24/09/2014 |

**Imagen, S.A.**

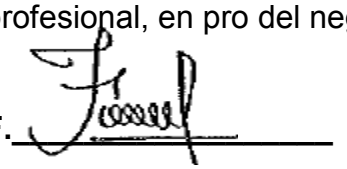
**Declaración y Filosofía de Riesgo Tecnológico**

**Auditoría Interna**

| P/T | BB-1-1 | |
|---|---|---|
| Elaboro: | Jfco | 23/09/2014 |
| Reviso: | Bmc | 24/09/2014 |

**Declaración:** ✔

La empresa denominada IMAGEN, S.A. ha definido como nivel de apetito al riesgo tecnológico, un impacto hasta de $25,000.00, mismo que es el máximo que cubre nuestra póliza de seguros ante cualquier eventualidad de magnitud grave.Para el efecto los criterios de impacto de acuerdo a los eventos que pueden generarse y materializarse, están en base a las siguientes consideraciones aprobadas por el Consejo de Administración: hasta $3,000.00 impacto bajo, hasta $12,500 impacto medio, hasta $25,000.00 impacto alto y arriba de $25,000.00 como un impacto grave. También se establece como punto de referencia la probabilidad de eventos de uno a cuatro en un periodo de un mes, siendo uno bajo y cuatro grave. Los niveles de criticidad de la información son dos, crítica o no crítica, siendo crítica cuando está relacionada a los procesos del negocio. Los niveles de sensibilidad son cuatro: pública, interna, privada 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 del riesgo tecnológico. Se determina y establece que un activo tecnológico es todo aquello que genera un valor a las operaciones de la organización, por lo cual el recurso humano aunque no es un objeto material valorizado, es considerado como parte del activo tecnológico por el conocimiento, capacidades que posee y la inversión que se realiza en su preparación profesional, en pro del negocio. ✔

**F.** 

**Faustino López**

**Presidente del Comité de Riesgos**

| | |
|---|---|
| ✔ | Verificado conforme |

**Imagen S.A.**
**Niveles de Impacto**
**Administración del Riesgo Tecnologico**

| P/T | BB-1-2 | |
|---|---|---|
| Elaboro: | Jfco | 23/09/2014 |
| Reviso: | Bmc | 24/09/2014 |

**TABLA CRITERIOS DE IMPACTO**

| Nivel | Criterio | Valor Máximo | Descripción |
|---|---|---|---|
| 1 | Bajo | $3,000 | Aplica cuando la perdida se estima entre $0.01 hasta $3,000, derivado de la materialización de un riesgo. |
| 2 | Medio | $12,500 | Aplica cuando la perdida se estima entre $3,001 hasta $12,500, derivado de la materialización de un riesgo. |
| 3 | Alto | $25,000 | Aplica cuando la perdida se estima entre $12,501 hasta $25,000, derivado de la materialización de un riesgo. |
| 4 | Grave | > $25,000 | Aplica cuando la perdida se estima por arriba de los $25,000, derivado de la materialización de un riesgo. |

BB-1-1 BB-4-1

**NOTA:** En la evaluación de los criterios no se observó inconsistencia alguna.

| | |
|---|---|
| ✔ | Verificado conforme |
| () | Cotejado con BB-1-1 |
| ( | Viene de |
| ) | Va para |

**Imagen S.A.**
**Niveles de Probabilidad**
**Administración del Riesgo Tecnológico**

| P/T | BB-1-3 | |
|---|---|---|
| Elaboro: | Jfco | 23/09/2014 |
| Reviso: | Bmc | 24/09/2014 |

**TABLA CRITERIOS DE PROBABILIDAD**

| Nivel | Criterio | Descripción |
|---|---|---|
| 1 | Bajo | Si el evento se registra una vez en un mes |
| 2 | Medio | Si el evento se registra dos veces en un mes |
| 3 | Alto | Si el evento se registra tres veces en un mes |
| 4 | Grave | Si el evento se registra cuatro o más en un mes |

BB-1-1 BB-4-1

**NOTA:** En la evaluación de los criterios no se observó inconsistencia alguna.

| | |
|---|---|
| ✔ | Verificado conforme |
| () | Cotejado con BB-1-1 |
| ( | Viene de |
| ) | Va para |

**Imagen S.A.**
**Niveles de Criticidad**
**Administración del Riesgo Tecnológico**

| P/T | BB-1-4 |
|---|---|
| Elaboro | Jfco 23/09/2014 |
| Revisó | Bmc 24/09/2014 |

**TABLA DE CRITICIDAD DE LA INFORMACIÓN**

| Nivel | Criterio | Descripción |
|---|---|---|
| 1 | No Crítica | Información no relacionada con los procesos del negocio. |
| 2 | Crítica | Información relacionada con los procesos del negocio. |

BB-1-1 BB-4-1

**NOTA:** No se observó inconsistencia alguna.

| | |
|---|---|
| ✓ | Verificado conforme |
| ( ) | Cotejado con BB-1-1 |
| ( | Viene de |
| ) | Va para |

**Imagen S.A.**
**Niveles de Sensibilidad**
**Administración del Riesgo Tecnológico**

| P/T | BB-1-5 |
|---|---|
| Elaboro | Jfco 23/09/2014 |
| Revisó | Bmc 24/09/2014 |

**TABLA DE SENSIBILIDAD DE LA INFORMACIÓN**

| Nivel | Criterio | Tipo | Descripciòn |
|---|---|---|---|
| 1 | Bajo | Publica | Destinada para el conocimiento del publico en general. |
| 2 | Medio | Interna | Desarrollada para el conocimiento de los colaboradores en el desarrollo diario de sus funciones. |
| 3 | Alto | Privada | Comprende información actual de clientes, proveedores, colaboradores, funcionarios, configuraciones, financiera. |
| 4 | Grave | Confidencial | Objetivos y estrategias de negocio |

( ) ( ) BB-1-1 ( ) BB-4-1

**NOTA:** En la evaluación de los criterios no se observó inconsistencia alguna.

| | |
|---|---|
| ✓ | Verificado conforme |
| ( ) | Cotejado con BB-1-1 |
| ( | Viene de |
| ) | Va para |

**Imagen S.A.**
**Auditoría Interna**
**Establecimiento de objetivos**

| P/T | BB-2 | |
|---|---|---|
| Elaboro: | Jfco | 23/09/2014 |
| Reviso: | Bmc | 24/09/2014 |

**Imagen, S.A.**
**Auditoria Interna**
**Objetivos Generales**

| P/T | BB-2-1 |
|---|---|
| Elaboro: | Jfco 23/09/2014 |
| Revisó: | Bmc 24/09/2014 |

**Cumplimiento**

| No. | Objetivo Establecido | SI | No |
|---|---|---|---|
| 1 | Fortalecer la confianza por parte del Consejo de Administración, entes reguladores y clientes | ✔ | |
| 2 | Contribuir al logro de los objetivos estratégicos | ✔ | |
| 3 | Apoyar al gobierno corporativo y principio de transparencia | ✔ | |

Porcentaje de cumplimiento de los objetivos generales 100%
Porcentaje de incumplimiento en los objetivos generales 0%

**NOTA:** Se observa una adecuado establecimiento y cumplimiento a los objetivos establecidos por la administración.

| ✔ | Verificado conforme |
|---|---|

**Imagen, S.A.**
**Auditoria Interna**
**Objetivos Generales**

| P/T | BB-2-2 |
|---|---|
| Elaboro | Jfco 23/09/2014 |
| Revisó | Bmc 24/09/2014 |

**Cumplimiento**

| No. | Objetivo Establecido | SI | No |
|---|---|---|---|
| 1 | Mejorar la eficacia y eficiencia operacional en Tecnología | ✔ | |
| 2 | Fortalecer el aprendizaje organizacional | ✔ | |
| 3 | Facilitar la asignación eficiente de recursos | ✔ | |
| 4 | Minimizar pérdidas financieras en la materialización de un riesgo tecnológico | ✔ | |
| 5 | Cumplir con los requisitos regulatorios aplicables a la empresa | ✔ | |
| 6 | Velar por la seguridad de las personas relacionadas con la organización | ✔ | |

Porcentaje de cumplimiento de sus funciones 100%
Porcentaje de incumplimiento a sus funciones 0%

**NOTA:** Se observa una adecuado establecimiento y cumplimiento a los objetivos establecidos por la administración.

| ✔ | Verificado conforme |
|---|---|

**Imagen S.A.**
**Auditoría Interna**
**Identificación de riesgos**

| P/T | BB-3 | |
|---|---|---|
| Elaboro: | Jfco | 23/09/2014 |
| Reviso: | Bmc | 24/09/2014 |

**Imagen, S.A.**
**Inventario de Activos Tecnológicos**
**Criterios de Criticidad y Sensibilidad de la Información**
**Año 2014**

| P/T | BB-3-1 | |
|---|---|---|
| Elaboro: | Jfco | 23/09/2014 |
| Reviso: | Bmc | 24/09/2014 |

| Activo Tecnologico | Tipo de Activo | Clase | Descripción | Valor | Sensibi-lidad | Critici-dad | Riesgo del Activo ($R_i$ * |
|---|---|---|---|---|---|---|---|
| Laptop | Soporte | Hardware | Laptop Samsung XPS 13, Ci7, 1.70Ghz, 4GB | 15,440.18 | 3 | 2 | Alto ✓ |
| Servidor | Soporte | Hardware | Servidor Proliant blades C-CLASS 2M223400VZ | 48,414.34 | 4 | 2 | Grave ✓ |
| Servidor | Soporte | Hardware | Servidor Proliant blades C-CLASS 2M223400W1 | 48,414.34 | 4 | 2 | Grave ✓ |
| UPS | Soporte | Hardware | Baterias para Ups | 9,754.71 | 1 | 1 | Bajo ✓ |
| Servidor | Soporte | Hardware | Almacenadora de Informacion CKM00093400166-CX4 | 551,906.25 | 4 | 2 | Grave ✓ |
| Barracuda | Soporte | Software | Barracuda BAR-SF-161860-200 | 33,463.27 | 2 | 2 | Medio ✓ |
| Switch | Red | Hardware | Switch RIE40C02877-SRW2024 | 4,375.00 | 2 | 2 | Medio ✓ |
| Py SwUSD | Base de Datos | Base de Datos | Base de Datos CCA | 0 | 4 | 2 | Grave ✓ |
| Py SwfGTQ | Base de Datos | Base de Datos | Base de Datos CCA | 0 | 4 | 2 | Grave ✓ |
| Roberto Alvarez | Persona | Persona | Roberto Albertino | 0 | 4 | 2 | Grave ✓ |
| Euralio Saban | Persona | Persona | Jesus Pineda | 0 | 4 | 2 | Grave ✓ |
| Estructura | Estructura | Estructura | Estructura Organizacional | 9,867,402.30 | 4 | 2 | Grave ✓ |
| | ✓ | ✓ | | ( ) | ✓ | ✓ | ✓ |

**Observación:** Se verifico el inventario de activos tecnológicos, el cual tiene como finalidad apoyar a detectar amenazas y vulnerabilidades. Los valores fueron cotejados con contabilidad.

( BB-1-5 ( BB-1-4

| | |
|---|---|
| ✓ | Verificado conforme |
| ( ) | Cotejado con Contabilidad |
| ( | Viene de |

**Imagen, S.A.**
**Inventario de Amenazas y Vulnerabilidades**
**Administración de Riesgo Tecnológico**
**Año 2014**

| PVT | RR.3.2 | |
|---|---|---|
| Elaboro: | Jico | 23/09/2014 |
| Revisó: | Elmc | 24/09/2014 |

| Amenazas | Vulnerabilidades | |
|---|---|---|
| Cambios no Autorizados | Actualizaciones no autorizadas en Base de Datos | ✓ |
| Cambios no Autorizados | Eliminación de información en Base de Datos | ✓ |
| Ausencia de pistas de auditoría | Incumplimiento a la metodología de desarrollo | ✓ |
| Ambiente no separados de producción y pruebas | Falta de segregación de funciones en el proceso de transición | ✓ |
| Ataque a red interna | Arquitectura no segura de la red | ✓ |
| Abusos de permisos de usuarios | Matriz de acceso segmentada | ✓ |
| Desalineación con la estrategia organizacional | Inconsistencias con el plan estratégico de la empresa | ✓ |
| Desalineación con la estrategia organizacional | Aumento de costos de mantenimiento, cambio o soporte de HW | ✓ |
| Desalineación con la estrategia organizacional | Aumento de costos de mantenimiento, cambio o soporte de SW | ✓ |
| Destrucción de equipos o de medios | Ausencia de protección física al edificio o data center | ✓ |
| Errores de uso de software | Ausencia de control de cambios en la configuración del software | ✓ |
| Errores de operación y administración | Entrenamiento insuficiente del personal | ✓ |
| Espionaje remoto | Tráfico sensible sin protección | ✓ |
| Indisponibilidad de servicios de TI | Ausencia de control en rendimiento del Hardware y Software | ✓ |
| Indisponibilidad del personal | Personal insatisfecho | ✓ |
| Acumulación del conocimiento en un sola persona | Falta de especialización y división del trabajo | ✓ |
| Indisponibilidad del personal | Ausencia del personal crítico | ✓ |
| Falla del equipo de telecomunicaciones | Punto único de falla | ✓ |
| Falsificación de derechos | Ausencia de identificación, autenticación del emisor y receptor | ✓ |
| Falla del equipo de telecomunicaciones | Líneas de comunicación sin protección | ✓ |
| Falla del equipo de telecomunicaciones | Conexión deficiente de los cables | ✓ |
| Falta de control en los procesos y sus componentes | Ausencia de mapa de procesos de los sistemas de información | ✓ |
| Falta de conocimiento de buenas prácticas | Ausencia de procesos de detección de necesidades de capacitación | ✓ |
| Falsa identificación de riesgos | Ausencia de procedimientos de identificación y valoración de riesgos | ✓ |
| Software mal diseñado | Falta de control en los procesos de desarrollo (QA) | ✓ |
| Codificación no estándar del software | Incumplimiento a la metodología de desarrollo | ✓ |
| Robo de equipo | Procedimientos inadecuados de seguridad física | ✓ |
| Insatisfacción del cliente interno | Incumplimiento a los acuerdos de servicio establecidos | ✓ |
| Daños en los equipos tecnológicos | Condiciones ambientales no adecuadas. | ✓ |
| Incumplimiento a políticas o procedimientos | Ausencia de políticas escritas | ✓ |
| Incapacidad de restaurar los sistemas en sitio alterno | Ausencia de copias de respaldo certificadas | ✓ |
| Desconocimiento de nuevos procedimientos | Ausencia de documentación técnica | ✓ |
| Utilización inadecuada de los recursos | Ausencia de mecanismos de monitoreo | ✓ |
| Pérdida del suministro de energía | Red energética inestable | ✓ |
| Ataques informáticos (internos o externos) | Inadecuada revisión de bitácoras | ✓ |
| Incumplimiento de proveedores | Ausencia de Acuerdos de Niveles de Servicios (SLA`s) | ✓ |

**Observación:** No se detectó inconsistencia alguna en la definición de las amenazas y vulnerabilidades para el riesgo tecnológico, cada cual hace referencia así misma.

| | |
|---|---|
| ✓ | Verificado conforme |

**Imagen S.A.**
**Auditoría Interna**
**Evaluación y respuesta a los riesgos**

| P/T | BB-4 | |
|---|---|---|
| Elaboro: | Jfco | 23/09/2014 |
| Reviso: | Bmc | 24/09/2014 |

**Imagen, S.A.**
**Matriz de Riesgo Tecnológico**
**Gerencia de TI**
**Año 2014**

| P/T | BB-4-1 | |
|---|---|---|
| Elabora: | JRco | 24/09/2014 |
| Revisa: | Emc | 25/09/2014 |

| No | Proceso | Sub proceso | Amenaza | Vulnerabilidad | Probabilidad | Impacto | Factor de Riesgo | Criticidad | Sensibilidad | Factor de Riesgo | Nivel de Riesgo | Nivel de Exposición al Riesgo |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Organizaciòn de la administraciòn del riesgo tecnològico | | | | | | | | | | | |
| 1.1 | | Gobierno de TI | Falta de Control Interno | Ausencia de políticas y procedimientos | 2.00 | 2.00 | 4.00 | 2.00 | 2.00 | 4.00 | 8.00 | Medio |
| 1.2 | | Funciones y responsabilidades | Inadecuada gestión del riesgo tecnológico | Ausencia de segragación de funciones | 2.00 | 2.00 | 4.00 | 1.00 | 2.00 | 2.00 | 4.00 | Bajo |
| 1.3 | | Plan estratégico de TI | Desalineación con la estrategia organizacional | Presupuesto inadecuado de TI | 1.00 | 4.00 | 4.00 | 2.00 | 4.00 | 6.00 | 10.00 | Medio |
| 1.4 | | Manual del riesgo tecnológico | Falta de control interno | Asuencia de procedimientos de Valoración del riesgo | 1.00 | 3.00 | 3.00 | 2.00 | 2.00 | 4.00 | 7.00 | Medio |
| 2 | Infraestructura de TI, sistemas de informaciòn, bases de datos y servicios de TI | | | | | | | | | | | |
| 2.1 | | Gestión de cambios | Cambios no autorizados | Modificaciones o eliminación de información | 1.00 | 4.00 | 4.00 | 2.00 | 2.00 | 4.00 | 8.00 | Medio |
| 2.2 | | Desarrollo de software | Ausencia de pistas de auditoría | Incumplimiento a la metodolgìa de desarrollo | 2.00 | 2.00 | 4.00 | 2.00 | 2.00 | 4.00 | 8.00 | Medio |
| 2.3 | | Administrador de base de datos. | Dependencia del personal | Concentración del conocimiento | 4.00 | 4.00 | 16.00 | 2.00 | 3.00 | 5.00 | 21.00 | Grave |
| 2,4 | | Monitoreos | Ataques internos o externos a la red | Ausencia de monitoreo | 2.00 | 3.00 | 6.00 | 2.00 | 2.00 | 4.00 | 10.00 | Medio |
| 2.5 | | Adquisición, mantenimiento e implementación | Inadecuada gestión de cambios | Cambios no autorizados | 2.00 | 1.00 | 2.00 | 2.00 | 2.00 | 4.00 | 6.00 | Medio |
| 2.6 | | Gestión de servicios de TI | Errores de operación y Administración | Falta de especialización y división del trabajo | 3.00 | 2.00 | 6.00 | 2.00 | 2.00 | 4.00 | 10.00 | Medio |
| 2.7 | | Ciclo de vida de los sistemas de información | Software obsoleto | Ausencia de control de software desarrollado | 1.00 | 1.00 | 1.00 | 1.00 | 2.00 | 3.00 | 4.00 | Bajo |
| 3 | Seguridad de la tecnologìa de la información | | | | | | | | | | | |
| 3.1 | | Gestión de Accesos | Abuso de derechos por los usuarios | Matriz de acceso segmentada | 2.00 | 2.00 | 4.00 | 2.00 | 3.00 | 5.00 | 9.00 | Medio |
| 3.2 | | Copias de respaldo | Pérdida de información crítica | Ausencia de procedimientos de back up | 4.00 | 4.00 | 16.00 | 2.00 | 4.00 | 6.00 | 22.00 | Grave |
| 3.3 | | Seguridad Física | Destrucción de equipo | Inadecuados procesos de seguridad física | 2.00 | 1.00 | 2.00 | 1.00 | 2.00 | 3.00 | 5.00 | Bajo |
| 4 | Continuidad de operaciones de tecnologìa de la informaciòn | | | | | | | | | | | |
| 4.1 | | Plan de continuidad de operaciones de TI | Inadecuado plan de continuidad de operacione | Obsolescencia de manuales e instructivos | 1.00 | 4.00 | 4.00 | 2.00 | 3.00 | 5.00 | 9.00 | Medio |
| 4.2 | | Pruebas al plan de continuidad de TI | Falta de conocimiento por el personal | Ausencia de un plan de pruebas | 1.00 | 3.00 | 3.00 | 2.00 | 2.00 | 4.00 | 7.00 | Medio |
| 4.3 | | Capacitación del personal clave | Errores de operación y administración | Entrenamiento insuficiente al personal | 1.00 | 1.00 | 1.00 | 2.00 | 2.00 | 4.00 | 5.00 | Bajo |
| 4.4 | | Centro de computo alterno | No continuidad del negocio | Ausencia de infraestructura tecnologica | 2.00 | 4.00 | 6.00 | 2.00 | 3.00 | 5.00 | 11.00 | Medio |
| 5 | Procesamiento de la informaciòn y tecerizaciòn | | | | | | | | | | | |
| 5.1 | | Procesamiento de la información. | Operaciones no adecuadas | Ausencia de infraestructura tecnologica | 1.00 | 4.00 | 4.00 | 2.00 | 3.00 | 5.00 | 9.00 | Medio |
| 5.2 | | Tercerización. | Incumplimiento del proveedor | Ausencia de niveles de servicio | 2.00 | 4.00 | 8.00 | 2.00 | 2.00 | 4.00 | 12.00 | Alto |

( BB-3-2 ( BB-3-2

**Observación:** La matriz fue evaluada en base a los criterios definidos por la administración, no observándose inconsistencia alguna en la evaluación. Sin embargo, se observa que la mayoría de riesgos estan evaluados en Medio y Grave.

( BB-1-3 ( BB-1-4 ( BB-1-2 ( BB-1-5

| | |
|---|---|
| ✓ | Verificado conforme |
| ( | Viene de |

**Imagen, S.A.**
**Auditoría Interna**
**Planes de tratamiento para riesgos altos**

| P/T | BB-4-2 | |
|---|---|---|
| Elaboro: | Jfco | 24/09/2014 |
| Reviso: | Bmc | 25/09/2014 |

| No. | Amenaza/Riesgo | Proceso | Nivel de Exposición | Plan de Acción | Fecha de Cumplimiento | |
|---|---|---|---|---|---|---|
| 1 | Dependencia del Personal | Infraestructura de TI, Sistemas de Información y Base de Datos | Grave | Plan de capacitación continuo a todo nivel | 15/01/2015 | ✓ |
| 2 | Pérdida de información critica | Seguridad de tecnología de información | Grave | Creación de procesos de back up automatizados | 31/03/2015 | ✓ |
| 3 | Incumplimiento del proveedor | Procesamiento de información y tercerización | Alto | Evaluación de proveedores con niveles de criticidad | 31/12/2014 | ✓ |
| 4 | Errores de operación y administración | Capacitación del personal clave de TI | Medio | Creación de plan de carreras para el personal clave | 31/01/2015 | ✓ |
| | () | () | () | | | |

**Observación:** Se verificaron los planes de acción observándose que los mismos corresponden a los riesgos con exposición alta, así también se ésta iniciando la gestión sobre los riesgos de exposición Medio.

| | |
|---|---|
| ✓ | Verificado conforme |
| () | Cotejado con BB-4-1 |

**Imagen S.A.**
**Auditoría Interna**
**Actividades de control para el Riesgo Tecnológico**

| P/T | CC | |
|---|---|---|
| Elaboro: | Jfco | 25/09/2014 |
| Revisó: | Dmc | 26/09/2014 |



**Imagen S.A.**
**Auditoría Interna**
**Infraestructura de TI, base de datos y servicios de TI**

| P/T | CC.1 | |
|---|---|---|
| Elaboro: | Jfco | 25/09/2014 |
| Revisó: | Dmc | 26/09/2014 |

**Imagen, S.A.**

**Gerencia de Tecnología**

**Informe de Monitoreo y Rendimiento** ✔

| P/T | CC-1-1 | |
|---|---|---|
| Elaboro: | Jfco | 25/09/2014 |
| Reviso: | Bmc | 26/09/2014 |

**Fecha: 13-08-2014**

**Participantes:**

Subdirector de Infraestructura &Subdirector de TI

**Actividad**

Informe del rendimiento de Infraestructura y Bases de Datos. **X** ) Z-5

**Descripción del proceso:**

**Almacenamiento**

1. Se realizó la actualización en el contenedor de servidores SAN EMC.
2. Se instaló la consola de administración Unisphere.
3. No se encontró comportamiento anormal, ni errores en el análisis de la reportería y logs (evaluados por el proveedor).
4. Detalla el estatus actual de los equipos en la SAN EMC
    a. Enclosure:
        i. Espacio utilizado 3.58TB
        ii. Espacio disponible 2.17TB
    b. VMWARE:
        i. Máquinas virtuales 45
        ii. Niveles de consumo de procesador 55%
        iii. Niveles de consumo de memoria 75%

**F. Responsable**_____

Subdirector de Infraestructura & Subdirector de TI

| | |
|---|---|
| ✔ | Verificado conforme |
| X | Verificado Inconforme |

Imagen, S.A.

Gerencia de TI -2014

Inventario de acuerdos para los servicios de TI

| P/T | CC.1.2 | |
|---|---|---|
| Elabora: | Jico | 25/09/2014 |
| Revisa: | Emc | 26/09/2014 |

| DUEÑO DEL PROCESO | TIPO DOCUMENTO | CÓDIGO DOCUMENTO | NOMBRE DEL DOCUMENTO | Ver | Formato | ESTADO DOCUMENTO | |
|---|---|---|---|---|---|---|---|
| Gerencia de TI | Acuerdo de nivel operativo de servicio | GTI-OLA-GTI-001 | Acuerdo de nivel operativo del servicio de internet | 1 | Digital | En espera de aprobación | ● |
| Gerencia de TI | Acuerdo de nivel operativo de servicio | GTI-OLA-GTI-002 | Acuerdo de nivel operativo del servicio antivirus | 1 | Digital | En espera de aprobación | ● |
| Gerencia de TI | Acuerdo de nivel operativo de servicio | GTI-OLA-GTI-003 | Acuerdo de nivel operativo del servicio enlace de comunicación | 1 | Digital | En proceso de revisión | ⊖ |
| Gerencia de TI | Acuerdo de nivel operativo de servicio | GTI-OLA-GTI-004 | Acuerdo de nivel operativo del servicio mesa de ayuda | 1 | Digital | En espera de aprobación | ● |
| Gerencia de TI | Acuerdo de nivel operativo de servicio | GTI-OLA-GTI-005 | Acuerdo de nivel operativo del servicio optimus | 1 | Digital | En proceso de revisión | ⊖ |
| Gerencia de TI | Acuerdo de nivel operativo de servicio | GTI-OLA-GTI-006 | Acuerdo de nivel operativo del servicio payswitch | 1 | Digital | En proceso de revisión | ⊖ |
| Gerencia de TI | Acuerdo de nivel operativo de servicio | GTI-OLA-GTI-007 | Acuerdo de nivel operativo del portal interno | 1 | Digital | En proceso de revisión | ⊖ |
| Gerencia de TI | Acuerdo de nivel operativo de servicio | GTI-OLA-GTI-008 | Acuerdo de nivel operativo del servicio remesas | 1 | Digital | En proceso de revisión | ⊖ |
| Gerencia de TI | Acuerdo de nivel operativo de servicio | GTI-OLA-GTI-009 | Acuerdo de nivel operativo del servicio de virtualización | 1 | Digital | En proceso de revisión | ⊖ |
| | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ❯ Z-5 |



**Observación:** Se detectó que los acuerdos ya han sido documentados hacia a lo interno no así a lo externo, de igual forma, no estan aprobados ni puestos en producción dichos acuerdos.

| | |
|---|---|
| ✓ | Verificado conforme |
| ● | En seguimiento |
| ⊖ | No implementado |
| ❯ | Va para |

**Imagen, S.A.**
**Gerencia de TI -2014**
**Gestión de incidentes de TI**

| P/T | CC-1-3 | |
|---|---|---|
| Elaboro: | Jfco | 25/09/2014 |
| Reviso: | Bmc | 26/09/2014 |

| Caso | Hora de modificación | Categoría | Sub categoría | Título del Incidente | Descripción | Estado | Gestor del Caso | Prioridad | Solución | |
|---|---|---|---|---|---|---|---|---|---|---|
| 3487 | 26/04/2014 15:52 | Auditoria | Software | Software en Servidores | Seguimiento a base de datos y desarrollo, solicito puedan proporcionarme los reportes del software instalado en todos los servidores. | **Cerrado** | spineda | Media | Se coloco la información en la carpeta compartida. | ✓ |
| 3673 | 13/06/2014 11:45 | Soporte Software | Administracion | Error de Ingreso | Envio la captura de pantalla, donde se aprecia el error que muestra el programa pedidos cliente, al momento de querer ingresar. Agradecere poder darle seguimiento y apoyarme en el acceso para realizar el día de hoy la solicitud de proveeduría. | **Cerrado** | Vreyes | Media | se verifico la versión del programa. | ✓ |
| 3690 | 05/07/2014 11:03 | Comunicaciones /Enlaces y Red | Permisos de Conexion | Error de Conexión | Te comento que desde que segmentaron la red, me da un error al momento de abrir o copiar un archivo desde una carpeta compartida. | **Cerrado** | Imena | Alta | se realizaron las verificaciones correspondientes. | ✓ |
| 3707 | 06/07/2014 17:58 | Soporte Optimus 4 | versiones | Cambiar Versiones | Te comento que intente ingresar a Optimus sin embargo, me genero el siguiente error por versionamiento del aplicativo. | **Cerrado** | spineda | Alta | Se reinstalo el programa de optimus en la PC indicada. | ✓ |
| 3729 | 01/08/2014 16:45 | Soporte Software | Administracion | Login Ogonzalez | Te comento que el día de hoy al encender mi maquina aparecia logeado el usuario: Ogonzales, sin embargo, no fui notificado que fueran hacerle mantenimiento preventivo a mi maquina o realizar alguna otra actividad en la misma. Agradecere poder indicarme si conoces o sabes a que se debio. | **Abierto** | adminhelp | Normal | | ) |
| 3798 | 23/08/2014 11:21 | Soporte Software | Administracion | Lentitud de Correo | Te informo que el día de hoy el correo ha estado mostrando demasiada lentitud, adjunto patallazo para que puedas visualizar, lleva en este estado aproximadamente 5 minutos. | **Abierto** | spineda | Normal | Se estara verificando la navegación. | ✗ |
| 3954 | 03/09/2014 14:16 | Instalacion Hardware PC Admon | Preparacion e Instalacion de PC | Primo PDF | Te comento que no tenemos instalado el Primo PDF y necesitamos guardar información en PDF para poder adjuntar al TeamMate. | **Cerrado** | adminhelp | Normal | Se realizo la instalación del programa. | ✓ |
| 4105 | 28/09/2014 17:03 | Comunicaciones /Enlaces y Red | Permisos de Conexion | Accesos | Solicito su apreciable a apoyo a fin de poder verificar las conexiones de red en mi maquina o las revisiones que corresponda, ya que no deja conectar a la base de datos del TeamMate y SAP. También revisando la conexión a red aparece el siguiente mensaje "Conectado a Red 2". Se intento ingresar por medio de escritorio remoto al servidor del TeamMate, pero de igual forma este esta deshabilitado. | **Abierto** | Imena | Alta | Se esta verificando el caso. | ✗ |

●

**Observación:** Aunque se lleva un adecuado control de los incidentes reportados a la Gerente de TI, se observó que no son atendidos de forma oportuna y adecuada

) Z-5

| | |
|---|---|
| ✓ | Verificado conforme |
| ✗ | Verificado Inconforme |
| ● | En seguimiento |
| ) | Va para |

**Imagen, S.A.**

**Gerencia de TI -2014**

**Inventario de Base de Datos**

| P/T | CC-1.4 | |
|---|---|---|
| Elaboro: | Jfco | 25/09/2014 |
| Reviso: | Bmc | 26/09/2014 |

| IP | Nombre | Descripción | Ambiente | Usuario | Diagrama de relación | Diccionario de Datos | Responsables | |
|---|---|---|---|---|---|---|---|---|
| 190.130.70.20 | BK_opt4 | Información historica | Producción | OperaOpt4 | ✗ | ✗ | Subdirector de TI y Auxiliar de DBA | ✓ |
| 190.130.70.51 | Opt_new | BD de compensación | Producción | OperaOpt4 | ✗ | ✗ | Subdirector de TI y Auxiliar de DBA | ✓ |
| 190.130.70.55 | Opt_new | Log | Producción | OperaOpt4 | ✗ | ✗ | Subdirector de TI y Auxiliar de DBA | ✓ |
| 190.130.70.90 | Opt_new | Almacenamiento electronico | Producción | OperaOpt4 | ✗ | ✗ | Subdirector de TI y Auxiliar de DBA | ✓ |
| 190.140.70.80 | Opt_new5 | BD de administración | Desarrollo | DesOpt | ⊘ | ⊘ | Programador Senior | ✓ |
| 190.140.70.81 | Opt_new5 | BD compensador | Desarrollo | DesOpt | ⊘ | ⊘ | Programador Senior | ✓ |
| 190.150.70.61 | Opt_4 | Administrador | Pruebas | PrOpt4 | ⊘ | ⊘ | Programador Senior / Subidirector de TI | ✓ |
| 190.150.70.62 | Opt_4 | Recepción | Pruebas | PrOpt4 | ⊘ | ⊘ | Programador Senior / Subidirector de TI | ✓ |
| 190.150.70.63 | Opt_4 | Log | Pruebas | PrOpt4 | ⊘ | ⊘ | Programador Senior / Subidirector de TI | ✓ |
| 190.150.70.64 | Opt_4 | Crea | Pruebas | PrOpt4 | ⊘ | ⊘ | Programador Senior / Subidirector de TI | ✓ |
| 190.190.50.25 | Imagen+ | DB remesas | Producción | Rem+ | ✗ | ✗ | Programador Senior / Subidirector de TI | ✓ |
| 190.190.60.26 | portalimag | portal interno de información | Producción | Pint2013 | ✗ | ✗ | Subdirector de TI y Auxiliar de DBA | ✓ |

Z-5

**Observación:** Se tuvo a la vista el inventario de bases de datos, sin embargo se observó que no se cuenta con diagramas de relación ni diccionarios de datos que ayuden a interpretarlas y gestionarlas de una mejor manera.

| | |
|---|---|
| ✓ | Verificado conforme |
| ✗ | Verificado Inconforme |
| ⊘ | No aplica |
| ) | Va para |

**IMAGEN, S.A.**
**PERFIL DE PUESTO** ✔
**ADMINISTRADOR DE BASE DE DATOS**

| P/T | CC-1-5 | |
|---|---|---|
| Elaboro: | Jfco | 25/09/2014 |
| Reviso: | Bmc | 26/09/2014 |

## I. PROPOSITO DEL PUESTO

Responsable de la planeación de las tareas administrativas y operativas de los sistemas de gestión de las bases de datos para su óptima utilización.

## II. FUNCIONES PRINCIPALES ✔

1. Participa activamente con los equipos de desarrollo de software en el análisis y diseño.
2. Realiza estudios de rendimiento en modelos de datos nuevos.
3. Velar que las variables de los DBMS se inicialicen correctamente en los nuevos sistemas de producción.
4. Realizar documentación asociada a la base de datos en proyectos nuevos.
5. Gestionar los cambios sobre las bases de datos.
6. Diseñar procedimientos de backup y restauración.

## III. FUNCIONES ESPECÍFICAS ✘

1. Realizar estudios de rendimiento de los sistemas en producción.
2. Realizar scripts de configuración y roll back a ser aplicados a las bases de datos.
3. Control de configuraciones sobre las bases de datos.
4. Reportar impactos tecnológicos por consultas nuevas a las bases de datos.
5. Reporte mensual de bases de datos nuevas implementadas.
6. Generar reporte de mejoras sobre la administración de base de datos

## IV. REQUERIMIENTOS MINIMOS

### Educación ✘

Estudiante universitario en la carrera de Ingeniería de Sistemas o capacitaciones técnicas en Sistemas de Gestión de Base de Datos.

**Experiencia** ✕

De 2 a 4 años en puesto similar (comprobable)

**Conocimientos** ✕

- Sistemas de gestión de base de datos.
- Scripts en base de datos
- Diferentes lenguajes de programación
- Proceso del negocio.

**V. RESPONSABILIDADES** ✕

- Reporte semanal de actividades realizadas en base de datos.
- Reporte mensual sobre mejoras ejecutadas en los gestores de base de datos.
- Reporte de rendimiento sobre las bases de datos

**Responsabilidad Financiera (Ninguna)**

**VI. COMPETENCIAS**

- Facilidad de adaptarse a los cambios
- Responsabilidad
- Integridad
- Servicio
- Comunicación asertiva

**VII. REPORTA A:**

Gerencia de TI

## VIII. CARACTERISTICAS PERSONALES

Edad: De 30 años en adelante
Género: Masculino o Femenino

Habilidad/capacidad de: Pensamiento estratégico, visionario, excelentes relaciones interpersonales y públicas, liderazgo y capacidad de influencia, coordinación de equipos de trabajo gerenciales, integridad y ética profesional.

## IX. CONDICIONES DE TRABAJO

Jornada y horario de trabajo:

- De lunes a viernes de 09:00 a 17:30 Horas.

Personal de confianza, no sujeto a las limitaciones de la jornada de trabajo.

**Observación:** Se observó que la persona que funge como Administrador de Base de Datos (DBA), no tiene los conocimientos necesarios para desempeñar dicha función, ya que no cuenta con formación académica según lo requerido y tampoco tiene capacitaciones en el tema.

| | |
|---|---|
| ✓ | Verificado conforme |
| ✗ | Verificado Inconforme |

**Imagen S.A.**

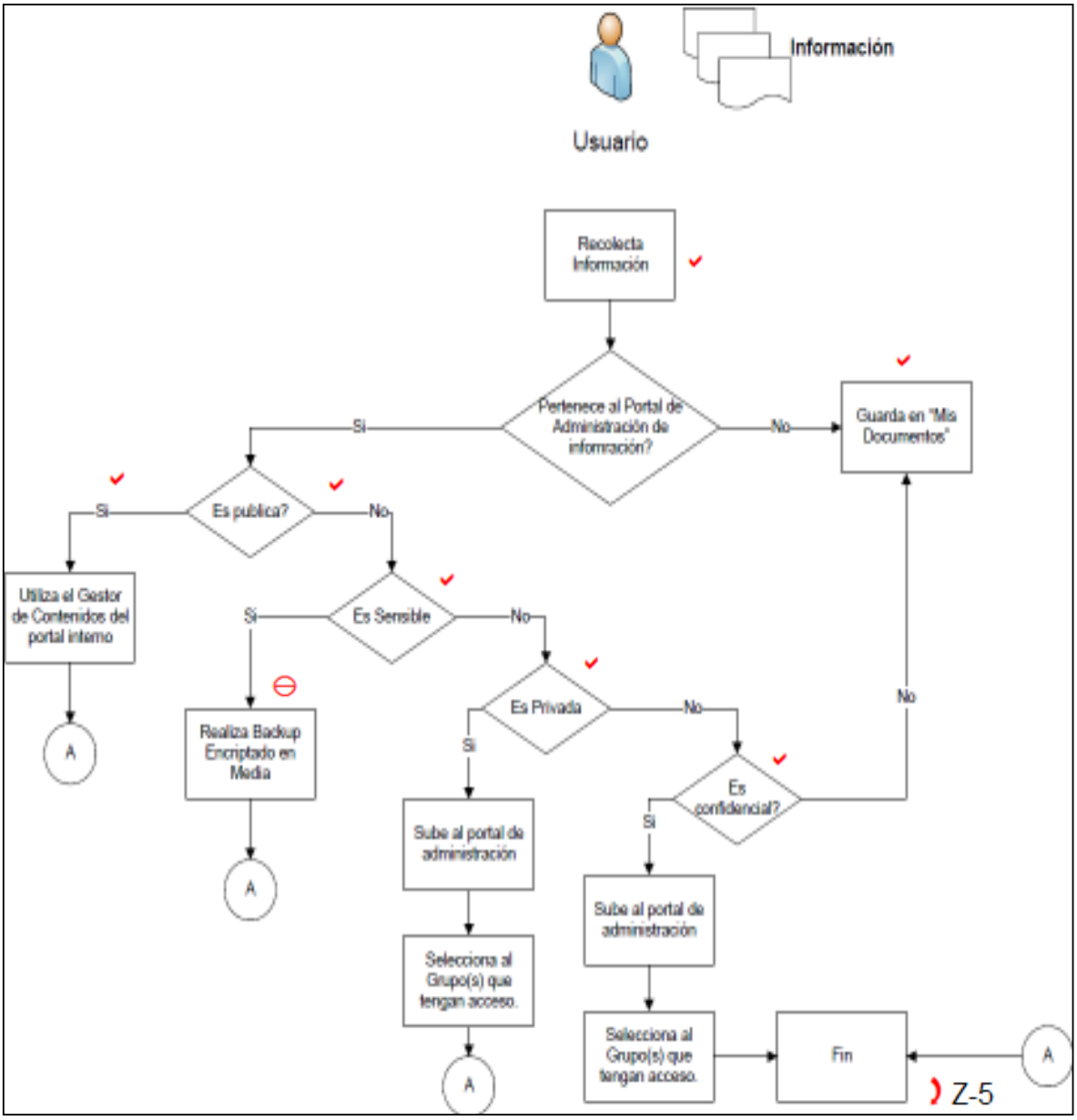
**Auditoría Interna**

**Seguridad de Tecnología de la Información**

| P/T | CC-2 | |
|---|---|---|
| Elaboro: | Jfco | 26/09/2014 |
| Reviso: | Bmc | 27/09/2014 |

**Imagen, S.A.**
**Gerencia de TI -2014**
**Proceso de clasificación de la información**

| P/T | CC-2-1 | |
|---|---|---|
| Elaboro: | Jfco | 26/09/2014 |
| Reviso: | Bmc | 27/09/2014 |

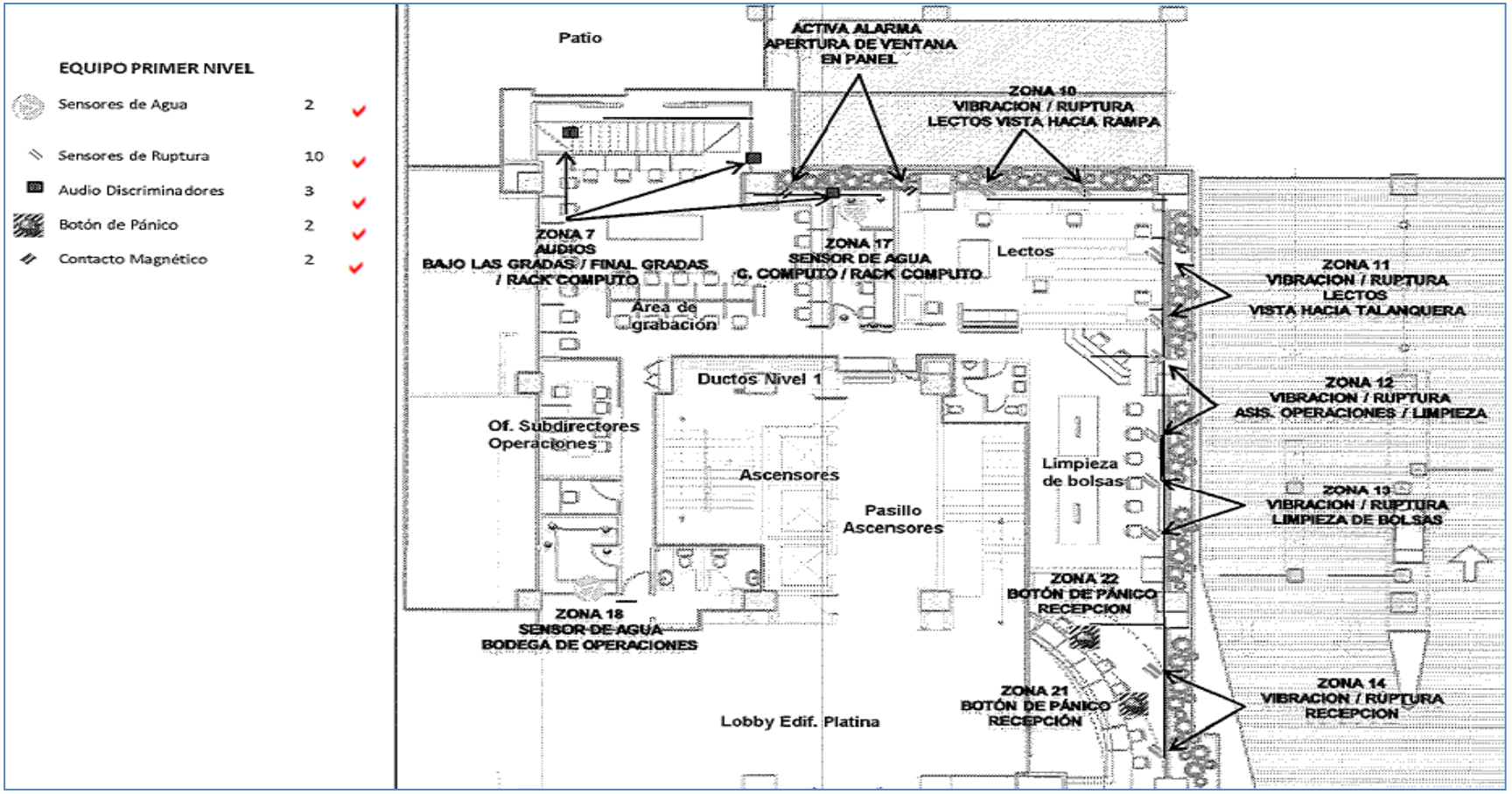



**Nota:** Aunque se cuenta con un proceso de clasificación de información por medio de una herramienta automatica, se observó que no todo el personal conoce el proceso y no ha realizado el proceso de clasificación de información, así mismo, se conoció por parte de la administración que no se cuenta con una política de clasificación que permita identificar que información es publica, interna, privada o confidencial.

| | |
|---|---|
| ✔ | Verificado conforme |
| ⊖ | No implementado |
| ) | Va para |

**Imagen, S.A**
**Gerencia de TI -2014**
**Equipo de Seguridad Física**

| P/T | CC-2-2 | |
|---|---|---|
| Elaboro: | Jfco | 26/09/2014 |
| Reviso: | Bmc | 27/09/2014 |




**Observación:** Se tuvo a la vista los planos de instalación del equipo de seguridad física, el cual fue evaluado no observándose inconsistencia alguna.

| | |
|---|---|
| ✔ | Verificado conforme |

**Imagen, S.A.**
**Gerencia de TI -2014**
**Matriz de acceso -Gerencia de TI-**

| P/T | CC.2.3 | |
|---|---|---|
| Elaboro: | Jfco | 25/09/2014 |
| Reviso: | Bmc | 27/09/2014 |

| No. | Nombre | Accesos | | | | | | | | Observaciones | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Red | Correo | Poral Interno | Codigo Tel. | Navegacion | VPN | MultiEnvios | Proveeduria | | |
| 1 | 00 Agente Seguridad | X | | | X | | | | | Usuario generico bajo la responsabilidad de analista de riesgo | ✔ |
| 2 | 00 Auxiliar Riesgos | X | X | | | X | | | | Usuario generico bajo la responsabilidad de subdirectora de riesg | ✔ |
| 3 | 00 Operador1 | X | X | | | | | | | Usuario generico bajo la responsabilidad de operaciones JI | ✔ |
| 4 | 00 oriesgos | X | | | | | | | | Deshabilitar para su eliminacion | ● |
| 5 | 00 remesas | X | | | | | | | | Deshabilitar para su eliminacion | ● |
| 6 | 00 Solicitud Pagos | X | X | | | | | | | Usuario generico bajo la responsabilidad de Gerencia IT | ⊘ |
| 7 | 00 tarificador | X | | | | | | | | Usuario generico bajo la responsabilidad del contador general | ✔ |
| 8 | 00 Team Central | X | X | | | | | | | Usuario generico bajo la responsabilidad de la Auditoría Interna | ⊘ |
| 9 | 00 Optimus 4.1 | X | X | | | | | | | Usuario generico bajo la responsabilidad de Gerencia IT | ⊘ |
| 10 | 00 Ventanilla 4 | X | X | | | | | | | Usuario generico bajo la responsabilidad de Gerencia IT | ⊘ |
| 11 | 00 Remesas Noche | X | X | | | X | | | | Usuario generico bajo la responsabilidad de operaciones JI | ✔ |
| 12 | Anibal Ubaldo Arias Marroquin | X | | | | | | | | | ✔ |
| 23 | Blanca de Leon | X | X | X | X | | | | X | | ✔ |
| 24 | Blanca Miriam Camey de Parada | X | X | X | X | X | X | | | | ✔ |
| 25 | Eddy Alfredo Mes Vasquez | X | | | | | | | | | ✔ |
| 46 | Eddy Orlando Granados Poroj | X | | | | | | | | | ✔ |
| 47 | Edgar Mauricio Perez Barrios | X | | | | | | | | | ✔ |
| 48 | Evelyn Gabriela Diaz de Leon | X | X | X | X | X | | | X | | ✔ |
| 59 | Hugo Leonel Guzman Chamorro | X | | | | | | | | | ✔ |
| 60 | Ilsy Ninett Florian Enriquez | X | | | | | | | | | ✔ |
| 72 | Irene Paola Morales | X | X | X | X | X | | | | | ✔ |
| 73 | José Alberto Yoc Senté | X | | | | | | | | | ✔ |
| 85 | Jose Leonardo Solares Calderon | X | X | | X | | | | | | ✔ |
| 86 | walter santos | X | | | | | | | | | ✔ |
| 99 | Xiomara Dalissa del Cid Virula | X | | | | | | | | | ✔ |
| 101 | Zoila Graciela Hernandez Noriega | X | | | | | | | | | ✔ |

**Observación:** Se tuvo a la vista la matriz de accesos llevada por la gerencia de TI, no observándose inconsistencia alguna. Los usuarios que no aplican es porque son usuarios en cajilla de seguridad en un banco.

| | |
|---|---|
| ✔ | Verificado conforme |
| ⊘ | No aplica |
| ● | En seguimiento |

**Imagen, S.A**

**Gerencia de TI**

**Inventario de copias de respaldo**

| P/T | CC.2.4 | |
|---|---|---|
| Elaboro: | Jfco | 27/09/2014 |
| Reviso: | Bmc | 28/09/2014 |

# Inventario de Copias de Respaldo de los Sistemas de Información

| Fecha de Generación | Entrante | Saliente | Ventanilla | Base de Datos CCB | CCB & CCA | Back-up Banco 15 | Back-up Banco 45 | Remesas + | SAP | Rechazos DBF´s | Disco "D" Operativo | Aplicativo Riesgos | Segunda Compe | Back-up Banco 04 | Portal Interno 2.0 | Bitacoras | Back Up Contingencias | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 02-sep ✓ | 1 | 1 | 2 | 1 | | 1 | 1 | | | | | | 1 | | | | | *8* |
| 03-sep ✓ | 1 | 1 | 2 | 1 | | 1 | 1 | | 2 | | | 1 | | | | 1 | | *11* |
| 06-sep ✓ | 1 | 1 | 2 | 1 | | 1 | 1 | | | 1 | | | | | | | | *8* |
| 07-sep ✓ | 1 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | | | | | | | 1 | | | *13* |
| 08-sep ✓ | 1 | 1 | 1 | 1 | 2 | 1 | 1 | | | | 1 | | | | | | | *9* |
| 09-sep ✓ | 1 | 1 | 1 | 1 | | 1 | 1 | | | | | | | | | | | *6* |
| 10-sep ✓ | 1 | 1 | 1 | 1 | | 1 | 1 | | | | | | | | | | | *6* |
| 13-sep ✓ | 1 | 1 | 2 | 1 | | 1 | 1 | | | 1 | | | | 1 | | | | *9* |
| 14-sep ✓ | 1 | 1 | 1 | 1 | | 1 | 1 | | | | | | | | | | | *6* |
| 15-sep ✓ | 1 | 1 | 1 | 1 | 5 | 1 | 1 | | | | | | | | | | | *11* |
| 16-sep ✓ | 1 | 1 | 1 | 1 | | 1 | 1 | | | | | | | | | | | *6* |
| 17-sep ✓ | 1 | 1 | 1 | 1 | | 1 | 1 | | | | | | | | | | | *6* |
| 20-sep ✓ | 1 | 1 | 2 | 1 | | 1 | 1 | | | 1 | | | | | | | | *8* |
| 21-sep ✓ | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | 2 | | | | | | | | | *9* |
| 22-sep ✓ | 1 | 1 | 2 | 1 | | 1 | 1 | | | | | | | | | | | *7* |
| 23-sep ✓ | 1 | 1 | 1 | 1 | | 1 | 1 | | | | | | | | | | | *6* |
| 24-sep ✓ | 1 | 1 | 1 | 1 | | 1 | 1 | | | | | | | | | | | *6* |
| 27-sep ✓ | 1 | 1 | 2 | 1 | | 1 | 1 | | | 1 | | | | | | | | *8* |
| | | | | | | | | | | | | | | | | | | *0* |
| | | | | | | | | | | | | | | | | | | *0* |
| | ***18*** | ***18*** | ***25*** | ***18*** | ***12*** | ***18*** | ***18*** | ***2*** | ***4*** | ***4*** | ***1*** | ***1*** | ***1*** | ***1*** | ***1*** | ***1*** | ***0*** | ***143*** |
| | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

**NOTA:** No se observo inconsistencia alguna en el proceso de inventario de copias de respaldo de los sistemas de seguridad

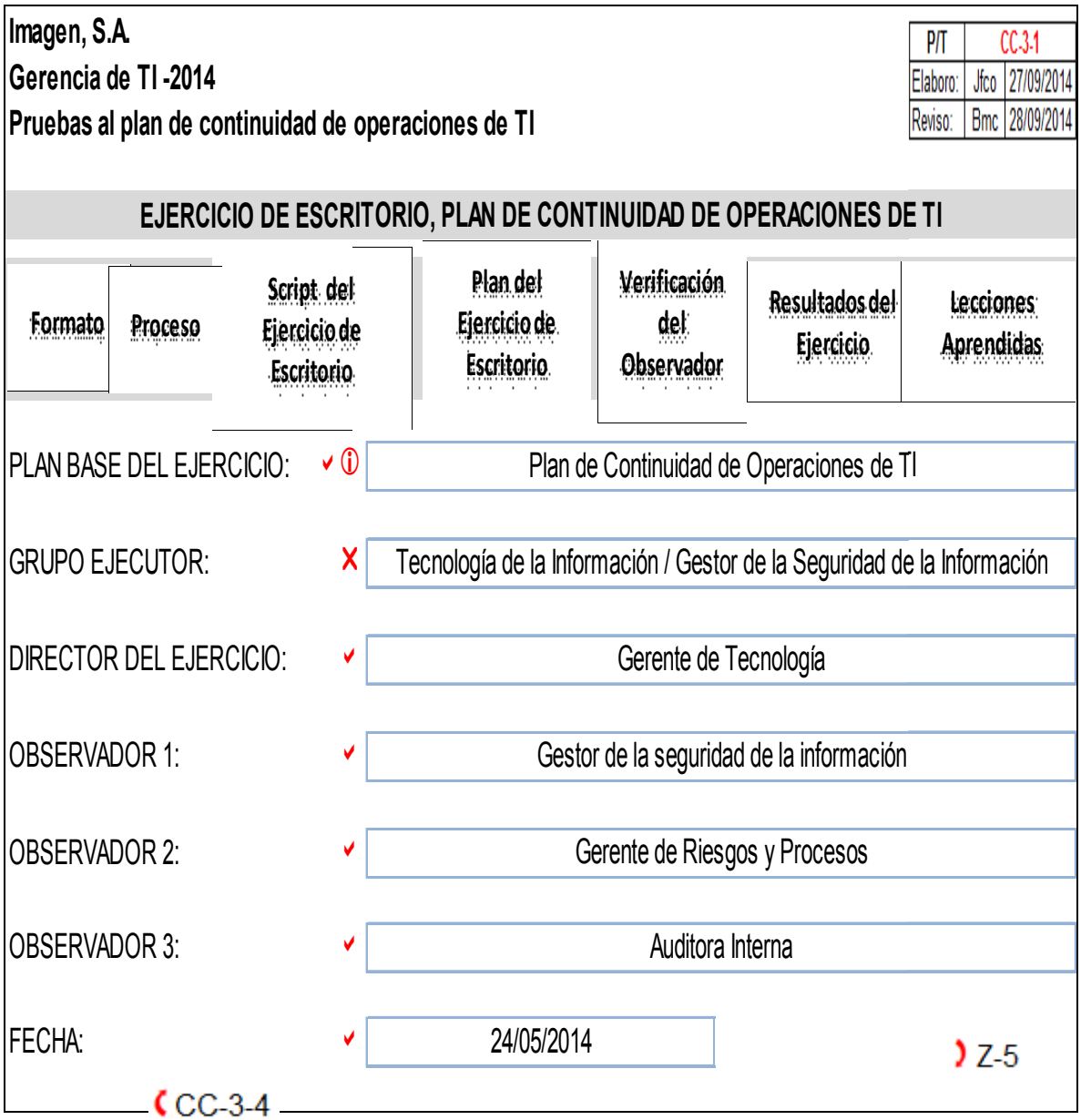
| ✓ | Verificado conforme |
|---|---|

**Imagen S.A.**

**Auditoría Interna**

**Continuidad de operaciones de TI**

| PT | CC-3 | |
|---|---|---|
| Elaboro: | Jfco | 27/09/2014 |
| Revisó: | Emc | 28/09/2014 |



Imagen, S.A.
Gerencia de TI -2014
Pruebas al plan de continuidad de operaciones de TI

| P/T | CC-3-1 | |
|---|---|---|
| Elaboro: | Jfco | 27/09/2014 |
| Reviso: | Bmc | 28/09/2014 |

EJERCICIO DE ESCRITORIO, PLAN DE CONTINUIDAD DE OPERACIONES DE TI

Formato | Proceso | Script del Ejercicio de Escritorio | Plan del Ejercicio de Escritorio | Verificación del Observador | Resultados del Ejercicio | Lecciones Aprendidas

| | | |
|---|---|---|
| PLAN BASE DEL EJERCICIO: | ✓ ⓘ | Plan de Continuidad de Operaciones de TI |
| GRUPO EJECUTOR: | X | Tecnología de la Información / Gestor de la Seguridad de la Información |
| DIRECTOR DEL EJERCICIO: | ✓ | Gerente de Tecnología |
| OBSERVADOR 1: | ✓ | Gestor de la seguridad de la información |
| OBSERVADOR 2: | ✓ | Gerente de Riesgos y Procesos |
| OBSERVADOR 3: | ✓ | Auditora Interna |
| FECHA: | ✓ | 24/05/2014 |

) Z-5

( CC-3-4

**Observación:** No se tienen definidas adecuadamente las responsabilidades dentro del plan de continuidad de operaciones de TI, no conociéndose las actividades ni responsables para el levantamiento de los servicios en el sitio alterno.

| | |
|---|---|
| ✓ | Verificado conforme |
| X | Verificado Inconforme |
| ⓘ | Informado |
| ( | Viene de |
| ) | Va para |

**Imagen, S.A.**
**Gerencia de TI -2013**
**Detalles del plan de pruebas**

| P/T | CC-3-2 | |
|---|---|---|
| Elaboro: | Jfco | 27/09/2014 |
| Reviso: | Bmc | 28/09/2014 |

**Fases para la ejecución del ejercicio**

| No. | Actividad |
|---|---|
| | **Fase I. Preparación** ✓ |
| 1 | Definir fecha para realizar el ejercicio |
| 2 | Llenar formato de Planificación del Ejercicio de Escritorio |
| 3 | Hacer convocatoria |
| 4 | Reservar el lugar para realizar la prueba |
| | **Fase II. Ejecución** ✗ |
| | **Gerente de TI** |
| 5 | Dar a conocer la Planificación del Ejercicio de escritorio a los participantes |
| 6 | Entregar formato de verificación de actividades del plan a los colaboradores participantes |
| 7 | Entregar formato de verificación de actividades del plan a los observadores |
| 8 | Revisar cada uno de los elementos del plan de continuidad de operaciones definidos para la prueba |
| | **Colaborador participante** |
| 9 | Completar el formato de verificación del guión de actividades correspondiente |
| | **Observador** |
| 10 | Completar formato de verificación del observador |
| 11 | Entregar formato de verificación al director del ejercicio, cuando finalice el mismo |
| | **Fase III. Presentación de Resultados** ✓ |
| 12 | Completar formato de presentación de resultados |
| 13 | Completar formato de lecciones aprendidas ⊘ |
| 14 | Presentar informe consolidado y documentos asociados a Gerente General, Auditoria Interna y Unidad de Riesgos ) CC-3-4 |

**Nota:** Se detectó que el personal que participo en la prueba al plan de continuidad de operaciones de TI, no tenía el conocimiento necesario para reactivar el sitio alterno.

| | |
|---|---|
| ✓ | Verificado conforme |
| ✗ | Verificado Inconforme |
| ⊘ | No aplica |
| ) | Va para |

**Imagen, S.A.**
**Gerencia de TI -2014**
**Elementos dentro del Plan de Continuidad de TI**

| INT | CC.1.1 | |
|---|---|---|
| Elaboro | Jlca | 27/08/2014 |
| Revisa: | Bmc | 28/09/2014 |

## Plan del Ejercicio de Escritorio ✔ ⓘ

**1 Objetivos :**

1. Revisar el Plan de continuidad de operaciones de TI
2. Verificar la aplicabilidad o viabilidad del Plan de Continuidad de Operaciones de TI
3. Contribuir a la difusión y entendimiento de los Planes de Continuidad del Negocio
4. Identificar oportunidades de mejora que permitirán afinar el Plan de Continuidad de Operaciones de TI
5. Contribuir al mantenimiento del Plan de Continuidad de Operaciones de TI

**2 Escenario**

El ejercicio de escritorio del BCP de la Gerencia de Riesgos y Procesos considera su aplicación para el siguiente escenario:
"Incendio de consideración, ocurrido a las 03: 00 a. m. (3 de la mañana) del día 02 de mayo del 2014 que se inicia en el 2º. piso del Edificio Platinos la zona 10, el cual genera daños serios a la infraestructura del edificio imposibilitando la utilización de sus instalaciones, incluyendo el Data Center que queda inoperativo".
Ello considera la utilización del sitio alterno de trabajo y data center alterno.

**3 Elementos del Plan Considerados para el alcance del presente ejercicio**

| | |
|---|---|
| **DEFINICIONES** | Aplica |
| **RESPONSABLES DE LA GESTIÓN** | Aplica |
| **ESTRATEGIAS GENERALES PARA LA RECUPERACIÓN DE LAS OPERACIONES DE TI** | Aplica |
| A nivel de Infraestructura - Instalaciones | Aplica |
| A nivel de Servicios de TI | Aplica |
| A nivel de Personal | Aplica |
| A nivel de Recursos | Aplica |
| A nivel de Registros Vitales | Aplica |
| A nivel de Proveedores | Aplica |
| A nivel de Procesos | Aplica |
| **GRUPOS Y ROLES DE RECUPERACIÓN** | Aplica |
| Conformación | Aplica |
| Guión de Actividades | Aplica |
| Personal asociado por Rol | Aplica |
| **RECURSOS ASOCIADOS** | Aplica |
| **PROTOCOLO DE LLAMADAS** | Aplica |
| **LISTA DE PROVEEDORES** | Aplica |
| **LISTA DE DOCUMENTOS DE CONSULTA** | Aplica |
| **ANEXOS** | Aplica |
| Procesos Críticos | Aplica |
| Servicios de TI | Aplica |
| Servicios de Apoyo | Aplica |
| Infraestructura – instalaciones | Aplica |
| Gestión de accesos | Aplica |
| Rotación de Personal | Aplica |
| Directorio Telefónico | Aplica |
| Check List de verificación de Registros Vitales | Aplica |
| Check list de habilitacióin del sitio alterno | Aplica |
| Listado de Insumos | Aplica |

**6 Participantes**

| | Nombre Participante | | Rol/Responsablidades |
|---|---|---|---|
| 1 | Gerente de Tecnología | ✔ | Director del ejercicio |
| 2 | Subdirector de infraestructura | ✔ | Encargado de reactivar el sitio alterno |
| 3 | Personal de TI | ✔ | Encargados de poner en alto los servicios de TI |
| 3 | Gestor de seguridad de la información | ✔ | Observador 1 |
| 4 | Gerente de riesgos y procesos | ✔ | Observador 2 |
| 5 | Auditora Interna | ✔ | Observador 3 |

| | |
|---|---|
| ✔ | Verificado conforme |
| ⓘ | Informado |

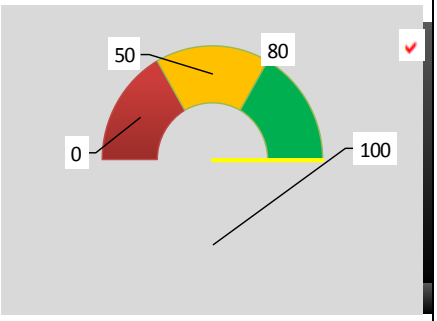
**Imagen, S.A.**
**Gerencia de TI -2014**
**Informe de resultado**

| PIT | CC-3-1 |
|---|---|
| Elaboro | Jfco 27/08/2014 |
| Revisa | Rmc 28/08/2014 |

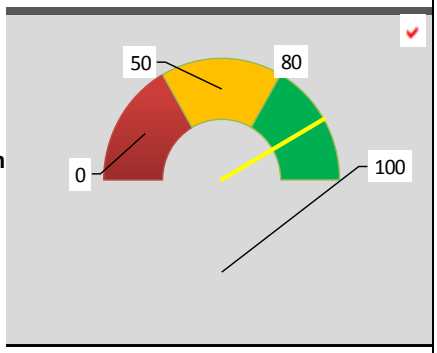
## Informe de Resultados

**Cumplimiento de Objetivos**

| | |
|---|---|
| **Que el 100% de los colaboradores de Tecnología que tienen un rol dentro del Plan de Continuidad de Operaciones de su área participen en la prueba** | **80** |
| **Indicadores** | |
| Porcentaje de asistencia en la prueba de escritorio | 80 |




| | |
|---|---|
| **Que los colaboradores de Tecnología conozcan su rol principal y el rol alterno dentro de Plan de Continuidad de Operaciones de TI en un 95%** CC-3-2 | **50** |
| **Indicadores** | **Ponderación** |
| Promedio de las notas del examen mayor o igual a 90 pts | 50 |




**Resumen Ejecutivo**

Todo el proceso fue ejecutado sin ninguna novedad.

**Logros Alcanzados**

Se verificaron todos los elementos incluidos en el Plan de Continuidad de Operaciones siendo el resultado satisfactorio.

**Grado de Seguimiento de los Procedimientos (Alto, Bajo)**

Bajo

**Incidencias Acontecidas**

No se tenian definidas adecuadamente las responsabilidades para el levantamiento de los servicios en sitio alterno.

**Oportunidades de Mejora**

Retroalimentación de las funciones y responsabilidades de cada uno de los involucrados en el plan de continuidad.

**Cambios a realizar en el Plan**

Ninguno

**Resultados de la Prueba** CC-3-1

Resultado Exitoso

**Observación:** Se detectó que no se tiene definidas adecuadamente las responsabilidades dentro del plan de continuidad de operaciones de TI.

| | |
|---|---|
| ✓ | Verificado conforme |
| ✗ | Verificado Inconforme |
| ⓘ | Informado |
| ( | Viene de |
| ) | Va para |

**Imagen, S.A.**
**Gerencia de TI -2014**
**Control de capacitaciones para la Gerencia de Tecnología de la Información**

| P/T | CC-14 | |
|---|---|---|
| Elabora: | Jlca | 27/09/2014 |
| Revisa: | Bmc | 28/09/2014 |

| No. | Listado de Cursos | Costo del Curso por Persona | Proyecto Asociado | Destinatario | Fecha | Proveedor Sugerido |
|---|---|---|---|---|---|---|
| 1 | Administración de Vlan (segmentación de red) | $2500 | PR02: JM102-2011 | Administrador de redes & Mesa de ayuda | 2 trimestre | Canella |
| 2 | Fastcore (Herramienta de gestión de riesgos e incidentes) | $500 | PR02: JM102-2011 | Personal de TI, Auditoría interna y Unidad de riesgos | 1 trimestre | AGSA |
| 3 | Manejo de certificados digitales / Controles criptográficos | $1800 | PE01: CREA | Subdirector de TI, Auxiliar de DBA y Subdirector de Infraestructura | 3 trimestre | Sisap |
| 4 | SAI, SAA, SAG (software de swift) | $6000 | PE02: SWIFT | Gerente de TI, Subdirecto de TI y Subdirector de infraestructura | Marzo/abril ($6000) | SWIFT |
| 5 | Inglés conversacional | $750 | PE02: SWIFT | Gerente de TI, Subdirector de TI, Subdirector de infraestructura y Administadore de redes | 1 semestre | SWIFT |
| 6 | VNX y Unisphere (servidores SAN) | $3500 | PI01: Implementación SAN | Subdirector de infraestructura | Según disponibilidad del proveedor | Martinexsa |
| 7 | VSphere / Virtualización con VmWare | $3750 | PI01: Renovación Servidores | Subdirector de infraestructura | A partir del mes de febrero | Canella / New Horizons |
| 8 | Procesos de integración de servicios electronicos | $600 | PI02: Integración remesas+ | Auxiliares de Soporte, Mesa de Ayuda, Programadores | 3 trimestre | E-Solution, S.A. |
| 9 | Herramienta BK Entorno Virtual (Herramienta de virtualización) | $1800 | PI04: DRP IT | Subdirector de TI, Subdirector de infraestructura y Mesa de ayuda | Según disponibilidad del proveedor | CA Technologies / Martinexsa |
| 10 | Capacitación sobre seguridad de la información | Sin Costo | PI06: Desempeño en el puesto de trabajo | Gerente de TI y Subdirectores | A partir del 3 trimestre | Interna |
| 11 | MySQL / SQL | $450 | PI06: Desempeño en el puesto de trabajo | Auxiliar de DBA | Disponibilidad del proveedor | New Horizons |
| 12 | Python (libro de consulta para desarrolladores) | $100 | PI06: Desempeño en el puesto de trabajo | Desarrolladores | Disponibilidad del proveedor | Sophos |
| 13 | Infraestructura de Microsoft 1er Nivel | $350 | PI06: Desempeño en el puesto de trabajo | Mesa de ayuda | Disponibilidad del proveedor | New H... |
| 14 | Administración de Equipos de seguridad: Tipping Point y Fortigate | $650 | PI06: Desempeño en el puesto de trabajo | Administrador de redes | Disponibilidad del proveedor | Sisap |

Z-5

**Fuente:** DNC de Tecnología realizado por la Gerencia de Recusos Humanos

**Observación:** Se llevo a cabo la evaluación de las capacitaciones al personal detectándose que el mismo se ha ejecutado en un 75%, sin embargo no existen cartas de responsabilidad en relación a la inversión realizada por la organización, que garanticen el retorno de la inversión

| | |
|---|---|
| ✓ | Verificado conforme |
| ⊖ | No implementado |
| ◊ | Cotejado con Contabilidad |
| ) | Va para |

**Imagen S.A.**

**Auditoría Interna**

**Procesamiento de información y tercerización**

| P/T | CC-4 | |
|---|---|---|
| Elaboro: | Jfco | 27/09/2014 |
| Reviso: | Bmc | 28/09/2014 |

**Imagen, S.A.**
**Gerencia de TI -2014**
**Control de Proveedores de TI**

| PT | CC.4.1 | |
|---|---|---|
| Elaboro: | Jco | 27/05/2014 |
| Revisó: | Bmc | 28/05/2014 |

| NO | Nombre o Razon Social | SERVICIO | Contacto | FECHA INICIO DE CONTRATO | FECHA VENCIMIENTO DEL CONTRATO | DIRECCION ELECTRONICA | TELEFONOS / FAX | TIPO DE MANTENIMIENTO | OBSERVACIONES |
|---|---|---|---|---|---|---|---|---|---|
| 1 | AYRE,S.A. (AIRETEC) | Mantenimiento del Equipo de Áire Acondicionado | Oscar R Mendoza / René Arturo Mendoza Stein / Lilian de Butz | 8-nov.-2005 | POR TIEMPO INDEFINIDO | ayre@intelnet.net.gt ; Lilian de Butz ( lbutz@airetec.com.gt ) | PBX : 2423-3000 / 2423-3001(FAX) | Correlativo, No Correlativo, llamados de Emergencia | Carta anual para renovación de contrato |
| 2 | BETA ASESORES | Soporte Sofware Remesas | | 1-feb.-2003 | | | | Mantenimiento de sistemas electronicos de uso bancario | |
| 3 | C.C.A. | Mantenimiento y Soporte de Lectoclasificadoras | | 15-nov.-2005 | POR 03 AÑOS | | | Mantenimiento programado preventivo, mantenimiento no preventivo, llamados de emergencia, | Carta anual para renovación de contrato |
| 4 | CANELLA, S.A (SOFTWARE) | Mantenimiento y soporte de Sofware y Harware | | | Por un año | www.canella.com.gt ; rveliz@canella.com.gt ( Raul Veliz ) ; msoto@canella.com.gt (Mauricio Soto ) | 23385900 | Soporte de sistemas, funcionamiento adecuado de programas, tanto estructura de datos como programas ejecutables. | Carta anual para renovación de contrato |
| 8 | COMCEL (ENLACE DE INTERNET) | Servicio de Conexión a Internet | | 15-abr.-2004 | se encuentra cancelado el servico, s/ carta adjunta al arch. | | 24280000 | | |
| 10 | SISTEMAS APLICATIVOS | Servicio y producto orientado a mejorar la seguridad de los sistemas aplicativos (Antivirus) | | 18-feb.-1998 | ??? | www.sisap.com.gt ; lcatalan@sisap.com.gt ( Lourdes de Catalan ) | 24104300 | | |
| 19 | GBM | contrato de mantenimiento de HW guateACH | | ?? | | | | | |
| 20 | TyT | hosting de equipo ACH | | 01 de enero 2008 | | | | | |
| 23 | Microsys Electronic | | Edgar Gonzales | | | mainframesalgo@hotmail.com | | | |
| 24 | Servicios Digitales Computarizados | | Luis Quiñonez | | | sedicomlq@intelnet.net.gt | | | |
| 25 | Ingenieria Avanzada | | Gurgi Juarez | | | gjuarez@ingenieria-avanzada.com | | | |
| 26 | Multisoft | | Walter Ocaña | | | walterocana@multisoftgt.com | | | |
| 27 | Widefense | | | | | | | | |
| 28 | Isertec | | Edgar Gonzales | | | egonzalez@isertec.com.gt | | | |

**Observación:** Se detectó que el control de proveedores de TI, no esta actualizada, ni contiene todos los datos que el control requiere.

| | |
|---|---|
| ✓ | Verificado conforme |
| X | Verificado Inconforme |
| ) | Va para |

) Z-5

**IMAGEN, S.A.**
**PERFIL DE PUESTO** ✔
**GESTOR DE SEGURIDAD DE LA INFORMACIÓN**

| P/T | CC-4-2 | |
|---|---|---|
| Elaboro: | Jfco | 29/09/2014 |
| Reviso: | Bmc | 30/09/2014 |

## X. PROPOSITO DEL PUESTO

Responsable de planear, coordinar y administrar los procesos de la seguridad informática en la organización, así como contribuir a la difusión de la cultura de la seguridad de la información entre los colaboradores.

## XI. FUNCIONES PRINCIPALES ✔

7. Definir la estrategia de seguridad informática y sus objetivos, e implementar las acciones congruentes con respecto a la estrategia definida.
8. Administrar los requerimientos de seguridad lógica y física.
9. Fungir como contralor del cumplimiento de los indicadores del desempeño de la Gerencia de IT.
10. Detectar necesidades y vulnerabilidades de la seguridad, y proponer sus respectivas soluciones de acuerdo al costo beneficio para la empresa.
11. Documentar las políticas, procedimientos y estándares de seguridad, así como darle seguimiento al cumplimiento de estándares internacionales y regulaciones que apliquen a la empresa.
12. Aplicar una metodología de análisis de riesgo que permita evaluar la efectividad de los controles, del cumplimiento con las normas de seguridad, e investigar incidentes de seguridad.
13. Calificar y cuantificar los riesgos tecnológicos para evitar su materialización.
14. Apoyar a las gerencias y comité de riesgos en el proceso de identificación de riesgos, identificación de mejoras a procesos y políticas de tecnología y preparación de informes periódicos del riesgo tecnológico.

## XII. FUNCIONES ESPECÍFICAS ✘

7. Velar por el cumplimiento de la confiabilidad, disponibilidad y resguardo de la información:
    a. Bases de datos.

b. Respaldos (por negocio y por ley).
c. Uptime y monitoreo de servicios.
d. Calidad del soporte técnico.
e. Registro del monitoreo de capacidades.
f. Administrar la seguridad lógica (perfilamiento, accesos).

8. Evaluar la seguridad del desarrollo de aplicativos (control de acceso, funciones criptográficas, filtros, bitácoras de seguridad de aplicativos).
9. Dar soporte de seguridad a la Gerencia de Tecnología.
10. Revisar el riesgo tecnológico y operativo en función de la seguridad de la información.
11. Cumplimiento de políticas en la función de seguridad de la información.
12. Apoyo en la difusión de la cultura de seguridad de la información.
13. Catalogar, perfilar, ponderar y cuantificar los riesgos tecnológicos.
14. Administración global del riesgo tecnológico.
15. Revisar procesos, documentación y cumplimiento de manuales, proponiendo las mejoras que correspondan.
16. Asegurar conocimiento tácito con conocimiento explícito.

## XIII. REQUERIMIENTOS MINIMOS

### Educación

Grado de Licenciatura en Informática, Ingeniería de Sistemas, Ingeniería Industrial y/o certificaciones en seguridad informática.

### Experiencia

En bases de datos, sistemas operativos, equipo de comunicación, auditoria, administración de riesgos, Control de calidad, administración de la seguridad lógica. Deseable en Administración de proyectos tecnológicos, diseño y documentación de procesos.

**Conocimientos**

- Específicos: algún estándar o marco de referencia como COBIT, ITIL, ISO/IEC 27001, BMP, PMI.
- Proceso del negocio.

## XIV. RESPONSABILIDADES ×

**Entregables**

- Reporte del % del cumplimiento del plan de trabajo anual.
- % de mejora de los resultados de auditorías recibidas (auditorías internas y auditorías externas, por parte de cualquier ente revisor).
- Mantener positivo el % de calidad y desempeño en el desarrollo de aplicaciones nuevas y por mantenimiento, por infraestructura y por mejora.
- Incrementar continuamente él % de niveles de madurez de la seguridad de la información.
- Mantener positivo el % de actualización de documentación (conocimiento explícito).
- Entrega de reportes a la Gerencia General según la periodicidad que ésta defina.

**Responsabilidad Financiera**

Administración del presupuesto y de activos fijos bajo su cargo.

## XV. COMPETENCIAS

- Facilidad de adaptarse a los cambios
- Responsabilidad
- Integridad
- Servicio
- Comunicación asertiva

## XVI. REPORTA A:

Gerencia General

## XVII. CARACTERISTICAS PERSONALES

Edad: De 30 años en adelante
Género: Masculino o Femenino

Habilidad/capacidad de: Pensamiento estratégico, visionario, excelentes relaciones interpersonales y públicas, liderazgo y capacidad de influencia, coordinación de equipos de trabajo gerenciales, integridad y ética profesional.

## XVIII. CONDICIONES DE TRABAJO

Jornada y horario de trabajo:

- De lunes a viernes de 08:00 a 17:00 horas

Personal de confianza, no sujeto a las limitaciones de la jornada de trabajo.

**Observación:** Se detectó que el gestor de seguridad de la información no está cumpliendo con sus funciones y responsabilidades definidas dentro del perfil de puesto, no dando respuesta a los requerimientos para la administración del riesgo tecnológico. ( CC-4-3 ) Z-5

| | |
|---|---|
| ✓ | Verificado conforme |
| X | Verificado Inconforme |
| ( | Viene de |
| ) | Va para |

**Imagen, S.A.**
**Auditoria Interna**
**Cédula de funciones del GSI**

| P/T | CC-4.3 | |
|---|---|---|
| Elaboro: | Jfco | 29/09/2014 |
| Reviso: | Bmc | 30/09/2014 |

| No. | Función | SI | No | Observaciones |
|---|---|---|---|---|
| 1 | Definir estrategia de seguridad informática | | X | Incumplimiento |
| 2 | Administrar la seguridad física y lógica | | X | Incumplimiento |
| 3 | Contralor del cumplimiento de los indicadores de TI | ✓ | | Verificado |
| 4 | Detectar y buscar soluciones a vulnerabilidades | | X | Incumplimiento |
| 5 | Documentar políticas y procedimientos de la seguridad | ✓ | | Verificado |
| 6 | Aplicar metodología para el análisis de riesgos de TI | | X | Incumplimiento |
| 7 | Apoyar en la identificación y análisis de riesgos de TI | ✓ | | Verificado |
| 8 | Evaluar la seguridad en el desarrollo de aplicativos | ✓ | | Verificado |
| 9 | Difusión de la cultura de riesgo tecnológico | | X | Incumplimiento |
| 10 | Administrar de forma global el riesgo tecnológico | ✓ | | Verificado |
| 11 | Administrar presupuesto y activos fijos bajo su cargo | ✓ | | Verificado |

Porcentaje de cumplimiento de sus funciones 55%
Porcentaje de incumplimiento a sus funciones 45%

) CC-4-2

**Observación:** El Gestor de seguridad de la información no esta cumplimiento con sus funciones y responsabilidades definidas en su perfil de puesto, no dando respuesta al riesgo tecnológico adecuadamente.

| | |
|---|---|
| ✓ | Verificado conforme |
| X | Verificado Inconforme |
| ) | Va para |

**Imagen S.A.**

**Auditoría Interna**

**Información y comunicación en la gestión del riesgo tecnológico**

| P/T | DD | |
|---|---|---|
| Elaboro: | Jfco | 29/09/2014 |
| Reviso: | Bmc | 30/09/2014 |

**Imagen, S.A.**
**Auditoría Interna**
**Reportes del Comité de Riesgos**

| P/T | DD-1 | |
|---|---|---|
| Elaboro: | Jfco | 29/09/2014 |
| Reviso: | Bmc | 30/09/2014 |

| No. | Información a Generar | Reporta a: | Periodicidad |
|---|---|---|---|
| 1 | Matriz del riesgo tecnológico y su evolución en el tiempo | Consejo de Administración | Semestral ✔ |
| 2 | Mapa de calor del riesgo tecnológico | Consejo de Administración | Semestral ✔ |
| 3 | Grado de efectividad de los planes de tratamiento sobre los riesgos | Consejo de Administración | Semestral ✔ |
| 4 | Nivel de cumplimiento de las políticas y procedimientos de riesgo | Consejo de Administración | Semestral ✔ |
| 5 | Principales mejoras realizadas a la Administración del Riesgo Tecnológico | Consejo de Administración | Semestral ✔ |
| 6 | Grado de cumplimiento a las disposiciones regulatorias | Consejo de Administración | Semestral ✔ |

**NOTA:** Se verifico la generación de la información y comunicación de la misma al ente competente, no observándose inconsistencia alguna.

✔ Verificado conforme

**Imagen, S.A.**
**Auditoría Interna**
**Reportes de la Unidad de Riesgos**

| P/T | DD-2 | |
|---|---|---|
| Elaboro: | Jfco | 29/09/2014 |
| Reviso: | Bmc | 30/09/2014 |

| No. | Información a Generar | Reporta a: | Periodicidad |
|---|---|---|---|
| 1 | Matriz del riesgo tecnológico y su tendencia en el tiempo. | Comité de Riesgos | Trimestral ✔ |
| 2 | Control sobre los planes de tratamiento y su seguimiento para la mitigación de riesgos. | Comité de Riesgos | Trimestral ✔ |
| 3 | Resultado de los monitoreos realizados a los riesgos tecnológicos. | Comité de Riesgos | Trimestral ✔ |
| 4 | Nivel de cumplimiento de las políticas y procedimientos de riesgo. | Comité de Riesgos | Trimestral ✔ |
| 5 | Comportamiento histórico, reincidencias y tendencia de los riesgos más significados. | Comité de Riesgos | Trimestral ✔ |
| 6 | Nivel de efectividad de los programas de capacitación y sensibilización impartidos en materia de la gestión de riesgos. | Comité de Riesgos | Trimestral ✔ |
| 7 | Nivel general de exposición al riesgo tecnológico, soportado en los reportes remitidos por la Gerencia de TI. | Comité de Riesgos | Trimestral ✔ |
| 8 | Resultado de las pruebas al plan de continuidad de operaciones de TI y planes de acción orientados a corregir las desviaciones detectadas. | Comité de Riesgos | Trimestral ✔ |
| 9 | Evaluación del riesgo tecnológico sobre proyectos o servicios nuevos. | Comité de Riesgos | Trimestral ✔ |

**NOTA:** Se verifico la generación de la información y comunicación de la misma al ente competente, no observándose inconsistencia alguna.

✔ Verificado conforme

**Imagen S.A.**

**Auditoría Interna**

**Nivel de madurez de TI y aspectos a mejorar**

| P/T | Z | |
|---|---|---|
| Elaboro: | Jfco | 30/09/2014 |
| Reviso: | Bmc | 01/10/2014 |

**Imagen, S.A.**

**Auditoría Interna**

| P/T | Z-1 | |
|---|---|---|
| Elaboro: | Jfco | 30/09/2014 |
| Reviso: | Bmc | 01/10/2014 |

## Nivel de madurez en los controles de TI

| | | | No implementado | | | Madurez >90% | Madurez 100% | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 0.00 - 0.30 | 0.301 - 0.60 | 0.601 - 0.90 | 0.901 - 0.989 | 0.99 - 1.00 | Efectividad | Efectividad | Efectividad |
| P | SP | Control | No existente | Inicial | En Proceso | Implementado | Mejorado | por Control | Subproceso | Del Proceso |
| | | **MADUREZ DE TI** | **0%** | **3%** | **42%** | **0%** | **55%** | | | |
| **Administración del Riesgo Tecnológico** | | | **0** | **1** | **16** | **0** | **21** | | | **84.18%** |
| | **Organización para la administración del Riesgo Tecnológico** | | 0 | 0 | 3 | 0 | 5 | | **88.57%** | |
| | | Acta de consititución del comité de riesgos | | | | | 1 | 100.00% | | Z-2 |
| | | Acta de reuniones periodicas del comité de riesgos | | | | | 1 | 100.00% | | |
| | | Documentación de politicas y procedimientos | | | 1 | | | 80.00% | | |
| | | Plan estrategico de TI | | | | | 1 | 100.00% | | |
| | | Estructura Organizacional de TI | | | 1 | | | 68.00% | | |
| | | Definición de responsabilidades | | | 1 | | 1 | 72.00% | | |
| | | Presupuesto de TI | | | | | 1 | 100.00% | | |
| | **Proceso para la Administración del Riesgo Tecnológico** | | 0 | 0 | 0 | 0 | 11 | | **100.00%** | |
| | | Declaración y filosofía sobre el Riesgo Tecnológico | | | | | 1 | 100.00% | | |
| | | Niveles de impacto | | | | | 1 | 100.00% | | |
| | | Niveles de probabilidad | | | | | 1 | 100.00% | | |
| | | Niveles de criticidad | | | | | 1 | 100.00% | | |
| | | Niveles de sensibilidad | | | | | 1 | 100.00% | | |
| | | Objetivos generales | | | | | 1 | 100.00% | | |
| | | Objetivos especificos | | | | | 1 | 100.00% | | |
| | | Catalogo de activos de TI | | | | | 1 | 100.00% | | |
| | | Inventario de amanezas y vulnerabilidades | | | | | 1 | 100.00% | | |
| | | Matriz del riesgo tecnológico | | | | | 1 | 100.00% | | |
| | | Planes de tratamiento para riesgos altos | | | | | 1 | 100.00% | | |
| | **Infraestructura de TI, base de datos y servicios de TI** | | 0 | 1 | 4 | 0 | 0 | | **65.00%** | |
| | | Informes de monitoreo y rendimiento | | | 1 | | | 64.00% | | |
| | | Inventario de acuerdos para los servicios de TI | | 1 | | | | 56.00% | | |
| | | Gestión de incidentes de TI | | | 1 | | | 76.00% | | |
| | | Inventario de base de datos | | | 1 | | | 64.00% | | |
| | | Administrador de base de datos | | | 1 | | | 68.00% | | |
| | **Seguridad de tecnología de la Información** | | 0 | 0 | 1 | 0 | 3 | | **93.00%** | |
| | | Procesos de clasificación de la información | | | 1 | | | 72.00% | | |
| | | Medidas de seguridad física | | | | | 1 | 100.00% | | |
| | | Matriz de accesos de TI | | | | | 1 | 100.00% | | |
| | | Inventario de copias de respaldo | | | | | 1 | 100.00% | | |
| | **Continuidad de Operaciones de TI** | | 0 | 0 | 5 | 0 | 0 | | **73.71%** | |
| | | Pruebas al plan de continuidad de operaciones de TI | | | 1 | | | 72.00% | | |
| | | Detalle de las pruebas al plan de continuidad | | | 1 | | | 72.00% | | |
| | | Elementos a considerar dentro del plan de pruebas | | | 1 | | | 72.00% | | |
| | | Resultado de las pruebas al plan de continuidad de TI | | | 1 | | | 72.00% | | |
| | | Capacitación al personal de TI | | | 1 | | | 76.00% | | |
| | **Continuidad de Operaciones de TI** | | 0 | 0 | 3 | 0 | 0 | | **84.80%** | |
| | | Proveedores de TI | | | 1 | | | 76.00% | | |
| | | Gestor de seguridad de la información (GSI) | | | 1 | | | 76.00% | | |
| | | Definición de responsabilidades del GSI | | | 1 | | | 72.00% | | |
| | **Información y comunicación en el Riesgo Tecnológico** | | 0 | 0 | 0 | 0 | 2 | | **100.00%** | |
| | | Reportes del comité de riesgos | | | | | 1 | 100.00% | | |
| | | Reportes de la unidad de riesgos | | | | | 1 | 100.00% | | |

| | |
|---|---|
| ✓ | Verificado conforme |
| ( | Viene de |
| ) | Va para |

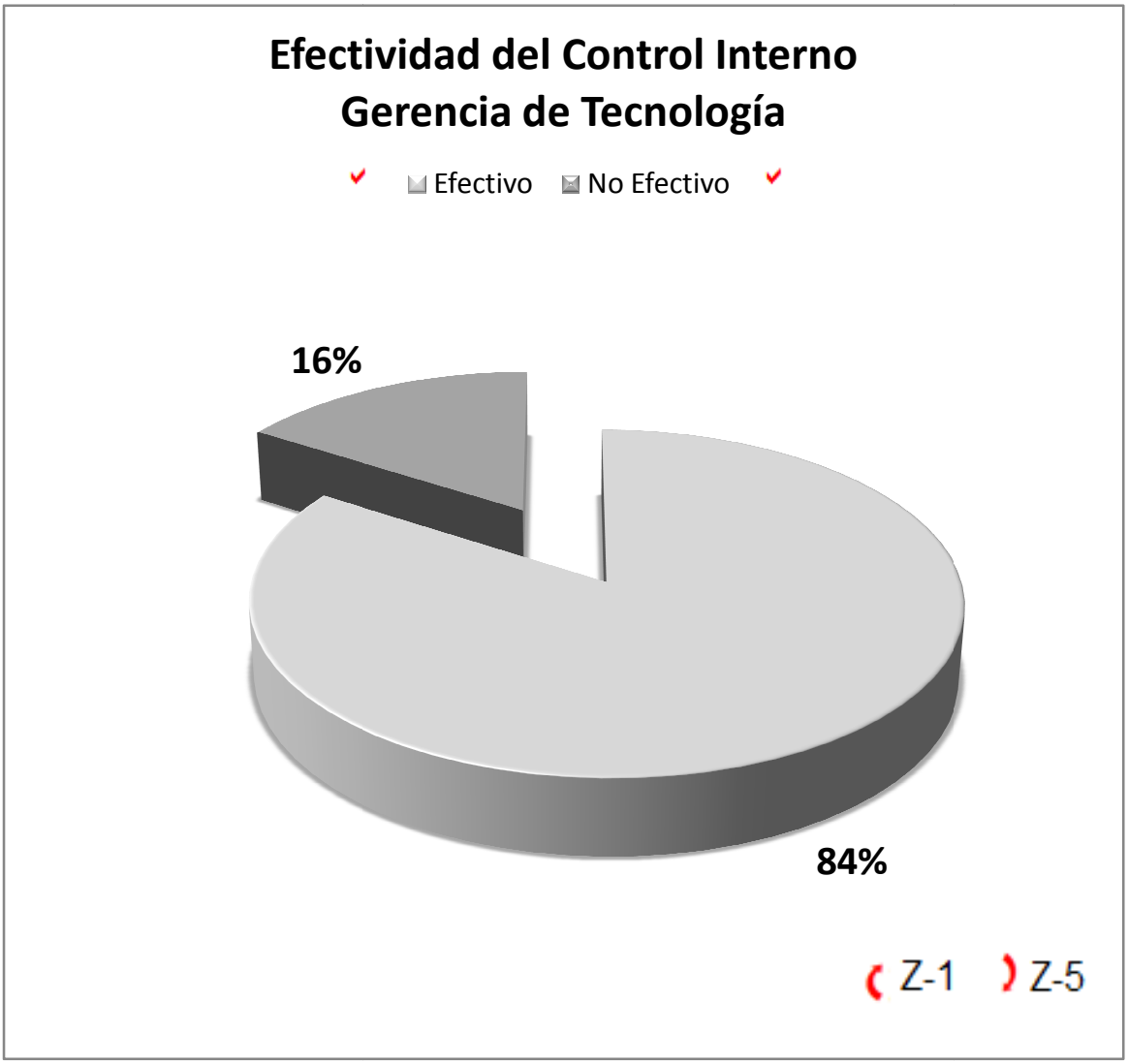
( Z-3

**Imagen, S.A.**

**Auditoría Interna**

**Efectividad del control interno en TI**

| P/T | Z-2 | |
|---|---|---|
| Elaboro: | Jfco | 30/09/2014 |
| Reviso: | Bmc | 01/10/2014 |




**Observación:** Se verifico que el control interno en la gerencia de Tecnología, es no efectivo derivado a que varios de los controles que soportan el proceso del riesgo tecnológico no son llevados adecuada y oportunamente.

| | |
|---|---|
| ✓ | Verificado conforme |
| ‹ | Viene de |
| › | Va para |

**Imagen, S.A.**

**Auditoría Interna**

**Evaluación de los criterios del control interno en TI**

| P/T | Z-3 | |
|---|---|---|
| Elaboro: | Jfco | 30/09/2014 |
| Reviso: | Bmc | 01/10/2014 |

| | | | Criterios del Control Interno ✔ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| P | SP | Control ✔ | Existe | | Implementado | | Documentado | | Caracteristicas C.I | | Efectivo | | |
| Administración del Riesgo Tecnológico | | | Si | No | Si | No | Si | No | Si | No | Si | No | X |
| **Organización para la administración del Riesgo Tecnológico** | | | | | | | | | | | | | |
| | | Acta de consititución del comité de riesgos | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Acta de reuniones periodicas del comité de riesgos | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Documentación de politicas y procedimientos | 1 | | | 0 | 1 | | 1 | | 1 | | 0.8 |
| | | Plan estrategico de TI | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Estructura Organizacional de TI | 1 | | 1 | | 1 | | 0.4 | | | 0 | 0.68 |
| | | Definición de responsabilidades | 1 | | 1 | | 1 | | 0.6 | | | 0 | 0.72 |
| | | Presupuesto de TI | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| **Proceso para la Administración del Riesgo Tecnológico** | | | | | | | | | | | | | |
| | | Declaración y filosofía sobre el Riesgo Tecnológico | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Niveles de impacto | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Niveles de probabilidad | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Niveles de criticidad | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Niveles de sensibilidad | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Objetivos generales | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Objetivos especificos | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Catalogo de activos de TI | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Inventario de amanezas y vulnerabilidades | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Matriz del riesgo tecnológico | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Planes de tratamiento para riesgos altos | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| **Infraestructura de TI, base de datos y servicios de TI** | | | | | | | | | | | | | |
| | | Informes de monitoreo y rendimiento | 1 | | 1 | | 1 | | 0.2 | | | 0 | 0.64 |
| | | Inventario de acuerdos para los servicios de TI | 1 | | | 0 | 1 | | 0.8 | | | 0 | 0.56 |
| | | Gestión de incidentes de TI | 1 | | 1 | | 1 | | 0.8 | | | 0 | 0.76 |
| | | Inventario de base de datos | 1 | | 1 | | 1 | | 0.2 | | | 0 | 0.64 |
| | | Administrador de base de datos | 1 | | 1 | | 1 | | 0.4 | | | 0 | 0.68 |
| **Seguridad de tecnología de la Información** | | | | | | | | | | | | | |
| | | Procesos de clasificación de la información | 1 | | 1 | | 1 | | 0.6 | | | 0 | 0.72 |
| | | Medidas de seguridad física | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Matriz de accesos de TI | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Inventario de copias de respaldo | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| **Continuidad de Operaciones de TI** | | | | | | | | | | | | | |
| | | Pruebas al plan de continuidad de operaciones de TI | 1 | | 1 | | 1 | | 0.6 | | | 0 | 0.72 |
| | | Detalle de las pruebas al plan de continuidad | 1 | | 1 | | 1 | | 0.6 | | | 0 | 0.72 |
| | | Elementos a considerar dentro del plan de pruebas | 1 | | 1 | | 1 | | 0.6 | | | 0 | 0.72 |
| | | Resultado de las pruebas al plan de continuidad de TI | 1 | | 1 | | 1 | | 0.6 | | | 0 | 0.72 |
| | | Capacitación al personal de TI | 1 | | 1 | | 1 | | 0.8 | | | 0 | 0.76 |
| **Continuidad de Operaciones de TI** | | | | | | | | | | | | | |
| | | Proveedores de TI | 1 | | 1 | | 1 | | 0.8 | | | 0 | 0.76 |
| | | Gestor de seguridad de la información (GSI) | 1 | | 1 | | 1 | | 0.8 | | | 0 | 0.76 |
| | | Definición de responsabilidades del GSI | 1 | | 1 | | 1 | | 0.6 | | | 0 | 0.72 |
| **Información y comunicación en el Riesgo Tecnológico** | | | | | | | | | | | | | |
| | | Reportes del comité de riesgos | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| | | Reportes de la unidad de riesgos | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |

❨ Z-4 ❩ Z-1

| | |
|---|---|
| ✔ | Verificado conforme |
| ❨ | Viene de |
| ❩ | Va para |

**Imagen, S.A.**

**Auditoría Interna**

**Evaluación de las características del control interno**

| P/T | Z-4 | |
|---|---|---|
| Elaboro: | Jfco | 30/09/2014 |
| Reviso: | Bmc | 01/10/2014 |

| P | SP | Control | Caracteristicas del Control | | | | | |
|---|---|---|---|---|---|---|---|---|
| Administración del Riesgo Tecnológico | | | Suficiente | Oportuno | Comprensible | Eficaz | Eficiente | X |
| **Organización para la administración del Riesgo Tecnológico** | | | | | | | | |
| | | Acta de consititución del comité de riesgos | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Acta de reuniones periodicas del comité de riesgos | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Documentación de politicas y procedimientos | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Plan estrategico de TI | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Estructura Organizacional de TI | 1 | 0 | 1 | 0 | 0 | 0.4 |
| | | Definición de responsabilidades | 1 | 1 | 1 | 0 | 0 | 0.6 |
| | | Presupuesto de TI | 1 | 1 | 1 | 1 | 1 | 1 |
| **Proceso para la Administración del Riesgo Tecnológico** | | | | | | | | |
| | | Declaración y filosofía sobre el Riesgo Tecnológico | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Niveles de impacto | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Niveles de probabilidad | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Niveles de criticidad | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Niveles de sensibilidad | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Objetivos generales | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Objetivos especificos | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Catalogo de activos de TI | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Inventario de amanezas y vulnerabilidades | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Matriz del riesgo tecnológico | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Planes de tratamiento para riesgos altos | 1 | 1 | 1 | 1 | 1 | 1 |
| **Infraestructura de TI, base de datos y servicios de TI** | | | | | | | | |
| | | Informes de monitoreo y rendimiento | 0 | 0 | 1 | 0 | 0 | 0.2 |
| | | Inventario de acuerdos para los servicios de TI | 1 | 0 | 1 | 1 | 1 | 0.8 |
| | | Gestión de incidentes de TI | 1 | 0 | 1 | 1 | 1 | 0.8 |
| | | Inventario de base de datos | 0 | 0 | 1 | 0 | 0 | 0.2 |
| | | Administrador de base de datos | 1 | 0 | 1 | 0 | 0 | 0.4 |
| **Seguridad de tecnología de la Información** | | | | | | | | |
| | | Procesos de clasificación de la información | 0 | 1 | 1 | 0 | 1 | 0.6 |
| | | Medidas de seguridad física | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Matriz de accesos de TI | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Inventario de copias de respaldo | 1 | 1 | 1 | 1 | 1 | 1 |
| **Continuidad de Operaciones de TI** | | | | | | | | |
| | | Pruebas al plan de continuidad de operaciones de TI | 1 | 0 | 1 | 0 | 1 | 0.6 |
| | | Detalle de las pruebas al plan de continuidad | 1 | 0 | 1 | 0 | 1 | 0.6 |
| | | Elementos a considerar dentro del plan de pruebas | 1 | 0 | 1 | 0 | 1 | 0.6 |
| | | Resultado de las pruebas al plan de continuidad de TI | 1 | 0 | 1 | 0 | 1 | 0.6 |
| | | Capacitación al personal de TI | 1 | 1 | 0 | 1 | 1 | 0.8 |
| **Continuidad de Operaciones de TI** | | | | | | | | |
| | | Proveedores de TI | 1 | 0 | 1 | 1 | 1 | 0.8 |
| | | Gestor de seguridad de la información (GSI) | 1 | 0 | 1 | 1 | 1 | 0.8 |
| | | Definición de responsabilidades del GSI | 1 | 1 | 1 | 0 | 0 | 0.6 |
| **Información y comunicación en el Riesgo Tecnológico** | | | | | | | | |
| | | Reportes del comité de riesgos | 1 | 1 | 1 | 1 | 1 | 1 |
| | | Reportes de la unidad de riesgos | 1 | 1 | 1 | 1 | 1 | 1 |

Z-3

| | |
|---|---|
| ✔ | Verificado conforme |
| ) | Va para |

**Imagen, S.A.**
**Auditoría Interna -2014**
**Cédula de Aspectos a Mejorar**

| PT | Z-5 | |
|---|---|---|
| Elaboró: | Jlco | 02/10/2014 |
| Revisó: | Bmc | 03/10/2014 |

| No. | Aspecto A Mejorar | Acciones A Tomar | Criticidad | Ref. | Pág. |
|---|---|---|---|---|---|
| 1 | Se observó que el Manual que rige la Administración del Riesgo Tecnológico no ha sido implementado, por lo cual no se brinda seguridad razonable en todo el proceso de la administración. | Implementar el Manual de Riesgo Tecnologico con el fin de garantizar un proceso estandar en la administración del riesgo tecnologico. | Alta | AA-3 | 117 |
| 2 | Se observó que la persona que funge Administrador de Base de Datos (DBA) no tiene los conocimientos necesarios para desempeñar dicha función, ya que no cuenta con formación académica según lo requerido y tampoco cuenta con capacitaciones en el tema. | Llevar a cabo una evaluación sobre el perfil del Administrador de Base de Datos (DBA) y los conocimientos necesarios para poder llevar a cabo la función que le compete. | Alta | AA-5 CC-1-5 | 119 / 140 |
| 3 | En la revisión a la estructura organizacional de TI se detectó concentración de actividades en el Subdirector de TI, derivado a que no existe un mecanismo de segregación de funciones y conocimientos hacia el Administrador de Base de Datos (DBA), quien está bajo la línea de mando del subdirector de Infraestructura. | Proceder a elaborar un plan de traslado de actividades a fin de evitar la dependencia del personal y/o perdida del capital intelectual. | Alta | AA-5 | 119 |
| 4 | Se detectó que algunas actividades o responsabilidades definidas para la unidad de riesgos y para el gestor de la seguridad de la información no estan siendo ejecutadas de conformidad a lo establecido. | Evaluar la gestión de la unidad de riesgos y del gestor de seguridad de la información, a fin de dar cumplimiento a lo requerido en sus perfiles de puesto. | Alta | AA-6 | 120 |
| 5 | Se observó que el reporte del rendimiento sobre infraestructura y base de datos, no muestra información en relación a bases de datos, derivado a que no se realiza un proceso de monitoreo sobre las mismas. | Establecer mecanismos de monitoreo que permitan conocer el rendimiento y capacidades de las bases de datos en tiempo real. | Alta | CC-1-1 | 136 |
| 6 | Se detectó que los acuerdos de servicios de TI están documentados, mas no implementados, por lo cual no se ejecutan actualmente. | Llevar a cabo la implementación de los acuerdos de servicio, a fin de garantizar que los requerimientos de los clientes están siendo atendidos de forma eficiente y adecuada. | Media | CC-1-2 | 137 |
| 7 | Aunque se lleva un adecuado control de los incidentes reportados a la Gerencia de TI, se observó que no son atendidos de forma oportuna y adecuada | Establecer métricas de respuesta a incidentes, a fin de darles respuesta oportunamente. | Baja | CC-1-3 | 138 |

| No. | Aspectos A Mejorar | Acciones a Tomar | Criticidad | Ref. | Pág. |
|---|---|---|---|---|---|
| 8 | Se tuvo a la vista el inventario de bases de datos, sin embargo se observó que no se cuenta con diagramas de relación ni diccionarios de datos que ayuden a interpretarlas y gestionarlas de una mejor manera. | Llevar a cabo la elaboración de diccionarios de datos y diagramas de relación para cada base de datos que se tenga en producción. | Alta | CC-1-4 | 139 |
| 9 | Aunque se cuenta con un proceso de clasificación de información por medio de una herramienta automatizada, se observó que no todo el personal conoce el proceso, así mismo se conoció por parte de la administración que no se cuenta con una política de clasificación que permita identificar que información es pública, interna, privada o confidencial. | Establecer una política para el proceso de clasificación de la información, así como trabajar en una cultura que permite ejecutar la política adecuadamente. | Media | CC-2-1 | 144 |
| 10 | Se observó que en las pruebas al plna de continuidad de las operaciones de TI, no se tenían definidas adecuadamente las responsabilidades para el levantamiento de los servicios en sitio alterno de forma adecuada y oportuna. | Establecer roles y responsabilidades adecuados dentro del Plan de Continuidad de Operaciones de TI, para dar una respuesta efectiva ante cualquier eventualidad. | Alta | CC-3-1 | 149 |
| 11 | Se llevo a cabo la evaluación de las capacitaciones al personal de TI, observandose que el mismo se ha cumplido en un 75%, sin embargo no existen cartas de responsabilidad en relación a la inversión realizada por la organización, ni el establecimiento de tiempo para el retorno del conocimiento hacia la organización. | Elaborar cartas de responsabilidad por cada capacitación que se conceda al personal de TI, con la finalidad de garantizar el retorno de la inversión en conocimiento y evitar así la perdida de capital intelectual. | Media | CC-3-5 | 153 |
| 12 | Se observó que la matriz de proveedores no está actualizada. | Proceder a actualizar los datos dentro de la matriz de proveedores a fin de contar con información oportuna y adecuada. | Media | CC-4-1 | 155 |
| 13 | Se detectó que el gestor de seguridad de la información no está cumplimiendo con sus funciones y responsabilidades definidas en su perfil de puesto, no dando respuesta al riesgo tecnologico adecuadamente. | Evaluar el perfil del Gestor de Seguridad de la Información, funciones y responsabilidades. | Alta | CC-4-2 | 156 |
| 14 | Se observó que los controles de TI relacionados con la Administración del Riesgo Tecnológico no son efectivos, ya que no han sido implementados, monitoreados o gestionados de forma adecuada y oportuna. | Proceder con la implementación, monitoreo y adecuada gestión de los controles de TI,a fin de poder cumplir con lo establecido en la regulación JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico. | Alta | Z-2 | 165 |

**5.5 Informe de Auditoría Interna**

**IMAGEN, S.A**
**INFORME DE AUDITORÍA INTERNA**
**AI- 10-2014**

Guatemala 08 de Octubre del 2014

Dirigido a:
Gerente General
Presidente del Comité de Riesgos
Presente.

Estimado Gerente General:

De conformidad a nuestro programa anual de auditoría, hemos concluido con la evaluación de la administración del riesgo tecnológico, la revisión cubrió el periodo del tercer trimestre del año 2014, dicha actividad fue realizada por el auditor Lic. Josué Chete durante el periodo del 10 de septiembre al 08 de octubre del año 2014.

Nuestro trabajo de auditoría fue efectuado de conformidad con el Marco para el Ejercicio Profesional de Auditoría Interna y limitada únicamente a lo que requiere la regulación JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico.

De acuerdo a los resultados obtenidos en esta auditoría, se concluye que los controles establecidos para la administración del riesgo tecnológico se aplican de manera adecuada, no obstante se observaron situaciones que afectan en alguna manera el proceso. Dichos aspectos encontrados se presentan a continuación con su nivel de criticidad.

# AUDITORÍA INTERNA
# ASPECTOS A MEJORAR Y ACCIONES A TOMAR

## ASPECTO A MEJORAR No. 1

**Nivel de criticidad: Alta**

Se observó que el Manual que rige la Administración del Riesgo Tecnológico no ha sido implementado, por lo cual no se brinda seguridad razonable en todo el proceso de la administración del riesgo tecnológico.

## CAUSA

Ausencia de un manual para la administración del riesgo tecnológico.

## EFECTO

Incumplimiento a lo requerido por la normativa JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico.

## ACCIONES A TOMAR

Implementar el Manual de Riesgo Tecnológico con el fin de garantizar un proceso estándar en la administración del riesgo tecnológico.

**ASPECTO A MEJORAR No. 2**

**Nivel de criticidad: Alta**

Se observó que la persona que funge Administrador de Base de Datos (DBA) no tiene los conocimientos necesarios para desempeñar dicha función, ya que no cuenta con formación académica según lo requerido y tampoco cuenta con capacitaciones en el tema.

**CAUSA**

Falta de conocimientos en la administración de Bases de Datos.

**EFECTO**

Inadecuada administración en las Bases de Datos, no protegiendo la integridad, confidencialidad y disponibilidad de la información de la organización.

**ACCIONES A TOMAR**

Llevar a cabo una evaluación sobre el perfil del Administrador de Base de Datos (DBA) y los conocimientos necesarios para poder llevar a cabo la función que le compete.

**ASPECTO A MEJORAR No. 3**

**Nivel de Criticidad: Alta**

En la revisión a la estructura organizacional de TI se detectó concentración de actividades en el Subdirector de TI, derivado a que no existe un mecanismo de segregación de funciones y conocimientos hacia el Administrador de Base de Datos (DBA), quien está bajo la línea de mando del subdirector de Infraestructura.

**CAUSA**

Concentración de actividades en personal clave.

**EFECTO**

Dependencia de personal en procesos claves de la organización.

**ACCIONES A TOMAR**

Proceder a elaborar un plan de traslado de actividades a fin de evitar la dependencia del personal y/o pérdida del capital intelectual.

**ASPECTO A MEJORAR No.4**

**Nivel de criticidad: Alta**

Se detectó que algunas actividades o responsabilidades definidas para la unidad de riesgos y para el gestor de seguridad de la información no están siendo ejecutadas de conformidad a lo establecido.

**CAUSA**

Incumplimiento a las funciones y responsabilidades definidas.

**EFECTO**

Inadecuada gestión de la administración del riesgo tecnológico.

**ACCIONES A TOMAR**

Evaluar la gestión de la unidad de riesgos y del gestor de seguridad de la información, a fin de dar cumplimiento a lo requerido en sus perfiles de puesto.

**ASPECTO A MEJORAR No. 5**

**Nivel de Criticidad: Alta**

Se observó que el reporte de rendimiento sobre infraestructura y base de datos, no muestra información en relación a bases de datos, derivado a que no se realiza un proceso de monitoreo sobre las mismas.

**CAUSA**

Ausencia de monitoreo a las bases de datos.

**EFECTO**

Debilidad en los sistemas informáticos de la organización.

**ACCIONES A TOMAR**

Establecer mecanismos de monitoreo que permitan conocer el rendimiento y capacidades de las bases de datos en tiempo real.

**ASPECTO A MEJORAR No. 6**

**Nivel de Criticidad: Media**

Se detectó que los acuerdos de servicios de TI están documentados, más no implementados, por lo cual no se ejecutan actualmente.

**CAUSA**

Ausencia de niveles de servicio de TI.

**EFECTO**

Inadecuada administración en la prestación de servicios de TI.

**ACCIONES A TOMAR**

Llevar a cabo la implementación de los acuerdos de servicio, a fin de garantizar que los requerimientos de los clientes están siendo atendidos de forma eficiente y adecuada.

**ASPECTO A MEJORAR No. 7**

**Nivel de Criticidad: Baja**

Aunque se lleva un adecuado control de los incidentes reportados a la Gerencia de TI, se observó que no son atendidos de forma oportuna y adecuada.

**CAUSA**

Inadecuada gestión de los incidentes de TI.

**EFECTO**

Interrupción de servicios, fallas en la infraestructura o errores en los procesos del negocio.

**ACCIONES A TOMAR**

Establecer métricas de respuesta a incidentes, a fin de darles respuesta oportunamente.

**ASPECTO A MEJORAR No. 8**

**Nivel de Criticidad: Alta**

Se tuvo a la vista el inventario de bases de datos, sin embargo se observó que no se cuenta con diagramas de relación ni diccionarios de datos que ayuden a interpretarlas y gestionarlas de una mejor manera.

**CAUSA**

Ausencia de diccionarios de datos y diagramas de las bases de datos en producción.

**EFECTO**

Fallas en la seguridad de los sistemas e interrupción de servicios de TI.

**ACCIONES A TOMAR**

Llevar a cabo la elaboración de diccionarios de datos y diagramas de relación para cada base de datos que se tenga en producción.

**ASPECTO A MEJORAR No.9**

**Nivel de Criticidad: Media**

Aunque se cuenta con un proceso de clasificación de información por medio de una herramienta automatizada, se observó que no todo el personal conoce el proceso, tampoco se cuenta con una política de clasificación que permita identificar qué información es pública, interna, privada o confidencial.

**CAUSA**

Ausencia de política para la clasificación de la información.

**EFECTO**

Uso inadecuado de la información de la organización.

**ACCIONES A TOMAR**

Establecer una política para el proceso de clasificación de la información, así como trabajar en una cultura que permite ejecutar la política adecuadamente.

**ASPECTO A MEJORAR No. 10**

**Nivel de Criticidad: Alta**

Se observó que en las pruebas al plan de continuidad de las operaciones de TI, no se tenían definidas adecuadamente las responsabilidades para el levantamiento de los servicios en sitio alterno de forma adecuada y oportuna.

**CAUSA**

Inadecuada segregación de funciones y responsabilidades en el Plan de Continuidad de Operaciones de TI.

**EFECTO**

Desconocimiento en el proceso de levantar el sitio alterno ante cualquier eventualidad que pueda suscitarse.

**ACCIONES A TOMAR**

Establecer funciones y responsabilidades adecuadas dentro del Plan de Continuidad de Operaciones de TI, para dar una respuesta efectiva ante cualquier eventualidad.

**ASPECTO A MEJORAR No.11**

**Nivel de Criticidad: Media**

Se llevó a cabo la evaluación de las capacitaciones al personal de TI, observándose que el mismo se ha cumplido en un 75%, sin embargo no existen cartas de responsabilidad en relación a la inversión realizada por la organización, ni el establecimiento de periodos de tiempo para el retorno del conocimiento hacia la organización.

**CAUSA**

Ausencia de controles que permitan retener el conocimiento de forma adecuada dentro de la organización.

**EFECTO**

Perdida de capital intelectual e inversiones mal gestionadas en el personal.

**ACCIONES A TOMAR**

Elaborar cartas de responsabilidad por cada capacitación que se conceda al personal de TI, con la finalidad de garantizar el retorno de la inversión en conocimiento y evitar así la perdida de capital intelectual.

**ASPECTOS A MEJORAR No. 12**

**Nivel de Criticidad: Media**

Se observó desactualización en el control de proveedores de TI.

**CAUSA**

Inadecuado control de la información relacionada con los proveedores de TI.

**EFECTO**

Información no oportuna o adecuada en relación a los proveedores en un evento que amerite contactarlos de forma inmediata.

**ACCIONES A TOMAR**

Proceder a actualizar los datos dentro del control de proveedores de TI, a fin de contar con información oportuna y adecuada.

**ASPECTO A MEJORAR No. 13**

**Nivel de Criticidad: Alta**

Se detectó que el gestor de seguridad de la información no está cumpliendo con sus funciones y responsabilidades definidas en su perfil de puesto, no dando respuesta al riesgo tecnológico adecuadamente.

**CAUSA**

Incumplimiento a funciones y responsabilidades.

**EFECTO**

Incumplimiento a lo regulatorio según la normativa JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico.

**ACCIONES A TOMAR**

Evaluar el perfil del Gestor de Seguridad de la Información, funciones y responsabilidades.

**ASPECTO A MEJORAR No. 14**

**Nivel de Criticidad: Alta**

Se observó que los controles de TI relacionados con la Administración del Riesgo Tecnológico no son efectivos, ya que no han sido implementados, monitoreados o gestionados de forma adecuada y oportuna.

**CAUSA**

Controles no efectivos de TI.

**EFECTO**

Incumplimiento a la normativa JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico.

**ACCIONES A TOMAR**

Proceder con la implementación, monitoreo y adecuada gestión de los controles de TI, a fin de poder cumplir con lo establecido en la regulación JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico.

**COMENTARIOS DEL AUDITADO**

El personal de Tecnología de la Información (TI) y la Gerencia General están de acuerdo con los aspectos a mejorar y con las acciones a tomar, e inician 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 TI y a los funcionarios de la organización.

Atentamente,

Lic. Miriam Camey
Auditora Interna

Cc / Archivo

# CONCLUSIONES

1. La adecuada administración del riesgo tecnológico con base a la regulación de la Junta Monetaria (JM-102-2011) permite brindar una mayor seguridad a los proceso de Tecnología, evitando así pérdidas derivado a fallas en la infraestructura de TI, sistemas de información o bases de datos, facilitando mejorar los procesos de negocio y apoyar al logro de los objetivos propuestos por la administración.

2. Para poder llevar a cabo un proceso de evaluación sobre la administración del riesgo tecnológico es necesario que el auditor a cargo tenga conocimientos básicos sobre tecnologías de información y mejores prácticas para su gestión, como también conocimiento en metodologías de administración de riesgos a fin de poder llevar un proceso de aseguramiento eficaz, para no caer en riesgo de auditoría de un falso aseguramiento.

3. El incumplimiento a las disposiciones de la regulación JM-102-2011 Reglamento para la administración del riesgo tecnológico, no tienen un efecto directo sobre la entidad en relación a sanciones o multas que la superintendencia de bancos pueda girar u otros entes reguladores, ya que según señala el artículo 25 del citado reglamento los que deben de velar porque se cumpla con el mismo deben de ser los bancos quienes contratan servicios terciarizados para el procesamiento de su información, por lo que al incumplir el efecto directo es sobre los clientes, no así, pueden estos entes emitir recomendaciones para la mejora del proceso establecido.

4. El incumplimiento a las disposiciones de la regulación JM-102-2011 pueden provocar pérdidas financieras en relación a la ruptura de relación con los clientes, provocando a la misma vez consecuencias de reputación o daños a la imagen para la entidad frente al sector bancario y con ello perder futuros procesos de negocio en el mercado financiero.

## RECOMENDACIONES

1. La administración del riesgo tecnológico no debe de limitarse únicamente a la regulación JM-102-2011 ya que estos son los requisitos mínimos que debe de cumplir una entidad para poder dar respuesta a los requerimientos de la superintendencia de bancos, una empresa en pro de su mejora continua y en busca de generar mayor valor a sus procesos de negocio, debe de buscar administrar sus riesgos de forma integral, llevando a cabo el análisis y aplicabilidad de mejores prácticas que permitan gestionar los procesos y servicios de TI de una manera mucho más eficaz.

2. Los auditores internos deben de cumplir con el requerimiento de ética profesional y deben realizar únicamente aquellos trabajos para los cuales tengan experiencia y pericia, no obstante, que deben de preparase en temas específicos como la administración de riesgos de tecnología para poder dar respuesta a los cambios constantes que ocurren en las organizaciones.

3. La evaluación al cumplimiento de la regulación JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico debe ser considerado por la auditoría interna en su plan de trabajo anual, a fin de verificar que no haya incumplimientos que puedan provocar una inadecuada gestión del riesgo tecnológico y con ello pérdidas financieras y daños a la imagen.

4. La auditoría interna por medio de sus evaluaciones debe generar valor a los procesos del negocio, detectando y reportando oportunamente aquellas amenazas que por incumplimientos puedan tener consecuencias graves con los socios de negocio y que puedan afectar negativamente futuras oportunidades de negocio con el sector bancario del país.

## REFERENCIAS BIBLIOGRÁFICAS


1. ABC de Educación Financiera. Superintendencia de Bancos. Guatemala, C.A.

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

3. Administración y Supervisión de Actividades de Banca Electrónica Transfronteriza. Comité de Basilea sobre supervisión bancaria. Año 2002.

4. Alineando CobiT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio del negocio. Un reporte para gestión del ITGI y la OGC. IT Governance Institute. Año 2008.

5. Álvarez Torres, Martín G. “Manual para la Elaboración de Manuales de Políticas y Procedimientos”. 14 Edición. Panorama Editorial S.A. de C.V. México. Año 2006.

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

7. Código de Comercio, Decreto 2-70 del Congreso de la República de Guatemala. Artículo 385,494.

8. Constitución Política de la República de Guatemala. Artículo 133.

9. Coopers & Lybrand e Instituto de Auditores Internos de España. Los nuevos conceptos del control interno (Informe COSO). Ediciones Díaz de Santos, S.A. 1997.

10. Duran & Asociados Consultores. El Riesgo Tecnológico como parte del negocio. Septiembre 2004.

11. El sistema de pagos de Guatemala: Evaluación y propuesta de modernización. Banco de Guatemala. Guatemala, C.A. Octubre, 2004.

12. Enciclopedia Omeba de Contabilidad, Economía, Finanzas y Dirección de Empresas. Tomo I. Bach, Juan René.

13. Echenique García, José Antonio. “Auditoría en Informática”. 2da edición. McGraw-Hill Interamericana editores, S.A. de C.V. Año 2001.

14. Gestión de la Seguridad Informática. Módulo de políticas de seguridad de la información. AGSA. Año 2012.

15. Gestión de Riesgos Corporativos, Marco Integrado. Committee of Sponsoring Organizations of the Tread way Commission (COSO). Año 2004.

16. Gestión de Riesgos Corporativos – Marco Integrado. Técnicas de Aplicación. Committee of Sponsoring Organizations of the Treadway Commission. Año 2004.

17. Grande Esteban, Ildefonso, Marketing de los Servicios. 4ª ed. Madrid, España. Año 2005.

18. Guzmán de León, Geovanni. “Tercerización de Tecnología de la Información, auditoría de tecnología de información para auditores internos”. Instituto de Contadores Públicos y Auditores. Año 2011.

19. Ley Orgánica del Banco de Guatemala, Decreto 16-2002. Artículo 2 y 3.

20. Ley de Supervisión Financiera, Decreto 18-2002. Artículo 1 y 2.

21. Marco de Trabajo COBIT 4.1. IT Governance Institute. Año 2007.

22. Malagarriga, Carlos C. Tratado elemental del derecho comercial II, contratos y papeles de comercio.

23. Marco Internacional para la Práctica profesional de Auditoría Interna. Instituto de Auditores Internos. Edición 2011.

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

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

26. Paul A. Samuelson& William D. Nordhaus. “Economía, con aplicaciones a Latinoamérica”. 19 Edición. McGraw-Hill Interamericana editores, S.A. de C.V. Año 2010.

27. Reglamento para la Administración del Riesgo Tecnológico. JM-102-2011.

28. Ruiz, Juan Carlos. Outsorcing. 10 Edición. Entrepreneur México. Año 2004.

29. Stecher, Otto. El mundo corporativo y globalizado. Mejores prácticas. Algunas lecciones en tercerización. Deloitte. Costa Rica. Año 2013

**Web grafía**

30. Cibercrimen. Página web: http://cibercrimenyriesgosenfacebook.blogspot.com/2010/06/2-que-escibercrimen.html

31. Concepto de empresa de servicios. Página web: http://deconceptos.com/ciencias-sociales/empresa-de-servicio

32. El sistema financiero y el desarrollo económico, aspectos teóricos. Banco de Guatemala. Página web: http://www.banguat.gob.gt/inveco/notas/articulos/envolver.asp?karchivo=1002&kdisc=si

33. Entornos Virtuales de Formación. Universidad de valencia. Página web: http://www.uv.es/bellochc/pedagogia/EVA1.wiki?0

34. Iniciativa de ley cibercrimen en Guatemala. Página web: http://jgramajo.wordpress.com/2009/10/07/ley-contra-el-cibercrimen/

35. ISO 27002/IEC
http://www.iso27002.es/

36. ISO 31000:2009
http://www.isaca.org/chapters8/Montevideo/cigras/Documents

37. Norma técnica para la generación de estadística básica.
http://www.snieg.mx/contenidos/espanol/normatividad/tecnica/Norma%20Técnica%20para%20la%20Generación%20de%20Estadística%20Básica.pdf

38. Sistemas de pagos
www.banguat.gob.gt

39. Tecnología en la Nube (Cloud Computing)
http://campusv.uaem.mx/cicos/imagenes/memorias/7mocicos2009/Articulos/p11%20%20Cloud%20Computing.pdf

# ANEXOS

**Anexo 1**

**Glosario de Términos**

**Riesgo:** Posibilidad de ocurrencia de cualquier evento interno o externo que pueda afectar a la empresa, ocasionándole pérdidas que disminuyan su capacidad para lograr sus objetivos y generar valor para sus accionistas, dueños, grupos de interés y beneficiarios.

**Riesgo Tecnológico:** Contingencia de que la interrupción, alteración, o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, provoque pérdidas financieras a la institución.

**Administración del Riesgo Tecnológico:** Proceso que consiste en identificar, medir, monitorear, controlar, prevenir y mitigar el riesgo tecnológico.

**Tecnología de la Información (TI):** Es el uso de la tecnología para obtener, procesar, almacenar, transmitir, comunicar y disponer de la información, para dar viabilidad a los procesos del negocio.

**Infraestructura de Tecnología de la Información (TI):** Es el hardware, software, redes, instalaciones y otros elementos que se requieren para desarrollar, probar, entregar, monitorear, controlar o dar soporte a los servicios de tecnología de la información. La infraestructura de TI excluye al recurso humano, los procesos y la documentación.

**Sistemas de Información:** Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

**Seguridad de la Información:** Conjunto de medidas preventivas y reactivas que permite resguardar y proteger la información buscando mantener la confidencialidad, integridad y disponibilidad sobre la misma.

**Información Estructurada:** Son los datos que están perfectamente definidos y sujetos a un formato muy concreto. En una base de datos son campos con una definición específica: una fecha, un valor numérico en una factura.

**Criticidad de la Información:** Es la clasificación de la información en diferentes niveles considerando la importancia que ésta tiene para la operación del negocio.

**Sensibilidad de la Información:** Es la clasificación de la información según el prejuicio que ocasione a la institución su alteración, destrucción, pérdida o divulgación no autorizada.

**Activos de Tecnología:** Son todos aquellos recursos que generan valor a la organización, es decir, aquello necesario para realizar las actividades productivas específicas de la organización. Estos pueden ser infraestructura, software y recurso humano.

**DBMS:** Sistemas de información de base de datos.

**CMDB:** Concepto introducido por ITIL, para facilitar la gestión de los servicios de TI y consiste en algunas herramientas que permiten mantener los elementos de configuración importantes para un servicio.

**Diagrama de Relación:** Es la representación gráfica que describe la distribución de datos almacenados en las bases de datos y la relación entre estos.

**Diccionario de Datos:** Es la documentación relativa a las especificaciones de los datos, tales como su identificación, descripción, atributos, el dominio de valores, restricción de integridad y ubicación dentro de una base de datos.

**Criptografía:** Técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

**Big Data:** Es una referencia a los sistemas que manipulan grandes conjuntos de datos. Es el término que popularmente designa un crecimiento, disponibilidad y uso exponenciales de la información estructurada y desestructurada. Volumen masivo de datos tanto estructurados como no estructurados que es tan grande que es difícil de procesar utilizando técnicas de bases de datos y de software tradicionales. Puede referirse a la tecnología (que incluye herramientas y procesos) que una organización necesita para manejar las grandes cantidades de datos e instalaciones de almacenamiento.

**Data Center:** Es un centro de procesamiento de datos, donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

**Servicios de TI:** Un conjunto de actividades que buscan responder a las necesidades de los clientes (usuarios) de tecnología de información, con el fin de entregar valor por medio de personal altamente capacitado en informática.

**Niveles de Acuerdo de Servicio (SLA`s):** Es una herramienta que ayuda al cumplimiento de los compromisos por parte de la Tecnología de la Información, sirve para fijar el nivel de calidad de TI, también constituye un punto de referencia para la mejora continua.

**Copias de Respaldo:** En ingles denominado back up, es una copia de los datos originales que se procesan, en un medio informático para su recuperación en caso de pérdida de la información original.

**ANEXO 2**
**Matriz de riesgo tecnológico**

| | | | Valoración de Activo Tecnologico | | | | |
|---|---|---|---|---|---|---|---|
| **Probabilidad** | **Impacto** | **Factor de Riesgo** | **Criticidad** | **Sensibilidad** | **Factor de Riesgo** | **Nivel de Riesgo** | **Color** |
| 3.00 | 3.00 | 9.00 | 1.00 | 1.00 | 2.00 | **11.00** | **Verde** |
| 3.00 | 4.00 | 12.00 | 1.00 | 2.00 | 3.00 | **15.00** | **Amarillo** |
| 4.00 | 2.00 | 8.00 | 2.00 | 4.00 | 6.00 | **14.00** | **Amarillo** |
| 4.00 | 4.00 | 16.00 | 2.00 | 3.00 | 5.00 | **21.00** | **Rojo** |
| 2.00 | 2.00 | 4.00 | 1.00 | 2.00 | 3.00 | **7.00** | **Verde** |
| 3.00 | 4.00 | 12.00 | 2.00 | 3.00 | 5.00 | **17.00** | **Rojo** |

| **Niveles de Valoración** | |
|---|---|
| Probabilidad: | de 1 a 4 |
| Impacto: | de 1 a 4 |
| Sensibilidad: | de 1 a 4 |
| Criticidad: | de 1 a 2 |

**ANEXO 3**
**Procesos y Controles definidos en la JM-102-2011**

**Procesos y Controles en la JM-102-2011**

| No. | Dom | Proc | Controles |
|---|---|---|---|
| | **Organización de la administración del riesgo tecnológico** | | |
| | | **Políticas y procedimientos** | |
| 1 | | | Políticas y procedimientos para gestionar el riesgo |
| 2 | | | Metodología para la evaluación del riesgo tecnológico |
| 3 | | | Políticas para elaborar, implementar y actualizar el plan estratégico |
| | | **Responsabilidad del Consejo de Administración** | |
| 4 | | | Aprobación de las políticas y procedimientos |
| 5 | | | Aprobación del plan estratégico de la TI |
| 6 | | | Aprobación del plan de continuidad del negocio de la TI |
| 7 | | | Definición del acta de constitución |
| | | **Comité de Gestión de Riesgos** | |
| 8 | | | Integración del comité de gestión de riesgos |
| 9 | | | Implementación de las políticas y procedimientos |
| 10 | | | Verificar el adecuado funcionamiento de las políticas y procedimientos |
| 11 | | | Ejecución de políticas y procedimientos |
| 12 | | | Monitoreo permanente de la adecuada organización para administrar la TI |
| | | **Unidad de Administración de Riesgos** | |
| 13 | | | Procedimiento para proponer al comité políticas y procedimientos para la administración del riesgo tecnológico |
| 14 | | | Procedimiento para proponer al comité, políticas y procedimientos para desarrollar el plan estratégico de la TI |
| 15 | | | Procedimiento para proponer al comité políticas y procedimientos para la continuidad del negocio |
| 16 | | | Procedimiento para la revisión anual de las políticas |
| 17 | | | Procedimiento para la revisión anual de los procedimientos |
| 18 | | | Procedimiento para la revisión anual del plan estratégico |
| 19 | | | Procedimiento para la revisión anual del plan de continuidad |
| 20 | | | Procedimiento medir, monitorear y registrar la revisión de la exposición del riesgo tecnológico |

| | | | |
|---|---|---|---|
| 21 | | | Procedimiento de análisis del riesgo inherente a las innovaciones en IT derivados nuevos productos |
| 22 | | | Procedimiento de análisis del riesgo inherente a las innovaciones en IT derivados nuevos servicios |
| 23 | | | Procedimiento para reportar la exposición del riesgo tecnológico y sus medidas correctivas |
| 24 | | | Procedimiento para evaluar el cumplimiento de las políticas y procedimientos |
| 25 | | | Procedimiento para evaluar la causa raíz de los incumplimiento de las políticas y procedimientos y su registro |
| | | **Plan estratégico de TI** | |
| 26 | | | Objetivos, presupuesto y plan alineado a la estrategia del negocio para gestionar la infraestructura |
| 27 | | | Objetivos, presupuesto y plan alineado a la estrategia del negocio para gestionar los sistemas de información |
| 28 | | | Objetivos, presupuesto y plan alineado a la estrategia del negocio para gestionar las bases de datos |
| | | **Organización de TI** | |
| 29 | | | Estructura organizacional |
| 30 | | | Plan de concientización y capacitación del recurso humano |
| 31 | | | Segregación de funciones |
| 32 | | | Desarrollo e implementación de perfiles y roles |
| 33 | | | Identificación y elaboración del mapa de procesos de TI |
| | | **Manual de administración del riesgo tecnológico** | |
| 34 | | | Creación y/o actualización del manual de administración del riesgo tecnológico |
| 35 | | | Aprobación del manual de riesgo tecnológico |
| 36 | | | Procedimiento para reportar actualizaciones y cambios al manual de administración de riesgos a los interesados |
| | **Infraestructura de TI, sistemas de información, bases de datos y servicios de TI** | | |
| | | **Esquema de la información del negocio** | |
| 37 | | | Identificación de los principales procesos de la TI |
| 38 | | | Identificación de los principales servicios del negocio (áreas y clientes) |
| 39 | | | Identificación de los principales proveedores del negocio |
| 40 | | | Mapa de procesos de la TI con los principales procesos del la TI |
| 41 | | | Mapa de procesos de la TI con los principales servicios (OLA) |
| 42 | | | Mapa de procesos de la TI con los principales proveedores (SLA) |
| 43 | | | Diagrama de red e infraestructura |
| 44 | | | Diagrama de servicios críticos |

| | | | |
|---|---|---|---|
| | | **Inventarios de infraestructura de TI, sistemas de información y de bases de datos** | |
| 45 | | | Inventario de infraestructura de la TI (registro de activos) |
| 46 | | | Inventario de sistemas de información |
| 47 | | | Inventario de bases de datos |
| | | **Administrador de base de datos** | |
| 48 | | | Perfil y manual de funciones aprobado para DBA |
| | | **Monitoreo de la infraestructura de TI, sistemas de información y bases de datos** | |
| 49 | | | Procedimiento para la evaluación y análisis de tendencias de la capacidad de la infraestructura |
| 50 | | | Procedimiento para la evaluación y análisis de tendencias de la capacidad de los sistemas de información |
| 51 | | | Procedimiento para la evaluación y análisis de tendencias de la capacidad de las bases de datos |
| 52 | | | Procedimiento y registro para reportar déficit en las capacidades de la TI |
| | | **Adquisición, mantenimiento e implementación de infraestructura de TI, sistemas de información y bases de datos** | |
| 53 | | | Procedimiento, instructivos y registros para la adquisición y desarrollo de activos de software y sus bases de datos |
| 54 | | | Procedimiento, instructivos y registros para la adquisición de activos de infraestructura |
| 55 | | | Procedimiento, instructivos y registros para la adquisición de servicios de telecomunicaciones |
| | | **Gestión de servicios de TI** | |
| 56 | | | Implementación de OLA`s con las principales áreas y clientes |
| 57 | | | Procedimiento de gestión de incidentes y su escalonamiento |
| 58 | | | Procedimiento para el análisis de factibilidad de proyectos |
| 59 | | | Procedimiento, instructivos y registros para el control de calidad del software y sus bases de datos |
| 60 | | | Procedimiento, instructivos y registros para la transición del software a las operaciones y sus bases de datos |
| 61 | | | Procedimiento, instructivos y registros para el control de calidad de la infraestructura |
| 62 | | | Procedimiento, instructivos y registros para la transición de la infraestructura a las operaciones |
| | | **Ciclo de vida de los sistemas de información** | |
| 63 | | | Manual DERCAS |
| 64 | | | Separación de ambientes y capacidades de desarrollo y producción |

| | | | |
|---|---|---|---|
| | **Seguridad de la tecnología de la información** | | |
| | | **Gestión de la seguridad de la información** | |
| 65 | | | Definir tabla de sensibilidad |
| 66 | | | Definir tabla de criticidad |
| 67 | | | Identificación de los principales activos de la TI con nivel de sensibilidad y criticidad |
| 68 | | | Procedimiento, instructivos y registros para el monitoreo del buen uso de activos críticos. |
| 69 | | | Procedimiento, instructivos y registros para el acceso físico a los activos y sistemas críticos |
| 70 | | | Procedimiento, instructivos y registros para el acceso lógico a los activos y sistemas críticos |
| 71 | | | Procedimiento, instructivos y registros para la administración de bitácoras en los sistemas críticos |
| 72 | | | Procedimiento, instructivos y registros para pruebas de intrusión y detección de vulnerabilidades en los sistemas críticos |
| 73 | | | Perfil y manual de funciones aprobado para el Oficial de seguridad o las veces de él |
| | | **Copias de respaldo** | |
| 74 | | | Procedimiento, instructivos y registros para el respaldo de las bases de datos |
| 75 | | | Procedimiento, instructivos y registros para el respaldo del sistema operativo |
| 76 | | | Procedimiento, instructivos y registros para el respaldo del las aplicaciones y su CMDB |
| 77 | | | Procedimiento, instructivos y registros para la restauración de respaldos de las bases de datos |
| 78 | | | Procedimiento, instructivos y registros para la restauración de respaldos del sistema operativo |
| 79 | | | Procedimiento, instructivos y registros para la restauración de respaldos aplicaciones y su CMDB |
| | | **Operaciones y servicios financieros a través de canales electrónicos** | |
| 80 | | | Implementar mecanismos para la protección de la infraestructura de los canales electrónicos |
| 81 | | | Implementar medidas de seguridad en el intercambio de información (Certificado Digital o Cifrado) |
| 82 | | | Programa semestral de concientización de clientes para el uso de canales electrónicos |
| 83 | | | Gestión de bitácoras de canales electrónicos |

| | | | | |
|---|---|---|---|---|
| | **Continuidad de operaciones de tecnología de la información** | | | |
| | | **Plan de continuidad de operaciones de TI** | | |
| 84 | | | Manual de continuidad del negocio (convenios internos, convenios con terceros, Plan de respuesta a emergencias, otros ) | |
| 85 | | | Procedimiento de reporte en caso de modificaciones al manual | |
| | | **Pruebas al plan de continuidad de operaciones de TI** | | |
| 86 | | | Procedimiento, instructivos y registros para las pruebas de la continuidad del negocio | |
| | | **Capacitación del personal clave para la continuidad de operaciones de TI** | | |
| 87 | | | Identificar al personal clave para la continuidad del negocio | |
| 88 | | | Procedimiento, instructivos y registros para las capacitación del personal clave de la continuidad del negocio | |
| | | **Centro de cómputo alterno** | | |
| 89 | | | Centro de cómputo alterno para la continuidad del negocio (infraestructura, bases de datos y sistemas de información) | |
| | **Procesamiento de la información y tercerización** | | | |
| | | **Procesamiento de la información** | | |
| 90 | | | Autorización para procesamiento externo de operaciones | |
| 91 | | | Centro de cómputo fuera del país (infraestructura, bases de datos, sistemas de información y personal capacitado) | |
| 92 | | | Replicación en línea a bases de datos locales | |
| | | **Tercerización** | | |
| 93 | | | Contrato de confidencialidad por tercerización de operaciones | |

## Anexo4
## Controles para un Servidor de Auditoría (Audit Server)

| MATRIZ DE CONTROLES, MONITOREO Y SEGURIDAD<br>AUDITORIA INTERNA | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *No.* | *Area del Proceso* | *Proceso* | *Reponsable del Proceso* | *Control* | *Query / Estrategia (Fuente de la Información)* | *Descripción Operativa* | *Objetivo* | *Peridiocidad* | *Estado o Madurez del Control* | *Fecha Cumplimiento* | *Tipo de Salida* | *Responsable del control* | *Mecanismo* | *Analisis a Realizar* | *Parametro, metricas o niveles de tolerancia* | *Campos mínimos Propuestos* |
| 1 | Riesgos y Procesos | Seguridad Fisica | Sud-director de R&P | Accesos a Areas Restringidas | Generar Archivo de Accesos No Permitidos. | Accesos no autorizados a areas restringidas, realizado por el personal de de la organización. | Validar los accesos no autorizados que se ejecutaron en el mes. | Mensual | **No lo Tengo** | 28/02/2013 | Grafica | Josué Chete | RP_Acessos No Validos | Analizar los acceso no autorizados que se generan mensualmente, identificando las areas mas expuestas y buscando la raiz de los intentos. | >3 | Fecha,hora, area, usuario. |
| 3 | Operaciones | Remesas | Sub-director JI | Archivos Check 21 sin encriptación | Archivo Txt, que incluya total de archivos generados y si cumplio estandar de encriptación. | Controlar si los archivos check 21 que se estan enviando cumplen con el proceso de encriptacion. | Verificar que se cumpla con la politica de encriptación de archivos de acuerdo a los estandares establecidos. | Diario | **No lo tengo** | 28/12/2013 | Alerta | Josué Chete | OP_Check21Encrip | Que riesgos se estan generando por no cumplir con la politica establecida. | Todos | Fecha, Nombre Archivo, usuario que envio. |
| 4 | Operaciones | Remesas | Supervisor JI | Matriz de Accesos | Generar Altas y Bajas de usuarios. | Verificar las altas y bajas de usuario en el aplicativo de forma mensual. | Tener un registro de las altas y bajas del aplicativo de manera oportuna. | Mensual | **No lo tengo** | 28/12/2013 | reporte | Josué Chete | OP_A&B_userremesas | Analizar las altas y bajas, con la finalidad de poder verificar si es razonable la cantidad de altas y bajas de usuario en el aplicativo. | >1 | Fecha, Usuario,Nombre, Apellido, Rol, quien dio de baja. |
| 6 | Contabilidad | Polizas Contables | Contador general | Polizas Reversadas Mensualmente | Excel con total de polizas reversadas trimestralmente. | Verificar trimestralmente las polizas reversadas por usuario y por fecha. | Verificar el % de polizas reversadas . | Trimestralmente | **No lo tengo** | 28/12/2013 | Excel reporte | Josué Chete | CG_PolRev | Analizar el porcentaje de polizas reversadas por usuario, para identificar el % de error que se esta dando contablemente. | >12 | Fecha, Poliza, Tipo de poliza, Descripción, Monto, Usuario, % de reversión. |
| 7 | Tecnología | Base de Datos | DBA | Sentencias no Autorizadas | Alerta de ejecución de sentencia no autorizada. | Sentencias no autorizadas que son ejecutadas por un tercero. | Garantizar la integridad de las bases de datos. | Diario | **No lo tengo** | 28/06/20103 | Alerta | Josué Chete | TI_SentenciasBD | Que las sentencias ejecutadas cuenten con la autorización correspondiente y no sean ejecutadas por terceros al DBA. | Todos | Fecha, Hora, usuario, base de datos, sentencia. |
| 8 | Tecnología | Seguridad Logica | Subdirector de Infraestructura | Puertos USB | Reporte de Puertos USB, abiertos sin autorizacion. | Verificar mensualmente los puertos USB que fueron abiertos y que no eran autorizados. | Garantizar la seguridad de la información en la red. | Mensual | **No lo tengo** | 28/06/20103 | Reporte | Josué Chete | TI_USB | Que no se esten permitiendo accesos a puertos cerrados a personal no autorizado para utilizarlos. | Todos | Fecha, Hora, Maquina, Usuario, accion realizada. |