



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Industrial

**DISEÑO DE UN MARCO INTEGRAL DE TRABAJO PARA GESTIONAR EL RIESGO
TECNOLÓGICO EN UNA ENTIDAD FINANCIERA SUPERVISADA POR LA
SUPERINTENDENCIA DE BANCOS DE GUATEMALA**

Jersson Ernie Fernández Mendizabal

Asesorado por el Ing. José Rolando Chávez Salazar

Guatemala, enero de 2018

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**DISEÑO DE UN MARCO INTEGRAL DE TRABAJO PARA GESTIONAR EL RIESGO
TECNOLÓGICO EN UNA ENTIDAD FINANCIERA SUPERVISADA POR LA
SUPERINTENDENCIA DE BANCOS DE GUATEMALA**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JERSSON ERNIE FERNÁNDEZ MENDIZABAL
ASESORADO POR EL ING. JOSÉ ROLANDO CHÁVEZ SALAZAR

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO INDUSTRIAL

GUATEMALA, ENERO DE 2018

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Oscar Humberto Galicia Nuñez
VOCAL V	Br. Carlos Enrique Gómez Dónis
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. José Francisco Gómez Rivera
EXAMINADOR	Ing. Oscar Estuardo de León Maldonado
EXAMINADOR	Ing. Sergio Roberto Barrios Sandoval
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la Ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

**DISEÑO DE UN MARCO INTEGRAL DE TRABAJO PARA GESTIONAR EL RIESGO
TECNOLÓGICO EN UNA ENTIDAD FINANCIERA SUPERVISADA POR LA
SUPERINTENDENCIA DE BANCOS DE GUATEMALA**

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Industrial, con fecha 28 de junio de 2016.



Jerссón Ernie Fernández Mendizabal

Guatemala, 18 de agosto de 2017

Ingeniero
José Francisco Gómez Rivera
Director
Escuela de Ingeniería Mecánica Industrial
Facultad de Ingeniería
Presente

Estimado Director de Escuela.

Por este medio hago constar que yo José Rolando Chávez Salazar, quien me identifico con el número de colegiado 4,317 he autorizado la última revisión del trabajo de graduación con el tema "**DISEÑO DE UN MARCO INTEGRAL DE TRABAJO PARA GESTIONAR EL RIESGO TECNOLÓGICO EN UNA ENTIDAD FINANCIERA SUPERVISADA POR LA SUPERINTENDENCIA DE BANCOS DE GUATEMALA**", presentado por el estudiante universitario Jersson Ernie Fernández Mendizabal, quien se identifica con el número de carnet 2009-15323, no teniendo más correcciones doy mi Vo. Bo.

Por lo que habiendo cumplido con los objetivos y requisitos de ley referido trabajo y existiendo la aprobación del mismo como Asesor y apruebo su contenido solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

*Ing. José Rolando Chávez Salazar
Acreditado
Ingeniero Industrial
Colegiado No. 4,317*

Ing. José Rolando Chávez Salazar

**UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA**

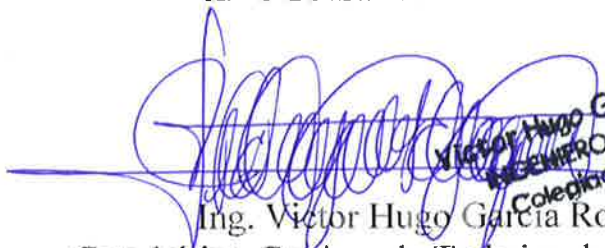


FACULTAD DE INGENIERÍA

REF.REV.EMI.151.017

Como Catedrático Revisor del Trabajo de Graduación titulado **DISEÑO DE UN MARCO INTEGRAL DE TRABAJO PARA GESTIONAR EL RIESGO TECNOLÓGICO EN UNA ENTIDAD FINANCIERA SUPERVISADA POR LA SUPERINTENDENCIA DE BANCOS DE GUATEMALA**, presentado por el estudiante universitario **Jersson Ernie Fernández Mendizabal**, apruebo el presente trabajo y recomiendo la autorización del mismo.

“ID Y ENSEÑAD A TODOS”


Victor Hugo García Roque
INGENIERO INDUSTRIAL
Colegiado No. 5133
Ing. Victor Hugo García Roque
Catedrático Revisor de Trabajos de Graduación
Escuela de Ingeniería Mecánica Industrial

Guatemala, octubre de 2017.

/mgp



REF.DIR.EMI.004.018

El Director de la Escuela de Ingeniería Mecánica Industrial de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el Visto Bueno del Revisor y la aprobación del Área de Lingüística del trabajo de graduación titulado **DISEÑO DE UN MARCO INTEGRAL DE TRABAJO PARA GESTIONAR EL RIESGO TECNOLÓGICO EN UNA ENTIDAD FINANCIERA SUPERVISADA POR LA SUPERINTENDENCIA DE BANCOS DE GUATEMALA**, presentado por el estudiante universitario **Jersson Ernie Fernández Mendizabal**, aprueba el presente trabajo y solicita la autorización del mismo.

“ID Y ENSEÑAD A TODOS”


Ing. Cesar Ernesto Urquiza Rodas
DIRECTOR a.i.
Escuela de Ingeniería Mecánica Industrial



Guatemala, enero de 2018.

/mgp

Universidad de San Carlos
de Guatemala



Facultad de Ingeniería
Decanato

DTG. 017.2018

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Industrial, al Trabajo de Graduación titulado: **DISEÑO DE UN MARCO INTEGRAL DE TRABAJO PARA GESTIONAR EL RIESGO TECNOLÓGICO EN UNA ENTIDAD FINANCIERA SUPERVISADA POR LA SUPERINTENDENCIA DE BANCOS DE GUATEMALA**, presentado por el estudiante universitario: **Jersson Ernie Fernández Mendizabal** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:


Ing. Pedro Antonio Aguilar Polanco
Decano

Guatemala, enero de 2018



/gdech

ACTO QUE DEDICO A:

Dios

Por ser mi fuerza motriz interior; por permitirme llegar a este momento tan especial en mi vida el cual he deseado con todo el corazón; además, por brindarme su amor y bondad.

Mis padres

Edgar Oliverio Fernández Rentería y Walkiria del Carmen Mendizabal Ramírez; por el amor y la paciencia con la que me educaron; por la fe con la cual me trasladaron sus valores que ahora han hecho de mí, un hombre de bien.

Mi hermana

Kryssia Walkiria Fernández Mendizabal, quien siempre ha estado a mi lado sin importar las circunstancias, por la ayuda que me ha proporcionado incondicionalmente.

Mi prometida

María Teresa Caballeros García, por el amor que todos los días me otorga desde que está a mi lado, porque nunca se cansa de comprenderme y ser mi soporte, mi compañera de vida y representar mis ganas de luchar para ser alguien.

Mi hijo

José André Fernández Caballeros, por
hacerme sentir que desde el cielo guía mis
pasos.

AGRADECIMIENTOS A:

**Universidad de San
Carlos de Guatemala**

Por ser el centro de enseñanza que inculcó en mí la responsabilidad, la conciencia, el trabajo, la humildad y la dedicación.

Facultad de Ingeniería

Por proporcionarme los conocimientos que ahora me permiten llevar el pan diario a mi hogar

**Ing. Pedro Luis Marroquín
Duarte**

Por ser un ejemplo para seguir y por darme la oportunidad de crecer profesionalmente y enseñarme a ver la vida desde un punto de vista práctico.

**Ing. Jorge Daniel Alfaro
Garcia**

Por sus innumerables e incansables consejos. Por trasladarme su invaluable formación y enseñarme que el trabajo se puede volver arte cuando se hace con el corazón.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	IX
LISTA DE SÍMBOLOS	XI
GLOSARIO	XIII
RESUMEN	XIX
OBJETIVOS.....	XXI
INTRODUCCIÓN	XXIII
1. ANTECEDENTES GENERALES	1
1.1. Entidad financiera	1
1.1.1. Ubicación.....	2
1.1.2. Historia	3
1.1.3. Misión	4
1.1.4. Visión.....	4
1.1.5. Valores	5
1.1.6. Organigrama.....	6
1.1.7. Consejo Directivo	7
1.1.8. Departamento de Tecnologías de Información.....	7
1.1.8.1. Antecedentes	8
1.1.8.2. Organigrama	9
1.1.8.3. Misión, visión y valores	10
1.1.8.4. Roles y responsabilidades	11
1.1.9. Gerencia de Administración de Riesgos y Procesos .	12
1.1.9.1. Roles y responsabilidades	13
1.2. Superintendencia de Bancos de Guatemala (SIB).....	13
1.2.1. Ubicación.....	14

1.2.2.	Historia	15
1.2.3.	Misión	15
1.2.4.	Visión	15
1.2.5.	Valores	16
1.2.6.	Organigrama	16
1.3.	Marco Teórico.....	18
1.3.1.	Definición de riesgos	18
1.3.2.	Tipos de riesgo.....	19
1.3.2.1.	Riesgos del entorno.....	19
1.3.2.2.	Riesgos generados en la empresa	20
1.3.3.	Definición de vulnerabilidades.....	22
1.3.4.	Regulaciones internacionales	23
1.3.5.	Regulaciones nacionales	25
1.3.6.	Enfoque de las entidades financieras del país	26
1.3.7.	Enfoque de seguridad de la información	27
1.3.8.	Enfoque de continuidad del negocio	28
1.4.	Metodologías para la gestión de riesgos tecnológicos	29
1.4.1.	COBIT 4.1 (Controles para Información y Tecnologías Relacionadas)	29
1.4.2.	MAGERIT (Análisis y Gestión de Riesgos de los Sistemas de Información).....	31
1.4.3.	Sistemas de Gestión	32
1.4.3.1.	ISO 20000 (Sistema de Gestión de Servicios de TI).....	32
1.4.3.2.	ISO 31000 (Sistema de Gestión de Riesgos)	33
1.4.3.3.	ISO 27001 (Sistema de Gestión de Seguridad de la Información).....	34

1.4.3.4.	ISO 22301 (Sistema de Gestión de Continuidad del Negocio).....	34
2.	SITUACIÓN ACTUAL	37
2.1.	Descripción de los servicios tecnológicos	37
2.2.	Descripción del Centro de Datos	39
2.2.1.	Ubicación.....	41
2.2.2.	Infraestructura física	41
2.2.3.	Gestión de capacidad	43
2.2.3.1.	Administración de la infraestructura tecnológica.....	44
2.2.4.	Sitio Alterno de Datos	45
2.2.5.	Gestión de configuración	47
2.3.	Descripción de los controles	48
2.3.1.	Seguridad física.....	48
2.3.2.	Seguridad lógica.....	51
2.4.	Presupuesto.....	53
2.5.	Atención de requerimientos e incidentes	55
2.5.1.	Gestión de solicitudes de servicio	55
2.5.1.1.	Canales de comunicación con el negocio	60
2.5.1.2.	Ciclo de vida de las solicitudes de servicio.....	60
2.5.2.	Administración de proveedores	63
2.5.3.	Acuerdos de nivel de servicio	64
2.5.4.	Acuerdos de nivel de operación	66
2.5.5.	Gestión de cambios.....	68
2.5.6.	Gestión de problemas.....	70
2.6.	Implementación de servicios nuevos o modificados	72

2.6.1.	Administración de proyectos	72
2.6.2.	Nuevas tecnologías.....	74
2.6.3.	Desarrollo de sistemas.....	77
2.6.4.	Administración de las bases de datos	80
2.6.5.	Aseguramiento de la calidad	82
2.6.6.	Liberación de servicios nuevos y modificados	83
2.7.	Análisis de desempeño.....	85
2.7.1.	Relación del negocio y tecnologías de información....	86
2.7.1.1.	Encuestas de satisfacción	87
2.7.2.	Gestión de disponibilidad y continuidad de los servicios	88
2.7.2.1.	Plan de Recuperación de Desastres (DRP).....	90
2.7.3.	Informes de desempeño.....	91
3.	PROPUESTA PARA DISEÑAR EL MARCO INTEGRAL DE TRABAJO PARA GESTIONAR EL RIESGO TECNOLÓGICO	93
3.1.	Organización para la administración del riesgo tecnológico	93
3.1.1.	Políticas y procedimientos.....	93
3.1.2.	Responsabilidades del Consejo Directivo	94
3.1.3.	Comité de Riesgos	95
3.1.4.	Departamento de Riesgos.....	96
3.1.5.	Planeación estratégica	97
3.1.6.	Planeación estratégica de tecnologías de información.....	98
3.2.	Recursos tecnológicos.....	99
3.2.1.	Clasificación de los recursos tecnológicos	99
3.2.2.	Mapas de interdependencia	100
3.2.3.	Base de datos de configuración	101

3.2.4.	Unidad de administración de bases de datos	103
3.2.5.	Monitoreo de los recursos tecnológicos.....	103
3.2.6.	Adquirir, mantener e implementar recursos tecnológicos.....	104
3.2.7.	Administración de los servicios tecnológicos.....	104
3.2.8.	Ciclo de vida de los sistemas de información	106
3.3.	Seguridad de la tecnología de información	107
3.3.1.	Seguridad de la información	107
3.3.1.1.	Identificación y clasificación de la información	108
3.3.2.	Copias de respaldo.....	109
3.3.3.	Protección de banca virtual	110
3.4.	Continuidad de los servicios tecnológicos.....	111
3.4.1.	Plan de continuidad de operaciones de tecnologías de información	112
3.4.1.1.	Plan de pruebas.....	113
3.4.1.2.	Preparación del personal clave.....	114
3.5.	Tercerización	114
3.5.1.	Procesamiento de información	114
3.5.2.	Proveedores	115
3.6.	Inversión inicial	116
4.	IMPLEMENTACIÓN DE LA PROPUESTA.....	119
4.1.	Creación de las políticas y los procedimientos	119
4.1.1.	Política de Gestión de Riesgo Integral.....	120
4.1.2.	Política general de administración de documentos de TI.....	122
4.1.3.	Política de clasificación de la información	125
4.1.4.	Política de seguridad de la información	131

4.1.5.	Acuerdos de Comité de Riesgos	134
4.1.6.	Acuerdos de Comité de Riesgo Operativo	135
4.2.	Gobierno corporativo y gobierno de TI	136
4.2.1.	Alinear la estrategia del negocio con la estrategia de TI	138
4.2.1.1.	Plan Estratégico de TI	138
4.3.	Análisis de Impacto de Negocios (BIA).....	140
4.3.1.	Identificación de las principales líneas de negocio...	143
4.3.2.	Identificación de los procesos críticos del negocio...	144
4.3.3.	Creación de los mapas de interdependencia tecnológica	147
4.4.	Organización de los activos tecnológicos	155
4.4.1.	Repositorio de base de datos de configuración	156
4.4.2.	Evaluación de desempeño y capacidad de los activos tecnológicos	160
4.4.2.1.	Plan de capacidad	165
4.4.3.	Jefatura de administración de bases de datos de información.....	169
4.5.	Administración de proveedores y contratos	171
4.5.1.	Definición de técnicas de selección de proveedores	174
4.5.2.	Procedimiento de contratación de proveedores	174
4.5.3.	Metodología de pruebas.....	176
4.5.4.	Creación de acuerdos de nivel de servicio.....	178
4.5.5.	Evaluación periódica de proveedores	179
4.6.	Manual de riesgo tecnológico	180
4.6.1.	Identificación del riesgo.....	181
4.6.2.	Análisis del riesgo	184
4.6.3.	Determinación del nivel de riesgo	185
4.6.4.	Priorización del riesgo	188

4.6.5.	Manejo del riesgo	189
5.	SEGUIMIENTO O MEJORA	193
5.1.	Resultados obtenidos.....	193
5.1.1.	Interpretación.....	194
5.2.	Evaluaciones periódicas	195
5.2.1.	Autoevaluación	195
5.2.2.	Auditorías internas.....	195
5.2.3.	Auditorías externas.....	196
5.3.	Medidas preventivas y correctivas	196
5.4.	Monitoreo y estadísticas	197
5.4.1.	Mensual.....	197
5.4.2.	Semestral	198
5.4.3.	Anual	198
	CONCLUSIONES	201
	RECOMENDACIONES	203
	BIBLIOGRAFÍA.....	205
	ANEXOS	207

ÍNDICE DE ILUSTRACIONES

FIGURAS

1.	Ubicación de la Entidad Financiera supervisada por la Superintendencia de Bancos de Guatemala.....	2
2.	Organigrama de la Entidad Financiera	6
3.	Organigrama del Departamento de Tecnologías de Información	10
4.	Ubicación de la Superintendencia de Bancos de Guatemala	14
5.	Organigrama general y funcional de la Superintendencia de Bancos de Guatemala	17
6.	Ubicación de la Sitio Alterno de Datos de la Entidad Financiera supervisada por la Superintendencia de Bancos de Guatemala	46
7.	Diagrama de Flujo de la Gestión de Solicitudes del Servicio.....	58
8.	Diagrama de Flujo del Subproceso de Investigación y Diagnóstico de la Gestión de Solicitudes del Servicio.	59
9.	Diagrama del ciclo de vida de la metodología de desarrollo de requerimientos nuevos.....	79
10.	Diagrama del ciclo de vida de la metodología de desarrollo para resolución de incidentes	80
11.	Esquema de Interrelación de Recursos Tecnológicos.....	151
12.	Esquema de Diagrama de Servicios Tecnológicos.....	154
13.	Primer Nivel –Objetivos de Control de COBIT 4.1-.....	183
14.	Segundo Nivel –Controles Implementados por el Departamento de Tecnologías de la Información-.....	183

TABLAS

I.	Índices de calificación de los usuarios sobre los servicios tecnológicos.....	88
II.	Elementos de la Base de Datos de Configuración.....	102
III.	Salarios de personal a contratar para la administración del riesgo tecnológico.....	117
IV.	Ubicación de Colaboradores para la administración de riesgo tecnológico.....	117
V.	Clasificación de documentos en Tecnologías de Información	125
VI.	Niveles de Impacto según sensibilidad de la información.....	127
VII.	Niveles de criticidad según la relación que guarda la información con los procesos de la Entidad Financiera	128
VIII.	Matriz de Clasificación de la Información, según su confidencialidad	129
IX.	Tipos de Impacto y nivel según los efectos producidos	142
X.	Grado de Criticidad de los procesos y subprocesos	145
XI.	Herramienta de Base de Datos de Configuración.....	157
XII.	Custodios de los activos tecnológicos en el Departamento de Tecnologías de la Información.....	160
XIII.	Umbrales establecidos para generar alertas, según el análisis de desempeño de los recursos utilizados en los activos tecnológicos ..	162
XIV.	Matriz del Modelo de Riesgo Tecnológico	188
XV.	Matriz de Calificación del Riesgo Tecnológico.....	189

LISTA DE SÍMBOLOS

Símbolo	Significado
\$	Dólar
=	Igual
>	Mayor
<	Menor
No.	Número
%	Porcentaje
Q	Quetzales

GLOSARIO

Antivirus	Sirve para evitar o combatir ataques cibernéticos en la red.
Auditoría	Es un examen crítico y sistemático que realiza un auditor o grupo de auditores independientes del sistema auditado, que puede ser a una persona, empresa, o producto, con el objeto de verificar que no existan errores en los mismos.
Auditorías Externas	Es el examen detallado, crítico y sistemático en una unidad económica, realizado por un Contador Público sin vínculos laborales con la empresa, con el objeto de emitir una opinión objetiva.
Auditorías internas	Actividad independiente y objetiva que supervisa para agregar valor y mejorar las operaciones de una empresa.
Bancos	Son entidades que se dedican a trabajar con el dinero, para lo cual reciben y tienen en su custodia depósitos hechos por las personas individuales y empresas, y así mismo, otorgan préstamos usando esos mismos recursos, actividad que se denomina intermediación financiera.

Bancos de Guatemala	Es el Banco Central de la República de Guatemala.
Bases de datos	Es un conjunto de información ordenada de manera que un programa ordenador pueda seleccionar rápidamente los de datos que necesite. También se puede definir como un sistema de archivos electrónico.
Centro de Datos	Es donde se procesa toda la información digital que generan y resguardan las unidades operativas de una empresa.
Diagrama	Es una representación gráfica de variaciones de un suceso y analiza las relaciones que tienen los elementos en las partes de un conjunto.
DRP	Plan de Recuperación de Desastres.
Entidad Financiera	Son intermediarios que administran y prestan dinero a personas individuales, empresas públicas o privadas, pueden ser: bancos, cajas de ahorros o cooperativas de crédito, o cualquier tipo de intermediarios financieros que, sin ser bancos, brindan préstamos, facilidades de financiamiento o dinero.

Estructura organizacional	Es el sistema utilizado para delimitar una jerarquía dentro de una empresa. Identifica cada puesto, su función, así como dónde y a quien se reporta dentro del área de trabajo de la empresa.
Gestión	Trámite que, junto con otros, se lleva a cabo para conseguir o resolver un problema determinado.
Gestión de Riesgos	Sirve para manejar la incertidumbre de amenaza, a través de una serie de actividades que incluyen evaluación de riesgo, estrategias de desarrollo para así manejar y mitigar los riesgos en una empresa.
Hardware	Es el conjunto de elementos físicos o tangibles que constituyen un computador o determinado sistema informático.
IEC	Comisión Electrotécnica Internacional.
Internet	Es la Red que interconecta las computadoras, teléfonos móviles, tabletas, impresoras y todo dispositivo que pueda tener una tarjeta de red.
Inversión	Se le denomina a la aportación de un capital para obtener una ganancia futura. Esta aportación supone un beneficio inmediato o a futuro.

ISACA	Asociación de Auditoría y Control de Sistemas de Información.
ISO	Organización Internacional para la Estandarización.
Junta Monetaria	Es la máxima autoridad del Banco de Guatemala. Las decisiones y actos de la Junta Monetaria están sujetos a los recursos administrativos.
NEC	Código Eléctrico Nacional.
OFAC	Es la Oficina de Control de Activos estadounidense (Office of Foreign Assets) es la organización dependiente del Ministerio de Hacienda de Estados Unidos.
ONU	Es la organización internacional constituida por 192 países soberanos. Estos se reúnen libremente para trabajar juntos a favor de la lucha contra la pobreza, la injusticia en el mundo la paz y seguridad de los mismos.
Regulación	Ajustar o poner en orden algo, normar el funcionamiento de un sistema, con reglas. El término suele utilizarse como sinónimo de una normativa.

Resolución	Acción procesal que surge en el marco legal y que resuelve contiendas de las partes involucradas, ordenando el cumplimiento de la misma.
RTU	Registro Tributario Unificado.
Software	Es el conjunto de programas y rutinas que permiten a un computador realizar diferentes tareas.
Superintendencia de Bancos de Guatemala	Es la entidad técnica encargada de ejercer la vigilancia e inspección de los bancos, empresas financieras, entidades afianzadoras, instituciones de crédito y seguros, así como otras instituciones financieras establecidas por la ley como: el sistema financiero nacional.
Tecnologías	Es un conjunto de conocimientos técnicos, científicamente ordenados, que permiten diseñar bienes, servicios que simplifiquen la adaptación del medio ambiente y la satisfacción de necesidades esenciales.

RESUMEN

El presente trabajo de investigación se realizó con el propósito de identificar, medir, monitorear, controlar y prevenir los riesgos tecnológicos, aumentando los beneficios de las tecnologías de información y minimizando los costos de operación.

Ante la inevitable creciente demanda de los servicios que dependen de la tecnología, aumenta la probabilidad de que las organizaciones no cumplan con las obligaciones contractuales pactadas con sus clientes y como resultado se vean afectados en los estados financieros. Existen muchos factores que se deben considerar para evitar la materialización de un riesgo, es por ello que, con todas las herramientas proporcionadas por la ingeniería, se planteó un conjunto de procesos que faciliten controlar los diferentes componentes de la infraestructura tecnológica.

Siguiendo la premisa anterior es importante resaltar, que el riesgo de origen tecnológico puede incidir sobre las metas y objetivos organizacionales, así como puede ser causa de otro tipo de riesgos al ser intrínseco el uso de tecnología. Por ello el daño, interrupción, alteración o falla derivada del uso de tecnologías de información puede implicar dificultades significativas en las organizaciones; tales como pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización, asimismo causar inconvenientes a nivel operativo y estratégico.

OBJETIVOS

General

Diseñar un marco integral de trabajo para gestionar el riesgo tecnológico en una entidad financiera supervisada por la Superintendencia de Bancos de Guatemala.

Específicos

1. Optimizar la efectividad y eficiencia de los recursos tecnológicos que soportan los procesos críticos de las principales líneas de negocio en una entidad financiera.
2. Identificar y visualizar de forma detallada y precisa los riesgos tecnológicos que pueden afectar el cumplimiento de los objetivos de la organización.
3. Identificar, medir, monitorear, controlar y prevenir los riesgos que puedan comprometer la continuidad del negocio.
4. Garantizar la seguridad de la información para no comprometer la imagen reputacional de la organización.
5. Plantear políticas, procedimientos, metodologías, herramientas y modelos que permitan gestionar el riesgo tecnológico en una entidad financiera.

6. Integrar los procesos del negocio, los servicios de tecnologías de la información y el recurso humano, a fin de cumplir con los objetivos de la organización.
7. Cumplir con el Reglamento para la Administración del Riesgo Tecnológico (Resolución JM-102-2011), emitido por la Junta Monetaria.

INTRODUCCIÓN

Actualmente la entidad financiera supervisada por la Superintendencia de Bancos de Guatemala emplea las tecnologías de información, con el fin de registrar todos los datos relacionados con el giro del negocio. Entre la información que la organización resguarda a través de la tecnología se puede mencionar todo lo referente a sus clientes, empleados, proveedores, partes interesadas, productos, servicios, logística, operaciones, procesos, entre otros.

En términos generales, se depende en alto grado de la tecnología para el desarrollo normal de las actividades y ello posibilita puntos de ruptura y/o vulnerabilidades en cuanto a seguridad o disponibilidad de todos los productos o servicios que se ofrecen a los clientes, por esta razón se hace necesario gestionar adecuadamente el riesgo tecnológico para asegurar y/o garantizar la integridad, disponibilidad, confidencialidad de la información así como también la continuidad de la prestación de los servicios, para impedir que se pueda incurrir en pérdidas financieras.

A pesar de que, los avances tecnológicos han reducido muchos costos en las diferentes industrias, adaptándose a las nuevas necesidades de las entidades y dando lugar a otras relacionadas con su operación diaria; en el negocio bancario las reglas simples del manejo de riesgo continúan siendo vitales, por ende, cabe resaltar que los beneficios de la administración apropiada del riesgo son las pérdidas que se evitan y no la generación de las ganancias adicionales.

En el presente trabajo de graduación, se plantea un conjunto de controles estratégicos que se deben tomar en consideración, como una forma de aseguramiento sobre la infraestructura tecnológica (nivel físico), sistemas de información (nivel lógico) y las medidas organizacionales (factor humano), que permitan utilizar efectiva y eficientemente los recursos tecnológicos y minimizar el impacto si se llegará a materializar un evento no deseado.

1. ANTECEDENTES GENERALES

1.1. Entidad financiera

La entidad financiera supervisada por la Superintendencia de Bancos de Guatemala a la cual se refiere el presente trabajo de graduación, de ahora en adelante la entidad financiera, el grupo, la organización, la institución, la empresa, la sociedad, la compañía o sólo la entidad; se encuentra conformada dentro del mercado financiero de Guatemala, en el sector formal (regulado), cuya autorización es de carácter estatal, bajo el criterio de caso por caso, por tal razón es un órgano facultado que está sujeto a la supervisión de la Superintendencia de Bancos de Guatemala.

La institución financiera abarca los sistemas bancarios y no bancarios, está constituida por un banco comercial especializado en operaciones crediticias, mercantiles, monetarias, cambiarias, fiduciarias y de inversión; asimismo por compañías de seguros, compañías de fianzas, entre otros, estas últimas regidas por leyes específicas.

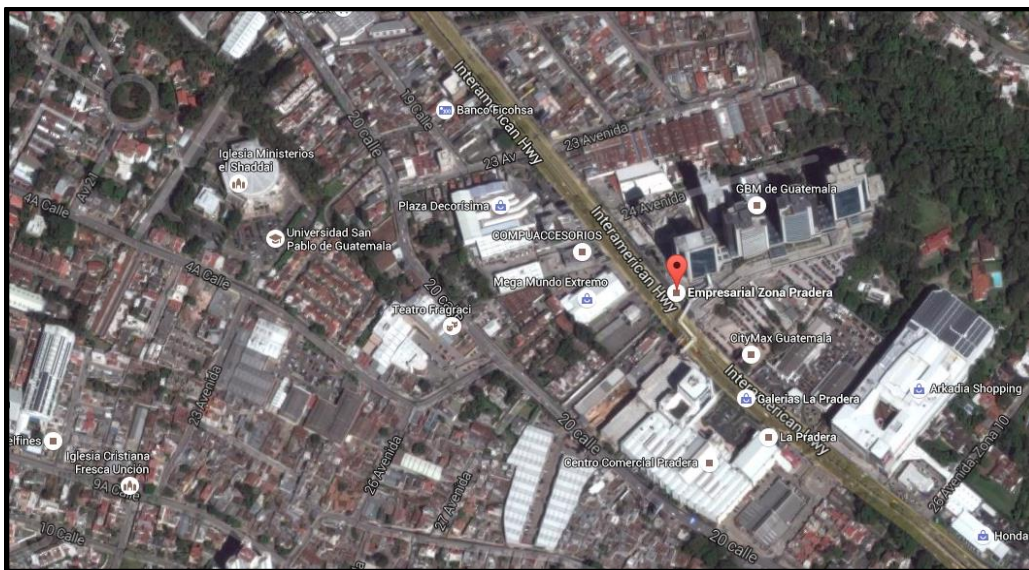
El grupo es un conglomerado de diferentes empresas que ofrece a una diversa base de entidades e individuos, un amplio portafolio de productos y servicios financieros que tienen un modelo de negocio fundamentado en el concepto de una “Banca más Humana”, en donde las relaciones de confianza, que construye con sus clientes son el eje fundamental para lograr prosperidad social, crecimiento, eficiencia y sostenibilidad para la organización.

Durante los años que ha operado en el mercado financiero de Guatemala, la Institución ha crecido de manera sostenible, generando valor compartido en lo económico, social y ambiental. Es una institución cada vez más grande, que provee varios servicios financieros, con el fin de aportar a sus clientes las soluciones bancarias que se adapten a sus necesidades actuales y les pueda ayudar a tomar las mejores decisiones que logren impactar positivamente en su vida.

1.1.1. Ubicación

La oficina central de la organización se encuentra ubicada en Boulevard Los Próceres 24-69 zona 10, Empresarial Zona Pradera Torre 3 oficina 917, ciudad de Guatemala, Guatemala Centroamérica.

Figura 1. **Ubicación de la entidad financiera supervisada por la Superintendencia de Bancos de Guatemala**



Fuente: Google/maps.com, captura satelital realizada el 16 de septiembre de 2015.

1.1.2. Historia

La institución financiera, surge de la fusión de dos entidades bancarias de sólido prestigio y larga tradición. Los orígenes se remontan al 30 de junio de 1926, cuando fue creado el Banco Central de Guatemala, que absorbió las funciones de la Caja Reguladora, entidad encargada de velar por la estabilidad internacional de la moneda, capitalizándose con aportes del Gobierno, pero con mayoría de la iniciativa privada.

Se realiza la primera sesión solemne de la nueva institución el 5 de julio de 1926, el 15 de septiembre de 1926 a las tres de la tarde, se realiza la primera sesión de trabajo de la Junta Directiva e inicia sus operaciones con el público. Como Banco Central inició la emisión de la nueva y actual unidad monetaria de Guatemala, "El Quetzal". Desde 1926 hasta 1945 la sociedad tuvo a su cargo la regulación de la emisión monetaria oficial y por ser el agente financiero del estado, también tuvo a su cargo, entre otros casos de relevancia histórica, la cancelación de la denominada "Deuda Inglesa".

El Gobierno de la Revolución de 1944 instituye el actual Banco de Guatemala, que asumió las funciones de Banco Central, por lo que el 10. de febrero de 1948 se renombró la institución, dando continuidad a la tradición de crédito y confianza del público guatemalteco. A mediados de la década de los cincuentas, un grupo de agricultores progresistas tuvo la visión de crear una nueva institución bancaria que diera soporte a esta importante actividad económica en el país. Con el aval del Gobierno, esta nueva institución abrió sus puertas al público el 16 de agosto de 1956.

Esta Institución se capitalizó con el aporte de más de 4 000 agricultores, quienes a partir de entonces, gracias al apoyo brindado al sector agrícola y la confianza que ha merecido el público, inició una etapa de crecimiento que le llevó a ocupar un lugar protagónico dentro del sistema bancario nacional. El treinta de noviembre del año 2000, como entidad fusionada, inicia una nueva etapa y con ello busca contribuir al fortalecimiento del sistema financiero y la promoción de nuevas oportunidades de inversión y empleo.

Como genuino heredero de una sólida y confiable tradición bancaria, y con la experiencia de más de 80 años de servicio a los guatemaltecos y centroamericanos, es una de las Entidades Financieras más accesible y confiable del país.

1.1.3. Misión

“Pertener genuinamente a esa nueva generación de organizaciones que no diferencian entre los negocios y la relación con la sociedad, que buscan crear relaciones más empáticas con todos sus grupos de interés; emprendiendo una renovación organizacional hacia el cumplimiento de un propósito denominado “una Banca más Humana”, un modelo de gestión que busca crear mayor conexión y compromiso social. No solo ser un actor económico sino un actor social, que ayuda a organizar mejor la sociedad, en pocas palabras: ser una Banca más Humana y Sostenible”.

1.1.4. Visión

“Ser una entidad financiera firme y sólida que continúe creciendo de forma rentable y sostenible, empleando los modelos de organización innovadora y confiable, que pone a las personas y a las relaciones en el centro”.

1.1.5. Valores

La organización cuenta con una consistente cultura corporativa que define la vida de la organización, incidiendo en su manera de actuar y permitiendo afrontar con éxito los retos del futuro.

Los empleados de la empresa, en sus relaciones diarias con los clientes, son la voz de la marca y los creadores de la “Banca más Humana”. Más allá de las relaciones comerciales, de la actividad en el sector financiero, en la institución se tiene claro que se está trabajando por un futuro mejor para las personas.

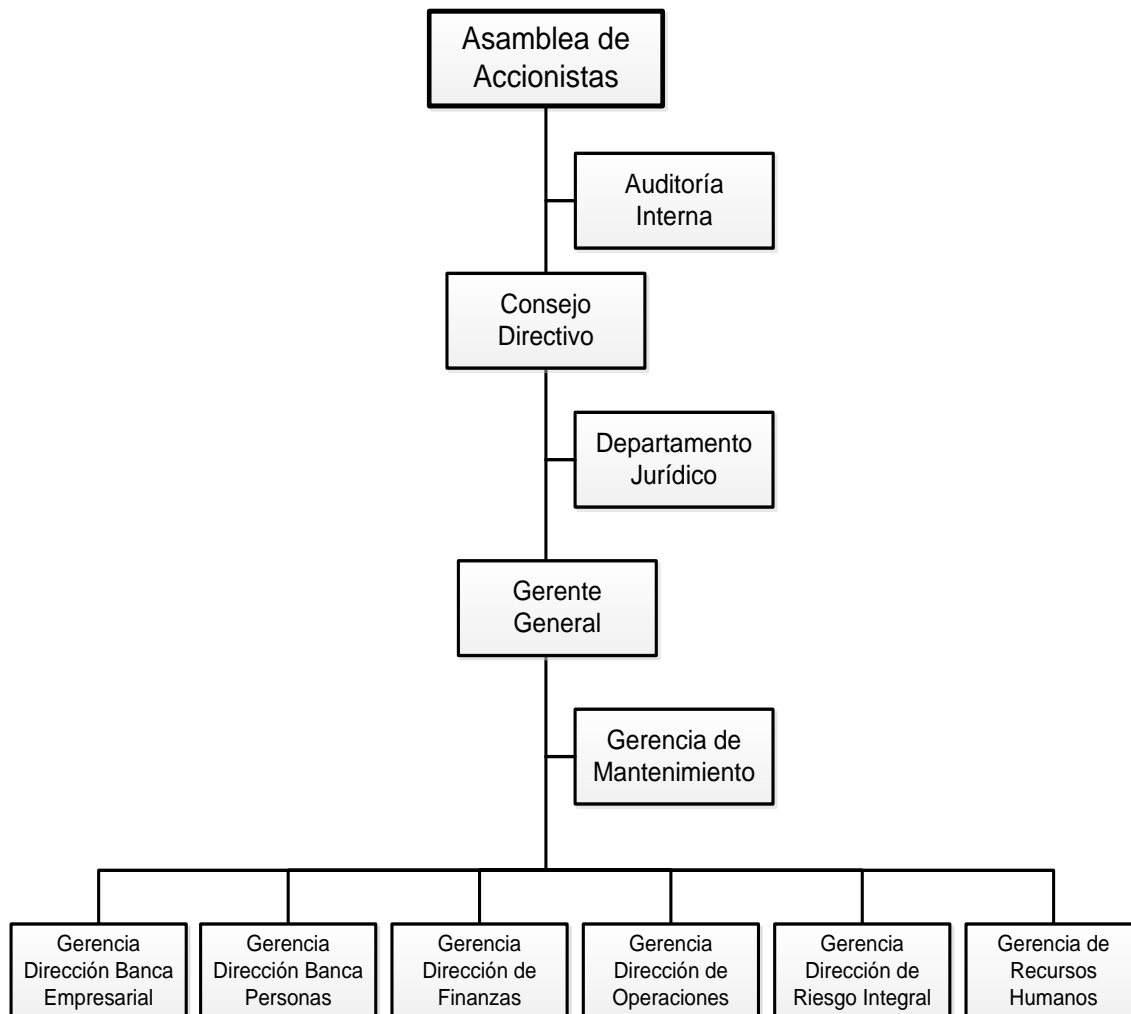
Para desarrollar esa cultura se establecieron los siguientes valores corporativos, que se materializan en compromisos con los clientes, con los empleados, con los accionistas y con la sociedad en general, y se concretan en criterios operativos:

- Calidez: el compromiso que se tiene de crear experiencias gratas con todas las personas con las cuales se relaciona la institución.
- Cercanía: la convicción de reconocer al otro como ser humano, interesarse por sus emociones, escucharlo y construir una relación de largo plazo.
- Inclusión: construir, con acciones, una banca en la que todos sean importantes y se encuentren involucrados para hacer una sociedad justa y equitativa.
- Respeto: sensibilidad que se refleja en el comportamiento para situarse en el lugar del otro, interesarse por sus emociones, ser receptivos con sus necesidades y hacer de la confianza la base fundamental de las relaciones construidas.

1.1.6. Organigrama

La estructura organizacional de la institución es de tipo lineal y cada puesto de trabajo cuenta con personal calificado de acuerdo a los perfiles de puesto establecidos por la Gerencia de Recursos Humanos.

Figura 2. **Organigrama de la Entidad Financiera**



Fuente: Entidad Financiera supervisada por la Superintendencia de Bancos de Guatemala.

1.1.7. Consejo Directivo

El Consejo Directivo y/o Consejo de Administración tiene todas las facultades que reconoce el Código de Comercio de la República de Guatemala, asimismo tiene como principal objetivo que se debata entre sus miembros las decisiones importantes del grupo, y que se marquen las directrices de funcionamiento al equipo ejecutivo. Todos los consejeros deben actuar en interés de la sociedad y de sus accionistas y tienen la misma responsabilidad por las decisiones del consejo.

1.1.8. Departamento de Tecnologías de Información

El Departamento de Tecnologías de la Información desempeña una de las funciones críticas que le permite a la entidad, proporcionar los diferentes servicios a sus clientes y todos los grupos de interés, esto se debe a que, la institución considera la información que custodia, como uno de los activos más importantes.

El Departamento de Tecnología de la Información es el que provee la disponibilidad de toda la infraestructura tecnológica donde se resguardan los datos de todos los grupos de interés, para esta labor se considera que dicha información debe ser confiable, íntegra y confidencial.

El Departamento de Tecnologías de Información ha trabajado en el desarrollo de diferentes herramientas que han permitido agilizar los procesos; optimizando la fluidez en el intercambio de información con las áreas operativas y de negocio, asimismo la integración de diferentes sistemas informáticos, que reducen el uso excesivo de documentos impresos y facilitan el acceso a la información a quienes tienen el privilegio.

1.1.8.1. Antecedentes

En septiembre del año 2010 el Consejo Directivo de la entidad financiera aprobó una suma importante para la construcción de un Centro de Datos, renovando la red de área local y la red de área ancha, asimismo se inició con la inversión de diferentes proyectos relacionados, la adopción de metodologías para la aplicación de buenas prácticas y estándares internacionales en temas de tecnologías de información.

Meses más tarde en 2011 se creó una figura de aseguramiento de la calidad del software, con base a las necesidades de optimizar la administración de los proyectos; establecer una metodología para el proceso de desarrollo de sistemas informáticos y la atención de incidentes por indisponibilidad de servicios tecnológicos. En este mismo año se inició con la documentación de los procesos y procedimientos más relevantes y se establecieron lineamientos que fueron autorizados como políticas para el buen funcionamiento de la infraestructura tecnológica.

En el 2012 la materialización de riesgos potenciales a los diferentes activos tecnológicos era inherente a las operaciones realizadas, por tal razón fue necesario implementar buenas prácticas que redujeran o mitigaran vulnerabilidades, este plan de acción se convirtió en un proyecto que posteriormente se delegó a un área en particular, generando así nuevos puestos de trabajo.

A mediados del 2012 el Departamento de Tecnologías de la Información se involucró en temas de operación institucional, haciendo énfasis en el control de tareas y proyectos para planificar de mejor forma las actividades a corto y mediano plazo, considerando la medición del desempeño y eficiencia de

manera objetiva y mejorando la organización de los procesos de requerimientos basados en estándares internacionales.

En el 2013 el Consejo Directivo aprobó una nueva suma para habilitar un Centro de Datos alterno con infraestructura tecnológica que soportará los servicios tecnológicos más críticos para la entidad, esta habilitación se realizó a en un sitio físico distinto en donde se construyó el Centro de Datos principal.

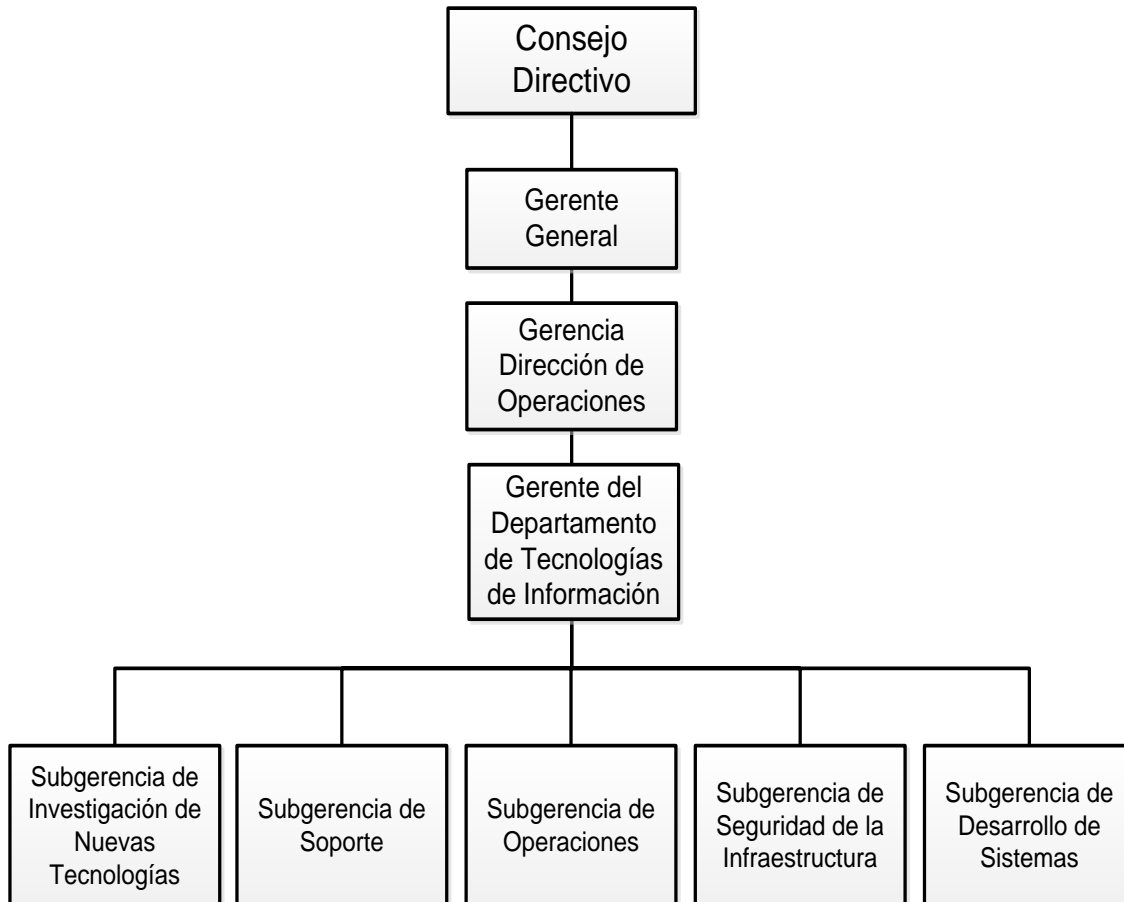
En los años 2014 y 2015 el Departamento de Tecnologías de la Información implementó distintos marcos de trabajo para administrar modelos de seguridad de la información, continuidad de operaciones de sistemas informáticos y un sistema de gestión integral para la provisión de servicios tecnológicos.

Actualmente el Departamento de Tecnologías de Información es el encargado de custodiar toda la información que se encuentra dentro de los sistemas, bases de datos, servidores, computadoras, respaldos y cualquier otro dispositivo de cómputo de la entidad financiera.

1.1.8.2. Organigrama

La estructura organizacional del Departamento de Tecnologías de Información es de tipo lineal y cada puesto de trabajo cuenta con personal calificado de acuerdo a los perfiles de puesto establecidos por la Gerencia de Recursos Humanos de la institución.

Figura 3. **Organigrama del Departamento de Tecnologías de Información**



Fuente: Entidad Financiera supervisada por la Superintendencia de Bancos de Guatemala.

1.1.8.3. Misión, visión y valores

La misión del Departamento de Tecnologías de la Información es: “Innovar, proveer y soportar la infraestructura tecnológica de la entidad financiera, orientada a los objetivos estratégicos del negocio”.

La visión del Departamento de Tecnologías de la Información es: “Ser el pilar tecnológico en el que se apoye el crecimiento de la institución, utilizando las buenas prácticas y estándares internacionales”.

El Departamento de Tecnologías de la Información ha plasmado todos sus valores en la siguiente política: “Somos proveedores de servicios de tecnología, orientados a la satisfacción de los usuarios. Mediante la aplicación del Sistema de Gestión de Servicios basado en la Norma internacional ISO/IEC 20000-1:2011 buscamos la mejora continua de manera oportuna, asegurando una posición competitiva, sólida, rentable y sostenible al automatizar los procesos para hacer realidad la promesa básica de nuestros grupos de interés”.

1.1.8.4. Roles y responsabilidades

Las funciones y responsabilidades generales del Departamento de Tecnologías de Información son las siguientes:

- Innovar, diseñar implementar evaluar sistemas informáticos del grupo, los cuales le permitan automatizar los procesos de negocio y generar competitividad en el país.
- Proporcionar soporte para el procesamiento de la información generada por las áreas operativas y de negocio de la entidad financiera.
- Proporcionar los medios de comunicación informática, tales como la red de área local, red de banda ancha, voz IP, entre otros.
- Establecer las acciones que garanticen la integridad, disponibilidad y confidencialidad de la información resguardada en la infraestructura tecnológica de la organización.

- Evaluar y optimizar el uso de los recursos tecnológicos informáticos, mejorando los procesos a su cargo, recomendando y/o disponiendo cuando se requiera de las acciones preventivas y correctivas.
- Implementar las disposiciones que emitan los entes legales y regulatorios relacionados con tecnología de la información y todo lo que se incluya en el ámbito de su competencia, dentro de los plazos requeridos.
- Provisionar los diferentes servicios tecnológicos y mantener un nivel aceptable en la disponibilidad de los mismos.
- Implementar metodologías, estándares y/o marcos de trabajo que permitan mejorar continuamente la efectividad y eficiencia de los servicios tecnológicos.
- Administrar las bases de datos de todos los sistemas informáticos del grupo, manteniendo un nivel de seguridad, respaldo y recuperación de las mismas.
- Gestionar la compra y mantenimiento de la infraestructura tecnológica de la empresa.
- Proveer el soporte de los equipos de cómputo conectados en la red interna de la compañía.

1.1.9. Gerencia de Administración de Riesgos y Procesos

La Gerencia de Administración Integral de Riesgos y Procesos es también tipificada como la Gerencia Dirección de Riesgo Integral dentro de la estructura organizacional de la sociedad, es el área responsable del diseño de políticas, sistemas, metodologías, modelos, procedimientos que permiten una efectiva gestión integral de los riesgos (crediticio, de mercado, liquidez, operativo, legal y otros).

1.1.9.1. Roles y responsabilidades

Es el área que tiene a cargo la responsabilidad de identificar, medir, monitorear, controlar, mitigar y divulgar todos los riesgos (crediticio, de mercado, liquidez, operativo, legal y otros) que enfrenta la institución. Esta unidad es independiente de todas las áreas operativas y de negocio, esto con el fin de evitar cualquier conflicto de interés y asegurar una adecuada separación de roles.

Su tamaño y alcance se encuentra directamente relacionado con el tamaño, volumen, estructura del grupo y complejidad de los riesgos en los cuales incurre.

1.2. Superintendencia de Bancos de Guatemala (SIB)

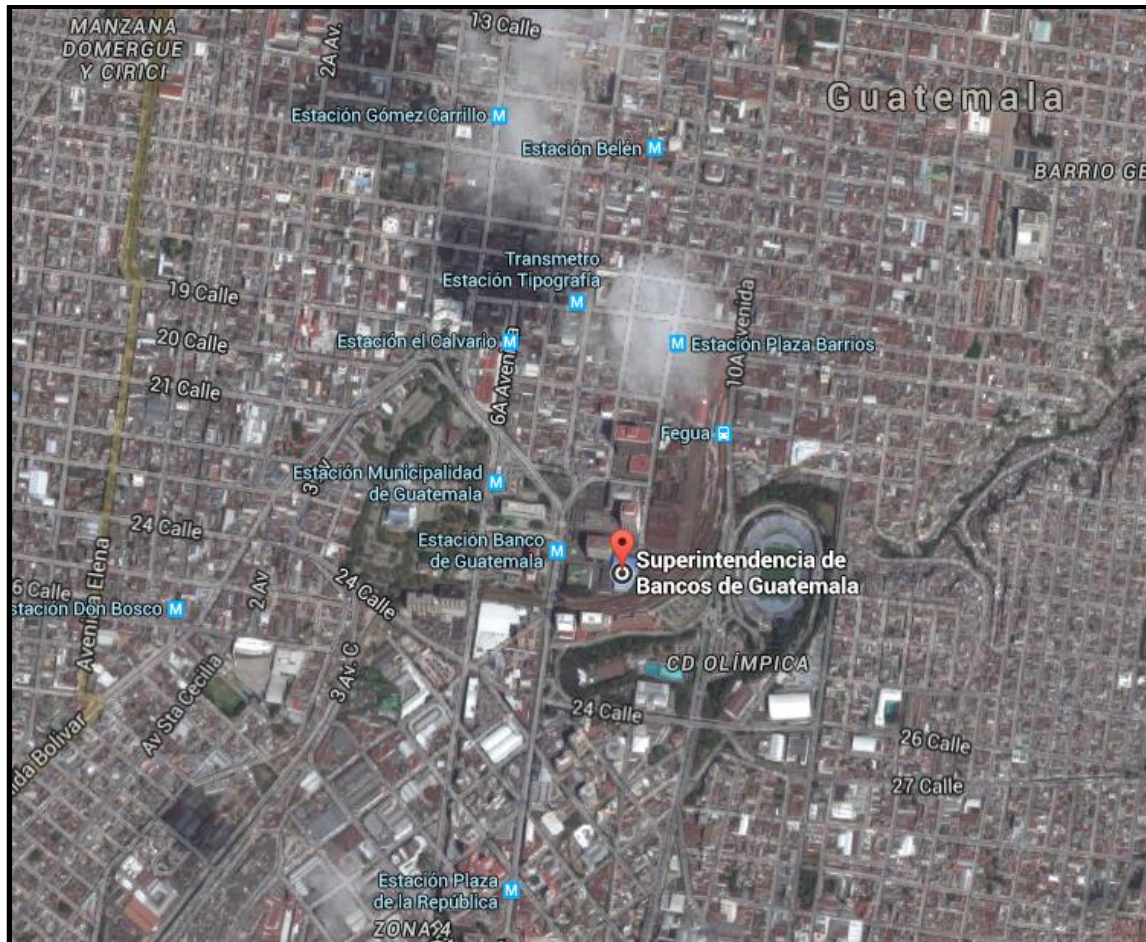
Es el órgano técnico creado por el estado, según el Decreto 18-2002 del Congreso de la República de Guatemala, que debe ejercer supervisión y vigilancia sobre los bancos, instituciones de crédito, empresas financieras, entidades afianzadoras, de seguros y otras instituciones financieras establecidas por la ley, que operan en el sistema financiero nacional. Esta entidad se encuentra regida por la Constitución, la Ley de la Supervisión Financiera, la Ley Orgánica del Banco de Guatemala, la Ley Monetaria y otras leyes. La Superintendencia de Bancos de Guatemala actúa bajo la dirección de la Junta Monetaria.

El concepto general, la supervisión y todas las funciones de la Superintendencia de Bancos de Guatemala se establecen en la Ley de Supervisión Financiera.

1.2.1. Ubicación

Las oficinas centrales de la Superintendencia de Bancos de Guatemala se encuentran ubicadas en 9A Avenida 22-00 zona 1, entrada por el callejón del edificio de Tribunales, ciudad de Guatemala, Guatemala Centroamérica.

Figura 4. Ubicación de la Superintendencia de Bancos de Guatemala



Fuente: Google/maps.com, captura satelital realizada el 16 de septiembre de 2015.

1.2.2. Historia

La Superintendencia de Bancos de Guatemala fue fundada en 1946, según lo describe el capítulo X, de la primera memoria de labores del Banco de Guatemala, correspondiente al período julio a diciembre de ese mismo año. Se dispuso en ese entonces, que el nombramiento del Superintendente de Bancos, debe provenir de una terna que la Junta Monetaria proponga al Tribunal y Contraloría de Cuentas.

El nombramiento inicial recayó en el señor José Joaquín Prieto Barrios, elemento que antes formaba parte del Departamento Monetario y Bancario del Ministerio de Economía y Trabajo. En la organización inicial, existía la oficina del Superintendente, y cuatro secciones principales: auditoría; estadística; jurídica; y, secretaría y archivo general.

Las labores de la Superintendencia de Bancos tuvieron formal principio el 2 de septiembre de 1946, siendo entre sus principales objetivos la estandarización de la nomenclatura contable del sistema bancario, como en el mecanismo de operación de los mismos.

1.2.3. Misión

“Promover la estabilidad y confianza en el sistema financiero supervisado”

1.2.4. Visión

“Ser una entidad de reconocida credibilidad y prestigio, que realiza una supervisión efectiva conforme a estándares internacionales, con personal calificado y comprometido con los valores institucionales”.

1.2.5. Valores

Los aspectos de fundamental importancia para la Superintendencia de Bancos de Guatemala, son las creencias y valores de la organización, las cuales quedaron resumidas e integradas en un Credo Institucional, que refleja en toda su dimensión, la calidad en cuanto a su conformación. Este credo tiene plasmado:

"CREO en la Superintendencia de Bancos, en su misión, en los principios filosóficos de su creación y en la función que realiza para lograr el desarrollo del sistema financiero del país, con excelencia y probidad.

CREO en la trascendencia de la misión de la Superintendencia de Bancos, y que en el cumplimiento de la misma, realiza una función social de reconocida importancia para el país.

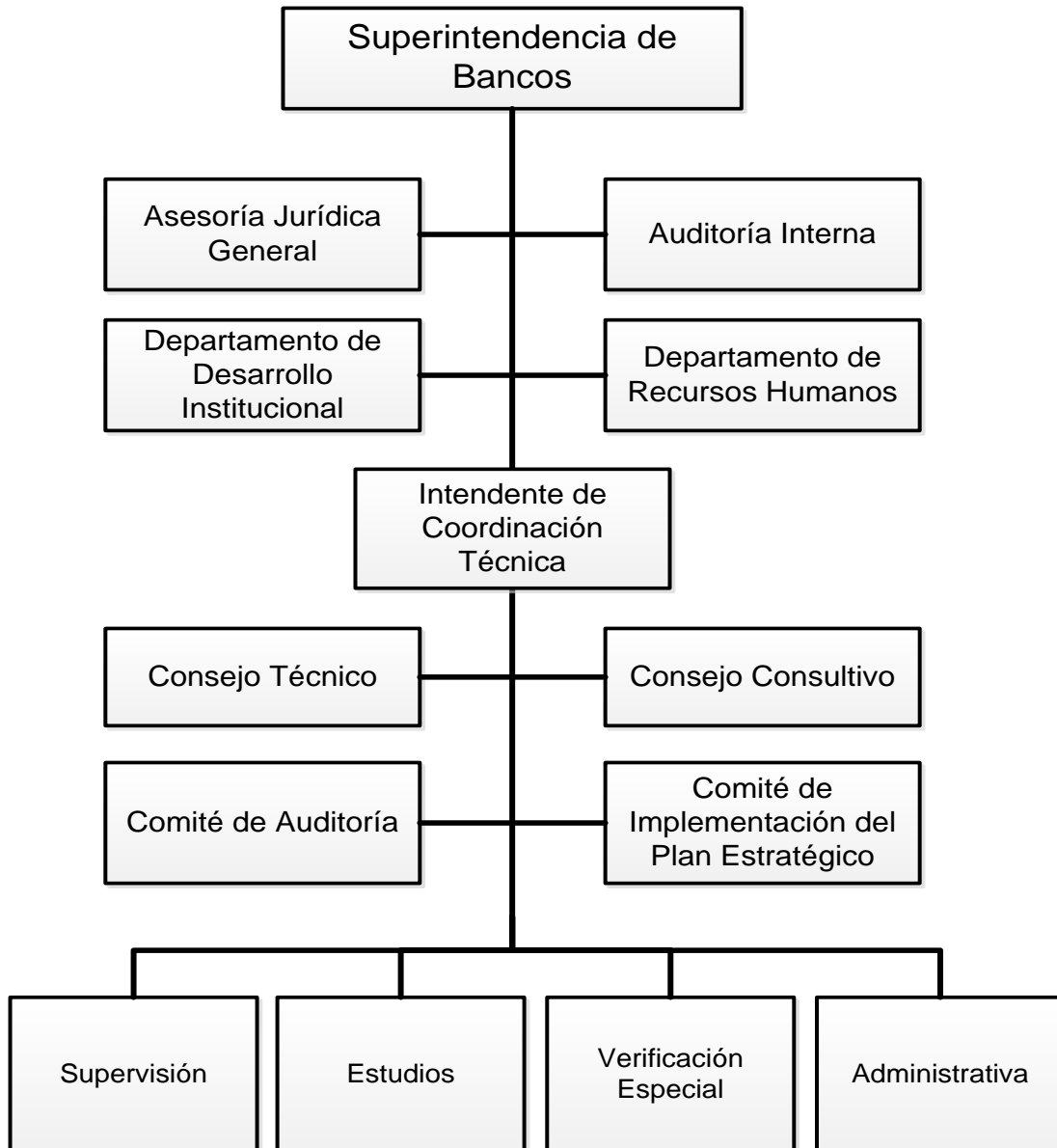
CREO en sus valores acuñados, y en el respeto y prestigio obtenido tanto a nivel nacional como internacional.

CREO en su más valioso recurso, su personal, identificado con la filosofía y los fines institucionales, comprometido y solidario, altamente calificado, responsable, honesto y disciplinado."

1.2.6. Organigrama

La estructura organizacional de la Superintendencia de Bancos está diseñada de tal manera, que apoye la implementación del modelo de supervisión y la estrategia definida.

Figura 5. **Organigrama general y funcional de la Superintendencia de Bancos de Guatemala**



Fuente: <http://www.sib.gob.gt/>.

1.3. Marco Teórico

A continuación se presenta una serie de definiciones que se deben considerar para comprender el entorno de riesgos inherentes en la operación de la entidad financiera supervisada por la Superintendencia de Bancos de Guatemala.

1.3.1. Definición de riesgos

Existen diferentes definiciones de riesgo que lo explican con distintas palabras, acordando todas y llegando a un mismo fin.

- El riesgo en general, está definido como la probabilidad de que una amenaza, peligro o incertidumbre, a que se ve enfrentada una persona o institución, por efecto o acción relacionada con sus líneas de negocio, operaciones y demás actividades, que pudieran afectar su situación actual.
- El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad.
- El riesgo es la probabilidad de que suceda un evento, impacto o consecuencia adversos. Se entiende también como la medida de la posibilidad y magnitud de los impactos adversos, siendo la consecuencia del peligro, y está en relación con la frecuencia con que se presente el evento.
- Es una medida de potencial de pérdida económica o lesión en términos de la probabilidad de ocurrencia de un evento no deseado junto con la magnitud de las consecuencias.

1.3.2. Tipos de riesgo

Es muy importante aclarar que existe una gran variedad de clasificación de riesgos, estos se encuentran relacionados directamente con el tópico y/o la materia que se esté estudiando y evaluando. Desde el punto de vista y perspectiva empresarial existen innumerables riesgos, generados tanto por el entorno como por el desarrollo normal de sus actividades, por tal razón se definirán los riesgos bajo el siguiente esquema:

1.3.2.1. Riesgos del entorno

Comprende los elementos tales como el país donde está ubicada la empresa, su naturaleza, la región y ciudad, además del sector, la industria y condiciones económicas, políticas, sociales y culturales.

En este orden de ideas se pueden presentar riesgos como:

- Riesgo asociado a la naturaleza: son todos aquellos que se encuentran relacionados con riesgos meteorológicos y climáticos como huracanes, lluvias, maremotos, sequías, que afectan el logro de objetivos de la organización.
- Riesgos asociados al país: se pueden encontrar riesgos como el que hace referencia al grado de peligro que representa este para las inversiones extranjeras.

1.3.2.2. Riesgos generados en la empresa

En la institución se pueden presentar diversos riesgos que, entre otros aspectos, consiguen afectar los procesos, recursos humanos, físicos, tecnológicos, financieros, organizacionales, a los clientes y hasta la imagen de la empresa.

En este orden de ideas se pueden presentar riesgos como:

- **Riesgo de reputación:** es el desprestigio que podría sufrir la empresa, que trae como consecuencia la pérdida de credibilidad y confianza del público ya sea por fraude, insolvencia, conducta irregular de los empleados, rumores, errores cometidos en la ejecución de alguna operación por falta de capacitación del personal clave o deficiencia en el diseño de los procedimientos, este riesgo puede traer efectos como disminución de la demanda, o la pérdida de negocios atribuibles al desprestigio generado.
- **Riesgo puro:** este riesgo al materializarse origina pérdida, como un incendio, un accidente, una inundación.
- **Riesgo especulativo:** al materializarse genera la posibilidad de convertirse instantáneamente en beneficio o pérdida, como una aventura comercial, la inversión en divisas ante expectativas de devaluación o revaluación, la compra de acciones, el lanzamiento de nuevos productos, entre otros.
- **Riesgo estratégico:** son las pérdidas ocasionadas por las definiciones estratégicas inadecuadas y errores en el diseño de planes, programas, estructura, integración del modelo de operación con el direccionamiento objetivo, asignación de recursos, estilo de dirección, además de

ineficiencia en la adaptación a los cambios constantes del entorno empresarial, entre otros.

- Riesgo operativo: es la posibilidad de pérdidas ocasionadas en la ejecución de los procesos y funciones de la empresa por fallas en procedimientos, sistemas, modelos o personas que participan en dichos procesos.
- Riesgo de mercado: podría generar ganancias o pérdidas a la empresa al invertir en bolsa, debido a la diferencia en los precios que se registran en el mercado.
- Riesgo precio de insumos y productos: se refiere a la incertidumbre sobre la magnitud de los flujos de caja debido a posibles cambios en los precios, que una empresa puede pagar por la mano de obra, materiales y otros insumos relacionados con el proceso de producción, y por los precios que puede demandar por sus bienes o servicios.
- Riesgo de crédito: consiste en que los clientes y las partes a las cuales se les ha prestado dinero fallen en el pago. La mayoría de las empresas se enfrentan ante este riesgo en cuentas por cobrar, pero esta exposición es más alta en las instituciones financieras.
- Riesgo legal: se refiere a la pérdida en caso de incumplimiento de la contraparte en un negocio y la imposibilidad de exigirle jurídicamente el cumplimiento de los compromisos adquiridos. También se puede presentar al cometer algún error de interpretación jurídica u omisión en la documentación, y en el incumplimiento de normas legales y disposiciones reglamentarias que pueden conducir a demandas o sanciones.

- Riesgo tecnológico: el uso de tecnologías de información genera riesgos como los virus, el vandalismo puro y de ocio en las redes informáticas, fraudes, intrusiones por hackers, el colapso de las telecomunicaciones que pueden derivarse en el daño de la información o la interrupción de los servicios.

También está el riesgo del constante cambio de tecnología lo que puede ocasionar que las empresas no estén preparadas para adoptarlas y esto incrementa sus costos, menor eficiencia, incumplimiento en las condiciones de satisfacción de los servicios prestados a sus clientes.

- Riesgos laborales: pueden ser accidentes de trabajo y enfermedades profesionales, los cuales ocasionarían daños tanto a la persona como a la misma empresa.
- Riesgos físicos: son los que afectan a los materiales como por ejemplo; corto circuito, explosión física, daño en la maquinaria, daño en equipos por su operación, por su diseño, fabricación, montaje o mantenimientos; deterioros de productos y daños en vehículos.

1.3.3. Definición de vulnerabilidades

La vulnerabilidad es la incapacidad de resistencia cuando se presenta un fenómeno amenazante, o la incapacidad para reponerse después de que ha ocurrido un desastre.

En otras palabras, la vulnerabilidad se podría definir como las características y las circunstancias de un sistema o bien que los hacen susceptibles a los efectos dañinos de una amenaza.

Los factores que componen la vulnerabilidad son la exposición, susceptibilidad y resiliencia. La exposición es la condición de desventaja debido a la ubicación, posición o localización de un sujeto, objeto o sistema expuesto al riesgo.

La susceptibilidad es el grado de fragilidad interna de un sujeto, objeto o sistema para enfrentar una amenaza y recibir un posible impacto debido a la ocurrencia de un evento adverso.

La resiliencia es la capacidad de un sistema, comunidad o sociedad expuestos a una amenaza para resistir, absorber, adaptarse y recuperarse de sus efectos de manera oportuna y eficaz, lo que incluye la preservación y la restauración de sus estructuras y funciones básicas.

1.3.4. Regulaciones internacionales

En los años 70, el crecimiento de mercados financieros internacionales y el flujo de dinero entre países realzaron la falta de una supervisión bancaria efectiva a un nivel internacional. Las autoridades de supervisión bancaria básicamente regulaban bancos domésticos y las actividades domésticas de bancos internacionales, mientras que las actividades internacionales de estos bancos no eran siempre supervisadas de cerca.

El colapso en 1974 del Bankhaus Herstatt en Alemania y del Franklin National Bank en Estados Unidos exhortó a los gobernantes de 10 bancos centrales a crear el Comité de Basilea para Supervisión Bancaria. (Coronel Hoyos, K. D. R. 2008).

El Banco de Pagos Internacionales (BIS por sus siglas en inglés: Bank for International Settlements), es la institución financiera internacional más antigua del mundo y sigue siendo el centro principal para la cooperación de bancos centrales internacionales y la búsqueda de la estabilidad financiera y monetaria. Además, da soporte al trabajo de los comités y organizaciones basados en Basilea, siendo un enlace de distribución de información estadística bancaria, de seguridades, tipos de cambio y mercados derivados.

En 1988 el Comité de Basilea, emitió el Acuerdo de Capital de Basilea, introduciendo un marco de trabajo que se convirtió en un estándar globalmente aceptado. La mayoría de países en el mundo, adoptaron las recomendaciones emitidas por el BIS en el acuerdo de 1988. Una revisión de este acuerdo de capital en el 2004, conocido como Basilea II, incluyó en sus estándares el riesgo operativo.

Tales estándares, que se están implementando a nivel mundial desde finales del 2006, apuntan a lograr una mejor y más transparente medición de varios riesgos a los que se enfrentan las instituciones financieras, limitando la posibilidad de contagio en caso de una crisis y fortaleciendo la infraestructura financiera global.

Internacionalmente, el marco de trabajo de COBIT y todos los productos y publicaciones relacionados que emitió el IT Governance Institute (ITGI), orienta a las organizaciones en la implementación de un adecuado gobierno de TI que garantiza el cumplimiento de los objetivos del negocio por medio del valor agregado que debe brindar la tecnología de información, la administración de los riesgos y recursos y la medición del desempeño.

Además integra estándares internacionales generalmente aceptados como COSO, ITIL, ISO 9001, ISO 27002, AS/NZ 4360:8 2004, entre otros; que lo convierten en un marco de trabajo completo y alineado con las mejores prácticas relativas a la tecnología de información.

1.3.5. Regulaciones nacionales

El Artículo 55 de la Ley de Bancos y Grupos Financieros, Decreto No. 19-2002 del Congreso de la República de Guatemala, norma lo relacionado con la administración de riesgos y establece que los bancos y las empresas que integran grupos financieros, deberán contar con procesos integrales que incluyan, según el caso, la administración de riesgos de crédito, de mercado, de tasas de interés, de liquidez, cambiario, de transferencia, operacional y otros a que estén expuestos, que contengan sistemas de información y un comité de gestión de riesgos, con el propósito de identificar, medir, monitorear controlar y prevenir los riesgos.

La Resolución JM-56-2011 Reglamento para la Administración Integral de Riesgos tiene por objeto regular los aspectos mínimos que deben observar las entidades, con relación a la administración integral de riesgos. La Resolución JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico tiene por 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.

Resolución JM-4-2016 Reglamento para la Administración del Riesgo Operacional tiene por objeto regular los aspectos que, como mínimo, deben observar los bancos, las sociedades financieras, las entidades fuera de plaza o

entidades *off shore* autorizadas por la Junta Monetaria para operar en Guatemala y las empresas especializadas en servicios financieros que formen parte de un grupo financiero, para la administración del riesgo operacional. Otras normativas relacionadas con riesgos:

- Resolución JM-93-2005 Reglamento para la Administración del Riesgo de Crédito.
- Resolución JM-117-2009 Reglamento para la Administración del Riesgo de Liquidez.
- Resolución JM-134-2009 Reglamento para la Administración del Riesgo Cambiario Crediticio.

1.3.6. Enfoque de las entidades financieras del país

El riesgo en general está definido como la probabilidad de que una amenaza, peligro o incertidumbre, a que se ve enfrentada una institución, en este caso bancaria, por efecto o acción relacionada con sus líneas de negocio, operaciones y demás actividades, pueda afectar su situación financiera.

La administración de riesgos, es el proceso mediante el cual se identifican, miden, monitorean, limitan, controlan, previenen, mitigan e informan los distintos tipos de riesgo a que se encuentran expuestas las entidades bancarias, teniendo como instrumento un conjunto de políticas, procedimientos y sistemas. (JM-102-2011).

El intento exhaustivo por minimizar el riesgo de cualquier tipo, es una tarea del día a día en las instituciones financieras. Se prevé mantener una cultura de riesgo, buscando crear conciencia en relación al mismo, adoptando igualmente las prevenciones en los casos posibles por parte de todos sus colaboradores.

Considerando que para el desarrollo normal de sus actividades, los bancos dependen en un alto grado del uso de tecnología de la información, lo que hace necesario gestionar adecuadamente el riesgo tecnológico para asegurar la integridad, disponibilidad, confidencialidad de la información, así como la continuidad de la prestación de sus servicios.

1.3.7. Enfoque de seguridad de la información

Las instituciones financieras consideran la información como uno de sus activos más importantes, por tal razón están anuentes, que deben gestionar todo tipo de riesgo que causen pérdidas en la confidencialidad, integridad y disponibilidad de la información. Es importante mencionar que hasta en la actualidad, no existe ninguna práctica, técnica y/o metodología que asegure al ciento por ciento la seguridad de la información o en otras palabras la inviolabilidad de los sistemas.

Actualmente existen diferentes metodologías que han sido adoptadas por las instituciones, las cuales tienen la finalidad de minimizar los riesgos relacionados a seguridad de la información. Las organizaciones se han enfocado en emplear técnicas de protección física y lógica esto se debe a que las amenazas pueden proceder desde diversas fuentes.

Al referirse a materia de seguridad informática, las instituciones financieras continúan invirtiendo recursos para contar con medidas preventivas y detectivas, estos se derivan de rigurosas evaluaciones de riesgos, establecimientos de políticas de seguridad informática, selección de controles, entre otras.

1.3.8. Enfoque de continuidad del negocio

Las instituciones financieras emplean diversos procesos con el fin de identificar, prevenirse y prepararse para los eventos que puedan interrumpir las actividades del negocio. La administración de la continuidad del negocio involucra a toda la organización y se enfoca en las principales líneas de negocio, recurso humano, terceros y tecnología asimismo incorpora estándares y mejores prácticas reconocidos internacionalmente en relación con la continuidad y disponibilidad del negocio incluyendo el DRI – Disaster Recovery Institute, el BCI –Business Continuity Institute y el estándar BS25999.

En los planes de continuidad del negocio se identifican y evalúan los riesgos que afectan la continuidad y disponibilidad de los procesos críticos y de los servicios e infraestructura de tecnologías de información. En relación con los servicios e infraestructura tecnológica se consideran aspectos como:

- Problemas de desempeño, capacidad, disponibilidad de los servicios y recursos tecnológicos.
- Obsolescencia tecnológica e ineficacia de la plataforma tecnológica
- Problemas o fallas en las actividades y procesos asociados a la operación de la plataforma tecnológica.
- Fallas en la plataforma tecnológica por accidentes, daños o siniestros
- Fallas en servicios de comunicaciones
- Pérdida de información o datos históricos de los sistemas de información
- Fallas de hardware o software
- Fallas por desastres naturales

1.4. Metodologías para la gestión de riesgos tecnológicos

El riesgo tecnológico implica la probabilidad de pérdidas antes fallas de los sistemas de información, por esta razón se considera la probabilidad de fraudes internos y externos; involucrando el riesgo legal y el riesgo reputación por fallas en la seguridad y disponibilidad de los servicios que se proveen a los clientes, los cuales se encuentran soportados por las tecnologías de la información.

No todos los riesgos merecen una misma importancia, por tal motivo las organizaciones deben focalizar de forma adecuada sus recursos, a fin de que se pueda tener un ambiente controlado que facilite el cumplimiento de los objetivos institucionales por los cuales se trabaja día con día. En este ámbito existen dos términos importantes a considerar ya que las metodologías deben integrar los impactos negativos que pueden ocasionar la materialización de los riesgos y la probabilidad de que estos ocurran.

Cuando se implementa y se mantiene una metodología formal para la gestión y administración de los riesgos tecnológicos, le permite a la organización establecer una base confiable para la toma de decisiones y la planificación.

1.4.1. COBIT 4.1 (Controles para Información y Tecnologías Relacionadas)

Es una herramienta que provee una guía de mejores prácticas presentado como marco de trabajo, dirigida al control y supervisión de las tecnologías de información. Este marco de trabajo tiene una serie de recursos que puede ser empleado como referencia para la gestión de la tecnología en una organización, entre los aspectos que incluye se pueden mencionar: objetivos de control,

mapas de auditoría, herramientas para su implementación y principalmente una guía de técnicas de gestión.

El marco de trabajo fue desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA), una asociación que apoya y patrocina el desenvolvimiento de metodologías y certificaciones para la realización de actividades de control en los sistemas informáticos.

Esta versión del marco de trabajo parte de la siguiente misión: “Investigar, desarrollar publicar y promover un conjunto de objetivos que controlen las tecnologías de información con autoridad, actualizados, de carácter internacionales y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores”.

El modelo de procesos de COBIT 4.1 está compuesto de cuatro dominios que contienen treinta y cuatro procesos genéricos administrando los recursos y activos tecnológicos para proporcionar la información al negocio de acuerdo con los requerimientos del negocio y gobierno. Los cuatro dominios del marco de trabajo son:

- Planear y organizar: provee las estrategias y tácticas que prevén identificar la manera en que las tecnologías de la información pueden contribuir de la mejor manera al logro de los objetivos del negocio.
- Adquirir e implementar: identificación de soluciones desarrollo o adquisición, cambios y/o mantenimiento de sistemas existentes.
- Entregar y dar soporte: cubre la entrega de los servicios tecnológicos

requeridos; incluyendo la calidad de la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.

- Monitorear y evaluar: este dominio indica que todos los procesos de tecnologías de información deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

1.4.2. MAGERIT (Análisis y Gestión de Riesgos de los Sistemas de Información)

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT es de interés a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT, les permitirá saber

cuánto valor está en juego y les ayudará a protegerlo, asimismo, el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

1.4.3. Sistemas de Gestión

En la actualidad la Organización Internacional para la Estandarización (ISO), ha desarrollado diferentes estándares normados y guías de prácticas que se han enfocado en la administración de procesos para generar valor de las tecnologías de información en las organizaciones que dependen de ellas.

ISO ha conformado diversos comités en conjunto con la Comisión Electrotécnica Internacional (IEC), a fin de desarrollar, promover, mantener normas en los campos de la terminología electrónica y tecnologías de la información. Los principales productos de ISO son sus estándares internacionales. ISO también publica informes técnicos, especificaciones técnicas, especificaciones disponibles públicamente, erratas técnicas, y guías.

1.4.3.1. ISO 20000 (Sistema de Gestión de Servicios de TI)

Es uno de los productos de ISO enfocado en la gestión de servicios de Tecnologías de Información, que define un conjunto de procesos necesarios para ofrecer un servicio eficaz. Esta norma es utilizada por las instituciones para obtener una certificación internacional que permita demostrar y validar que la organización sigue las mejores prácticas para la entrega de sus servicios tecnológicos.

La norma ISO 20000 se focaliza exhaustivamente en la administración de servicios de TI y recoge procesos básicos para el establecimiento, la implementación, operación, monitorización, revisión, mantenimiento y mejora del sistema global de la gestión de servicios soportados por la tecnología.

La norma se encuentra en su versión 2011 y es aplicable a cualquier organización, ya sea grande o pequeña, en cualquier sector o parte del mundo donde confían en los servicios de TI, dicha norma es particularmente aplicable para proveedores de servicios internos de tecnologías de información, tales como departamentos de división tecnológica, proveedores externos o incluso organizaciones subcontratadas.

La norma ha estado impactando positivamente en algunos de los sectores que necesitan y dependen de la tecnología para subsistir, tales como subcontratación de negocios, telecomunicaciones, finanzas y el sector público.

1.4.3.2. ISO 31000 (Sistema de Gestión de Riesgos)

Es uno de los productos de ISO, que señalan una familia de normas sobre la gestión del riesgo en estándares. El propósito principal es proporcionar los principios y directrices reconocidos internacionalmente para administración de riesgos desde el punto de vista estratégico y operativo. En la actualidad la familia de ISO 31000 incluye:

- ISO 31000: 2009 –gestión de riesgos – principios y directrices
- ISO/IEC 31010 –gestión de riesgos- evaluación del riesgo, evaluaciones técnicas del riesgo.

- ISO Guide 73:2009 –gestión de riesgos – vocabulario gestión

1.4.3.3. ISO 27001 (Sistema de Gestión de Seguridad de la Información)

Es la norma internacional emitida por la ISO, que describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente fue publicada en el 2013. ISO 27001 puede ser implementada en cualquier tipo de organización con o sin fines de lucro, privada o pública, pequeña o grande, proporciona una metodología que incluye los siguientes puntos: objeto de campo y aplicación, referencias normativas, términos y definiciones, contexto de la organización, liderazgo, planificación, soporte, operación, evaluación de desempeño, mejora continua, objetivos de control y controles de referencia.

La norma ISO 27001 es certificable y le permite a la organización demostrar a sus clientes que, al cumplir los requisitos contractuales, la seguridad de su información es primordial. Las recomendaciones y/o requerimientos de la norma apoyan a las organizaciones a verificar independientemente que sus riesgos en materia de seguridad de la información estén correctamente identificados, evaluados y gestionados al tiempo que formaliza sus procesos, procedimientos y documentación de protección de la información.

1.4.3.4. ISO 22301 (Sistema de Gestión de Continuidad del Negocio)

Es la norma desarrollada por la ISO que proporciona un marco de referencia para gestionar la continuidad del negocio en una organización. La norma está concebida para cualquier organización, grande o pequeña, con o sin

fines de lucro, privada o pública; por tal razón es aplicable a cualquier tipo o tamaño.

Si una institución se adapta correctamente a las recomendaciones y/o requerimientos plasmados, disminuirá la posibilidad de ocurrencia de un incidente disruptivo y, en caso de producirse, la organización estaría preparada para responder en forma adecuada y reducir drásticamente el daño potencial o los impactos negativos que podría producir el evento desencadenado.

La continuidad del negocio es parte de la gestión general e integral del riesgo en una compañía y se encuentra directamente relacionada con la gestión de seguridad de la información y los servicios de tecnologías de información.

Entre las recomendaciones que emite la norma como base para gestionar la continuidad son las políticas, guías, estándares y procedimientos implementados por una organización. Todo el diseño, implementación soporte y mantenimiento debe estar fundamentado en la obtención de un buen plan de continuidad del negocio, recuperación de desastres y en algunos casos, soporte al sistema.

En ocasiones el plan de contingencias se confunde con la gestión de recuperación tras un desastre, pero son conceptos aislados. La recuperación ante desastres es una pequeña parte de un plan holístico de gestión de la continuidad.

2. SITUACIÓN ACTUAL

2.1. Descripción de los servicios tecnológicos

El Departamento de Tecnologías de la Información es quien actualmente se encarga de proveer todos los servicios de tecnología que requiere la institución financiera para crear y proporcionar los productos y servicios financieros a sus clientes finales.

El grupo tiene actualmente registradas seis empresas que conforman el Grupo, las cuales tienen fines similares y están sujetas a la inspección de la Superintendencia de Bancos de Guatemala.

El Departamento de Tecnologías de la Información no tiene interacción directa con los clientes finales de la empresa. Para ello la institución ha designado a sus áreas operativas y del negocio, sin embargo, el logro de los objetivos planteados por la organización y la Junta Directiva, si se encuentran relacionados directamente con el Departamento de Tecnologías de la Información.

Partiendo de la premisa anterior, los clientes del dicho departamento son los usuarios internos de la organización, esta última área mencionada ha diseñado un catálogo de servicios que acordó con las áreas operativas y del negocio, definiendo así sus Acuerdos de Nivel de Servicio (SLA's) y sus Acuerdos de Nivel de Operación (OLA's).

El Departamento de Tecnologías de la Información para la definición de sus servicios considero los siguientes aspectos:

- Para cada uno de los servicios se establecieron los requisitos, tanto internos para el departamento, como también los que debía cumplir el usuario.
- Los servicios incluyen los objetivos acordados, las características del trabajo y las excepciones.
- La definición de servicios se revisa en conjunto con los usuarios internos en intervalos periódicos, cabe mencionar que esto depende de un análisis profundo sobre el cambio y mejora de los servicios en el tiempo, lo cual no lo está realizando el Departamento de Tecnologías de la Información de forma efectiva.

Basados en los puntos anteriores, fue estructurado un catálogo de servicios tecnológicos, el cual no está totalmente alineado con los cambios y modificaciones del servicio.

Prácticamente los servicios que provee el Departamento de Tecnologías de la Información se encuentran clasificados en siete ramas, automatización de procesos mediante el uso de la tecnología, soporte, protección de información resguardada en la infraestructura tecnológica, adquisición e implementación de nuevas tecnologías, administración y optimización de los repositorios de información, telecomunicaciones y generación de reportes con información masiva.

2.2. Descripción del Centro de Datos

En el Centro de Datos se procesa toda la información digital que generan y resguardan las unidades operativas y del negocio, en el Centro de Datos se almacena, se administra y se distribuye la información digital de la organización, a todos los colaboradores y procesos autorizados, con el fin de que se puedan consultar y/o modificar.

El Centro de Datos de la organización es físico y la arquitectura que tiene, es capaz de facilitar las actuales funcionalidades de red avanzada, asimismo los requerimientos de ancho de banda y velocidad de las aplicaciones tecnológicas en la actualidad. El Centro de Datos tiene un alto nivel de fiabilidad y seguridad, de tal forma que tiene controles físicos y lógicos rigurosos que permiten proteger la información y que la misma se encuentre disponible sin interrupciones a quienes tienen el privilegio de acceder a la red local de la institución y la utilización, con el fin de generar valor a la organización.

El Departamento de Tecnologías de la Información trabaja de forma rutinaria para que no exista degradación en el acceso a la información y que con ello se corra el riesgo de poner en peligro los negocios trazados, independientemente del tamaño.

Los datos resguardados por los usuarios internos de la entidad no son estáticos, están en constante modificación, se interrelacionan unos con otros, por tal motivo se genera nueva información constantemente. El crecimiento puede llegar a ser exponencial, esto implica que no solo deben estar protegidos mediante medidas de seguridad (física y lógica), sino también de tener procesos y métodos que permitan prever dicho crecimiento y que no se vea

truncada la generación de la información tanto por la agilidad como también por la capacidad de almacenamiento.

Los procesos y métodos que le permiten a la sociedad contar con un ambiente controlado en el Centro de Datos, tienen gestiones de mantenimiento, administración de equipos y de comunicación.

El Centro de Datos principal de la institución tiene una categoría de TIER IV, esta clasificación fue ideada por el Uptime Institute el cual se plasmó en el estándar ANSI/TIA-942 y que básicamente establece cuatro categorías, en función de la redundancia de los componentes que soportan el Centro de Datos, siendo la indicada la más alta. En resumen, las características de los controles implementados por el Departamento de Tecnologías de la Información en relación a la redundancia son:

- El Centro de Datos tiene repetición y superfluidad en sistemas vitales
- Tiene dos dispositivos de refrigeración independiente, doble fuente
- Tiene dos caminos distintos de suministro eléctrico, proporcionado por la Empresa Eléctrica de Guatemala Sociedad Anónima.
- El Centro de Datos está sujeto a un suelo elevado
- Para la redundancia de energía eléctrica, cuenta con dos generadores eléctricos que emplean combustible fósil y generador auxiliares UPS.
- Todos los equipos computacionales que conforman la infraestructura tecnológica tienen doble fuente y no requieren de paradas operacionales para las operaciones de mantenimiento básicas.
- La disponibilidad prevista en el año es de un 99,995 %, esto quiere decir que se permite perder la continuidad de los servicios tecnológicos por 26 minutos en el año.

2.2.1. Ubicación

El Centro de Datos principal se encuentra localizado en las oficinas centrales de la organización, la cual está ubicada en Boulevard Los Próceres 24-69 zona 10, Empresarial Zona Pradera Torre 3 oficina 917, ciudad de Guatemala, Guatemala Centroamérica.

2.2.2. Infraestructura física

La infraestructura física del Centro de Datos ha tenido un impacto significativo en el rendimiento, la eficiencia y la confiabilidad de los usuarios internos, para que estos objetivos se cumplieran la institución consideró la especificación de un diseño simplificado, eficiencia operativa, visibilidad y control. Tomando en consideración los parámetros mencionados en el párrafo anterior, la estructura del Centro de Datos integró las siguientes variables:

- Instalación de rutas, estas fueron diseñadas para trazar y manejar independientemente cables de datos de cobre, cables de fibra óptica y cables de alimentación eléctrica. Estas características proporcionan facilidad a la hora de identificar daños y/o incidentes.
- Un sistema de alarma y supresión contra incendios que cumple con los requerimientos de las normas NEC (Código Eléctrico Nacional), NFPA 72, 75 y 2001; este tiene la capacidad de ser activado de forma manual o automática; asimismo un monitoreo continuo del ambiente, activación de sirenas y estrobos, activación de un sistema de supresión de gas y conexión y activación de aire.
- Un sistema de aire acondicionado que está conformado por dos

dispositivos. El primero es un sistema de presión cuyas características permiten mantener una temperatura adecuada a través de dos partes, una que maneja el aire de salida en la parte inferior del suelo elevado y la otra de retorno del mismo aire en la parte superior; este dispositivo cuenta con un tablero digital en el que muestra el grado de temperatura y proporciona diferentes controles proactivos en tiempo real.

Entre los componentes de este dispositivo se encuentran ventiladores, humidificadores y cilindros de presión, posee una interfaz de red que permite el monitoreo y posee un sistema de notificaciones por medio de correo electrónico.

El otro dispositivo es un aire acondicionado de Confort que es utilizado como redundancia en caso de falla del primer dispositivo mencionado. Este módulo tiene tres termostatos electrónicos ubicados estratégicamente, los cuales se encuentran calibrados de tal forma que según el grado de temperatura que tenga el ambiente, se activa para estabilizarla según el umbral definido.

- Un sistema ininterrumpido de energía son diversas baterías organizadas (UPS) que funcionan en condiciones normales con energía que llega desde la acometida eléctrica y que proporciona un suministro durante aproximadamente 30 minutos, en caso fallara la energía que provee la planta de combustible fósil.
- Un sistema de detector de humedad que se encuentra cerca de toda la línea de tubería utilizada por el aire acondicionado, con el fin de detectar la cantidad mínima de humedad que pueda producirse por posibles fugas o mal funcionamiento de este último sistema mencionado. El detector de

humedad posee una interfaz de red que notifica por medio de correo electrónico, incidentes que se pueden llegar a materializar en tiempo real.

- Un sistema de cámara NETBOTZ que consiste en un dispositivo ubicado dentro del Centro de Datos, cuya función principal es detectar y notificar la actividad humana que puede poner en riesgo la disponibilidad de la infraestructura tecnológica.

El sistema trabaja a través de movimiento, sonido, temperatura, apertura de la única puerta de acceso y registro de imágenes. Al igual que los demás dispositivos, este sistema cuenta con una interfaz de red que comunica a través de correo electrónico, la materialización de cualquier evento. Todas las notificaciones pueden ser parametrizables a través de una consola administrativa.

2.2.3. Gestión de capacidad

El Departamento de Tecnologías de la Información ha implementado un proceso que le permite monitorear y evaluar desde diferentes perspectivas los activos tecnológicos que conforman la infraestructura, es importante mencionar que actualmente dicha evaluación no ha permitido que se pueda predecir el consumo de los recursos críticos que le permiten a la unidad proveer los servicios tecnológicos que soportan a las áreas operativas y del negocio de la entidad financiera. Por tal razón se encuentra muy ambiguo el proceso de prevención y detección de incidentes a causa de la falta de capacidad.

El proceso de monitorización actual solo tiene como alcance la infraestructura tecnológica que conforma el Sistema Central de Banco, esto

deja a la deriva o en descubierto todos los demás recursos primordiales que soportan los procesos críticos del grupo financiero.

La premisa actual se basa en asegurar que el Departamento de Tecnologías de la Información tendrá en todo momento la capacidad suficiente para satisfacer las demandas actuales y futuras de acuerdo a las necesidades del negocio, sin embargo, esto no se cumple a cabalidad por la falta de madurez de los controles implementados.

2.2.3.1. Administración de la infraestructura tecnológica

La gerencia del Departamento de Tecnologías de la Información ha creado una unidad que le reporta a la Subgerencia de Operaciones (esto según la estructura organizacional), dicho grupo de trabajo es el encargado de gestionar los recursos relacionados directamente con la infraestructura tecnológica, para tal efecto tienen implementados procesos de monitorización de diferente índole los cuales le permiten administrar la infraestructura tecnológica disponible a fin de garantizar la disponibilidad de los servicios tecnológicos.

La infraestructura tecnológica de la entidad financiera está conformada por servidores físicos y servidores virtuales, en estos equipos es donde se albergan todos los sistemas de información, bases de datos, aplicaciones, herramientas web que soportan los procesos críticos y clave para la estrategia del negocio. Todos los recursos relacionados tales como la memoria RAM, los procesadores, el almacenamiento y otros relevantes, son responsabilidad de la unidad mencionada en el párrafo anterior.

Actualmente las herramientas tecnológicas que administra la unidad de Administración del Sistema permiten la prevención, detección y aplicación de acciones correctivas en caso de que ocurran incidentes, sin embargo, estas herramientas no han sido metrizadas y/o configuradas, de tal forma que los controles efectuados no tienen efectividad.

2.2.4. Sitio Alternativo de Datos

Actualmente la organización ha contratado a un proveedor de servicios tecnológicos para la habilitación de un Sitio Alternativo de Datos. En este Centro de Datos se encuentra una réplica exacta de todos aquellos servicios tecnológicos críticos según el juicio del Departamento de Tecnologías de Información. Es importante mencionar que las condiciones actuales del Sitio Alternativo de Datos no son las mismas que el Sitio Principal de Datos.

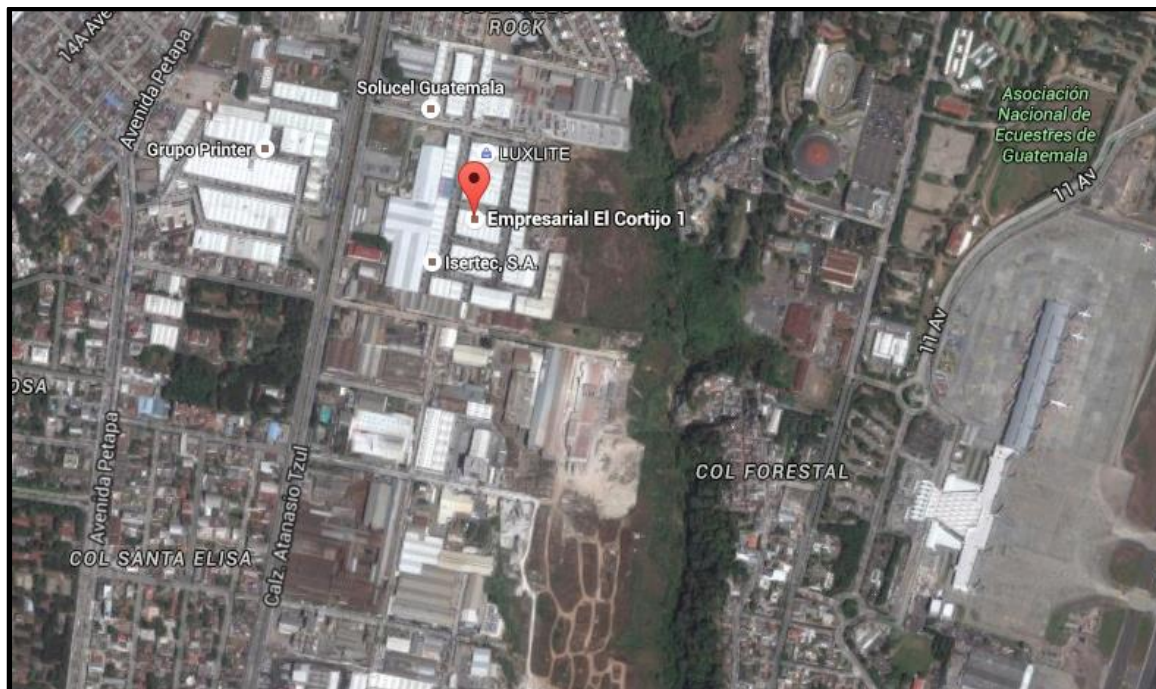
El servicio contratado con el proveedor solo es de colocación, es decir, toda la administración de los recursos es responsabilidad de la empresa, sin embargo, los controles de seguridad física, lógica y de disponibilidad si es responsabilidad del proveedor. Una de las razones por las cuales el Sitio Alternativo de Datos no tiene las mismas magnitudes que el Sitio Principal de Datos es el alto costo que este representa, por tal razón una de las principales metas es optimizar los recursos.

En pocas palabras la función principal del Sitio Alternativo de Datos es que se puedan proveer los servicios tecnológicos que soportan los procesos críticos del negocio, en caso se materialice un evento no deseado que predisponga de indisponibilidad todos los servicios tecnológicos que se albergan en el Sitio Principal de Datos.

Desde la perspectiva anterior el Departamento de Tecnologías de Información no es el área más adecuada para decidir qué servicios se deben replicar en el Sitio Alternativo de Datos y cuales se deben habilitar en caso de contingencia; para ello se debe considerar la elaboración de un Análisis de Impacto del Negocio (BIA) que sea elaborado por un departamento el cual tenga una visión global y particular de todos aquellos procesos operativos y de negocio críticos.

El Sitio Alternativo de Datos se encuentra ubicado en Avenida Ferrocarril 19-97 zona 12, Cortijo Empresarial I, Bodega 609, ciudad de Guatemala, Guatemala Centroamérica.

Figura 6. **Ubicación del Sitio Alternativo de Datos de la entidad financiera supervisada por la Superintendencia de Bancos de Guatemala**



Fuente: Google Maps, captura satelital realizada el 16 de marzo de 2017.

2.2.5. Gestión de configuración

El Departamento de Tecnologías de la Información actualmente ha implementado un proceso en el que prevé llevar un control de la configuración de los activos tecnológicos. La descripción de la configuración son todos aquellos elementos intrínsecos y extrínsecos tales como especificaciones técnicas y todos los detalles que permiten describir el hardware y software que conforman la infraestructura tecnológica.

Los datos mencionados incluyen típicamente las versiones y actualizaciones que se han aplicado a los paquetes de software instalados, asimismo la ubicación y las direcciones de red de los dispositivos de hardware.

Un objetivo importante de la gestión de configuración es asegurar que los cambios realizados sobre un activo tecnológico no afectarán negativamente a cualquiera de los otros activos, ni a los servicios tecnológicos que provee el Departamento de Tecnologías de la Información; sin embargo, esta condición no se cumple ya que existe un coordinador de la gestión quien debe solicitar mensualmente la información de los cambios en configuración que sean mayores o bien sean considerados críticos por las áreas que se identificaron como fuente de información, o bien las áreas que administran y custodian los activos tecnológicos.

Este procedimiento deja de ser preventivo, detectivo e inclusive correctivo, las áreas no llevan un control exhaustivo que les permita conocer todos los cambios que realizan sobre los activos, existen muchas razones por las cuales se deban realizar cambios sobre los activos, entonces todos los equipos tecnológicos, bases de datos y sistemas de información carecen incluso de una base de datos y/o repositorio de almacenamiento de información en donde se

pueda documentar cómo se ha configurado el hardware y el software, rastrear los cambios y enviar una alerta al administrador si se realiza un cambio en contra de las políticas corporativas o normas de cumplimiento.

De la gestión de configuración, el coordinador emite un reporte, con los cambios que se realizaron en el mes sobre los servicios tecnológicos que provee el Departamento de Tecnologías de la Información, esto no está relacionado con el objetivo de la gestión.

2.3. Descripción de los controles

Los controles a los cuales se hace referencia a continuación son todos aquellos que están relacionados a la seguridad de los activos tecnológicos críticos, específicamente a todos aquellos que se encuentran dentro del Centro de Datos principal.

2.3.1. Seguridad física

El Departamento de Tecnologías de la Información es el encargado de custodiar todos los activos tecnológicos que posee la organización, por tal motivo con el apoyo de diferentes áreas y departamentos ha implementado diversos controles físicos de seguridad, con los cuales prevé asegurar la confidencialidad, disponibilidad e integridad de los datos resguardados en la infraestructura tecnológica, bases de datos y sistemas de información. Entre los controles se pueden mencionar:

- **Sistemas de cámaras de seguridad:** en toda la infraestructura física del edificio en donde está localizada la institución, se ha implementado un circuito cerrado de cámaras de video en tiempo real, sin embargo, existen

tres cámaras instaladas de forma estratégica en los alrededores del Centro de Datos. El proceso de administración, mantenimiento, almacenamiento y respaldos no es gestionado por el Departamento de Tecnologías de la Información.

- Cerrojo y picaportes de puertas: actualmente todas las puertas de acceso al Centro de Datos principal se cierran y bloquean, a través de un sistema eléctrico que únicamente es desbloqueado por lectores de proximidad y lectores biométricos de seguridad, sin embargo, para el caso de emergencias se tienen las llaves de los cerrojos, mismas que pueden entregarse solo a un listado de personal sensible en caso se llegará a materializar algún evento no deseado que provocará algún incidente.
- Acceso normal al Centro de Datos: el Centro de Datos es considerada como un área restringida. Todos los colaboradores internos de la compañía tienen tarjetas de proximidad, sin embargo, solo las personas autorizadas pueden ingresar al Centro de Datos. La activación, desactivación y modificación de los permisos de dicha tarjeta de proximidad en relación al Centro de Datos, es responsabilidad del Departamento de Seguridad que no le reporta directamente al Departamento de Tecnologías de la Información.

Actualmente se debe enviar una solicitud por escrito la cual debe ser validada por la Subgerencia de Operaciones del Departamento de Tecnologías de la Información al Departamento de Seguridad, esta autorización debe ser revisada y firmada por el gerente del Departamento de Tecnologías de la Información y el jefe inmediato de la persona quien dispondrá del privilegio.

- Libros auxiliares de registro de ingreso de personal no autorizado: en algunos casos se debe autorizar el acceso temporal a algunas personas al Centro de Datos, esto podría ser por diferentes trabajos que se deben efectuar, como por ejemplo los procesos de mantenimiento que se dan a los diferentes dispositivos.

Para tal efecto se dispone de dos libros ubicados en dos puertas diferentes del Departamento de Tecnologías de la Información, en este se deben anotar las personas e indicar a quien visitan, los guardias de seguridad verifican que la información sea correcta y contactan al personal interno, que si dispone de los permisos para ingresar al Centro de Datos. Los colaboradores internos deben estar en todo momento junto a los visitantes.

- Egreso de dispositivos: para el egreso de cualquier dispositivo que se encuentre instalado en el Centro de Datos principal, se debe realizar previamente un requerimiento a la Subgerencia de Operaciones del Departamento de Tecnologías de la Información, notificando los motivos por los cuales es necesario proceder a dar de baja de las herramientas de control.

La persona que retira el equipo debe estar completamente identificada y el personal interno deberá realizar las verificaciones correspondientes, firmar un formulario y entregarlo al Departamento de Seguridad para una última revisión y validación, este departamento es el encargado de resguardar los formularios, asimismo está facultado para realizar los rechazos correspondientes en caso la información o los datos sean incongruentes.

2.3.2. Seguridad lógica

La Subgerencia de Seguridad de la Infraestructura del Departamento de Tecnologías de la Información efectúa distintos procesos de monitorización con el fin de mantener bajo control cualquier materialización de riesgos inherentes o problemas inminentes sobre seguridad informática en los servicios, software, hardware. Dicha área emplea distintas herramientas que generan información con los resultados de los activos que fueron monitoreados.

Entre los principales controles de seguridad lógica que tiene implementados actualmente la entidad financiera sobre los activos tecnológicos, se pueden mencionar:

- Monitoreo de alertas sobre correos electrónicos de dudosa procedencia: uno de los principales medios de comunicación que emplea la entidad es el correo electrónico, y ya que uno de los activos más importantes para la misma es la información, se han configurado distintos equipos que tienen la capacidad de analizar y bloquear todos aquellos correos entrantes y salientes que probablemente pueden contener virus y/o no fueron solicitados, no deseados o con remitente no conocido, en inglés a esto se le conoce como spam y habitualmente son correos de tipo publicitario que se envían en grandes cantidades (incluso masivas).

El Departamento de Tecnologías de la Información ha instalado dos dispositivos para analizar el tráfico de correos entrante y el tráfico de correos saliente, con el primero se evita que toda la basura informática se resguarde en la infraestructura tecnológica de la compañía, asimismo previene que se acceda a páginas web o links que contengan virus, el dispositivo de salida se utiliza para analizar la información que se origina

de la infraestructura tecnológica de la entidad y se envíe internamente y/o externamente, con ello se previene que el tráfico de información confidencial llegue a personas a quien no debía llegar.

- Monitoreo de equipos de cómputo con posibles infecciones de virus (*malware*): el Departamento de Tecnologías de la Información tiene una herramienta tecnológica que emplea como sistema de control preventivo, detectivo y correctivo, cuando la infraestructura tecnológica se conecta a internet y se infecta por los distintos tipos de virus informáticos. La Subgerencia de Seguridad de la Infraestructura se encarga de revisar y evaluar las distintas alertas que se generan en dicha herramienta tecnológica y se encargan de realizar la actualización de las bases de datos.
- Monitoreo vulnerabilidades en el sistema operativo de la infraestructura tecnológica: el Departamento de Tecnologías de la Información utiliza distintas soluciones tecnológicas para realizar análisis sobre toda la infraestructura tecnológica que se encuentra conectada a la red interna y que por el sistema operativo, se pueden explotar vulnerabilidad que generen o puedan dañar, exponer y bloquear los datos de las áreas operativas y del negocio del grupo.
- Bloqueo de Puertos USB: la tecnología USB (universal serial bus) es utilizada actualmente para interrelacionar distintos dispositivos con los equipos de cómputo. Entre los dispositivos existe un tipo que tiene la característica funcional de almacenamiento de datos, por tal razón el Departamento de Tecnologías de la Información tiene el control de toda la infraestructura tecnológica que pueden tener habilitados los puertos mencionados. Con ello se evita que pueda existir fuga de información no

autorizada, asimismo se previene la infección de virus que puede transportarse en las memorias externas si no existiera esta restricción y/o control.

- **Monitoreo de accesos sensibles:** periódicamente las áreas de la organización realizan evaluaciones sobre los permisos que fueron otorgados a los distintos colaboradores internos. Para efectuar este análisis se genera un reporte en el que se detallan las autorizaciones sensibles que tiene cada colaborador.

El área que realiza las evaluaciones definió los accesos sensibles como todos aquellos que tienen un alto riesgo y que pueden provocar impactos negativos muy altos sobre los datos. El objetivo principal es identificar todos aquellos usuarios que tienen accesos sensibles y no los requieren para realizar su trabajo.

2.4. Presupuesto

Actualmente el Departamento de Tecnologías de la Información emplea los recursos financieros que vienen de un proceso de autorización en cascada desde el Consejo Directivo, la recaudación de la información para elaborar el presupuesto incluye todos los costos fijos, variables y gastos recurrentes, asimismo las inversiones para un año completo.

Al Departamento de Tecnologías de la Información se le asigna un presupuesto de recursos financiero que debe ejecutar para un año completo; se ha implementado un proceso que consiste en calendarizar los gastos recurrentes en el año, de tal forma que se pueda mantener y optimizar el funcionamiento de la infraestructura que soporta los servicios tecnológicos.

Existe un coordinador del proceso quien realiza todas las actividades correspondientes para consolidar la información que le permita realizar el presupuesto y planificación de gastos del siguiente año. Para dicho proceso el coordinador solicita a las subgerencias que conforman el Departamento de Tecnologías de la Información los datos indicados abajo con su respectiva prioridad, descripción y costo.

Los datos son básicamente cursos de capacitación al personal, nuevas soluciones tecnológicas que se convierten en proyectos, renovación de servicios contratados, renovación de licencias de software, gastos recurrentes (salarios de personal y otros), nuevas plazas y otros que tengan alto impacto de inversión.

Una vez se haya consolidado esta información el coordinador realiza una revisión con las personas involucradas, con el objeto de ajustar y afinar una versión preliminar e integrada, una vez aprobado se traslada el documento al gerente del Departamento de Tecnologías de la Información quien realiza ajustes y autoriza la versión final que se envía a la Gerencia Dirección de Finanzas, en dicha versión se incluye los rubros relacionados con mobiliario y equipo, tecnología nueva que apoyará a las áreas operativas y de negocio, mobiliario y equipo.

Según las observaciones de la Gerencia Dirección de Finanzas se realizan ajustes al presupuesto en base a las prioridades asignadas en conjunto con la Gerencia Dirección de Operaciones y la Gerencia General, los datos relevantes que se dan a conocer son todos aquellos relacionados con los gastos recurrentes y la estimación de los proyectos tecnológicos nuevos y de renovación.

Es importante mencionar que, aunque la información presupuestaria se revise con la Gerencia General, la inversión de tecnología no se encuentra correctamente alineada a los objetivos estratégicos del negocio, por tal razón pareciera que el Departamento de Tecnologías de la Información avanza hacia una dirección distinta. Esto genera el riesgo de que no se cumplan las expectativas trazadas por las áreas operativas y del negocio, en su defecto por las partes interesadas de la organización.

Mensualmente el coordinador del proceso realiza un reporte en donde se pueden visualizar cada uno de los montos que fueron presupuestados y los montos que se han ejecutado hasta el momento.

2.5. Atención de requerimientos e incidentes

Todos los usuarios internos de la institución, a quienes el Departamento de Tecnologías de la Información provee los servicios tecnológicos, solicitan diferentes requerimientos y reportan incidentes sobre dichos servicios.

La cantidad de usuarios internos cada vez es más amplia, el Departamento de Tecnologías de la Información ha implementado distintos procesos que prevén eficientizar la atención requerimientos y resolución de incidentes relacionados con los sistemas de información, las bases de datos y la infraestructura tecnológica.

2.5.1. Gestión de solicitudes de servicio

El objetivo principal de este proceso implementado por el Departamento de Tecnologías de la Información es atender un requerimiento de forma efectiva y resolver un incidente que cause o pueda causar interrupción en la prestación

del servicio tecnológico, cubriendo todos los aspectos que garantizan la continuidad, disponibilidad y calidad. Esta atención y resolución incluye todos los servicios que se encuentran en el catálogo de servicios establecido. En el proceso de la gestión de solicitudes del servicio se efectúan los siguientes subprocesos:

- Identificación y registro: todos los requerimientos e incidentes son reportados por los usuarios internos a través de los medios autorizados, en esta etapa del proceso la primera línea de atención verifica que la solicitud se encuentre dentro del catálogo de servicios ya que muchas veces los requerimientos e incidentes pueden ser errores operativos que los usuarios internos confunden, asimismo se debe comprobar que la solicitud no se esté duplicando por el sistema.

En esta etapa también se le asigna una prioridad a dicha solicitud, esto básicamente se realiza a través de una matriz de priorización que en base a las variables de urgencia e impacto tiene una clasificación crítica, alta, media, baja.

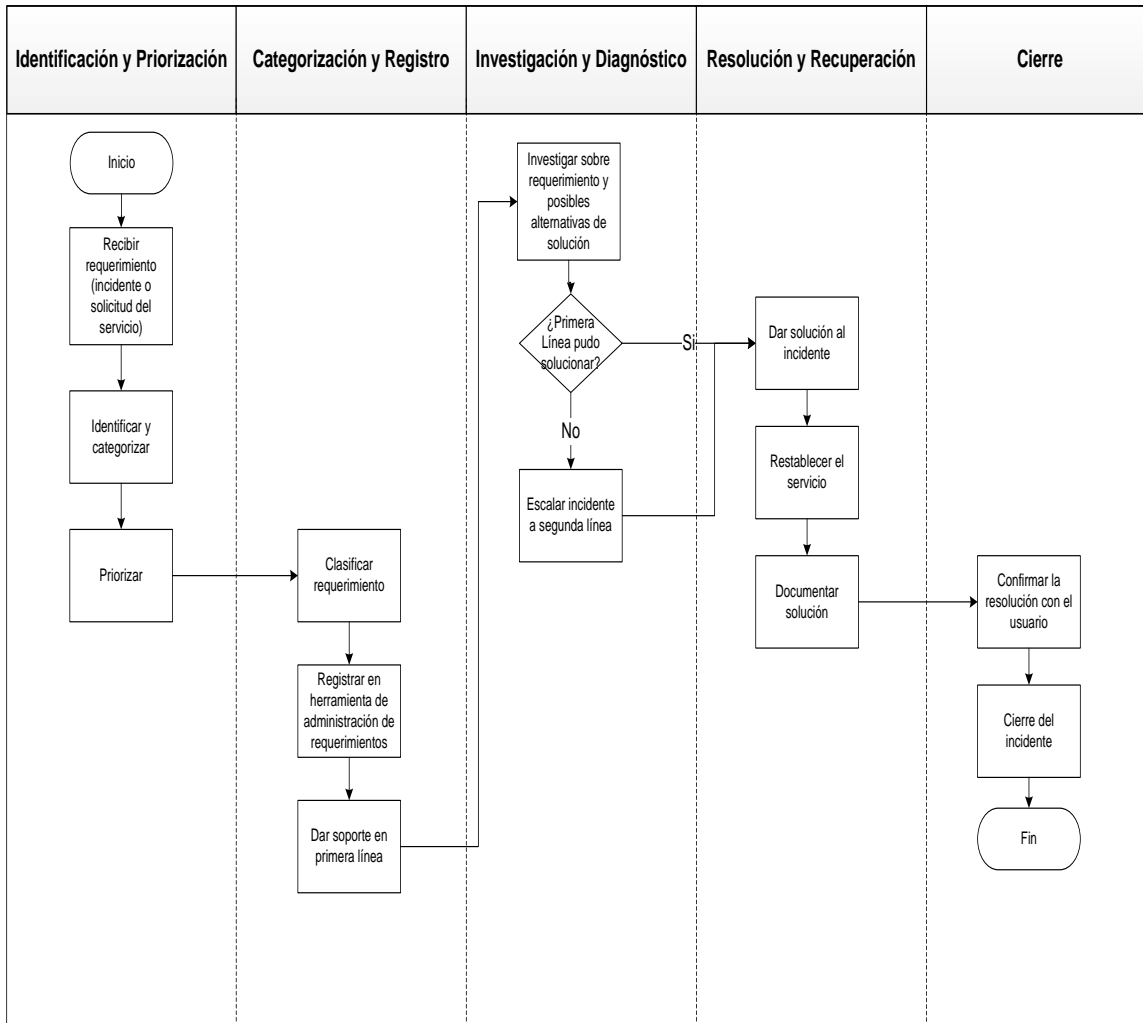
- Investigación y diagnóstico: esta etapa del proceso se aplica básicamente para determinar qué línea puede y debe atender y resolver el requerimiento, existe la primera línea que se encarga del análisis básico de la solicitud, la segunda línea son colaboradores, analistas y técnicos especialistas y la tercera línea son los proveedores de las soluciones.
- Resolución y recuperación: en esta etapa es cuando se aplican todas acciones para atender y resolver la solicitud de servicio, es importante mencionar que se tiene una herramienta en donde se debe documentar que actividades fueron las que se efectuaron, esto serviría como una

base de datos de conocimiento, sin embargo, los colaboradores no describen correctamente las tareas y la información solo ocupa espacio ya que no se puede utilizar como direcciones o procedimientos al momento que sean solicitados servicios similares.

- Cierre: esta es la última etapa del proceso, básicamente los usuarios internos reciben un formulario en donde se les indican las comprobaciones que deben realizar, asimismo que sean realizadas las que ellos consideren convenientes y de esta forma si todo funciona de acuerdo a la solicitud realiza, el usuario confirma el cierre del requerimiento o la resolución definitiva del incidente.

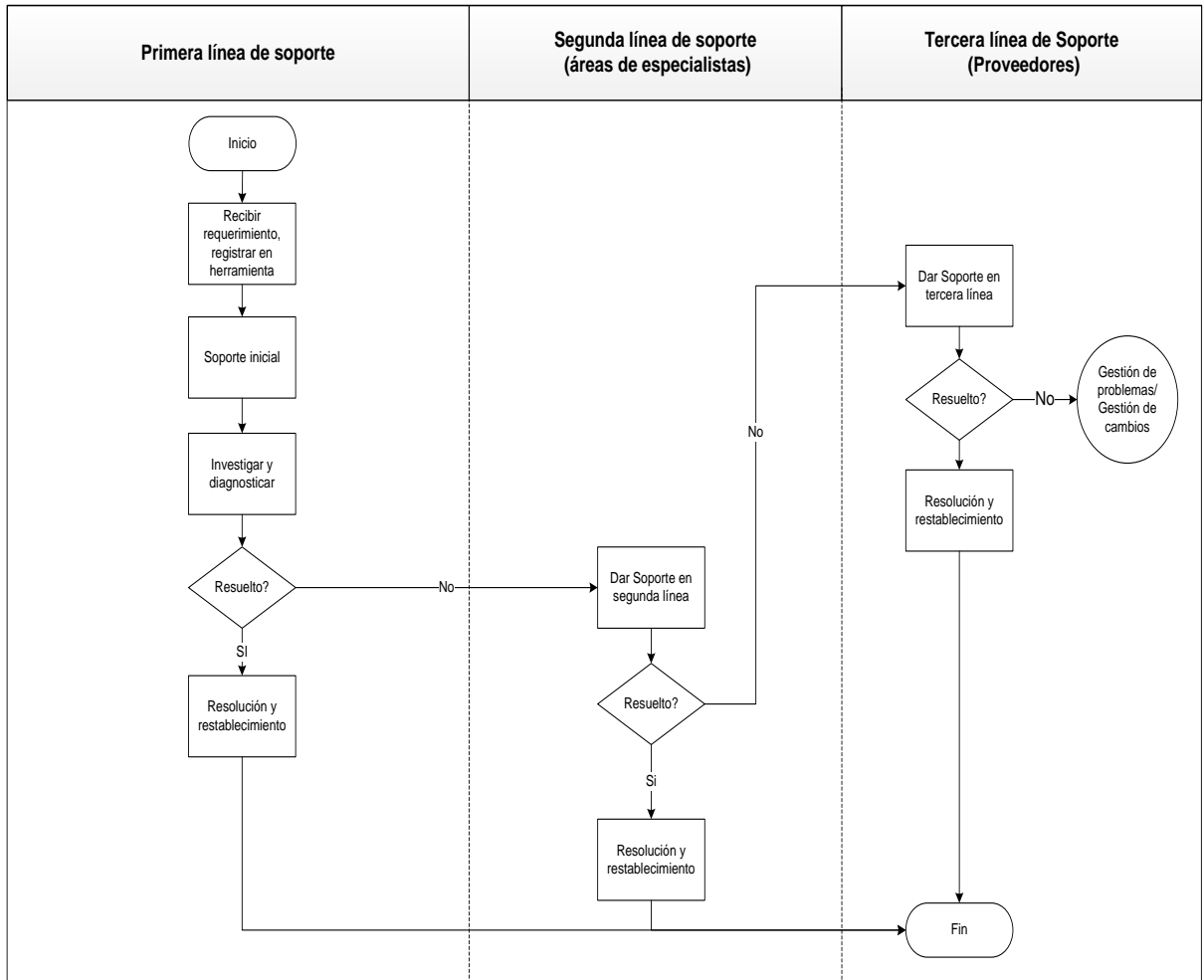
Para entender todas las etapas del proceso en forma gráfica, a continuación, se agrega un diagrama de flujo en donde se puede visualizar de forma simplificada:

Figura 7. Diagrama de Flujo de la Gestión de Solicitudes del Servicio



Fuente: Departamento de Tecnologías de la Información.

Figura 8. **Diagrama de Flujo del Subproceso de Investigación y Diagnóstico de la Gestión de Solicitudes del Servicio**



Fuente: Departamento de Tecnologías de la Información.

2.5.1.1. Canales de comunicación con el negocio

El Departamento de Tecnologías de la Información ha establecido tres canales de comunicación que son la puerta de entrada de toda la información sobre solicitudes de servicio que realizan los usuarios internos. Los canales son teléfono, correo electrónico, medios escritos (memorándums firmados). La unidad que se encarga de administrar los tres canales de comunicación mencionados fue designada por el Departamento de Tecnologías de la Información, su nombre es Mesa de Ayuda, esta también es el área que tiene el papel de primera línea.

2.5.1.2. Ciclo de vida de las solicitudes de servicio

Con base a los distintos factores que se encuentran inherentes en las etapas de atención de un requerimiento o resolución de un incidente, la herramienta que emplea el Departamento de Tecnologías de la Información para la administración de requerimientos e incidentes dispone de diferentes estados, los cuales deben asignarse a la solicitud del servicio lo más acorde al proceso que sigue. A continuación, se describen los estados y cada una de las acciones que deben realizarse para cambiar de uno a otro:

- **Nuevo:** este estado se activa automáticamente cuando se está ingresando la solicitud del usuario a la herramienta mencionada, los requerimientos e incidentes son canalizados a través de mesa de ayuda; en el caso que otras unidades del Departamento de Tecnologías de la Información reciban directamente el reporte de un usuario interno; crean el caso dentro de la herramienta o lo envían a la mesa de ayuda para que la solicitud del servicio sea registrada.

- **Asignado:** este estado se activa cuando se coloca el requerimiento o incidente a la unidad que dará seguimiento y atención a la solicitud del usuario; el mismo puede referirse a todos aquellos casos que no se han empezado a trabajar por los colaboradores.

- **Cancelado:** el colaborador interno del Departamento de Tecnologías de la Información asigna el estado cancelado, cuando la naturaleza del caso no permite ejecutar acciones oportunas para resolver la solicitud del usuario, para tal efecto solicitan autorización a su jefe o supervisor para asignar el presente estado, asimismo comunican al usuario los argumentos que justifican la cancelación de su solicitud.

- **En curso:** el presente estado se asigna al caso en el momento que el colaborador interno del Departamento de Tecnologías de la Información empiece a trabajar con el requerimiento o incidente.

- **Pendiente:** este estado se asigna al caso, cuando por alguna razón deben pausarse las acciones que se están ejecutando para brindar el seguimiento y atención a la solicitud del usuario. El colaborador interno del Departamento de Tecnologías de la Información podría asignar el estado Pendiente por cualquiera de las siguientes razones:
 - La acción necesaria de un tercero, un proveedor interno o externo
 - Cambios en infraestructura
 - Espera de la certificación de cierre por parte del usuario que solicitó el servicio o reportó el incidente.
 - Otras razones debidamente justificadas

Este estado permite conocer los requerimientos y/o incidentes que se necesitan de un agente externo y que no pueden ser controlados por el colaborador que tiene asignado el caso.

- Resuelto: la herramienta de administración de requerimientos e incidentes asigna automáticamente el estado resuelto una vez que recibe por parte del usuario la certificación de la solicitud de servicio. El colaborador que atendió el requerimiento o incidente puede colocar este estado, si el usuario no ha certificado la resolución luego de tres veces que se envió el formulario.

- Cerrado: el estado cerrado, es de uso exclusivo para la unidad de Mesa de Ayuda, dicha área es la única autorizada para asignar este estado a todos los casos que tengan un servicio relacionado. Los colaboradores de la mesa de ayuda para cambiar el caso ha estado cerrado validan en la herramienta de administración de requerimientos e incidentes cualquiera de los siguientes puntos:
 - Que adjunto al caso se encuentre el formulario de certificación contestado por el usuario.
 - Correo de autorización del Subgerente para finalizar la atención del caso.
 - Si el requerimiento o incidente pertenece al listado de servicios recurrentes que no requieren certificación ya que existen algunos que no deben ser certificados por un usuario.

2.5.2. Administración de proveedores

El Departamento de Tecnologías de la Información ha implementado un proceso que tiene como objetivo proporcionar los estándares y requisitos mínimos relacionados con: selección, registro y evaluación de proveedores (hardware, software, y servicios), asegurando a los usuarios que se cuenta con socios de negocio que comparten el compromiso de servicio y calidad. Este proceso establece que todo proveedor debe estar formalizado legalmente mediante un contrato en el que se deben establecer como mínimo los siguientes puntos:

- Alcance y niveles de servicio: cualquier contrato o propuesta debe incluir alcance, niveles de servicio y procesos de comunicación con los proveedores.
- Alineación de los acuerdos de nivel de servicio de los proveedores y de la organización: los acuerdos de nivel de servicio de los proveedores deben cumplir con lo necesario para que se pueda cumplir con los tiempos internos firmados entre el Departamento de Tecnologías de la Información y los usuarios.
- Interfaces de procesos entre proveedores y el Departamento de Tecnologías de la Información: el proceso de solicitud de información y entrega de información se deberá dejar documentada.
- Asegurar que los proveedores tienen definidas y documentadas las subcontrataciones que realizan: se contempla para este punto que se debe verificar claramente si el proveedor tiene definidas y documentadas las subcontrataciones que realiza solicitando evidencia de estos contratos.

- Revisión de proveedores: se conviene que debe realizarse por lo menos una revisión anual de los acuerdos o contratos con los proveedores y el desempeño de los mismos, para asegurar que cumplen con las necesidades, esta revisión la debe realizar el responsable del proveedor.
- Proceso para disputas contractuales: el manejo del proceso para disputas contractuales es manejado por el Departamento de Jurídico de la sociedad (esto según la estructura organizacional).
- Terminaciones y transferencia de obligaciones: se define el proceso para terminaciones y transferencia de obligación de contratos con proveedores.
- Evaluación del desempeño de los proveedores: cada responsable del proveedor evaluará el cumplimiento de su proveedor y se reportará al coordinador de la gestión de proveedores mensualmente.

Es importante resaltar que el proceso de gestión de proveedores es muy ordenado y los controles relacionados con los mismos son rigurosos y se siguen a cabalidad por toda la organización (la gestión parte de políticas institucionales), esto porque la institución debe velar para que la relación que se entable con cualquier proveedor no genere ningún riesgo latente.

2.5.3. Acuerdos de nivel de servicio

El Departamento de Tecnologías de la Información es el encargado custodiar todos los activos tecnológicos, sin embargo, no es el dueño de toda la información que en ellos se almacena. Tomando en consideración esta premisa, pone a disposición los diferentes servicios tecnológicos para los usuarios internos de la institución, haciendo siempre hincapié que todos los cambios y/o mejoras que se relacionen directamente con los sistemas de información o bases de datos deben pasar por cada uno de los procesos de

autorización correspondiente que fueron definidos por las áreas operativas y del negocio.

Anualmente el Departamento de Tecnologías de la Información revisa los servicios tecnológicos que provee y ha designado a cada una de las subgerencias que forman parte del mismo (según la estructura organizacional) como responsables de los diferentes servicios, es decir, las responsabilidades de cada subgerencia son con base a los activos tecnológicos que administra.

Cabe mencionar que esta forma de definir los servicios separó los roles de cada unidad y los mismos no quedaron de forma integral, se hace esta mención ya que se logró identificar qué, para la determinación de los niveles de servicio, algunos servicios que se entregan a los usuarios de la institución dependen de otros sub-servicios tecnológicos (es decir, de otros niveles de servicios internos a cargo de otras subgerencias en el Departamento de Tecnologías de la Información).

Por tal razón cuando se establecieron los niveles de servicio por cada unidad se estimó que las otras subgerencias del Departamento de Tecnologías de la Información de las cuales dependía el servicio también entregarían los sub-servicios con cierto nivel supuesto y esta suposición no se basó en fundamentos claros, únicamente fue de forma empírica, dejando una brecha sobre las verdaderas variables que podrían estar involucradas en la entrega de los servicios. Para cada uno de los acuerdos de nivel de servicio el Departamento de Tecnologías de la Información, incluyó lo siguiente:

- Código de SLA: a todos los acuerdos de nivel de servicio se les asignó un código único con el cual se pudieran identificar específicamente.
- Área: es la subgerencia o unidad que está involucrada en la ejecución del

servicio.

- Nombre del servicio: es el título del servicio
- Vigencia del SLA: es el tiempo en meses de la vigencia del servicio
- Revisión del SLA: se coloca la fecha de próxima revisión de los términos definidos.
- Servicios provistos: se coloca una breve descripción entendible para el usuario final de los servicios y sub-servicios incluidos.
- Servicios excluidos: son los servicios que no forman parte del acuerdo
- Vía de recepción: son los medios autorizados en el que las unidades del Departamento de Tecnologías de Información reciben la solicitud de requerimiento o reporte de incidente (ejemplo: teléfono, correo, entre otros).
- Vía de respuesta: son los medios de comunicación por el cual la unidad del Departamento de Tecnologías de la Información mantendrá informado al usuario durante el proceso de la ejecución del servicio y al finalizar.
- Tiempo de respuesta: es el tiempo máximo de los servicios y sub-servicios que están incluidos dentro del acuerdo.
- Horario de atención: es horario hábil en que se presta el servicio
- Atención fuera de horario: es el horario inhábil para la entidad financiera en que se ejecuta el servicio.
- Penalización: el incumplimiento del servicio o de alguno de los términos definidos es de acuerdo a lo establecido en Reglamento Interior de Trabajo.

2.5.4. Acuerdos de nivel de operación

El Departamento de Tecnologías de la Información estableció todas las relaciones técnicas internas que eran necesarias para que se defieran los

acuerdos de nivel de servicio, es decir, los sub-servicios técnicos que deben realizarse para que se puedan proveer los servicios a los usuarios.

Para este punto también se designó a cada una de las subgerencias que integran el Departamento de Tecnologías de la Información, como responsables de los sub-servicios relacionados a los activos tecnológicos que custodian, sin embargo, cabe mencionar que el departamento en ningún momento relacionó los acuerdos de nivel de servicio con los acuerdos de nivel de operación, por tal razón estos últimos acuerdos mencionados solo se documentaron y nunca fueron efectivos.

Los puntos incluidos en los acuerdos de nivel de operación son:

- Código del OLA: a todos los acuerdos de nivel de operación se les asignó un código único con el cual se pudieran identificar específicamente.
- Área: es la subgerencia o unidad que está involucrada en la ejecución del sub-servicio.
- Nombre del OLA: es el título del sub-servicio
- Descripción: son todos los detalles técnicos que están incluidos en el servicio.
- Vigencia del OLA: es el tiempo en meses de la vigencia del servicio
- Servicios provistos: se coloca una breve descripción entendible para el usuario final de los servicios y sub-servicios incluidos.
- Servicios excluidos: son los sub-servicios que no forman parte del acuerdo.
- Componentes Soportados: son los elementos tecnológicos para la ejecución del OLA (Software, Hardware).
- Vía de Recepción: son los medios autorizados en el que las unidades del Departamento de Tecnologías de Información reciben la solicitud de

requerimiento o reporte de incidente (ejemplo: teléfono, correo, entre otros).

- Tiempo de Respuesta: es el tiempo máximo de los sub-servicios que están incluidos dentro del acuerdo.

2.5.5. Gestión de cambios

El Departamento de Tecnologías de la Información tiene definido y documentado un proceso para registrar, evaluar, aprobar, implementar y revisar todos los cambios relacionados a los servicios tecnológicos, esto con el fin de minimizar los impactos negativos que se puedan llegar a materializar en caso se presentará algún evento no deseado a causa del cambio propuesto.

Existe un coordinador del proceso quien ha definido cinco razones principales por las cuales se puede realizar un cambio que pudiera relacionarse directamente con los servicios y/o activos tecnológicos, estas razones son:

- Solución de errores conocidos: según los diferentes estándares que se encuentran relacionados con la provisión de servicios tecnologías de la información, se indica que existen algunos errores que se presentan con frecuencia sobre los activos tecnológicos (infraestructura, sistemas de información y bases de datos), a estos errores se les aplican soluciones temporales, pero probablemente para solucionar el error de raíz, es necesario realizar cambios que afectan los servicios tecnológicos o por lo menos los indisponen por algún tiempo breve.

Esta actividad no se ejecuta correctamente en el Departamento de Tecnologías de la Información, no se están documentando de forma adecuada los errores conocidos y las diferentes subgerencias realizan

cambios sin notificar al coordinador general del proceso de gestión de cambios.

- Cambios en infraestructura del Centro de Datos Principal y el Sitio Alternativo: la Subgerencia de Operaciones del Departamento de Tecnologías de la Información es el encargado de todo lo que se encuentra en ambos, Centro de Datos.

Sin embargo, únicamente notifican al coordinador del proceso de gestión de cambios cuando deben realizar modificaciones sobre los activos tecnológicos y consideran que podría predisponerse de los servicios en horarios hábiles, sin embargo, la teoría indica que se debería notificar todo cambio no importando si este es menor, mayor o crítico, inclusive de emergencia, ya que al presentarse algún incidente se realizan los cambios si notificarle al coordinador.

- Desarrollo de nuevos sistemas: diariamente la Subgerencia de Desarrollo de Sistemas del Departamento de Tecnologías de la Información, realiza cambios sobre las aplicaciones que automatizan los procesos operativos y del negocio, sin embargo, también implementan nuevos sistemas de información y estos no son reportados al coordinador de cambios.
- Cumplimiento legal o regulatorio: los cambios que surgen por diferentes mitigaciones de hallazgos de algunas auditorías internas o externas, derivan cambios directamente que afectan los servicios tecnológicos o en su defecto los activos tecnológicos, sin embargo, algunos de ellos si se reportan porque el coordinador de cambios es también el coordinador de todos los hallazgos que ingresan al Departamento de Tecnologías de la Información, sin embargo, en muchas ocasiones no se reportan todas las

modificaciones.

- Cambios proactivos en mejorar los servicios: estos cambios se reportan en un 80 %, pero siempre existen brechas donde el coordinador debe solicitar la información ya que la unidad responsable de las modificaciones no registra los cambios.

En términos generales el coordinador del proceso de la gestión de cambios tiene políticas y procedimientos muy elaborados y correctamente documentados, sin embargo, estos términos no se han llevado a la realidad y la práctica y el Departamento de Tecnologías de la Información tiene muchas vulnerabilidades en cuanto a la evaluación, priorización y ejecución de cambios, ya que de todas las modificaciones que se realizan sobre los activos tecnológicos solo se documentan aproximadamente el 1 % y este proceso se debería efectuarse de la mano con el proceso de la gestión de configuración mencionado con anterioridad.

2.5.6. Gestión de problemas

El Departamento de Tecnologías de la Información ha implementado un proceso de gestión que tiene por objeto resolver todas las causas raíz de las interrupciones que afectan la disponibilidad de los servicios tecnológicos.

Según el proceso documentado por el coordinador de la gestión de problemas, indica que el alcance del mismo se enfoca en los siguientes ámbitos:

- **Ámbito reactivo:** en el que se analizan los incidentes de importancia significativa, los cuales ya se materializaron y es necesario buscar la

causa raíz para proponer las soluciones definitivas.

- **Ámbito proactivo:** este se activa el proceso de monitorización sobre los servicios tecnológicos y se analiza la configuración de los elementos que conforman los activos tecnológicos con el fin de prevenir incidentes.
- **Incidentes Repetitivos:** es cuando algún tipo de incidente se convierte en recurrente y tiene un impacto negativo en los servicios tecnológicos, en el proceso se determinan las causas y se proponen las posibles soluciones.
- **Error conocido:** es cuando se conoce la causa de un incidente, pero solo se aplican soluciones temporales y se deben determinar las causas raíz para erradicar el problema.

Según la documentación uno de los controles del proceso es contar con una base de datos de conocimientos, misma que se alimenta con la información de la gestión de incidentes, sin embargo, en el Departamento de Tecnologías de la Información este control es inefectivo porque no se tiene una clara base de datos de incidentes.

Asimismo, el coordinador de la gestión de problemas no se encuentra involucrado directamente en proceso de identificación de problemas y la puerta de entrada del Departamento de Tecnologías de Información, mesa de ayuda, carece de las instrucciones adecuadas para clasificar los problemas, por lo menos los incidentes repetitivos.

Si un problema fuese identificado, este debería de activar los procesos de la gestión de cambios y la gestión de configuración, sin embargo, las tres gestiones actualmente trabajan de forma aislada y esta desintegración no devuelve resultados efectivos, con ellos existen muchos problemas que existen y no se han resuelto de raíz, generando riesgos innumerables de

confidencialidad, disponibilidad e integridad de la información de las áreas de negocio y operativas de la organización.

El coordinador de la gestión de problemas debe generar un reporte con los problemas que se materializaron en un mes calendario, sin embargo, según se revisó la evidencia y los registros muestran que desde junio del 2015 no se ha analizado ningún problema. Esto difiere con la información que se presentan en diferentes registros generados por otros procesos.

2.6. Implementación de servicios nuevos o modificados

La tecnología es una herramienta que se encuentra en constante cambio, por tal razón el Departamento de Tecnologías de la Información ha implementado distintos controles con los que prevé mitigar riesgos que se pueden llegar a materializar por las adaptaciones innumerables que se realizan a los servicios y la automatización tecnológica de los procesos que ejecutan las áreas operativas y de negocio. Los controles que se describen a continuación tienen el fin de minimizar los impactos negativos que se pueden presentar cuando la tecnología no genera el valor agregado que requiere la organización.

2.6.1. Administración de proyectos

El Departamento de Tecnologías de la Información ha designado a un coordinador de proyectos interno que tiene como función principal la administración eficiente de los recursos que integran una propuesta para la implementación de nuevos servicios tecnológicos o la modificación de los mismos.

Básicamente el coordinador de proyectos debe administrar los recursos de las propuestas que se originan internamente en el Departamento de

Tecnologías de la Información; las que se encuentran relacionados con las áreas operativas y del negocio que deben ser ejecutados por las unidades del Departamento de Tecnologías de la Información; y las propuestas que son ejecutados por servicios contratados con proveedores externos.

En la documentación del coordinador de proyectos se tienen políticas y procedimientos que establecen distintos lineamientos, entre ellos el ciclo de vida de los proyectos, el cual está clasificado según las fases de inicio, planificación, implementación y control, estabilización y cierre.

Según los lineamientos se indica que toda propuesta será considera como proyecto cuando se deba llevar a cabo una serie de actividades programadas con un inicio y un final establecidos, los cuales permitan obtener un producto o servicio que cumpla con los requerimientos y expectativas del usuario interno de la organización. Asimismo, se establecen las responsabilidades del coordinador de proyectos, entre las que se pueden mencionar:

- Proveer apoyo para la administración de proyectos en materia de tecnología.
- Dirección centralizada y coordinada de las propuestas que se vuelven proyectos.
- Gestionar y coordinar las actividades y los recursos necesarios de cada propuesta para su implementación y estabilización.
- Coordinar y supervisar el cumplimiento de entregables y fechas del cronograma de trabajo.
- Verificar el cumplimiento del alcance y el costo original del proyecto
- Administrar de forma coordinada cualquier cambio en el alcance, cronograma y costo.
- Coordinar las pruebas y certificaciones

- Coordinar la comunicación del proyecto
- Coordinar la actualización del avance de las actividades del proyecto
- Coordinar la entrega de documentación obligatoria por cada proyecto
- Entregar informes sobre el estado actual de los proyectos

Es importante resaltar que en este proceso se han considerado de forma metódica y minuciosamente cada una de las variables relacionadas, el mismo se encuentra documentado y se realiza de forma ordenada, en el Departamento de Tecnologías de la Información ningún proyecto es iniciado sin el visto bueno del coordinador de proyectos, esta gestión si se ha logrado integrar de forma adecuada con la gestión de cambios y la gestión de configuración de los activos tecnológicos.

2.6.2. Nuevas tecnologías

El Departamento de Tecnologías de la Información ha designado a la Subgerencia de Investigación de Nuevas Tecnologías para poder realizar los análisis correspondientes de todas aquellas nuevas propuestas de tecnología que automatizaran a los procesos operativos y de negocio. Es importante mencionar que existe una Subgerencia de Desarrollo de Sistemas que tiene funciones similares, sin embargo, la diferencia con la Subgerencia de Nuevas Tecnologías es que se realizan investigaciones de las herramientas y soluciones que existen en el mercado y fueron desarrolladas por entidades que tienen este fin.

La clasificación y análisis de los proveedores de software se basa en rigurosos requisitos definidos con las áreas que serán beneficiadas con las nuevas tecnologías, tomando como referencia las funcionalidades que se

necesitan satisfacer. Este proceso se trabaja de la mano con la administración de proyectos, se consideran los mismos lineamientos.

En las políticas y procedimientos implementados por la Subgerencia de Investigación Nuevas Tecnologías se ha definió un sistema de variables que se debe considerar para la evaluación de criterios sobre la selección de proveedores, la cual debe ser transparente e imparcial. Entre los criterios se pueden mencionar el precio, los acuerdos de nivel de servicio que propone el proveedor, la experiencia en el sector, el tiempo de entrega o implementación, las garantías, la certificación de calidad, sus políticas, procedimientos y la entrega del código fuente (en caso la herramienta a contratar solo es software).

Asimismo, la Subgerencia de Investigación de Nuevas Tecnologías considera los siguientes aspectos de control para analizar una propuesta e iniciarla como proyecto formal:

- Viabilidad Técnica del proyecto: es necesario que la investigación del proyecto incluya el detalle, análisis y observaciones relacionados con la evaluación de los activos tecnológicos existentes; es decir, la evaluación de la capacidad instalada y comparada con los requerimientos óptimos (no mínimos) del proyecto evaluado.

De acuerdo con este análisis se determina si los requerimientos tecnológicos (Hardware y Software) actuales son óptimos para el proyecto propuesto o si es necesario adquirir o mejorar los existentes (es necesario calcular el costo respectivo).

- Viabilidad Operativa del proyecto: en este aspecto se incluye la descripción de las principales funcionalidades de la solución actual y las funcionalidades que se espera de un nuevo sistema, se comparan las

funcionalidades de cada uno de los sistemas propuestos y se analizan las brechas existentes. Se incluyen las observaciones negativas y positivas de cada alternativa.

Se realiza el análisis adicional de otros factores que no corresponden a la funcionalidad (garantías, casos de éxito, tiempos de entrega, entre otros). De igual forma se incluye la disponibilidad de personal que estará involucrado en el proyecto: líder del proyecto, coordinador, proveedor de información, personal que participará en las pruebas, personal que se hará cargo del sistema una vez esté en producción y personal de soporte tecnológico.

- Viabilidad Económica /Financiera: en este control se analiza el costo o inversión de cada uno de los rubros que representen la etapa inicial y mantenimiento del proyecto durante cinco años. Para este estudio se considera el costo de todos los recursos para desarrollar, implementar y mantener en operación el proyecto estudiado.

Este detalle se realiza por cada una de las propuestas analizadas, y se solicita al proveedor toda la información necesaria para la implementación y mantenimiento del sistema, cuando son proyectos en materia de tecnología no todos son evaluados por el retorno de inversión que generen a lo largo del tiempo, por lo que, en caso aplique el análisis económico debe centrarse en el análisis de inversión/beneficios de acuerdo con los beneficios tangibles, reducción o ahorro de costos administrativos y operativos, porcentaje de nuevos productos o clientes, mejora en los procesos (automatización), cumplimiento de normativas y regulaciones obligatorias, entre otros beneficios. Se evalúa el presupuesto actual o si es un proyecto para el siguiente año.

- Análisis ROI: en caso aplique, el proyecto incluye un análisis del retorno de Inversión en donde se conoce la tasa de variación que sufre el monto de la inversión al convertirse en los beneficios esperados.

Los controles indicados son los fundamentales, sin embargo, las evaluaciones de nuevas tecnologías pasan por diferentes análisis tanto técnicos como administrativos, en cada evaluación se incluyen validaciones que reafirmen el compromiso de seguridad de la información y faciliten la integración de continuidad del negocio en caso fuera necesario.

2.6.3. Desarrollo de sistemas

El Departamento de Tecnologías de la Información ha designado a la Subgerencia de Desarrollo de Sistemas como el área encargada de desarrollar software que automatice diferentes procesos operativos y/o de negocio a través de las herramientas y/o soluciones que se tienen licenciadas por la compañía.

La Subgerencia de Desarrollo de Sistemas no analiza herramientas ya creadas por otras compañías, se tienen diferentes analistas que se encargan de la creación de aplicaciones, asimismo de proveer el soporte en segunda línea (proceso de gestión de incidentes) para todas aquellas herramientas que ya se encuentran implementadas.

La Subgerencia de Desarrollo de Sistemas ha implementado una metodología en la que debe documentar, analizar, diseñar, desarrollar, probar, liberar y dar mejora continua a los distintos requerimientos realizados sobre los sistemas de información.

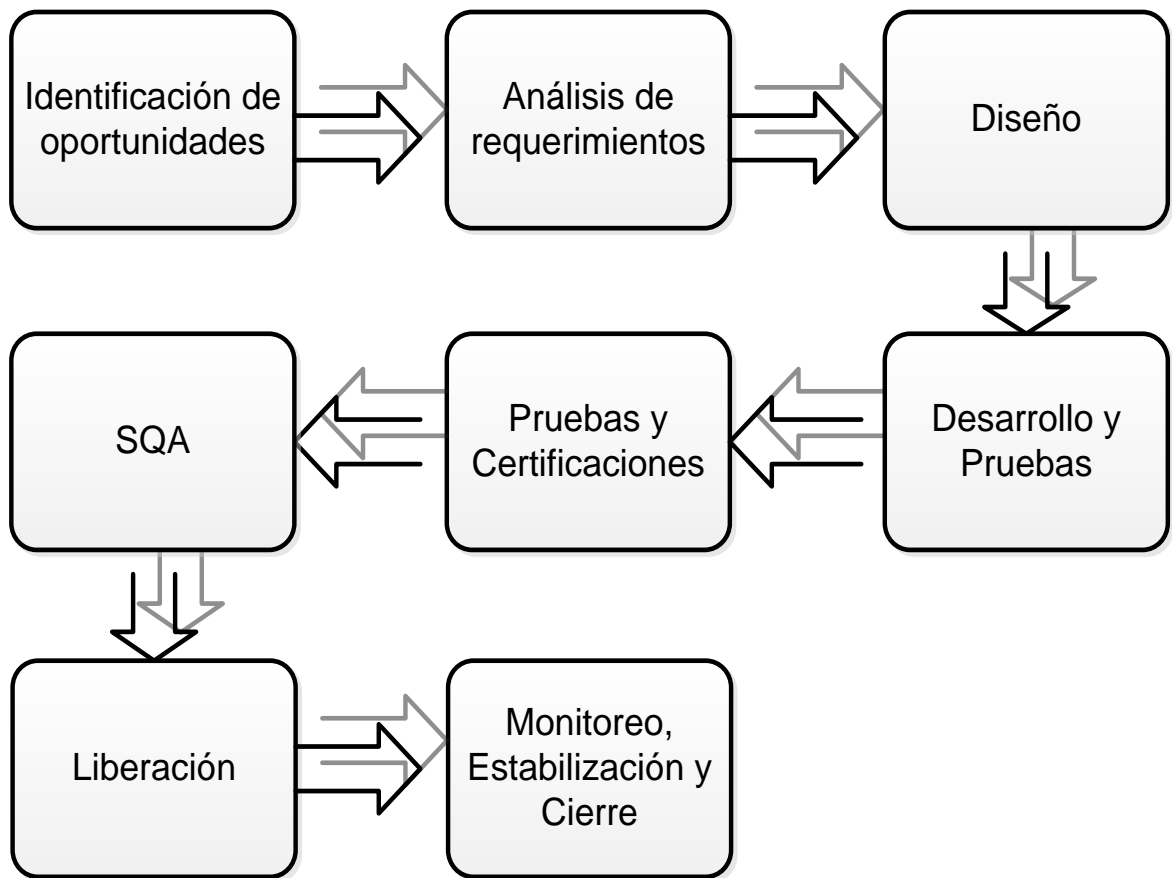
Entre los principales objetivos de esta metodología se pueden mencionar, conocer y satisfacer las necesidades de los usuarios; asegurar la uniformidad y calidad tanto del desarrollo como del sistema en sí; conseguir mayor nivel de rendimiento y eficiencia del personal asignado al desarrollo; ajustarse a los plazos y presupuestos planificados; generar de forma adecuada la documentación asociada a los sistemas; facilitar el mantenimiento posterior de los sistemas; aplicar procesos estandarizados y mejores prácticas.

La metodología implementada tiene diferentes controles asociados que han permitido cerrar las brechas entre diferentes riesgos que existían, a grandes rasgos dicha metodología tiene diferentes etapas que fueron constituidas para contemplar las tareas que se deben realizar en el ciclo de vida del desarrollo de los sistemas de información.

Es importante mencionar que la Subgerencia de Desarrollo de Sistemas emplea diferentes controles para todos aquellos cambios, mejoras o mantenimientos (soporte) que se realizan en el día a día a los sistemas de información ya implementados, esto como parte de la resolución de incidentes.

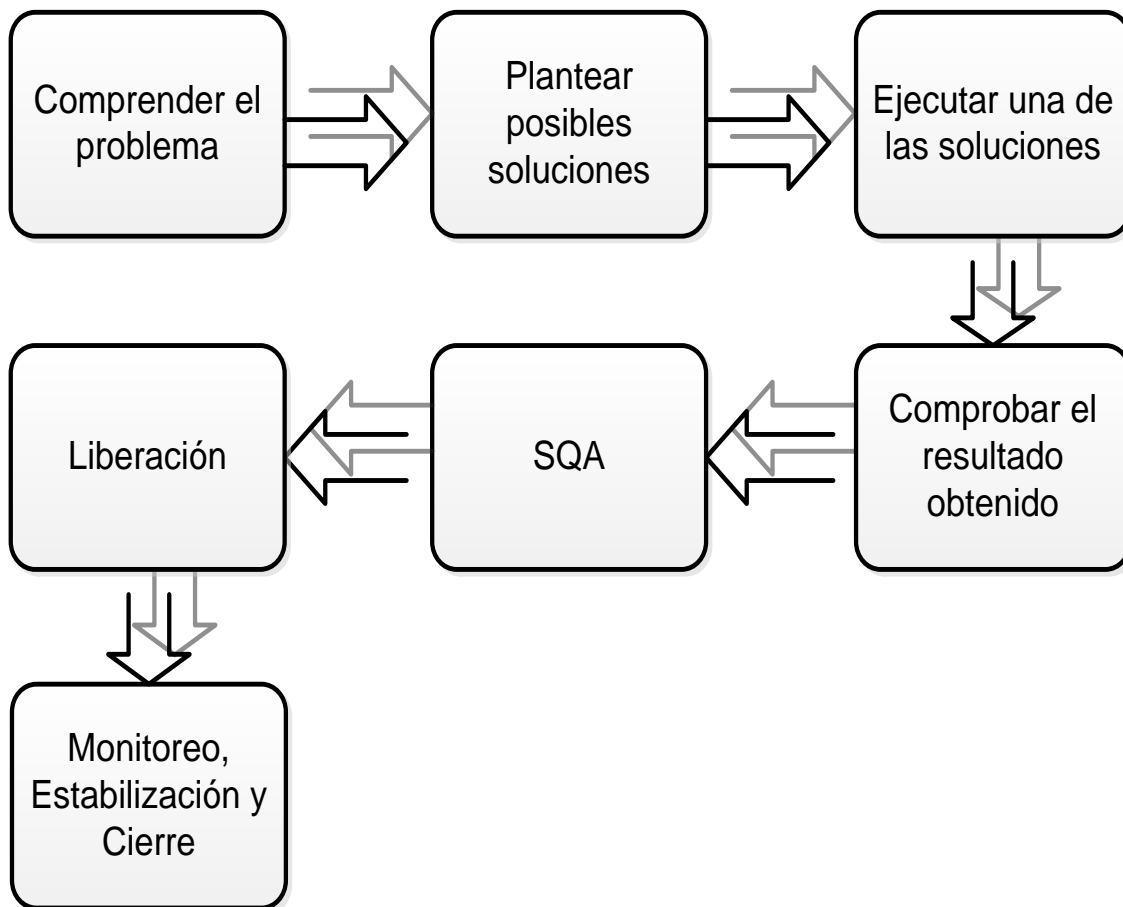
Las siguientes figuras que se muestran a continuación, presentan las diferencias entre las etapas del ciclo de vida de la metodología que se aplica a todos aquellos requerimientos que nacen a partir de un requerimiento de desarrollo nuevo y las etapas del ciclo de vida de la metodología que se aplica a todos aquellos requerimientos de soporte o resolución de incidentes.

Figura 9. **Diagrama del ciclo de vida de la metodología de desarrollo de requerimientos nuevos**



Fuente: Departamento de Tecnologías de la Información.

Figura 10. **Diagrama del ciclo de vida de la metodología de desarrollo para resolución de incidentes**



Fuente: Departamento de Tecnologías de la Información.

2.6.4. **Administración de las bases de datos**

El Departamento de Tecnologías de la Información ha designado a una unidad llamada Jefatura de Administración de Bases de Datos, la cual reporta a

la Subgerencia de Operaciones. Dicha unidad es la responsable de todos los controles relacionados con las bases de datos donde se encuentra almacenada la información.

Con base a distintos factores y características para satisfacer diversas necesidades de la institución, la Jefatura de Administración de Bases de Datos gestiona diferentes manejadores de bases de datos que corresponden a numerosas marcas, para tal efecto ha implementado distintas políticas que permiten proteger los tres pilares más importantes de la información, su confidencialidad, integridad y disponibilidad.

En las bases de datos se encuentra toda la información, por tal razón esta unidad se relaciona directamente con la misma. Considerando esta afirmación, el objetivo fundamental de la Jefatura de Administración de Bases de Datos es definir y establecer los criterios y mejores prácticas para la administración y el uso responsable de los servicios de bases de datos que se encuentran en producción, el término producción se emplea para hacer referencia a la información real que utilizan las áreas operativas y del negocio de la entidad financiera.

Entre las obligaciones de la unidad se debe mencionar la administración de los usuarios que tienen el privilegio de acceder a la base de datos. Por tal razón se definió un procedimiento documentado para la creación, modificación y eliminación de usuarios de bases datos, entre las etapas consideradas en este proceso se puede mencionar:

- Creación de usuarios
- Creación / Modificación de grupos o roles de usuarios
- Asignación / Modificación de permisos a usuarios

- Creación de perfiles
- Asignación de roles
- Reinicio de contraseñas
- Bloqueo de usuarios
- Eliminación de usuarios
- Revisión de la fecha de vencimiento de contraseñas
- Bloqueo por intentos fallidos

Los lineamientos relacionados a los puntos anteriores se publicaron y oficializaron entre las áreas que consumen directamente e indirectamente los servicios de bases de datos, del Departamento de Tecnologías de la Información se pueden mencionar, la Subgerencia de Desarrollo de Sistemas y la Subgerencia de Investigación de Nuevas Tecnologías quienes consumen los servicios en el proceso de atención de requerimientos y resolución de incidentes ya que probablemente es necesario crear, dar mantenimiento, soporte y/o actualizar alguna base de datos nueva o existente.

2.6.5. Aseguramiento de la calidad

Como parte de la metodología de desarrollo existe una etapa llamada aseguramiento de la calidad de software (SQA por sus siglas en ingles) que tiene la función de asegurar que las políticas, procesos y procedimientos son apropiados para el desarrollo de software y la implementación de la solución creada y/o modificada.

Para llevar a cabo esta tarea el Departamento de Tecnologías de la Información se asignó un área responsable quien revisa de principio a fin los requerimientos que realizan las áreas operativas y de negocio; los aspectos que incluye en la evaluación son la definición de la solicitud, el diseño del software,

el estándar de la programación, código, cambios, configuración, pruebas, versiones, documentación y la integración de los productos en todas las interfaces de la herramienta a implementar.

En resumen el aseguramiento de la calidad tiene como finalidad primaria determinar si las necesidades de los usuarios han sido cubiertas de forma satisfactoria y si los estándares establecidos en la metodología del ciclo de vida del desarrollo se han cumplido.

2.6.6. Liberación de servicios nuevos y modificados

El Departamento de Tecnologías de la Información dispone de un control adicional en que se propone gestionar de forma efectiva los servicios nuevos y las actualizaciones que se realizan de los existentes, apoyando en la planificación, diseño, construcción, pruebas y liberación de componentes que conforman el hardware y el software en los ambientes definidos de producción.

Existe un coordinador de este proceso, sin embargo, por los registros que se pudieron observar, se logró determinar que el control únicamente sirve para el análisis de información y elaboración de estadísticas, en todo lo que se encuentra relacionado a software, sin embargo, no analiza de forma profunda las brechas que pudieran llegar a existir sobre la liberación del mismo software y sobre los cambios que se pudieran llegar a materializar sobre el hardware, este control tampoco se encuentra alineado de forma adecuada con el proceso de la gestión de cambios y el proceso de la gestión de configuración.

El proceso de liberación de servicios nuevos o modificados se encuentra correctamente documentado, sin embargo, tampoco se ha logrado llevar completamente a la práctica, la falta de esta actividad no ha permitido que se

pueda madurar el control por tal razón resulta ser una carga de trabajo adicional que según el coordinador no ha generado el valor agregado al sistema de gestión de servicios de tecnologías de la información, en la documentación se mencionan los siguientes lineamientos indicados abajo:

- Política de liberación: existe un documento en donde se encuentran las políticas para la liberación de cambios o nuevos servicios en los ambientes de producción.
- Planificación de liberación: según los controles documentados se debe planificar la liberación de las nuevas o actualizadas versiones de servicios en ambientes de producción, evaluando los requisitos de recursos y el impacto en los usuarios internos de la empresa.
- Preparación de la liberación: en esta actividad se procede a adaptar las instalaciones de hardware o software, modificando si es preciso los medios de almacenamiento y todos aquellos componentes y elementos de configuración necesarios (en caso de que aplique).
- Adiestramiento: según la documentación es necesario impartir capacitación, de acuerdo con lo realizado en el plan de liberación a distintos niveles.
- Coordinar fechas de liberación: para realizar los cambios en los ambientes de producción, esto se debería administrar a través del proceso de gestión de cambios.
- Reporte de resultados: es necesario generar informes que deberán ser llenados por el área que liberó el servicio tecnológico.
- Evaluación y mejora de procesos: la efectividad y eficiencia del proceso se revisa según la frecuencia planificada. En esta etapa del proceso, se debería elaborar un plan de mejora en el que se desarrollen las propuestas, incluyendo: deficiencias, oportunidades de mejora detectadas, expectativas y beneficios de las mismas, posibles impactos,

riesgos dentro y fuera del proceso, requerimientos de recursos, materiales, necesidades de capacitación y pruebas.

Las propuestas de mejoras son revisadas por los grupos afectados para lograr el acuerdo y proceder a su implementación.

- Plan de remediación: para todas las liberaciones que se realicen en los ambientes de producción es necesario definir un plan de remediación que se pueda aplicar en caso la implementación del nuevo servicio o el modificado no funcione correctamente y por tal razón se tenga como regresar a un estado anterior.
- Las liberaciones de emergencia. deberán ser realizadas en base al proceso de cambios de emergencia que se define en la gestión de cambios, (esto no se encuentra integrado).
- Pruebas: previo a liberar nuevos cambios o servicios en los ambientes de producción, deberán realizarse las pruebas necesarias para certificar los cambios.
- Reporte de liberación: el coordinador del proceso genera un reporte mensual en donde considera los fallos en las liberaciones y este mismo le sirve al Departamento de Tecnologías de la Información para mantener una bitácora de conocimiento de errores.

Es necesario reiterar que, de los puntos mencionados, no todos son efectuados, porque no existe una sub-etapa de control en donde se verifique que todas las actividades documentas se estén efectuando.

2.7. Análisis de desempeño

El Departamento de Tecnologías de la Información ha nombrado a un coordinador para que verifique de forma periódica que todos los procesos de

control, los cuales prevén mitigar riesgos en la provisión de los servicios tecnológicos, generen resultados positivos siendo de esta forma efectivos y procurando llegar a ser eficientes.

2.7.1. Relación del negocio y tecnologías de información

El Departamento de Tecnologías de la Información ha implementado un proceso que tiene la intención de establecer los mecanismos necesarios con el fin de mejorar continuamente la relación que existe entre los servicios tecnológicos que se proveen y todos los usuarios de la entidad, considerando la búsqueda de la satisfacción del cliente y la entrega de valor a través de una correcta alineación estratégica de las necesidades de las distintas áreas.

El objetivo principal de los mecanismos que se establecen en este proceso de gestión es conocer las necesidades y los cambios en el entorno del negocio, para que se pueda responder efectivamente. Por tal razón el coordinador de este proceso debe comprender dicho entorno y alinear los proyectos y/o propuestas tecnológicas que se prevén desarrollar para contribuir a las estrategias y objetivos planteados por la organización a corto, mediano y largo plazo.

Al integrar esta información el resultado debería ser un plan estratégico de tecnología de la información que coopere con la institución y camine en la misma dirección.

Adicionalmente a los canales de comunicación que tiene establecidos el Departamento de Tecnologías de la Información con el negocio, también ha implementado un correo electrónico en el que todos los usuarios de la

institución que consideren necesario comunicar una queja sobre la prestación de los servicios tecnológicos, puedan hacerlo y recibir una retroalimentación inmediata.

Para el tratamiento de los reportes que se reciben en el correo mencionado se ha establecido una metodología de registro, identificación, revisión y seguimiento.

El coordinador del proceso de análisis de desempeño mensualmente elabora un reporte con las quejas recibidas y lo analiza en conjunto con el gerente del Departamento de Tecnologías de la Información, esto con el fin de conocer el índice de satisfacción de los usuarios y que se puedan implementar las acciones preventivas, detectivas y correctivas en búsqueda de mejorar el servicio.

2.7.1.1. Encuestas de satisfacción

Cada vez que los colaboradores del Departamento de Tecnologías de la Información resuelven una solicitud de servicio, la herramienta que administra los requerimientos e incidentes, envía una solicitud al usuario para confirmar el que la atención proporcionada fue la adecuada y la resolución cumplió con las expectativas que dicho usuario esperaba.

El usuario recibe un formulario en donde se le solicitan distintas pruebas que le permiten corroborar que la solución aplicada al requerimiento o incidente fue la óptima, asimismo se le solicita que pueda calificar el servicio, tomando en consideración si fue entregado lo que solicitó y la calidad de atención que recibió.

El usuario tiene un listado en el que puede indicar cuál es el índice de satisfacción, las literales definidas para la calificación son:

Tabla I. **Índices de calificación de los usuarios sobre los servicios tecnológicos**

Índice	Descripción
5	Deficiente de lo solicitado
6	Muy por debajo de lo solicitado
7	Menos de lo solicitado
8	Requiere mejorar lo solicitado
9	Lo solicitado
10	Satisfactorio a lo solicitado
11	Más de lo solicitado
12	Excedió lo solicitado

Fuente: Departamento de Tecnologías de la Información.

El coordinador de análisis de desempeño mensualmente genera un reporte estadístico para conocer el resultado de las calificaciones colocadas por los usuarios, todas aquellas notas que se encuentran debajo del nueve (9, lo solicitado), se analizan profundamente y se indaga con el usuario para poder obtener retroalimentación e intentar mejorar el servicio.

2.7.2. Gestión de disponibilidad y continuidad de los servicios

El Departamento de Tecnologías de la Información ha implementado un proceso el cual tiene por objeto aplicar las medidas de control que impidan una

imprevista y grave interrupción de los servicios tecnológicos, debido a desastres naturales y otras fuerzas de causa mayor, tenga consecuencias catastróficas para el negocio. La estrategia de este proceso es que combina equilibradamente controles proactivos que buscan minimizar las consecuencias de una grave interrupción del servicio y controles reactivos cuyo propósito es reanudar el servicio tan pronto como sea posible.

El negocio en sí de la entidad es mantener la disponibilidad absoluta de los servicios tecnológicos, por otro lado los cambios tecnológicos implican una renovación constante de equipos y servicios que deben monitorearse menos, pero que de igual forma pueden correr diferentes riesgos que pueden poner en peligro la disponibilidad de la información resguardada en la infraestructura tecnológica.

El mayor reto del Departamento de Tecnologías de la Información es evolucionar, sin el mínimo margen de error pues los sistemas de información son usados por clientes y partes interesadas en cualquier momento, por tal razón siempre existe la necesidad de optimizar los recursos tecnológicos para que estos funcionen ininterrumpidamente de manera fiable, cumpliendo con los acuerdos de nivel de servicio establecidos.

Este proceso dispone de diferentes actividades de monitorización por diversas herramientas, que son empleadas diariamente por las unidades del Departamento de Tecnologías de la Información que custodian directamente los activos tecnológicos. Todas las tareas de monitorización generan informes que le permiten conocer de manera integral cual es el porcentaje de disponibilidad de los servicios en un período determinado.

El Departamento de Tecnologías de la Información se ha fijado la meta de proveer los servicios con un 99,99 % de disponibilidad, para conocer este dato se ha nombrado a un coordinador de la gestión que a través de información variada que solicita a las unidades correspondientes, aplica distintas fórmulas para conocer en promedio cual es el porcentaje que se tuvo en periodo en particular.

Según la evidencia que se tuvo en observación se logró identificar que este proceso es efectivo para el Departamento de Tecnologías de la Información, esto debido a que gracias a los datos que se genera en los distintos reportes, se han podido implementar distintas acciones que continúan mejorando el porcentaje de disponibilidad de los servicios tecnológicos.

2.7.2.1. Plan de Recuperación de Desastres (DRP)

El Departamento de Tecnologías de la Información como parte de la gestión de disponibilidad y continuidad de los servicios, ha creado un plan que tiene por objetivo contar con los servicios tecnológicos necesarios en caso se materialice un evento catastrófico no deseado que predisponga el centro de datos principal e imposibilite la provisión de dichos servicios.

En principio el plan documentado sirve actualmente como guía y modelo para recuperar las operaciones de tecnología en el centro de datos alterno. Se han considerado los procesos administrativos y operativos importantes de cada unidad del departamento mencionado, con el fin de que sean recuperados los servicios en un tiempo estipulado que no afecte los acuerdos de nivel de servicio.

Es importante mencionar que el plan se encuentra muy bien documentado, sin embargo, la práctica vuelve a jugar un papel importante ya que el Departamento de Tecnologías de la Información fue quien a través de su criterio empírico definió que servicios serían replicados en el Centro de Datos Alterno, dicha actividad debe ser establecida y administrada por un ente y/o área de la empresa que tenga el pleno conocimiento del entorno del negocio y su vez pueda definir qué procesos son críticos para la organización.

Los servicios tecnológicos que actualmente se replican en el Centro de Datos Alterno son importantes, sin embargo, no se pudo determinar si son los que necesita la empresa para mantenerse en caso se materializará un evento no deseado.

Según los registros que se tuvieron a la vista, se logró determinar que este plan no ha sido utilizado en ningún momento por el Departamento de Tecnologías de la Información, inclusive ni en ambientes controlados para comprobar que las actividades documentadas son capaces de dar continuidad a las operaciones de tecnologías de la información.

2.7.3. Informes de desempeño

El coordinador del análisis de desempeño mensualmente solicita a los coordinadores de los diferentes procesos de gestión, información relevante que emplea para evaluar y validar el estado actual del Departamento de Tecnologías de la Información en base a las metas trazadas. Al consolidar la información, realiza un análisis exhaustivo que le permite proponer acciones que mejoren continuamente la provisión de los servicios tecnológicos.

Los reportes que se generan en el análisis del desempeño son presentados a la Gerencia Dirección de Operaciones que según la estructura organizacional de la entidad financiera es a quien reporta el Departamento de Tecnologías de la Información. Se llevan a cabo distintas reuniones con el objetivo de evaluar el cumplimiento de los objetivos del negocio y como los servicios tecnológicos aportan valor.

La adecuada interpretación de los resultados obtenidos le ha facilitado al Departamento de Tecnologías de la Información, tomar decisiones importantes y emplear métodos de comunicación eficaces.

3. PROPUESTA PARA DISEÑAR EL MARCO INTEGRAL DE TRABAJO PARA GESTIONAR EL RIESGO TECNOLÓGICO

3.1. Organización para la administración del riesgo tecnológico

La organización deberá implementar la estructura de un gobierno corporativo, en el cual se reconozca a todos los involucrados para la organización, desde inversionistas hasta terceros interesados; esto con el fin de que las decisiones a considerar sean para el beneficio de la institución en general.

Básicamente en un gobierno corporativo se delegan de forma vertical y estricta las responsabilidades y prácticas ejecutadas por el Consejo Directivo y la administración ejecutiva, con el objetivo de proveer dirección estratégica en todos los ámbitos, garantizando que los objetivos sean alcanzados, administrando apropiadamente los riesgos y verificando que los recursos de la empresa sean empleados responsablemente.

3.1.1. Políticas y procedimientos

Para la correcta administración del riesgo tecnológico, la definición de políticas y documentación de procedimientos que se prevean establecer, serán la estructura y base fundamental en las que serán soportadas las decisiones relacionadas con tecnologías de la información, para el cumplimiento de los objetivos institucionales.

En las políticas y procedimientos se deberán contemplar como mínimo las metodologías, herramientas, modelos de medición del riesgo tecnológico y análisis de puntos clave estratégicos, asimismo lo más adecuado y sencillo será agrupar los lineamientos de la siguiente forma:

- Infraestructura de TI, sistemas de información, bases de datos y servicios de TI.
- Seguridad de tecnología de la información
- Procesamiento de información y tercerización

3.1.2. Responsabilidades del Consejo Directivo

El Consejo Directivo será responsable en principio por la gestión de los recursos asignados a Tecnologías de la Información. Sin perjuicio de cualquier otra disposición legal aplicable a dicha unidad, se considera oportuno que sea participante activo como mínimo en los siguientes temas, para el adecuado funcionamiento y ejecución de la administración del riesgo tecnológico:

- Verificar, corregir (cuando sea necesario) y aprobar anualmente las políticas y procedimientos relacionados con la administración del riesgo tecnológico.
- Proveer los lineamientos para la creación de un Plan Estratégico Organizacional del cual se derive un Plan Estratégico de Tecnologías de Información.
- Aprobación de los recursos mínimos necesarios para la creación de un Plan de Continuidad de Operaciones de TI.
- Conocer anualmente reportes sobre la exposición al riesgo tecnológico, los cambios sustanciales de tal exposición y su evolución en el tiempo.
- Aprobar las medidas preventivas y correctivas adoptadas para la gestión

del riesgo tecnológico.

- Conocer anualmente reportes sobre el cumplimiento de las políticas y procedimientos aprobados, asimismo las propuestas sobre acciones a adoptar con relación a los incumplimientos.

El Consejo Directivo deberá constar en un acta todos los lineamientos acordados.

3.1.3. Comité de Riesgos

El Comité de Riesgos deberá ser designado por el Consejo Directivo y estar integrado por un miembro de dicha unidad, asimismo por autoridades y funcionarios con participación y voto para líneas importantes de negocio y relacionadas en la consecución de los objetivos importantes para la compañía.

El Comité de Riesgos podrá contar con atribuciones relacionadas a la gestión de diversos riesgos, por tal motivo será el responsable de la dirección de la administración del riesgo tecnológico. Bajo esta premisa el Comité deberá encargarse de la implementación, adecuado funcionamiento y ejecución de las políticas y procedimientos aprobados para este propósito, adicional deberá coordinar lo siguiente:

- La creación anual del Plan Estratégico Institucional, Plan Estratégico de TI, Plan de Continuidad de Operaciones de Tecnologías de Información.
- La creación, modificación y mantenimiento de un Manual de Administración del Riesgo Tecnológico.
- Analizar, evaluar y proponer los cambios necesarios a las políticas y procedimientos relacionados con tecnologías de información.
- Definir la estrategia para la implementación de las políticas y

procedimientos aprobados para la administración de riesgo tecnológico y su adecuado cumplimiento.

Las sesiones y acuerdos del comité deberán constar en acta suscrita por quienes intervinieron.

3.1.4. Departamento de Riesgos

La empresa dentro de su esquema organizacional deberá constituir permanentemente un área que se dedique única y exclusivamente a la identificación, medición, monitoreo, control, prevención y mitigación de riesgos, es decir, una unidad que gestione el riesgo de forma holística en toda la organización.

El Departamento de Riesgos, en el ámbito de administración del riesgo tecnológico, deberá como mínimo realizar lo siguiente:

- Crear y modificar las políticas y procedimientos para la administración del riesgo tecnológico, asimismo el Plan Estratégico, el Plan Estratégico de TI, el Plan de Continuidad de Operaciones de TI.
- Revisar al menos anualmente y/o cuando se considere necesario las políticas y procedimientos y proponer su actualización al Comité de Riesgos, atendiendo los cambios en la estrategia o situación de la institución o cuando lo requiera la normativa.
- Monitorear periódicamente la exposición al riesgo tecnológico y mantener registros históricos sobre dicho monitoreo, así como medir el riesgo tecnológico.
- Analizar y evaluar el riesgo tecnológico inherente de los proyectos de innovación en Tecnologías de la Información, los cuales se implementen

en la institución y los que se deriven de los nuevos productos y servicios propuestos por las unidades de negocios.

- Reportar al comité semestralmente y/o cuando sea necesario 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 de Riesgos las medidas correctivas correspondientes, las cuales deben ser acordadas con el Departamento de Tecnologías de la Información.
- Implementar la metodología adecuada para determinar el nivel de cumplimiento de las políticas y procedimientos aprobados, asimismo identificar causas de posibles incumplimientos e indicar si estos se presentan en forma reiterada, proponer medidas correctivas y preventivas. Mantener el registro histórico sobre tales incumplimientos.

3.1.5. Planeación estratégica

La administración ejecutiva deberá documentar de forma adecuada un plan estratégico de negocios, el cual les permita a los funcionarios y autoridades de la entidad financiera, conocer hacia donde está orientada la organización. Con estos lineamientos como base, todos los insumos serán direccionados para la consecución de propósitos y objetivos comunes, por tal motivo los activos tecnológicos de información y todo lo relacionado.

La administración del riesgo tecnológico está directamente relacionada con la planeación estratégica de la organización, esto se debe a que las evaluaciones que se realizan para identificar y monitorear los riesgos se hacen considerando la directriz que toda la organización debe seguir, teniendo como objetivo final el alcanzar las metas fijadas, mismas que podrían traducirse en crecimiento económico, financiero, humano o tecnológico. Por el giro de

negocio que tiene la empresa sus planes estratégicos pueden ser a corto, mediano y largo plazo.

3.1.6. Planeación estratégica de tecnologías de información

La sociedad deberá tener un plan estratégico de tecnologías de la información que se encuentre alineado con el plan estratégico de negocios, esto con el fin de formular, implantar y evaluar las decisiones internacionales que se deben hacer para gestionar la infraestructura de TI, los sistemas de información, las bases de datos y los planes de carrera de los colaboradores directamente relacionados con tecnologías de la información.

Los aspectos que como mínimo deberá contemplar la entidad en el Plan Estratégico de Tecnologías de información son:

- Los objetivos de tecnologías de la información deberán estar alineados con la estrategia de negocios.
- Indicar las oportunidades, limitaciones y desempeño de tecnologías de la información.
- La descripción de proyectos, actividades específicas y estrategias para la consecución de objetivos.
- Detallar el presupuesto financiero para la ejecución del plan

3.2. Recursos tecnológicos

El Departamento de Tecnologías de la Información deberá implementar la metodología adecuada, que le permita contar con inventarios actualizados de todos los activos y/o recursos tecnológicos. Este control deberá ser riguroso y estricto, debido a que existe una cantidad innumerable de riesgos relacionada a la ejecución de controles débiles en inventarios.

3.2.1. Clasificación de los recursos tecnológicos

El Departamento de Tecnologías de la Información deberá dar un tratamiento diferente a cada uno de los recursos tecnológicos, esto se debe a que los mismos están relacionados a distintos procesos de la organización.

Por este motivo el Departamento de Riesgos deberá designar el Recurso Humano necesario, a fin de poder identificar cuáles son los procesos más importantes y/o críticos para la organización, de esta forma el Departamento de Tecnologías de la Información podrá organizarse para poder clasificar los recursos tecnológicos, esta acción es primordial para poder conocer cuales activos de tecnología de información son los críticos para que el negocio pueda dar continuidad a sus operaciones en caso se viera afectado por un evento no deseado que predispusiera de la operaciones.

El Departamento de Tecnologías de la Información luego de conocer la relación que tienen los activos tecnológicos con los procesos críticos e importantes para la organización, deberá establecer los lineamientos que le permitan administrar el riesgo y asegurar la disponibilidad de la tecnología de información.

3.2.2. Mapas de interdependencia

Está claro que toda organización cuenta con diferentes procesos que según su finalidad representan cierta importancia para el cumplimiento de metas y objetivos trazados. Por esta razón al igual que los recursos tecnológicos, los procesos también deben ser clasificados, una vez se conozca una estructura definida para los procesos, la empresa deberá emplear distintas metodologías para hacer un inventario en el que se deberá indicar y/o señalar que proceso es crítico, de alto, medio y/o bajo impacto para la organización.

Según la relación que guarden los activos tecnológicos con esta disposición así será el tratamiento para mitigar el riesgo tecnológico inherente al que podrían encontrarse expuestos.

Los Mapas de Interdependencia básicamente son esquemas que representan la interrelación que tienen los recursos e insumos que son necesarios para ejecutar algún proceso, notoriamente se incluyen los activos tecnológicos.

De esta forma la organización deberá elaborar lo siguiente:

- Esquemas de información sobre procesos donde se pueda visualizar la interrelación que existe entre el recurso humano, mobiliario y equipo, infraestructura física, proveedores, sistemas de información y otros procesos.
- Esquemas donde se pueda visualizar de forma técnica, que requieren los sistemas de información suscritos en los esquemas de información de procesos, indicando como mínimo cuál es la infraestructura tecnológica,

bases de datos, dispositivo de almacenamiento, seguridad y red, asimismo colaboradores del Departamento de Tecnología y proveedores de tecnologías de la información.

3.2.3. Base de datos de configuración

El Departamento de Tecnologías de la Información ha implementado un control para registrar la configuración de los recursos tecnológicos, este proceso tiene algunas vulnerabilidades que se deben corregir.

La base de datos de configuración (CMDB, por sus siglas en ingles), es un repositorio donde se puede visualizar la especificación técnica actual e histórica de cada uno de los activos tecnológicos; actualmente se actualiza de forma mensual, sin embargo, el Departamento de Tecnologías de la Información deberá implementar un control automático o manual para que cada vez que se realiza un cambio sobre algún parámetro de los elementos de tecnología, este se vea reflejado en la base de datos, resguardando asimismo el estado anterior, por motivos de seguridad y de disponibilidad en caso se tuviera que aplicar un plan de restauración.

La CMDB que muestra la información de los recursos tecnológicos deberá como mínimo incluir los siguientes elementos por cada activo:

Tabla II. **Elementos de la Base de Datos de Configuración**

Elementos de Configuración		
Infraestructura Tecnológica	Especificaciones Técnicas	Tipo
		Nombre
		Función
	Ubicación Física	Tipo de Mantenimiento
Sistemas de Información	Características de los sistemas de información	Centro de Datos
		Nombre
		Función
		Lenguaje de programación
		Versión
		Estructura del sistema
		Desarrollado por...
	Componentes	
Documentación Técnica	Solución de Problemas	
Documentación usuario	Manual	
Instancias de Bases de Datos	Manejadores	Nombre
		Versión
		Mantenimiento
Bases de Datos	Descripción General	Nombre
		Manejador
		Sistema de Gestión Archivos
		Versión
		Diccionario de Datos
		Diagramas de relación
		Administrador

Fuente: Resolución JM-102-2011.

3.2.4. Unidad de administración de bases de datos

La organización reconoce que en las bases de datos se encuentra toda la información, por tal razón en el Departamento de Tecnologías de la Información existe la Jefatura de Administración de Bases de Datos, esta unidad deberá garantizar la seguridad, integridad, disponibilidad y confidencialidad de la información, a través de políticas documentadas para la gestión adecuada de accesos, creación, actualización o eliminación de estructuras.

3.2.5. Monitoreo de los recursos tecnológicos

Una de las estrategias de la entidad financiera es proporcionar la máxima disponibilidad de los servicios que provee a sus clientes; muchos de estos servicios están respaldados por los procesos y recursos tecnológicos, estos últimos deberán estar ligados a un proceso de verificación y monitoreo que permita conocer la capacidad y el desempeño, ya que puede existir el riesgo de que se materialicen incidentes que predispongan de los servicios por causa del desconocimiento del estado actual y en tiempo real de los activos tecnológicos.

La infraestructura tecnológica y las bases de datos constantemente están cambiando, no se mantienen en un formato estático, dicho esto es necesario que el Departamento de Tecnologías de la Información tenga siempre el recurso disponible para soportar la demanda de los servicios.

El Departamento de Tecnologías de la Información deberá conocer las tendencias de la demanda de los servicios tecnológicos, considerando esto se deberá realizar semestralmente un plan de capacidad en donde se pueda evaluar el recurso humano, tecnológico y financiero. Básicamente el plan

deberá priorizar las áreas que pueden sufrir alguna carencia de insumos, y el resultado será concentrarlos donde sea necesario para no incurrir en falencias.

3.2.6. Adquirir, mantener e implementar recursos tecnológicos

La Subgerencia de Investigación de Nuevas Tecnologías del Departamento de Tecnologías de la Información, ha implementado controles rigurosos para la adquisición e implementación de recursos tecnológicos, el fin de los controles mencionados es garantizar la disponibilidad y continuidad de los servicios de tecnologías de la información, sin embargo, se deberán revisar las políticas y procedimientos para asegurar que como mínimo se contemplan los siguientes aspectos:

- Selección de proveedores formales, que se encuentren relacionados al giro del negocio de la empresa, contratados bajo el principio de imparcialidad, sin beneficio individual. Se debe considerar la factibilidad tecnológica y económica.
- En lo referente a implementación de nuevos recursos tecnológicos se deberá considerar la realización de pruebas, el registro de incidentes o posibles cambios, el monitoreo del proyecto de inicio a fin, hasta la estabilización.

3.2.7. Administración de los servicios tecnológicos

El Departamento de Tecnologías de la Información ha definido acuerdos de nivel de servicio (SLA por sus siglas en ingles), acuerdos de nivel de operación (OLA por sus siglas en ingles), y un catálogo de los servicios

tecnológicos que le proveen a las diferentes áreas y departamentos de la empresa.

A través del catálogo definen cuales son los requerimientos que atienden y los incidentes que resuelven, por tal razón para administrar correctamente los recursos se deberá como mínimo verificar que se consideren los siguientes aspectos:

- El catálogo deberá definir los servicios tecnológicos de información en forma entendible para todos los usuarios y colaboradores de la organización. Básicamente se prevé que todo el personal de la organización deberá emplear el catálogo mencionado, para poder realizar requerimientos al Departamento de Tecnología de Información.
- Los acuerdos de nivel de servicio se deberán firmar entre el Departamento de Tecnologías de la Información con los funcionarios y autoridades de la compañía, como mínimo se debe mencionar los compromisos de las áreas y/o departamentos, los compromisos de las áreas de Tecnologías de Información, los requerimientos de soporte para el servicio de tecnología, las condiciones, el registro, monitoreo y actualización para la mejora continua.
- El Departamento de Tecnologías de la Información tiene implementado un proceso de gestión de incidentes y un proceso de gestión de problemas, ambos se encuentran bien estructurados ya que están basado en los lineamientos establecidos por la norma ISO 20000, sin embargo, se deberán verificar aspectos tales como la clasificación, registro, atención, análisis de tendencias y monitoreo de los incidentes presentados por los usuarios. Se deberá tener correctamente

documentado el escalamiento de incidentes y en qué circunstancias aplica, esto mismo con la identificación, análisis, registro y monitoreo de la causa raíz de los posibles problemas y su posterior resolución.

- El Departamento de Tecnologías de la Información tiene documentado un proceso de gestión de cambios de los activos tecnológicos bastante completo y riguroso, sin embargo, se considera oportuno revisar que si se incluyen aspectos tales como la evaluación del impacto, priorización y autorización del cambio, así como el tratamiento de los cambios de emergencia, la realización de pruebas el registro y monitoreo del cambio.

Los controles del proceso de gestión de cambios deberán ser automatizados debido a la cantidad de cambios que se realizan sobre los activos tecnológicos, estos controles tendrán que estar de la mano con el proceso de gestión de la configuración.

3.2.8. Ciclo de vida de los sistemas de información

El Departamento de Tecnologías de la Información para la implementación de nuevos sistemas de información o modificaciones en los que ya se encuentran implementados, ha adoptado una metodología bastante amplia con el fin de garantizar la disponibilidad de todas las herramientas tecnológicas.

La metodología deberá asegurar que las actividades de desarrollo de sistemas, ambiente de pruebas y de producción se realizan por separado, asimismo que los lineamientos documentados y ejecutados garantizan el análisis, diseño, desarrollo, pruebas, puesta en producción, mantenimiento, control de versiones y control de la calidad de los sistemas de información.

3.3. Seguridad de la tecnología de información

La organización deberá gestionar la seguridad de la información en todos los ámbitos. En la institución la información se puede presentar en diferentes medios, sin embargo, el resguardo principal está en las bases de datos.

3.3.1. Seguridad de la información

El Departamento de Riesgos deberá considerar los controles expuestos por la norma ISO 27001, a fin de poder garantizar la seguridad de la información. Para este sistema de gestión también se deberá designar a una persona responsable para que pueda liderar y dirigir un Sistema de Gestión de Seguridad de la Información en la organización.

Los controles que se deben considerar serán todos aquellos que la institución pueda aplicar, sin embargo, como al inicio no será un tema de certificación sino más bien de gestión y mitigación de riesgos tecnológicos, es recomendable priorizar los recursos.

La Jefatura de Administración de Bases de Datos gestiona los controles lógicos para la seguridad de la información en estos activos, por tal razón la Subgerencia de Seguridad Informática del Departamento de Tecnologías de Información deberá estar involucrado para que exista una unidad ejecutora y una verificadora, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos, así como mitigar los riesgos de pérdida, extracción indebida y alteración de la información.

Es importante mencionar que en temas de seguridad de la información no solo es importante considerar los controles lógicos, si no también son

relevantes los controles físicos como por ejemplo, las medidas de acceso biométrico, la ubicación de la infraestructura física, cámaras de video vigilancia, guardias de seguridad, registro de visitantes, importación y extracción de equipos, entre otros.

El delegado oficial de la organización, en temas de seguridad de la información deberá estar por encima estructuralmente del Departamento de Tecnologías de Información, asimismo será revisor y aprobador antelar de los controles implementados, por esta razón deberá considerar lo siguiente:

- Deberá identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
- Deberá implementar las directrices para que todos los empleados y usuarios de los activos de información devuelvan los mismos al terminar su empleo, contrato o acuerdo.
- Desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación adoptado por la organización.

3.3.1.1. Identificación y clasificación de la información

El delegado oficial de seguridad de la información en la organización deberá realizar un inventario y clasificación de los activos y/o repositorios de información, para tal efecto deberá considerar lo siguiente:

- Todos los activos tecnológicos y no tecnológicos deberán estar claramente identificados.
- Se deberá indicar quien es el propietario del activo, asimismo quien

custodiará dicho recurso, todos deben tener ambos campos.

- La información se deberá clasificar en función de los requisitos legales, valor, criticidad en la consecución de metas y objetivos para la organización, sensibilidad a divulgación o a modificación no autorizada.
- Se deberá desarrollar e implementar un conjunto de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado.

La entidad financiera deberá realizar un inventario de activos de información, incluyendo como mínimo:

- Información básica del activo (nombre, observaciones, proceso, entre otras).
- Nivel de clasificación de la información
- Información relacionada con su ubicación, tanto física como electrónica
- Los usuarios y derechos de acceso

El sistema de clasificación definido deberá primordialmente basarse en la confidencialidad de la información como principio, para cada activo se deben establecer criterios específicos y tratamientos adecuados, esto también puede estar relacionado con los procesos importantes para el grupo, los cuales se encontrarán definidos en el Análisis de Impacto del Negocio (BIA).

3.3.2. Copias de respaldo

El Departamento de Tecnologías de la Información deberá realizar copias de seguridad o copias de respaldo con el fin de disponer de un medio para recuperar los recursos tecnológicos, en caso de que llegara a materializarse un evento que pueda generar indisponibilidad.

Existen diferentes copias de seguridad, en este caso el grupo deberá elegir cuidadosamente el método para los diferentes activos tecnológicos, esto se debe principalmente a que algunos no podrían perder mucho tiempo en cuanto a pérdida de información y otros son irrelevantes y solo es necesario recuperar la configuración.

Este es otro de los puntos que se derivan de una combinación entre la criticidad del recurso, según lo indica el BIA y la relación con la información que se resguarda. Para realizar las copias de respaldo, el Departamento de Tecnologías de la Información deberá considerar como mínimo los siguientes aspectos:

- Indicar la información a respaldar, periodicidad y validación o pruebas de dichas copias.
- Documentar los procedimientos de restauración de las copias de respaldo
- Congruencia con la estrategia institucional para la continuidad del negocio y la continuidad de operaciones de los recursos tecnológicos.
- Metodología y localización de las copias de respaldo, documentación del procedimiento de restauración.

3.3.3. Protección de banca virtual

La banca virtual es una de las principales herramientas empleadas por la estrategia de la institución, por el ofrecimiento de los servicios financieros a los clientes las veinticuatro (24), horas del día los siete (7), días de la semana, sin necesidad de salir de la comodidad del hogar o moverse de sitio.

En esta herramienta cien por ciento tecnológica se ve expuesta de múltiples formas la seguridad de la información de los clientes, por tal razón es importante gestionar y mitigar los riesgos inherentes a su operación, básicamente la entidad deberá implementar como mínimo lo siguiente:

- Mecanismos para la protección y control de los recursos tecnológicos relacionados con la banca virtual.
- Medidas de seguridad para el intercambio de información a través de los canales electrónicos.
- Certificados digitales de seguridad, cifrado de datos u otro mecanismo que permita garantizar la transferencia de información.
- Programas de concientización de seguridad para clientes
- Registro y bitácoras de las transacciones efectuadas

3.4. Continuidad de los servicios tecnológicos

La continuidad de los servicios tecnológicos constituye la principal preocupación de la empresa, básicamente la inversión para contar con redundancia de los recursos tecnológicos es una cantidad bastante alta, por tal razón se deberá planificar una estructura compleja a fin de que los activos que se incluyan en los procedimientos para dar continuidad a los servicios sean aquellos que soportan directamente los procesos críticos del negocio.

Es decir, los procesos que podrían generar un impacto altamente negativo en la permanencia de la organización, esto básicamente será el resultado del Análisis de Impacto del Negocio que tendrá como prioridad el Departamento de Riesgos.

Considerando lo anterior, la información que empleará el Departamento de Tecnologías de Información para identificar cuáles son los activos tecnológicos críticos y por ende los que serán parte de los procedimientos de continuidad de operaciones de tecnologías de información, serán los Mapas de Interdependencia de Negocio porque en ellos se indicarán los servicios tecnológicos y esto se deberá interpretar como, cuales sistemas de información, que infraestructura tecnológica y cuales bases de datos soportan dichos servicios.

3.4.1. Plan de continuidad de operaciones de tecnologías de información

La institución deberá contar con un plan de continuidad del negocio, es decir, deberá considerar los recursos tales como personas, infraestructura física, procesos y tecnología; el Departamento de Riesgos deberá coordinar la elaboración de dicho plan, sin embargo, el Departamento de Tecnologías de Información deberá crear los procedimientos técnicos y administrativos para el Plan de Continuidad de Operaciones de TI.

Para que la compañía pueda asegurar la disponibilidad y continuidad de los servicios tecnológicos, deberá crear un plan que se encuentre acorde a las necesidades de la institución, es decir, este plan estará en común acuerdo con el BIA y por ende con el Plan Estratégico organizacional. Para tal efecto deberá incluir como mínimo lo indicado abajo en los procedimientos de recuperación:

- Los objetivos y alcance del plan de continuidad de operaciones de tecnologías de información.
- Identificación de los procesos críticos de la organización.

- Identificación de los procesos de Tecnologías de Información que son necesarios para soportar los procesos críticos de la organización.
- Procedimientos técnicos y Plan de Comunicación de Crisis
- Responsabilidades del personal sensible de tecnologías de información y el listado de proveedores críticos (internos, críticos).
- Recursos necesarios para la recuperación

3.4.1.1. Plan de pruebas

Al finalizar la documentación del Plan de Continuidad de Operaciones de Tecnologías de Información, es importante considerar que se debe llevar a la práctica para garantizar la validez y funcionalidad, asimismo determinar la compatibilidad de los procedimientos e instalaciones.

Los resultados obtenidos harán que se determinen las áreas que necesitan realizar cambios, dichas modificaciones harán que la documentación cada vez se asemeje más a la realidad y por ende exista una mejora continua.

Las pruebas se deben planificar de tal forma que no se vean afectadas las operaciones de la entidad, esta planificación deberá trasladarse al Comité de Riesgos para que se aprueben las fechas previstas.

Los resultados de las pruebas deben documentarse y antes de cada una de ellas deberá definirse el alcance y los escenarios. Debido a que los recursos tecnológicos de la sociedad se encuentran expuestos a constantes cambios, se recomienda que se realicen pruebas como mínimo tres veces en un año calendario.

3.4.1.2. Preparación del personal clave

Para la ejecución del Plan de Continuidad de Operaciones de TI los colaboradores deberán estar debidamente capacitados, el Departamento de Tecnologías de Información tendrá que proporcionar constante entrenamiento y formación, esto con el fin de que todo el personal sensible se encuentre actualizado en los procedimientos de recuperación de los servicios tecnológicos.

3.5. Tercerización

Como ya se ha mencionado, el Departamento de Tecnologías de Información ha implementado controles ordenados y rigurosos, relacionados con la administración de todos los servicios contratados con terceros, esto se debe al cuidado de la imagen del grupo, en guardar relaciones adecuadas con otras entidades individuales y jurídicas.

Básicamente la institución deberá asegurar en todo momento que los servicios que fueron contratados serán proporcionados según los términos firmados en lineamientos contractuales legales, los cuales deben ser validados por un notario en funciones activo y colegiado. El Departamento de Tecnologías de la Información deberá constantemente asegurar que adecuará los controles que se aplican a los proveedores, a fin de evitar la materialización de cualquier riesgo inherente.

3.5.1. Procesamiento de información

Por distintos servicios financieros que ofrece la organización, en los que se pueden mencionar tarjeta de crédito, débito, cheques, entre otros; muchas

veces es necesario trasladar cierta información a proveedores o entidades. La transferencia de información con terceros debe ser de forma segura y con los mismos aspectos y parámetros de seguridad con el que se manejan en los distintos recursos tecnológicos.

Por tal razón la Subgerencia de Seguridad Informática del Departamento de Tecnologías de Información y el Departamento de Riesgos, deberán realizar los análisis correspondientes a fin de garantizar que el intercambio de información no presentará ningún riesgo alto en cuanto a la vulneración de datos confidenciales. Todos los aspectos que se deben evaluar deberán ser documentados en la Política de Control de Proveedores institucional.

3.5.2. Proveedores

Es importante mencionar a los proveedores de nuevo, esto se debe a que, según el reglamento emitido por la Junta Monetaria, la Resolución JM-102-2011, todas las entidades individuales y jurídicas que guarden alguna relación con el grupo, por intercambio de servicios para el procesamiento de información, deben cumplir con lo establecido en el reglamento mencionado y además incluir ciertas cláusulas en los contratos donde se suscriba lo siguiente:

- La Superintendencia de Bancos tendrá libre acceso a las instalaciones de los proveedores y podrá inspeccionar los elementos relacionados con el servicio contratado por la empresa.
- El proveedor deberá proporcionar a la Superintendencia de Bancos, cuando esta lo requiera, toda la información y/o documentos relacionados con los servicios contratados por la institución.
- El proveedor deberá guardar estricta confidencialidad de las operaciones y servicios que realice y demás datos a los que tenga acceso por motivo

de su relación.

3.6. Inversión inicial

El proceso de implementación de la propuesta del marco integral de trabajo para la administración de riesgo tecnológico depende de diversas variables. Sería muy difícil cuantificar un solo monto que abarcará la suma total de la inversión que debe realizar la compañía, esto se debe a que muchos de los controles que se tienen que automatizar tienen diferentes costes en el mercado, o el precio es básicamente el tiempo que estará involucrado un colaborador ya contratado.

Asimismo, el evaluar los controles previo a la implementación, es primordial y fundamentalmente crítico, esto se traduce en que la organización debe considerar el hecho de que no es viable tener un proceso sumamente controlado porque dichos controles pueden superar los costos de operación y en muchas ocasiones donde está el riesgo está el negocio.

Es importante mencionar que la tecnología cambia día con día y por ende el costo de los servicios fluctúa constantemente con el tiempo. A continuación, se realiza una propuesta sobre los principales recursos que debe adquirir la sociedad, básicamente la inversión inicial está fundamentada en la contratación de tres personas que estarán a cargo de la gestión y administración del riesgo tecnológico, la manera como se deberán ubicar es la que se muestra a continuación:

Tabla III. **Salarios de personal a contratar para la administración del riesgo tecnológico**

No. Personas	Plaza	Salario Mensual
1	Coordinador de Riesgos Tecnológicos	Q 12 500,00
1	Analista de Riesgos Tecnológicos II	Q 10 000,00
1	Analista de Riesgos Tecnológicos I	Q 7 500,00
Total del Salario Mensual		<u>Q 30 000,00</u>

Fuente: Gerencia de Recursos Humanos.

Tabla IV. **Ubicación de Colaboradores para la administración de riesgo tecnológico**

Plaza	Área a la cual reporta
Coordinador de Riesgos Tecnológicos	Departamento de Riesgos
Analista de Riesgos Tecnológicos II	Departamento de Tecnologías de Información
Analista de Riesgos Tecnológicos I	Departamento de Tecnologías de Información

Fuente: Gerencia de Recursos Humanos.

Algunos controles mencionados en la propuesta no tienen costos porque solo están basados en la creación de políticas debidamente documentadas, configuración en los elementos de los recursos tecnológicos, desarrollo de software por la Subgerencia de Desarrollo de Sistemas del Departamento de Tecnologías de Información (colaboradores que ya se encuentran en la planilla), entre otros.

Sin embargo, para todos aquellos controles que tengan costo asociado, se estará indicando en el momento de la implementación, esto se debe a que la evaluación sobre la viabilidad de la contratación se realizará en el momento en el que se evalúen las ofertas de los distintos proveedores.

4. IMPLEMENTACIÓN DE LA PROPUESTA

4.1. Creación de las políticas y los procedimientos

La piedra angular para la administración del riesgo tecnológico fue la redacción adecuada de políticas y procedimientos que deberán inculcarse en todos los colaboradores relacionados con tecnologías de información. Es importante mencionar que para la creación de documentos se tuvo bastante cuidado en la administración de los mismos, esto con el fin de evitar la redundancia de lineamientos o duplicar temas que ya se habían descrito en otros documentos.

Si se debía profundizar en algún tópico lo necesario fue ampliar el documento existente y no crear nuevos. Se tuvo el especial cuidado en respetar las normas existentes de la organización para darle formato a los documentos y el uso de fuentes.

En cuanto a la redacción de políticas se procuró en la medida posible no ocupar más de dos páginas y tampoco incluir detalles. Los principios para la construcción de los procedimientos fueron facilitar al personal el entendimiento de cómo ejecutar su trabajo, como tomar las decisiones de forma ágil en diferentes niveles jerárquicos, capacitación de personal de nuevo ingreso, reducir el desperdicio organizacional y apoyar en el cumplimiento de las metas del Departamento de Tecnologías de Información.

4.1.1. Política de Gestión de Riesgo Integral

El Departamento de Riesgos creó un Manual de Administración de Riesgo Integral, considerando lo expuesto en la Resolución JM-56-2011 emitida por la Junta Monetaria.

Dicho manual hace referencia a una política que tiene el objetivo principal de formalizar la representación del Departamento de Riesgos sobre la estructura organizacional de la empresa. Se definió que esta unidad reporta directamente al Comité de Riesgos y que funcionaría de forma independiente a todas las áreas y departamentos, con esto se garantizó que la gestión de recursos dependiera directamente de la Administración Ejecutiva o Gerencia General. Entre los lineamientos más importantes que se incluyeron en la política figuran los siguientes:

- Las responsabilidades de las áreas y departamentos sobre la identificación y evaluación de los riesgos inherentes a su operación, sus productos, y servicios.
- Definición de controles para la mitigación de los riesgos identificados y evaluados, mediante la ilustración de una matriz.
- Periodicidad de ejecución de autoevaluaciones para determinar constantemente el nivel de exposición a los distintos riesgos inherentes y la eficiencia de los controles ya implementados.
- Instrucciones para realizar análisis de falencias en los controles y como se deben estructurar los planes de acción para la implementación de los mismos.

La Política de Gestión del Riesgo Integral es una derivación y/o ampliación de una política creada por la sociedad, donde establecen el modelo de control

interno basado en COSO, en la cual figuran todos los involucrados e interesados en la organización como responsables del funcionamiento del sistema de administración de riesgos.

En la presente política el Departamento de Riesgos también definió las principales líneas del negocio con sus productos y servicios que provee a los clientes, básicamente esto se fundamentó en distintos aspectos que fueron recopilados con todas las áreas y departamento del grupo. Se incluyeron los parámetros que se deben considerar para evaluar los riesgos inherentes sobre los productos o servicios nuevos.

La política incluyó la definición de las distintas autoridades de riesgo, entre los cuales se pueden mencionar:

- Jefe de riesgo operativo
 - Coordinador de riesgo legal
 - Coordinador de riesgo tecnológico
- Jefe de riesgo de mercado
- Jefe de riesgo de liquidez
- Jefe de riesgo crediticio

El Coordinador de Riesgo Tecnológico estará bajo la gestión del Jefe de Riesgo Operativo, siempre siguiendo los lineamientos de COSO. Se dictaminó que todo evento significativo de pérdida operativa o de mercado debe ser conocido por el Departamento de Riesgos, con el fin de que se puedan evaluar los factores y se registren en las cuentas contables de la organización.

En la política también se establecieron las responsabilidades específicas del Consejo Directivo, Comité de Riesgos y el Departamento de Riesgos, asimismo como los funcionarios y autoridades deben apoyar en la administración de todos los riesgos inherentes en la organización, se consideraron las tareas expuestas en la propuesta de este trabajo de investigación. Se definieron de forma general los procedimientos para los riesgos de mercado, riesgos de liquidez y riesgos crediticios, asimismo para el riesgo operativo, en lo que a este último respecta se pueden mencionar:

- Las características y periodicidad para la elaboración de matrices de riesgo operativo de las áreas y departamentos.
- Aspectos a considerar en las autoevaluaciones de riesgo operativo sobre los procesos implementados.
- Según el resultado de las autoevaluaciones que se debe considerar para la creación de planes de acción.
- El Departamento de Riesgos consolidará toda la información en lo que respecta a resultados de las autoevaluaciones y las propuestas de planes de acción para mitigar riesgos.

4.1.2. Política general de administración de documentos de TI

Para la creación, modificación y eliminación de políticas y procedimientos en el Departamento de Tecnologías de Información, se elaboró una política donde se definieron las normas y lineamientos, por tal razón se incluye toda la documentación relacionada con Tecnologías de información y por ende la administración del riesgo tecnológico también debe cumplir con los estatutos enmarcados.

Entre los puntos que se incluyeron en el documento se pueden mencionar:

- Creación del Documento todas las políticas y procedimientos creadas en el Departamento de Tecnologías de Información los cuales se encuentren relacionados a los requerimientos legales, para la administración de riesgos tecnológicos o que sea bajo cualquier fin, deberán efectuarse bajo el acoplamiento del Coordinador de Riesgos Tecnológicos y los Analistas de Riesgos Tecnológicos, la documentación deberá indicar el alcance dentro de la organización.
- Aprobación de documentos nuevos, actualizados y/o modificados, las políticas y procedimientos son revisados en primera instancia por la Subgerencia dueña en el Departamento de Tecnologías de la Información, para que se pueda proporcionar el visto bueno, según los resultados de dicha revisión esta documentación se debe trasladar al Comité de Riesgos, para su aprobación.

Es importante mencionar que todos los documentos que se encuentran relacionados con la administración del riesgo tecnológico y/o son de cumplimiento regulatorio, deben estar autorizados por el Consejo Directivo; en todo caso el Departamento de Tecnologías de la Información crea una política o procedimiento interno al área este podrá ser autorizado únicamente por el Gerente de dicha unidad.

- Publicación y difusión de documentos, todas las políticas y procedimientos aprobados por el Comité de Riesgos y el Consejo Directivo son publicados en un repositorio digital asignado al Departamento de Tecnologías de la Información. En este repositorio se administran los accesos a los usuarios que únicamente tienen el privilegio, es decir, cada colaborador de la entidad financiera podrá acceder únicamente a lo que le corresponde.

La difusión de las políticas y procedimientos se realiza por correo electrónico a todos los involucrados o bien a todo el Departamento de Tecnologías de la Información si en caso, es un documento que aplique a todas las subgerencias.

- Actualización de documentos las políticas y procedimientos se deberán revisar como mínimo una vez por año, esto considerando si existe algún cambio. Al finalizar la actualización deberá de nuevo ser revisado por el subgerente de área y posteriormente aprobado por el Comité de Riesgos en caso fuera de cumplimiento regulatorio o se encuentre relacionado con administración de riesgo tecnológico.
- Eliminación de documentos cuando el Departamento de Tecnologías de Información considere que un documento ya no es indispensable, el Coordinador de Riesgo Tecnológico deberá solicitar la autorización de eliminación al Comité de Riesgos, en caso el documento sea de cumplimiento regulatorio o se encuentre relacionado con la administración del riesgo tecnológico, en otro caso la eliminación la puede autorizar el Gerente del Departamento de Tecnologías de Información.

En la política también se definió la metodología para dar formato y redacción a los documentos del Departamento de Tecnologías de la Información, básicamente se incluyó lo siguiente:

- Codificación de documentos considerando lo expuesto por la Norma ISO 20000 los tipos de documentos que podría llegar a tener el Departamento de Tecnologías de Información son:

Tabla V. **Clasificación de documentos en tecnologías de información**

Tipo de documento
Política
Plan
Proceso, Manual, Procedimiento
Registro: podría incluir formularios, informes
Guías o instructivos

Fuente: Norma ISO 20000-2:2011.

Se estableció que, para todos los documentos, independientemente cual sea su tipo, serán nombrados con una codificación única, en donde deberá identificarse qué tipo de documento es, a que área pertenece y un correlativo de control. Es importante mencionar que no se podrá reutilizar el correlativo de algún documento eliminado.

- Inventario de Documentos, los Analistas de Riesgos Tecnológicos estarán a cargo del listado oficial de documentos del Departamento de Tecnologías de la Información, los campos que como mínimo se deben incluir en el inventario son, el área dueña del documento, la fecha de creación del documento, la fecha de autorización, fecha de próxima revisión.

4.1.3. Política de clasificación de la información

Para poder gestionar, administrar y custodiar correctamente los activos tecnológicos, se creó la Política de Clasificación de la Información esto con el

fin de definir los parámetros, aspectos y criterios para clasificar la información de toda la entidad financiera. El alcance establecido hizo referencia a toda la información relacionada con los procesos que ejecuta la organización, ya sea porque se encontrará en papel, archivos electrónicos, sistemas de información y bases de datos.

Dentro de la gestión de la información se identificaron diferentes responsabilidades, entre las cuales se pueden mencionar:

- Creación de un inventario de los datos que conforman la información y su desglose, básicamente en la entidad financiera con anterioridad fue creada la figura de un Coordinador de Seguridad de la Información, entre sus obligaciones está la elaboración de listados sobre los distintos recursos en donde se almacena la información, por tal motivo también que tipo de información se almacena, con qué proceso se encuentra relacionada quienes son los dueños de la información y por ende sus custodios.
- Clasificación de la información, los propietarios de los activos de información deberán clasificar los datos resguardados según la criticidad y sensibilidad que representan para la organización.
- Etiquetado de la información, básicamente al conocer los niveles de criticidad y sensibilidad de la información se sabrá con qué nivel de confidencialidad se debe etiquetar, para que las personas autorizadas y no autorizadas lo consideren antes de tener acceso, modificación, mantenimiento y/o eliminación.
- Custodio de la información, para muchos recursos de información, no

siempre el dueño (creador de los datos) es quien custodia directamente los activos donde se almacena, por tal razón según se encuentre etiquetada la información, su custodio debe implementar los controles necesarios para garantizar la integridad y disponibilidad de la información.

Para la clasificación de la información, en la política se consideraron dos aspectos relevantes para la información:

- Sensibilidad de la información, básicamente determinada por el nivel de impacto que tendría en cuanto a la divulgación no autorizada considerando los siguientes niveles:

Tabla VI. **Niveles de Impacto según sensibilidad de la información**

Nivel Sensibilidad	Aspectos
Muy Alto	Al quedar expuesta la información podría dañar de forma irreparable al negocio y/o la reputación organización.
Alto	Al quedar expuesta la información se podría incurrir en elevados costos operativos, legales y daños considerables a la imagen de la organización
Medio	Al quedar expuesta la información se podría dañar el negocio y/o la imagen de la organización
Básico	Al quedar expuesta la información

Fuente: Política de Clasificación de la Información, entidad financiera.

- Criticidad de la información, este corresponde al nivel de importancia que tiene la información en el desarrollo de los procesos de la entidad financiera, básicamente se clasificó de la siguiente forma:

Tabla VII. **Niveles de criticidad según la relación que guarda la información con los procesos de la entidad financiera**

Nivel Criticidad	Aspectos
Muy Alta	Es de vital importancia en la ejecución de procesos críticos para la entidad financiera, el que no se encuentren disponibles estos datos tiene drásticas consecuencias la institución.
Alta	Es importante en la ejecución de procesos críticos para la organización, el que no se encuentren disponibles estos datos puede causar problemas para la institución.
Media	Los datos tienen relevancia para la ejecución de los procesos críticos de la institución, sin embargo, al no contar con la información, existen métodos alternativos.
Básica	El no contar con los datos no afecta de ninguna manera el desarrollo de los procesos críticos de la empresa.

Fuente: Política de Clasificación de la Información, entidad financiera.

En la política se estableció básicamente que la combinación de los criterios de sensibilidad y criticidad para los datos, generaban un criterio

importante para describir la confidencialidad de la información, por esta razón se creó una matriz que mostraba como debían ser clasificados los datos:

Tabla VIII. **Matriz de Clasificación de la Información, según su confidencialidad**

		SENSIBILIDAD			
		BASICO	MEDIO	ALTO	MUY ALTO
CRITICIDAD	MUY ALTA	Sin Clasificar	Reservada	Restringida	Secreta
	ALTA	Sin Clasificar	Reservada	Restringida	Restringida
	MEDIO	Pública	Reservada	Reservada	Reservada
	BÁSICO	Pública	Pública	Sin Clasificar	Sin Clasificar

Fuente: Política de Clasificación de la Información, entidad financiera.

De acuerdo a los niveles de confidencialidad expuestos en la matriz, toda la información almacenada en los distintos medios (papel, archivos electrónicos, sistemas de información y bases de datos), se debe etiquetar para que de esta

forma los datos no se encuentren expuestos a correr algún riesgo de divulgación y/o extracción.

Como parte de la política fue creado un procedimiento de etiquetado de los medios en donde se ve plasmada la información. Todos los dueños de los datos son los responsables de etiquetar la información de acuerdo a lo siguiente:

- Documentos impresos, deberán tener una marca de agua a lo largo de todo el documento si su clasificación de confidencialidad es “Secreta”, para todo lo demás se deberá señalar en la esquina inferior derecha sobre cada página. Si se tiene carpeta deberá etiquetarse también.
- Archivos electrónicos, se deberá considerar lo mismo que los documentos impresos, tomando en cuenta las características que las herramientas tecnológicas permitan, la idea es transmitirle al visor el nivel de confidencialidad que se tiene.
- Correos electrónicos, todos los correos electrónicos cuando salen de la infraestructura tecnológica de la institución tienen un enunciado que hace referencia al nivel de confidencialidad de la información y por ende su eliminación sin en caso el receptor no es a quien debía dirigirse el mismo.
- Sistemas de Información, todos los datos que se encuentren registrados en un sistema de información propio de la sociedad, no se pueden etiquetar, sin embargo, de forma general esta información será restringida y estará bajo el control de la administración de los usuarios que será responsabilidad del Coordinador de Seguridad de la Información quien a través de los inventarios deberá implementar las medidas para gestionar

roles, perfiles y/o usuarios.

- Medios de almacenamiento masivo, dispositivos tales como discos compactos, memorias extraíbles, entre otros; estarán restringidos para almacenar información, todos los equipos de cómputo tendrán bloqueados los puertos donde se puede leer o extraer datos por este medio.

El Coordinador de Seguridad de la Información estará constantemente realizando planes de concientización y sensibilización para todos los colaboradores que emplean los datos registrados en cualquier medio y ejecutan los procesos.

4.1.4. Política de seguridad de la información

Entre las políticas referenciadas, la presente, es punto de partida para la administración del riesgo tecnológico, básicamente es donde se empiezan a materializar los controles para proteger la información que se encuentra resguardada en los sistemas de información, la infraestructura tecnológica y bases de datos.

Básicamente esta política fue creada y estructurada a fin de emitir políticas institucionales que permitan garantizar la protección de todos los datos e información creada y procesada por la organización. Los pilares en los cuales se basa es la mitigación de riesgos de divulgación, acceso o modificación no autorizada, pérdida o interrupción, mal uso o robo lo cual se puede producir de forma intencional o sin intención, en pocas palabras garantizar la integridad, confidencialidad y disponibilidad de la información.

Para construir esta política básicamente se realizó empleando los principios recomendados por la Norma ISO/IEC 27001: 2013, considerando todos los controles que se podían aplicar al giro del negocio:

- Seguridad de los colaboradores, en esta sección de la política básicamente se definen las responsabilidades que tiene la entidad financiera en dejar de forma clara y concisa las obligaciones de los empleados y como estas obligaciones son revisadas periódicamente, asimismo las acciones disciplinarias que se le aplicarían a los colaboradores en caso no se cumpla lo expuesto en la política. Básicamente con relación a los empleados se contemplaron reglas para todo el personal de nuevo ingreso, acuerdos de confidencialidad sobre la información a la cual estarán expuestos, los términos y condiciones contractuales, términos de sensibilización y concientización.
- Seguridad Física, en la política se consideró que al final, todos los medios en donde se almacena la información, se concentran en las diferentes infraestructuras físicas y edificios de la empresa; por tal razón fue necesario indicar los lineamientos para implementar los controles de acceso físico del personal a las áreas públicas, de oficina, accesos restringidos, mediante tarjetas de proximidad o dispositivos biométricos; la identificación de áreas de carga y descarga, puntos de revisión y verificación tanto a visitas como a empleados y como deben dejarse las oficinas, escritorios y equipos de cómputo cuando las personas las dejan sin atención.
- Operación y gestión de los equipos de cómputo y equipos de telecomunicaciones, en esta parte de la política es donde brevemente se hace referencia a la forma en cómo se deben manejar todos los

incidentes de seguridad, los cuales se pueden materializar a causa de probables vulnerabilidades. Básicamente lejos de sacar provecho a dichas vulnerabilidades, los colaboradores deben reportar el incidente a donde corresponde, para dicha gestión se ha creado un equipo de respuesta que tiene como prioridad resolverlos en la manera más efectiva y eficiente posible.

En esta sección se contemplan los lineamientos para el uso adecuado de todos los equipos de cómputo, el uso de navegación a internet, las diferentes medidas de protección contra el software malicioso (virus de computadoras), los parámetros de tecnología que deben contemplarse para intercambiar la información, cual es el uso correcto del correo electrónico y la seguridad en las redes inalámbricas.

- Control de accesos lógicos, todos los colaboradores de la compañía deberán tener acceso únicamente a la información que necesitan para el desarrollo legítimo de sus funciones, es decir, se les proporcionaran privilegios de acceso a la información de la forma mínima.

Algunos proveedores necesitarán acceso a la información, por tal motivo el personal tercerizado deberá firmar puntualmente que está de acuerdo con las políticas de seguridad de la información de la organización. Se definió que todos los dueños de la información con el apoyo de sus custodios deberán realizar periódicamente una revisión de los derechos de acceso.

4.1.5. Acuerdos de Comité de Riesgos

El Comité de Riesgos es el responsable de la administración de todos los riesgos inherentes en las operaciones del grupo, básicamente riesgo de crédito, liquidez, mercado y operacional, por tal razón se estableció como el mayor ente dentro de la organización con autoridad y propósito de identificar, medir, monitorear, controlar, prevenir y mitigar los riesgos mencionados.

Este comité es la conexión entre el Consejo Directivo y la Administración Ejecutiva en temas relacionados a los riesgos. Se creó un documento donde se definen cuáles son los lineamientos a los cuales se encuentra expuesto el Comité, entre los cuales se puede mencionar:

- Frecuencia de Reuniones: el Comité de Riesgos se reunirá mediante una reunión donde se constituirán todos los integrantes, dicha reunión será como mínimo una vez cada trimestre o cuando la situación lo amerite.
- Integrantes: el comité estará integrado por miembros del Consejo Directivo (dos como mínimo), el Gerente General, Gerente de Riesgo Integral, Gerente de Finanzas, Auditor Interno de la organización, Gerente Director de Operaciones.
- Autoridad: deberá requerir los informes que considere necesarios a fin de mitigar los riesgos inherentes a la organización, el requerimiento lo podrá realizar a quien considere oportuno, independientemente de la unidad.
- Informe Anual: se estableció que el Comité deberá presentar un reporte anual al Consejo Directivo, en este se tendrán que exponer los resultados de la gestión de dicho Comité, asimismo se deberá definir una estrategia general para la implementación de políticas, procedimientos y sistemas aprobados para la administración integral de riesgo y su adecuado cumplimiento.

- Gestión: todos los temas discutidos, las actuaciones y decisiones tomadas dentro de las reuniones deberán quedar plasmadas en un acta legal, que deberán firmar todos los integrantes.

4.1.6. Acuerdos de Comité de Riesgo Operativo

La administración de Riesgo Tecnológico depende directamente del Riesgo Operativo, por tal razón se definió un Comité de Riesgo Operativo el cual pudiera evaluar a nivel institucional los impactos que podrían desencadenarse en caso se materializará un riesgo tecnológico.

La administración del Riesgo Tecnológico será responsabilidad del Departamento de Tecnologías de la Información a quien se le asignan recursos financieros y quien tiene la potestad de invertirlos en los controles que llegase a necesitar para la mitigación de riesgos, sin embargo, cuando es necesario el apoyo de áreas operativas y de negocio, se convoca el riesgo operativo para solicitar la aprobación de los planes de acción propuestos, considerando esta disposición se creó un documento para hacer referencia a todas las responsabilidades que tiene el Comité de Riesgo Operativo:

- Coordinar el desarrollo de Evaluaciones de Riesgo Operacional a todas las áreas y departamentos.
- Evaluar los nuevos procesos, productos, canales, sistemas, proyectos y demás ideas con el fin de determinar posibles inconsistencias y puedan generar riesgos.
- Revisar los riesgos operativos que pueden generar un alto impacto negativo, con el objetivo de generar planes de acción para su mitigación, y si es del caso soportar y dar seguimiento a dichas acciones.
- Velar por el cumplimiento efectivo de la gestión del riesgo operacional

(políticas, procedimientos, planes).

- Realizar un seguimiento permanente de las etapas y elementos constitutivos de la gestión del riesgo operacional que se llevan a cabo en la entidad.
- Monitorear el nivel de riesgo operacional de la entidad mediante el seguimiento a los diferentes indicadores establecidos.
- Promover y apoyar la administración y programa de continuidad del negocio a través de la toma de decisiones, la disposición de recursos de acuerdo con las necesidades del negocio.

4.2. Gobierno corporativo y gobierno de TI

Considerando lo expuesto por las buenas prácticas del marco de trabajo de COBIT 4.1 se documentaron los acuerdos para un buen gobierno corporativo en la organización y el gobierno de tecnologías de información, básicamente se definió un conjunto de obligaciones y responsabilidades que debe ejecutar el Consejo Directivo y la Administración Ejecutiva a fin de proveer dirección y estrategia, garantizando que los objetivos sean alcanzados, estableciendo que los riesgos son administrados apropiadamente y verificando que los recursos de la empresa son usados responsablemente.

En los acuerdos también se definió como el Consejo Directivo evaluaría la gestión de la Administración Ejecutiva y como este último realizará lo propio respecto de los funcionarios que dirija. En el documento se definieron las obligaciones considerando lo siguiente:

- La Gerencia General es la responsable de implementar un sistema de control adecuado. La integridad y la ética deben ser elementos que aporten ejemplo a los demás empleados. Debe dirigir a los funcionarios y

autoridades que a su vez son responsables en sus respectivas áreas.

- El Consejo Directivo fija las pautas y la visión global de la organización, este debe tener un papel activo en el conocimiento de las acciones que se ejecutan. Debe asegurarse de contar con las vías de comunicación efectivas con la alta dirección y las áreas financieras, legales y de auditoría interna.
- La auditoría interna debe desempeñar un papel de supervisión sobre la eficiencia y permanencia de los sistemas de control. Para ello debe contar con una ubicación jerárquica adecuada.
- Los empleados en general tienen la responsabilidad de participar en el esfuerzo de aplicar el control interno, cuyos detalles deben ser incorporados a la descripción de los puestos de trabajo. Ellos deben comunicar al nivel superior las desviaciones que detecten a los códigos de conducta, a las políticas establecidas o la legalidad de las acciones realizadas.

Con relación al Gobierno de Tecnologías de Información, se definió que este le reporta al Gobierno Corporativo tomando en cuenta lo siguiente:

- Definición de indicadores clave los cuales fueran medibles, esto a través de los objetivos de control definidos por COBIT en su versión 4.1.
- Implementar la mejora continua, alineando los recursos de TI con la organización y los principales estándares de establecidos para la industria financiera.
- Buscando la línea de comunicación directa entre la estrategia del negocio

y las estrategias de todas las áreas y departamentos de la organización.

4.2.1. Alinear la estrategia del negocio con la estrategia de TI

Considerando los términos definidos en la política de Gobierno Corporativo y Gobierno de TI, básicamente se estableció que el Departamento de Tecnologías de la Información debe orientar todos sus esfuerzos para poder cumplir con los objetivos trazados en el Plan Estratégico de la organización.

Una de las estrategias de la institución es contar con servicios tecnológicos en un 99,99 % de disponibilidad, dicha táctica le permite a la entidad financiera ser completamente atractiva en el mercado financiero de Guatemala, traduciendo esto, teóricamente le da la oportunidad al Departamento de Tecnologías de Información a generar valor al negocio, ordenando sus procesos de tal forma que respondan a estructuras organizativas adecuadas a funciones específicas, gestión del riesgo tecnológico efectivo y gestión del rendimiento de los recursos e insumos eficiente.

4.2.1.1. Plan Estratégico de TI

El Departamento de Tecnologías de la Información ha documentado las estrategias con las cuales prevé generar valor para la organización, en términos generales, se creó un documento que tiene el objetivo de ser la guía orientadora para la toma de decisiones en todos los temas relacionados a tecnologías de soporte para la empresa.

El Plan definido se concentra en tres aspectos fundamentales basados en la Situación Actual del Departamento de Tecnologías de la Información, iniciando con una reseña histórica, mostrando detalles, estadísticas y

parámetros de cómo ha evolucionado con respecto al tiempo, los proyectos que se prevén desarrollar a fin de contribuir al cumplimiento de los objetivos del negocio y la brecha entre la óptima implementación de los proyectos y la estabilización de los mismos.

En el Plan Estratégico de TI se definieron los roles y responsabilidades de cada subgerencia del Departamento de Tecnologías de Información, con relación a la toma de decisiones, se establece la visión, misión y política general del departamento mencionado. En el documento también se definieron los objetivos generales y específicos de Tecnologías de Información y su alcance sobre la organización.

Se documentaron los proyectos que tiene a cargo el Departamento de Tecnologías de Información, a corto, mediano y largo plazo, para cada proyecto aprobado por el Consejo Directivo se le indicó lo siguiente:

- Nombre del Proyecto: la identificación única para tipificar cada una de las actividades que acompañarán el proyecto.
- Línea del Negocio: a que línea del negocio estará soportando y/o mejorando/automatizando el proyecto.
- Justificación del Proyecto / Riesgo que mitiga o minimiza: básicamente se explica por qué prevaleció este proyecto entre el catalogo del Departamento de Tecnologías de Información.
- Criticidad o Importancia: cuál es la prioridad que tiene el proyecto
- Objetivo o estrategia: con cual objetivo del Plan Estratégico de la organización se alinea el proyecto.

En Plan Estratégico de TI se recalcan las funciones y objetivos específicos de cada subgerencia del Departamento de Tecnologías de Información, asimismo los planes de carrera para los empleados y la planificación de

entrenamiento programado. En el plan también se menciona como se monitoreará, el plan dura el tiempo en el que se prevé ejecutar, como será medido en que períodos se realizarán reportes si en caso existe un posible desvío y como se realizará su actualización en temas de los proyectos a mediano y largo plazo.

En el plan estratégico se resaltó el compromiso que tiene el Consejo Directivo en la asignación de recursos y consecución de los objetivos previstos para tecnologías de información.

4.3. Análisis de Impacto de Negocios (BIA)

En seguimiento a la propuesta realizada para la administración del riesgo tecnológico, se realizó un análisis de impacto al negocio que permitiera identificar la importancia relativa de los procesos y subprocesos que se llevan a cabo por las áreas y departamentos.

En el análisis efectuado por la organización se pretendió identificar los procesos de negocio críticos que más afectarán los ingresos, activos y clientes, esto con el fin de asignar las estrategias de recuperación que pudieran ser necesarias durante una interrupción prolongada de las actividades. Básicamente el principio es destacar todos los procesos y los activos que requieren protección adicional. En el BIA realizado en la organización, detalló una evaluación que en su entorno identificó:

- Los procesos de negocio más importantes de toda la organización
- La duración máxima de interrupción que un proceso/subproceso de negocio puede soportar antes de que afecte gravemente la organización.
- Las repercusiones financieras, productivas y organizaciones de una

interrupción prolongada de la actividad.

- Una valoración del impacto sobre la empresa a corto plazo de las pérdidas permanentes.
- Las prioridades del plan de continuidad del negocio
- Los datos más importantes que son precisos proteger y la (antigüedad de los mismos) para restablecer con éxito las operaciones del negocio.
- Las técnicas para equilibrar los costes de recuperación con los diferentes umbrales de riesgo.

El resultado del análisis realizado en toda la organización permitió lo siguiente:

- Eficaz análisis en profundidad de las funciones más importantes en el entorno del negocio.
- Conocimiento de las pérdidas financieras y repercusiones intangibles de una interrupción prolongada.
- Identificación de los recursos vitalmente esenciales para respaldar los procesos del negocio.
- Definición del tiempo objetivo de recuperación sobre el cual se diseñará el plan de recuperación de desastres y por ende los planes de continuidad del negocio.

Cuando se realizó el análisis, se consideraron cinco diferentes tipos de impacto que los procesos o subprocesos podrían generar en caso se materializará algún incidente que predispusiera de su disponibilidad. Para los procesos y subprocesos no solo se consideró el tipo de impacto si no también el nivel de impacto de acuerdo a lo siguiente:

Tabla IX. **Tipos de Impacto y nivel según los efectos producidos**

Tipos de Impacto y Efectos Producidos	Niveles			
	Leve	Medio	Grave	Catastrófico
Pérdida de ingresos (% de facturación)	0,1	0,1 a 1	1 a 10	Mayor a 10
Pérdida de beneficios (%)	0,01	0,01 a 0,1	0,1 a 1	Mayor a 1
Incremento de costes y/o gastos (%)	0,1	0,1 a 1	1 a 10	Mayor a 10
Impacto Comercial	Interrupción corta en el suministro de servicios o productos con mínimo impacto la operativa de los clientes, la pérdida en ventas se recupera al reanudar la actividad	Obliga al cliente a cambiar de proveedor de forma transitoria. Las ventas no realizadas no se recuperan	Pérdida de algunos clientes de forma definitiva. Impacto leve en la cartera de prospectos	Pérdida de clientes clave. Impacto grave en la cartera de prospectos.
Impacto operacional	Produce retrasos en funciones no vitales	Produce retrasos leves en funciones vitales	Produce retrasos graves en funciones vitales	Produce la interrupción inmediata de funciones vitales

Continuación de la tabla IX.

Impacto en la Imagen	Conocido solamente por algunos clientes. Sin presencia en los medios de comunicación	Pérdida de confianza en un producto o servicio específico o en una parte de la organización. Comentarios adversos en medios locales	Pérdida de confianza en una gama de productos o servicios o en varias áreas de la organización. Comentarios adversos en los medios nacionales	Pérdida de la confianza en el mercado y daños a la imagen de marca. Campaña continuada en los medios nacionales. Impacto en la Bolsa
Incumplimiento de obligaciones legales	Produce una falta leve en el cumplimiento de algún contrato	Produce una falta en el cumplimiento de algún contrato que obliga a renegociar	Produce una falta grave en el cumplimiento de algún contrato	Deja a la organización al margen de la ley

Fuente: Análisis de Impacto de Negocio (BIA), entidad financiera

4.3.1. Identificación de las principales líneas de negocio

Considerando los parámetros indicados en la tabla anterior entonces se comenzó a realizar el análisis con cada una de las áreas y departamentos, como resultado se identificaron distintos procesos y subprocesos que con base a un promedio establecido entre los tipos de impacto y nivel producido según los efectos generados, se clasificaron con cierto grado de criticidad, a dicho aspecto se añadió la relación que tenían los procesos y subprocesos con las principales líneas de negocio.

La entidad financiera en la Planeación Estratégica incluyó las tácticas comerciales en las cuales se enfocaría principalmente para el mercado guatemalteco. Básicamente las líneas principales del negocio serán todas aquellas que la Gerencia General y Administración Ejecutiva potenciará y de las cuales obtendrá mejores beneficios según su plan de negocio. Estas líneas de negocio incluyen los productos y servicios financieros que se ofrecerán a los clientes.

4.3.2. Identificación de los procesos críticos del negocio

Como resultado del análisis de impacto al negocio, considerando las líneas principales de negocios y los niveles de impacto que los procesos y subprocesos de las áreas y departamentos pueden derivar en caso se llegará a materializar algún evento que predispusiera en su operatividad normal, se clasificaron según los grados de criticidad que a continuación se mencionan:

Tabla X. **Grado de Criticidad de los procesos y subprocessos**

Grado de Criticidad	Descripción del Grado de Criticidad
Crítico	La interrupción del proceso por un tiempo determinado (mayor a 6 horas) puede causar pérdida de ingresos, pérdida de beneficios, incremento en costes y/o gastos, impacto comercial, impacto operacional, daños en la imagen reputacional e incumplimiento de obligaciones legales
Importantes para la estrategia de negocio	Procesos que son clave para la estrategia de Negocio.
Alto	Aquellos procesos que son importantes e indispensables para la correcta operación, estos generan impactos graves.
Medio	La causa de una interrupción, pueden provocar ineficiencias operáticas o generan impactos medios.
Básico	Estos procesos pueden tener interrupciones prolongadas ya que no son procesos indispensables para realizar otro proceso solamente se generan impactos leves.

Fuente: Análisis de Impacto de Negocio (BIA), entidad financiera.

La identificación de los procesos críticos, importantes para la estrategia de negocio, altos, medios o básicos; es importante y preciso para la administración de riesgo tecnológico, esto se afirma por que el Departamento de Tecnologías de la Información deberá priorizar y focalizar los recursos que tiene a disposición para poder generar valor y alinearse a la estrategia de negocio, lo que también quiere decir que cualquier desviación de recursos tecnológicos que no apoyen directa o indirectamente la consecución de objetivos de la organización, representarán riesgos latentes que deben ser mitigados.

La ejecución del Análisis de Impacto del Negocio (BIA), fue realizado bajo la coordinación del Departamento de Riesgos, para cada uno de los procesos identificados como críticos e importantes para la estrategia de negocio, se describieron detallando los siguientes puntos:

- Nombre del proceso: este dato fue la identificación primaria, con el mismo se diferencian todos los procesos.
- Alcance: existían procesos muy similares en cuanto a la ejecución o transformación de insumos, por tal razón se definió este punto para detallar que clientes, colaboradores, productos o servicios enmarcaba el proceso identificado.
- Descripción: en esta columna se definieron los insumos necesarios y un breve resumen sobre cómo se realiza el proceso, cabe mencionar que la institución, siempre bajo la coordinación del Departamento de Riesgos, a través del Coordinador de Riesgo Operativo, documentaron los procesos para que se pudieran conocer todos los detalles de la ejecución de los mismos, esta actividad se continúa realizando.

- Tiempo Objetivo de Recuperación (RTO): con cada responsable del proceso se definió este tiempo, el cual posteriormente se utilizaría para adaptar el Plan de Recuperación de Desastres del Departamento de Tecnologías de la Información.
- Pérdida Financiera: con base a datos estadísticos se calculó un promedio de la pérdida monetaria tangible si el proceso no se ejecutará en un día o el mes.
- Punto Objetivo de Recuperación (RPO): este dato también se emplea para las diferentes estrategias de recuperación de los servicios tecnológicos, es básicamente el volumen de datos en riesgo de pérdida que los responsables de procesos consideraron tolerable.
- Período Máximo Tolerable de Interrupción (MTPD): este tiempo fue descrito también por los dueños de los procesos, básicamente es para determinar a partir de qué punto en el tiempo la no disponibilidad de los procesos empieza a generar los impactos negativos en la empresa.

4.3.3. Creación de los mapas de interdependencia tecnológica

Cuando se finalizó el Análisis de Impacto al Negocio (BIA), era necesario conocer dos puntos muy importantes, el primero es la interrelación de los recursos o insumos empleados, pero desde la vista del negocio, el segundo la interrelación que existe entre los activos tecnológicos empleados para proveer los servicios tecnológicos que soportan los procesos críticos e importantes para la estrategia de negocio.

Los aspectos indicados son la base para la creación del Plan de Continuidad de Operaciones de TI, esto se debe a que el Departamento de Tecnologías de la Información en la elaboración de su Plan de Recuperación de Desastres (DRP), entabló un contrato con un tercero para que este pudiera proveer la infraestructura física, con un 99,99 % de disponibilidad, en donde se pudiera construir una pequeña réplica del Centro de Datos, básicamente el Centro de Datos Alterno.

Según los términos del contrato las obligaciones del tercero se definen solo como de colocación, es decir, ellos proveen el espacio físico, los controles de temperatura, los controles de seguridad física, los controles contra incendio, entre otros que se definen un Centro de Datos bajo el estándar TIER III. Dichos acuerdos hacen que el Departamento de Tecnologías de la Información sea el responsable de la infraestructura tecnológica que coloca, es decir, solo los colaboradores de la entidad pueden administrar los servidores, las bases de datos y aplicativos o sistemas de información instalados en el centro de datos alternativo.

Por los costos que representa el contar con dos centros de datos, la sociedad decidió priorizar la infraestructura tecnológica que debería ser colocada en el Centro de Datos Alterno, esto quiere decir que este último no es una réplica exacta de lo que se encuentra en el Centro de Datos Principal. Por tal motivo en el Centro de Datos Alterno se albergarán los principales servicios tecnológicos que soportan los procesos críticos e importantes para la estrategia de negocio, ya que de estos procesos es de lo que depende la continuidad de la organización.

Se inició con la elaboración de los mapas de interdependencia desde el punto de vista del negocio, para poder realizarlos se consideraron los siguientes aspectos:

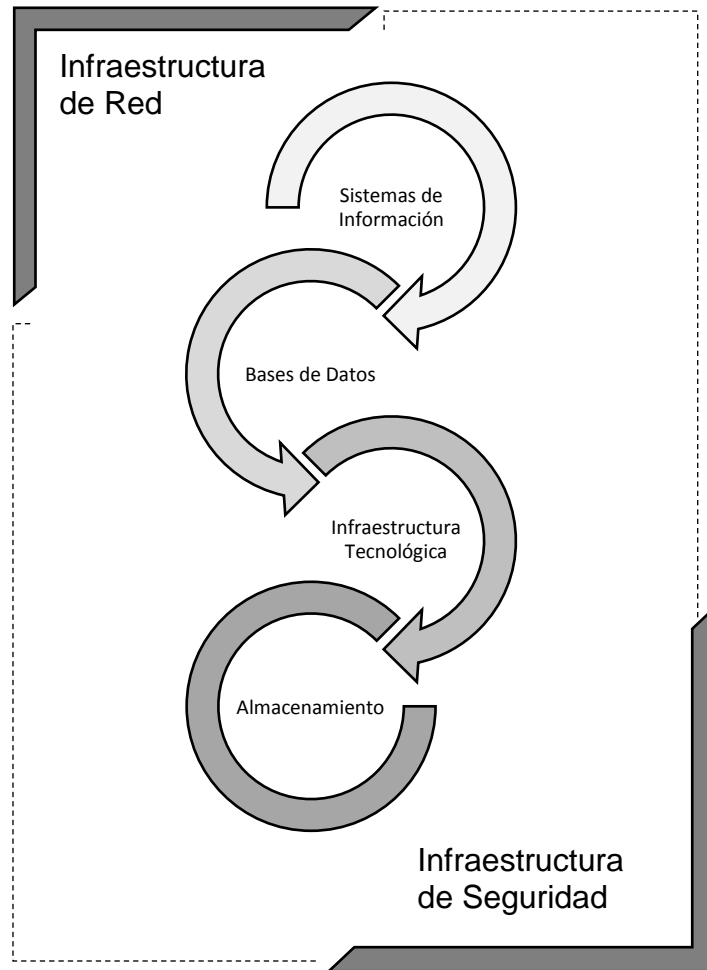
- **Recurso Humano:** en los mapas se incluyó el nombre de los puestos de los colaboradores involucrados, asimismo una breve descripción de las actividades a su cargo en el proceso / subproceso. Se mencionaron las áreas que son de apoyo y una descripción sobre las actividades en las que están relacionadas.
- **Proveedores:** en los casos que aplicara o en donde estuviera relacionado algún tercero se indicó, esto con el fin de determinar la importancia relativa de este proveedor en el proceso / subproceso.
- **Recurso Tecnológico:** en esta columna se indicaron en primer lugar la información y datos físicos puntuales que fueran necesarios para la ejecución del proceso, entre estos se pueden mencionar formularios, boletas, libretas, cheques, pólizas, entre otros.

Los dueños de los procesos indicaron los sistemas de información que emplean para la ejecución del proceso / subproceso, asimismo las herramientas de software y el hardware (cantidad de equipos de cómputo, teléfonos por voz IP, impresoras entre otros); esto será básicamente el insumo que utilizará el Departamento de Tecnologías de Información, para clasificar los activos tecnológicos críticos que soportan los procesos / subprocesos críticos e importantes para la estrategia de negocio.

- Procesos: en el mapa de interdependencia vista negocio, se hizo referencia a procesos relacionados con los procesos / subprocesos que se estaban diagramando, esto también para determinar los insumos y/o para que otro proceso era importante. Se mencionaron procesos tanto externos al área como también internos.
- Mobiliario, Equipo y Materiales: entre la información relevante se indicó el espacio físico empleado, los materiales (enseres y útiles de oficina), como también escritorios, sillas entre otros.

Para conocer el esquema gráfico del mapa de interdependencias vista negocio, elaborado por la entidad véase anexo 1. Tal y como se mencionó, de los mapas de interdependencias vista negocio se consideraron los datos indicados en las columnas de Recurso Tecnológico, esto básicamente para iniciar con la elaboración de los mapas de interdependencia tecnológicos, para ampliar este tema es necesario detallar un esquema de interrelación tecnológica. (Ver figura 11)

Figura 11. **Esquema de Interrelación de Recursos Tecnológicos**



Fuente: Manual de Administración de Riesgo Tecnológico, entidad financiera.

Para ampliar lo indicado en el esquema anterior, básicamente los sistemas de información son la primera vista de todo usuario de tecnología, en estos se pueden incluir las herramientas tecnológicas tales como procesadores de texto, hojas de cálculo, creadores de presentaciones, los sistemas que gestionan los datos, en una organización se refiere a la información de clientes, CRM, ERP, entre otros.

Los repositorios de esta información son las bases de datos que se encuentran alojadas en la infraestructura tecnológica lo cual tiene el nombre comúnmente conocido por servidores, y estos últimos se apoyan en dispositivos de almacenamiento virtual en donde la información ya se transforma a datos binarios.

Los cuatro elementos mencionados viajan en el espacio y tiempo gracias a los avances en infraestructura de red o telecomunicaciones, y todo tiene un perímetro de seguridad para garantizar únicamente el acceso a quienes lo tengan permitido, gracias a la infraestructura de seguridad.

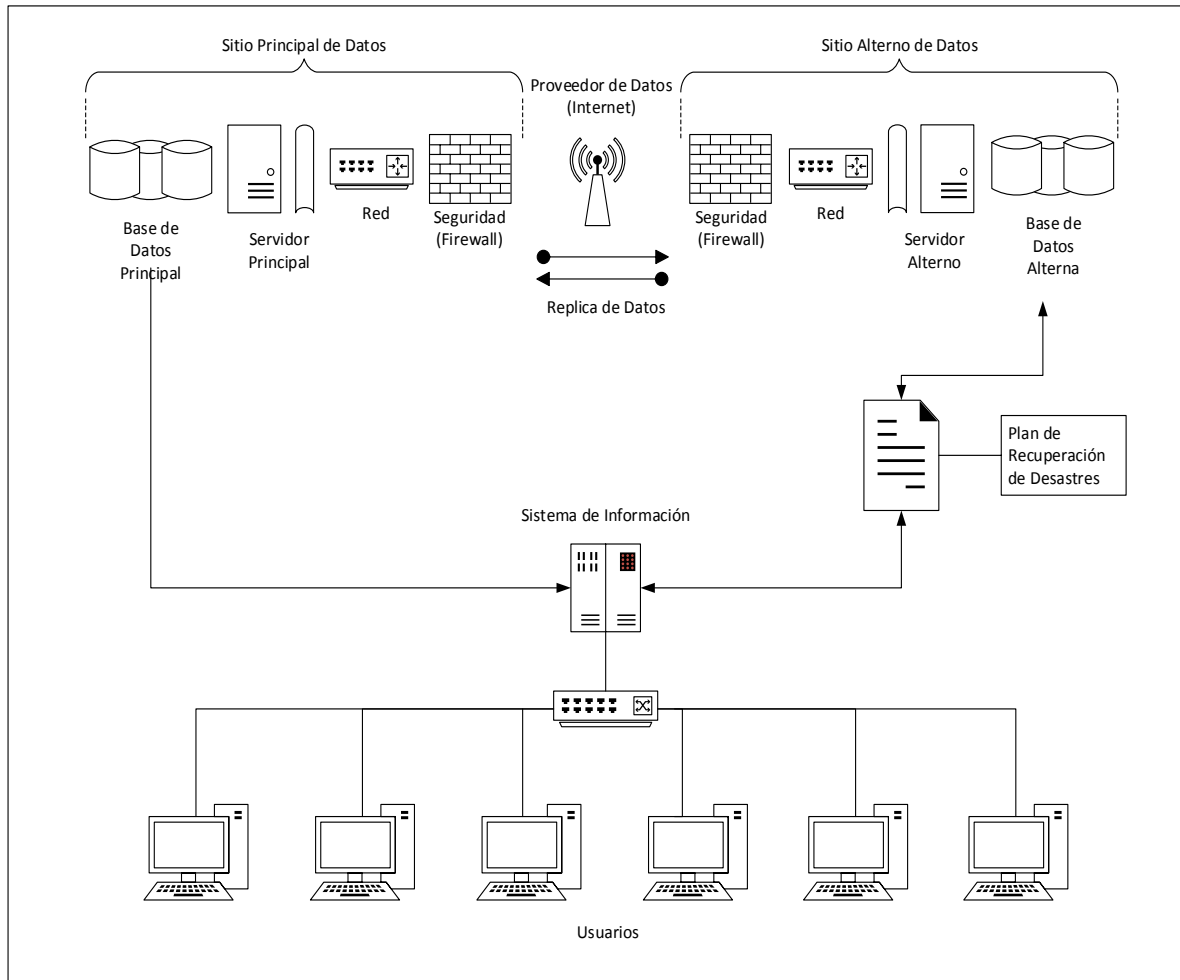
Cuando en los mapas de interrelación vista negocio, se menciona un sistema de información o bien una herramienta tecnológica, el Departamento de Tecnologías de Información, para cada proceso crítico o importante para la estrategia del negocio, lo tradujo en los elementos tecnológicos que se mencionan en el esquema ilustrado, por tal motivo estos elementos mapeados para los procesos / subprocesos críticos fueron los que básicamente se consideraron para replicar en el Sitio Alterno de Datos.

Como no todos los procesos / subprocesos son críticos o importantes para la organización, no todos los elementos tecnológicos instalados en el Sitio Principal de Datos, son críticos, con esto básicamente se priorizaron los elementos que se catalogaron como críticos, para dichos elementos que también se colocó la réplica en el Sitio Alterno de Datos se creó un Plan de Recuperación de Desastres, armando un procedimiento para los sistemas de información, un procedimiento para las bases de datos, servidores e infraestructura de Red.

Con ello nace el Plan de Continuidad de Operaciones de TI, con la integración de estos procedimientos, por defecto los sistemas de información funcionan empleando los elementos tecnológicos que se encuentran en el Sitio Principal de Datos, si algún evento no deseado o un incidente se materializan en este sitio.

Entonces a través del Plan de Recuperación de Desastres se habilita el Sitio Alternativo de Datos, en el que la información se replica de forma instantánea, para entender esto se ilustra lo siguiente:

Figura 12. Esquema de Diagrama de Servicios Tecnológicos



Fuente: Departamento de Tecnologías de Información.

La razón por la cual la replicación de información entre el Sitio Principal de Datos y el Sitio Alternativo de Datos es instantánea, también surge del Análisis de Impacto del Negocio (BIA), esto se debe a que según el Punto Objetivo de Recuperación (RPO), en el cual el área dueña del proceso/subproceso indica en qué punto atrás en el tiempo es óptimo recuperar los datos, en promedio la institución no podía pasar más de un minuto sin perder información, todo el Plan de Recuperación de Desastres (DRP), se basa en este lineamiento.

Para conocer el esquema gráfico del mapa de interdependencias tecnológico, elaborado por la entidad financiera, véase anexo 2.

4.4. Organización de los activos tecnológicos

Conocer la interrelación de los elementos tecnológicos que soportan todos los procesos / subprocesos de la organización es de vital importancia para la ejecución de actividades en el Departamento de Tecnologías de la Información, en donde todos los procesos internos giran básicamente para proveer la disponibilidad de los servicios tecnológicos.

En la empresa existe un alto porcentaje de relación entre el negocio, los beneficios que genera y la administración adecuada del riesgo tecnológico, por tal motivo los sistemas tecnológicos de información son una cantidad considerablemente grande que es necesario contar con herramientas para tener inventarios actualizados, que de forma automática se actualicen, estos controles no deben dejar desapercibido, ningún elemento porque de alguna forma todos se integran para proveer un servicio tecnológico que genere valor para la institución.

Al referirse a organización de los elementos tecnológicos, se considera que se debe conocer la configuración de los parámetros que lo conforman, los cambios relacionados que se tengan para adaptar las necesidades de la institución, los aspectos de seguridad que rodean los activos, incluyendo análisis de vulnerabilidades, el desempeño que presentan en el tiempo, la capacidad que tienen que soportar servicios, entre otros aspectos.

4.4.1. Repositorio de base de datos de configuración

Con el fin de mantener ordenado y actualizado un inventario sobre todos los activos tecnológicos del grupo, el Departamento de Tecnologías de Información desarrolló internamente una herramienta tecnológica, que tiene la función principal de ser la Base de Datos de Configuración, conocida comúnmente como CMDB, por sus siglas en inglés (*Configuration Manager Data Base*).

Esta herramienta cuenta con controles automáticos que monitorean constantemente todos los sistemas de información, bases de datos, servidores, infraestructura de telecomunicaciones, e infraestructura de seguridad, con el objetivo de conocer cómo se encuentran configurados los elementos tecnológicos, con ellos se mitiga el riesgo de que se realicen cambios sobre algún activo y este no se registre, la herramienta guarda registros de quien realiza cambios y envía alertas a los custodios principales y dueños de activos de información en caso se realice algún cambio que pueda no estar autorizado.

La herramienta se encuentra dividida para clasificar y describir los elementos que conforman los activos tecnológicos, en el sistema básicamente se encuentra de la siguiente forma:

Tabla XI. **Herramienta de Base de Datos de Configuración**

Servidores (Infraestructura)	Elementos de configuración	
	-Descripción	-Número de Serie
	-Tipo de Equipo	-Marca
	-MAC ADDRESS	-Memoria RAM
	-Modelo	-Ubicación
	-Procesador	-Criticidad
	-Estado	-Licencia
	-RAC	-Acceso Remoto
	-Versión OS	-Voltaje
	-Garantía	-Instalación Eléctrica
	-Proveedor	-Vencimiento Garantía
	Mantenimiento	
	-Fecha de último mantenimiento	- <i>Service Pack</i>
	-Fecha de actualización (parches)	- <i>Framework</i>
-Dirección IP	-Redundancia	
Sistemas de Información	Elementos de configuración	
	-Descripción	-Dueño
	-Lenguaje de Programación	-Custodio
	-Fuente	-Criticidad
	-Origen de Desarrollo	-Tipo de Aplicación
	-Fecha de puesta en marcha	-Conexión Externa
	-Proveedor	-Versión

Continuación de la tabla XI.

Activos	Descripción	
Base de Datos	Elementos de configuración	
	-Descripción General	-Versión Manejador
	-Motor	-Instancia
	-Servidor	<i>-File Name</i>
Infraestructura de Telecomunicaciones	Elementos de Configuración	
	-Descripción	-Proveedor
	<i>-Router</i>	-Prioridad
	-Ancho de Banda	
	-Disponibilidad	

Fuente: Departamento de Tecnologías de la Información.

La herramienta tecnológica por la sencilla razón de que fue desarrollada internamente se adapta a cualquier necesidad que considere necesario el Departamento de Tecnologías de Información, sin embargo, los principios empleados para su funcionamiento fueron todas las recomendaciones indicadas en la Norma ISO 20000-2:2012.

Para evidenciar todos los cambios realizados en los elementos de los recursos tecnológicos, se ha designado a un responsable a quien se le nombró como Gestor de Configuración, persona que mensualmente genera un reporte con el resumen de las modificaciones realizadas, el reporte incluye un análisis de los cambios efectuados, resaltando los más críticos.

La herramienta que funciona como la CMDB se integró perfectamente con otra herramienta que tiene el Departamento de Tecnologías de la Información para administrar los requerimientos e incidentes que son realizados por las diferentes áreas y departamentos.

Básicamente la herramienta es un Sistema de Gestión de Incidentes que tiene diferentes campos para describir y detallar las solicitudes o reportes realizados, en uno de esos campos se coloca el recurso tecnológico relacionado, es porque puede ser cualquiera, de esta forma se generan también reportes para conocer cuál es el recurso tecnológico en el que más incidentes se materializan y por ende es necesario ponerle más atención o bien el más crítico desde el punto de vista de estar involucrado con los procesos de la organización frecuentemente.

En la herramienta tecnológica CMDB, se diseñaron algoritmos de tal forma que con base a diferentes características que tienen los activos tecnológicos (sistemas de información, bases de datos, servidores, infraestructura de telecomunicaciones, infraestructura de seguridad de red), pudieran estar constantemente monitoreados, entonces es por esta razón que la herramienta no solo tiene la capacidad de indicar cuales son los cambios que se realizan.

También tiene la funcionalidad de mostrar la disponibilidad de los mismos, es decir, en qué momento se encuentran funcionando correctamente o en qué momento fallan, de esta forma también envía alertas para alarmar a los custodios con el fin de aplicar las medidas, en la medida más rápida posible y resolver cualquier incidente.

4.4.2. Evaluación de desempeño y capacidad de los activos tecnológicos

Los activos tecnológicos funcionan de acuerdo a la configuración de sus elementos, es decir, deben estar constantemente monitoreados, esto con el fin de que sean eficientes y efectivos para soportar los procesos de las áreas y departamentos de la organización. Todos los activos se monitorean diariamente, es por eso que se definieron custodios, básicamente en el Departamento de Tecnologías de Información los responsables son:

Tabla XII. **Custodios de los activos tecnológicos en el Departamento de Tecnologías de la Información**

Subgerencia	Jefaturas Custodios	Activos Tecnológicos
Subgerencia de Soporte	Jefatura de Soporte	Equipos de Cómputo
Subgerencia de Operaciones	Jefatura de Comunicaciones	Equipo de Telecomunicaciones
	Jefatura de Infraestructura	Servidores (físicos y virtuales)
	Jefatura de Administración de Bases de Datos	Bases de Datos
Subgerencia de Seguridad de Infraestructura	Jefatura de Seguridad Informática	Infraestructura de Seguridad de Red

Continuación de la tabla XII.

Subgerencia de Desarrollo de Sistemas	Jefatura de Desarrollo Interno	Sistemas de Información
Subgerencia de Investigación de Nuevas Tecnologías	Jefatura de Implementación	Sistemas de Información desarrollados por terceros

Fuente: Departamento de Tecnologías de la Información.

Cada una de las jefaturas que custodian los activos tecnológicos debe evaluar su desempeño. Los resultados los debe consolidar en un reporte el cual tendrá que enviar mensualmente a un colaborador que fue nombrado como Gestor de Capacidad.

Con relación a los servidores, la Jefatura de Infraestructura se apoya en diferentes herramientas tecnológicas que también realizan una acción de monitoreo de forma automatizada, esto configurado según los parámetros definidos por el área.

Dichas herramientas proporcionan información histórica y del estado actual de los recursos, esta información es utilizada para prever incrementos de capacidad, así como prevenir la indisponibilidad de los Sistemas de Información.

Con la información generada, se efectúan informes en los que se muestran todos aquellos servidores con distintas alertas que sobrepasan los umbrales definidos, básicamente estos umbrales se establecen como el fin de que se puedan alertar de forma temprana el uso de los recursos tecnológicos. Según los resultados que se vean reflejados en los informes se les notifica a todos los custodios involucrados a fin de que se puedan adoptar acciones tempranas a fin de optimizar los recursos asignados a los activos tecnológicos.

Tabla XIII. **Umbrales establecidos para generar alertas, según el análisis de desempeño de los recursos utilizados en los activos tecnológicos**

Umbral	Tipo de alerta
85 %	Alarma 1
90 %	Advertencia
95 %	Crítico

Fuente: Gestión de Capacidad del Departamento de Tecnologías de Información.

Básicamente las herramientas tecnológicas que monitorean los servidores mandan notificaciones a los custodios cuando por ejemplo se encuentran a un 85 %, 90 % y 95 % demandando su capacidad, los custodios interpretan la información e inmediatamente deben aplicar las acciones correctivas. Los sistemas de información constantemente son demandados debido a que cada día es más la dependencia que se tiene de los servicios tecnológicos.

Considerando esto se incrementa la demanda de los servidores por crecimiento normal de los sistemas o bien por la gestión de nuevos proyectos y el cumplimiento de los acuerdos de nivel de servicio establecidos. Los principales elementos que monitorea la Jefatura de Infraestructura son el procesador del servidor, memoria RAM, y almacenamiento.

Las bases de datos de los sistemas de información se alojan en servidores básicamente estas consumen el almacenamiento, por tal razón la Jefatura Administración de Bases de Datos debe monitorear el desempeño y rendimiento de dichas bases de datos, con el fin de que no se emplee almacenamiento que no debe utilizarse. Para el monitoreo se emplean herramientas tecnológicas también que se encuentran en el mercado bajo licenciamiento.

Estas herramientas pueden ser configurables y básicamente se considera el mismo principio que con los servidores. La demanda de las bases de datos también se puede incrementar por uso o bien por la gestión de nuevos proyectos.

Tanto los servidores como las bases de datos tienen definidos planes de acción para mitigar cualquier incidente que se pueda causar a razón de un colapso por la demanda de su capacidad.

La Jefatura de Comunicaciones evalúa el desempeño de los recursos que tiene asignados, los cuales prácticamente son, cableado estructurado, teléfonos de voz IP, comunicación LAN, y la demanda de los enlaces de internet. Existe una cantidad innumerable de métodos que se pueden aplicar para el análisis de estos recursos, aunque básicamente también se tienen herramientas con las

que básicamente se optimizan tanto los recursos de LAN como WAN (enlaces de internet).

En lo que corresponde a los Teléfonos de voz vía IP, se apoyan en una planta telefónica proporcionada por un proveedor el cual proporciona todo el soporte necesario, en este tipo de servicio la jefatura emplea una redundancia llamada n+1 con el fin de que, si se daña una planta telefónica, entre a funcionar la otra y si en caso se daña también entra a funcionar una tercera, estas plantas telefónicas se encuentran ubicadas físicamente en distintas zonas del país.

La Jefatura de Seguridad Informática evalúa el desempeño de tres equipos que son los más demandados en los servicios tecnológicos, es decir estos tres equipos son los más críticos para proteger y garantizar la seguridad en la red de la organización, los equipos son antivirus, antispam y el corta fuegos.

El antivirus es un hardware y software que se adquiere a un proveedor y básicamente es el encargado de actualizar todas las políticas que considere oportunas, por tal razón la Jefatura de Seguridad Informática debe registrar todos los equipos de cómputo y servidores que protege bajo esta herramienta, por tal razón lo que se debe monitorear es que todos los equipos tengan instalado el antivirus correctamente y que se tenga la cantidad de licencias para poder suplir la demanda.

Con relación al antispam básicamente la Jefatura de Seguridad Informática toma como parámetro la cantidad de correos por hora que transitan por las interfaces de entrada y salida, con el objeto de visualizar los picos que existieron en el transcurso del año/mes/semana/día, asimismo el tamaño

promedio de los correos. Los datos anteriores se consolidan y se comparan con las capacidades y limitaciones que tiene el equipo instalado en la red.

El corta fuegos es un sistema bien complejo en el que se analiza prácticamente lo siguiente, la cantidad de interfaces actuales de enlaces de internet, todas las transacciones que pasan en las interfaces, los tipos de red privadas virtuales que se han creado como protocolos de seguridad para compartir información con redes externas de la organización y las sesiones concurrentes que habilitan todos los trabajadores al momento realizar conexiones a internet.

Actualmente el Departamento de Tecnologías de Información solo analiza la capacidad y el desempeño de los activos tecnológicos que se encuentran custodiados bajo la Subgerencia de Operaciones y la Subgerencia de Seguridad de Infraestructura, esto se debe a que son las bases estructurales para que funcionen correctamente los servicios tecnológicos.

4.4.2.1. Plan de capacidad

El objetivo de crear y establecer un plan de capacidad es básicamente asegurar que los recursos humanos, tecnológicos y financieros, requeridos por los servicios tecnológicos, puedan satisfacer las necesidades de la compañía de manera efectiva y puntual.

Lo que básicamente se realiza en el plan es realizar pronósticos considerando que los servicios tecnológicos se estarán proporcionando a los todos los usuarios de la organización en las mismas condiciones, suponiendo que seguirán creciendo en una misma proporción como se ha presentado históricamente, es decir, se define este aspecto principal como factor cualitativo

que se acopla a los modelos matemáticos que se emplean según el comportamiento de datos.

Las técnicas cualitativas son muy importantes por el giro de negocio de la empresa, sin embargo, son opiniones subjetivas que se basan muchas veces en estimados. Para el enfoque cuantitativo es donde se emplean los datos registrados en las evaluaciones de desempeño y se convierten a variables causales que permiten prever la demanda.

En el plan de capacidad básicamente se realizan los pronósticos tabulando y graficando el conjunto de datos recopilados en las evaluaciones de desempeño mensual que realizan los diferentes custodios de los activos tecnológicos, al graficarlos se observa detenidamente la forma y comportamiento que sigue la curva resultante, si es difícil de observar se puede alisar la curva, es decir, incrementar y/o reducir la escala que se está utilizando para realizar la gráfica. Con base al comportamiento de la curva se puedan emplear modelos matemáticos tales como:

- Familias Estables o Modelos de Series de Tiempo: el análisis de las series en el tiempo se basa en la idea de que es posible utilizar información relacionada con la demanda de los servicios tecnológicos registrada en el pasado y con ello predecir la demanda futura, es decir, observa lo que ha ocurrido a lo largo de un período de tiempo y utilizan una serie de datos pasados para realizar una proyección futura.

Asimismo, las familias estables emplean un conjunto de datos que siguen un comportamiento hasta cierto punto de vista estable en un tiempo. Por tal razón con este método se pronostica la demanda de aquellos servicios tecnológicos que no importando la fecha en la cual se encuentren, la

demanda se mantiene en los mismos niveles. Para aclarar este punto es importante mencionar que, en una institución financiera, la demanda de algunos servicios tecnológicos varía según las fechas en el país, es decir, se registran más transacciones al referirse a épocas y festividades tales como fin de mes, quincena, semana santa, día de la madre, asuetos nacionales, navidad, año nuevo entre otros.

- Modelos de Correlación (Ascendentes – Descendentes): a diferencia de la previsión de series temporales, estos modelos consideran diferentes variables que están de alguna manera correlacionadas por la demanda que se quiere pronosticar, básicamente se emplean modelos matemáticos para describir las relaciones funcionales que existen entre dos o más variables (dependientes o independientes), este método es más poderoso que el de las series temporales.

En primer lugar, se observa el gráfico de datos para ver si aparecen lineales o por lo menos una parte de ellos, es importante aclarar que el método lineal se refiere a la clase de regresión especial en la que la relación entre, las variables forma una recta. Este método es útil para el pronóstico a largo plazo de eventos importantes, así como la planeación agregada.

- Series Estacionales (Curvas Cíclicas): cuando el conjunto de datos consolidado en las evaluaciones de desempeño realizadas a los activos tecnológicos sigue un comportamiento repetitivo periódicamente (curvas que contienen picos y valles) se pueden definir como series de datos ordenados en forma cronológica, estos están formados por uno o más componentes de demanda, por ejemplo una tendencia, factor estacional y un comportamiento cíclico. Existen servicios tecnológicos que durante

una línea de tiempo parece ser que se repiten. Esto regularmente se presenta en el uso de la memoria RAM, o bien en el equipo del antispam.

- Familias Combinadas: existen algunos elementos de tecnologías que son demandados siguiendo un patrón repetitivo (cíclico) y de la misma forma tiende a crecer y/o decrecer en función del tiempo (comportamiento ascendente y/o descendente). Esto regularmente se da cuando la demanda de los servicios tecnológicos varía por la constante gestión de proyectos nuevos.

El Departamento de Tecnologías de la Información empleó los modelos matemáticos indicados, basándose en el comportamiento de los datos consolidados mensualmente por el Gestor de Capacidad. Como estos datos son únicamente históricos de los elementos tecnológicos demandados, según la gestión de proyectos que se deriven de la institución, los cuales son de apoyo al negocio, se evalúan puntalmente si existirá algún incremento acelerado en la demanda.

Es importante indicar como se gestionaron algunos aspectos considerados para la previsión de los distintos recursos relacionados con los servicios tecnológicos:

- El recurso humano del Departamento de Tecnologías de la Información, en la medida posible registra en el Sistema de Gestión de Incidentes todos los datos (tiempos de planeación y ejecución) de las tareas operativas que tiene bajo su responsabilidad, estos datos son empleados para realizar las previsiones de recurso humano futuro, suponiendo que los servicios tecnológicos seguirán creciendo.

El tiempo registrado es estimado intentando asemejarse a la realidad, pero puede existir cierta diferencia ya que los colaboradores ejecutan tareas emergentes que no tienen previstas y por ende no las pueden registrar, este es un punto que debería cambiar.

- Los pronósticos de los activos tecnológicos realizados en el Plan de Capacidad, se generaron a partir de los modelos matemáticos indicados y referencias estadísticas, estos no prevén la demanda de forma precisa y/o exacta ya que existen muchos factores extrínsecos que no son objeto de los métodos, asimismo existen otros elementos que no pueden ser controlados ni por el Departamento de Tecnologías de la Información, ni tampoco por la entidad, pueden ser cambios en el sistema financiero del país. Sin embargo, los resultados sirven como información útil para adoptar acciones preventivas que puedan soportar el panorama en general, de esta forma no es el único documento que emplean los funcionarios para tomar decisiones ya que estos pueden variar.

4.4.3. Jefatura de administración de bases de datos de información

El Departamento de Tecnologías de la Información ha delegado la autoridad de establecer los criterios y mejores prácticas para la administración y el uso responsable de los servicios de bases de datos alojados en los servidores de producción a la Subgerencia de Operaciones, quien a su vez lo ha relegado a la Jefatura de Administración de Bases de Datos de Información.

Esta jefatura ha creado una política de aplicación obligatoria para todos los colaboradores que se encuentran involucrados directamente con la

organización, coordinación, operación y soporte de cualquier de las bases de datos en donde se almacena la información de la organización.

La Jefatura de Administración de Bases de Datos de Información deberá garantizar que todos los elementos y parámetros de las bases de datos de la institución, están configurados de forma adecuada, de tal forma que se pueda garantizar la disponibilidad, confidencialidad e integridad de la información. Los lineamientos que como mínimo se consideraron en la jefatura para gestionar la seguridad de los datos son:

- Los servicios de administración de usuarios de bases de datos, tales como la creación de usuarios, creación/modificación de grupos o roles de usuarios, asignación/modificación de permisos a usuarios, creación de perfiles, asignación de roles, reinicio de contraseñas, bloqueo de usuarios, eliminación de usuarios, fecha de vencimiento de contraseña, bloqueo por intentos fallidos.
- Realizar diagramas de entidad-relación (ER, por sus siglas en inglés), con el fin de ilustrar la relación e interacción de las que integran una base de datos, a través de los campos que las conforman. Básicamente en estos diagramas se debe identificar claramente las tablas maestras, las tablas hijas, las llaves primarias, las llaves foráneas, las llaves únicas la relación entre las tablas maestra y tablas hijas (de uno a uno, de muchos a uno o viceversa, de muchos a muchos).
- Documentar diccionarios de datos a fin de definir cada una de las tablas, campos, dominios, tipos de datos, formatos, valores por defecto, reglas asociadas e índices.

- Tanto como para los diagramas de entidad relación, así como los diccionarios de datos, el Departamento de Tecnologías de la Información ha creado una herramienta que se encuentra integrada con la Base de Datos de Configuración, básicamente cualquier creación, modificación y/o eliminación de algún parámetro debe obligatoriamente documentarse.

4.5. Administración de proveedores y contratos

La gestión de los servicios que sean contratados con terceros resalta sobre la administración de riesgo tecnológico. Muchos de los servicios tecnológicos que el Departamento de Tecnologías de la Información proporciona a las diferentes áreas y departamentos, dependen en un cierto grado de un proveedor, ya sea por un servicio de soporte o mantenimiento, asimismo como para el procesamiento de información o bien para enlaces de datos (internet).

Con base al Reglamento para la Administración del Riesgo Tecnológico, Resolución JM-102-2011, el contratado y/o proveedor que procese datos de una entidad, deberá garantizar el resguardo de la confidencialidad de dicha información, tendrá que establecer acuerdos de nivel de servicio con la compañía y establecer en el contrato que la Superintendencia de Bancos de Guatemala tendrá libre acceso a sus instalaciones, infraestructura tecnológica, sistemas de información y bases de datos relacionadas con la entidad con quien definió la obligación contractual.

Para cumplir con lo indicado por el reglamento, el Departamento de Tecnologías de la Información estableció una serie de lineamientos para gestionar las relaciones constituidas con terceros, a fin de que proporcionen los servicios por los cuales fueron contratados bajo estándares y requisitos

mínimos definidos para el beneficio de la empresa y paralelamente del proveedor.

Como parte de la administración correcta de los servicios contratados con terceros, los cuales tengan un fin tecnológico, se definieron políticas para que se pudieran establecer de forma clara las obligaciones:

- Todas las compras de infraestructura tecnológica, equipo de telecomunicaciones, infraestructura de seguridad, sistemas de información, deberá estar respaldada por un contrato formal, como lo establece la ley. El contrato deberá contar como mínimo con lo siguiente:
 - Objeto principal del contrato
 - Descripción detallada del producto o servicio a contratar, es importante mencionar que se deben incluir todas las características posibles que no dejen lugar a duda de lo que se necesita.
 - Acuerdos de niveles de servicio, considerando el fin del servicio o producto y redactar los mismos en base a ello, se debe incluir obligatoriamente el medio por el cual se realizarán los reportes de falla y cuales deberán ser los niveles de escalamiento, incluir tiempo de respuesta bien detallados para los servicios, así como las sanciones que se pueden aplicar en caso de incumpliendo por parte del proveedor.
 - Datos financieros y económicos, especificando el alcance
 - Forma y condiciones de pago especificando con detalles los montos por cada etapa y periodicidad según la entrega del servicio. Para beneficio de la organización, se deberá negociar que los pagos sean contra entrega del bien o servicio, de tal manera que el proveedor el comprometido.

- En el caso de proyectos, indicar cuál será el calendario de trabajo y las fechas de entrega de actividades o tareas relevantes.
- La dirección física de ambas partes
- Mencionar en forma detallada las sanciones por incumplimiento en alguna de las partes.
- Señalar si es necesario un período de capacitación, entrenamiento o instrucción a colaboradores de la sociedad.
- Agregar que se deberán contemplar nuevos requerimientos legales que surjan en el camino y que no se pudieron contemplar.
- Si el proveedor estará a cargo de subcontrataciones deberá definir el proceso que emplea para gestionar la relación con otras partes involucradas.
- En el caso que el proveedor procesara datos de la entidad financiera se deberá agregar lo establecido por la Resolución JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico, en el artículo 25, desde el inciso (a) hasta el (e).

Se estableció que el Departamento Jurídico será el único que deberá certificar todos los contratos que se celebren.

En el caso que sea necesario renovar, cancelar o transferir las obligaciones de un contrato, se tuvo que haber evaluado formalmente el servicio proporcionado por el proveedor, asimismo si es directamente una cancelación, se deberán dejar plasmadas por escrito las causas e implicaciones que derivan de esta acción.

Es importante resaltar que todas las Entidades que conforman el sistema financiero del país, las cuales están sujetas a la revisión y supervisión de la Superintendencia de Bancos de Guatemala, se encuentran obligadas a cumplir

los requisitos establecidos por una unidad que se encuentra bajo el mando de esta última, llamada Intendencia de Verificación Especial (IVE).

Intendencia de Verificación Especial (IVE) quien básicamente se encarga garantizar que las relaciones que entablan las Entidades Bancarias con clientes, bancos corresponsables, proveedores, entre otros; tengan los controles adecuados que prevengan el lavado del dinero y financiamiento del terrorismo, para tal efecto han creado una política nacional llamada “Conozca a su proveedor”, en donde debe quedar plasmada una verificación realizada en listas de OFAC y ONU (Organizaciones Internacionales) de los representantes legales de las empresas que proporcionarán los bienes y servicios.

4.5.1. Definición de técnicas de selección de proveedores

El proceso de selección de todos los proveedores, tanto los que se encontrarán relacionados con tecnologías de la información, como los que no, deberá ser transparente e imparcial, en este tendrá prioridad el beneficio de la compañía ante el beneficio propio de algún colaborador o de terceros.

La selección de los proveedores será realizada únicamente por las áreas y departamentos que serán responsables de los bienes o servicios, considerando todo lo relativo a compra, gasto o inversión.

Para la adquisición de un bien o servicio en particular, se deberán evaluar como mínimo tres proveedores que lo ofrezcan, solo se exceptuarán los casos en que por la naturaleza del producto no existiera más de un oferente.

4.5.2. Procedimiento de contratación de proveedores

Los proveedores deberán estar asignados en todo momento a un área o dependencia responsable de la relación. Las áreas deberán certificar la calidad del servicio o las condiciones y características del bien adquirido.

Los proveedores de servicios deberán registrarse en un único sistema que fue desarrollado por el Departamento de Tecnologías de Información, esto con el fin de llevar un único control, en la herramienta tecnológica se debe registrar como mínimo lo siguiente:

- Contrato
- Ubicación
- Observaciones generales o descripción breve
- Razón Social
- Nombre Comercial
- Dirección
- Teléfono
- Sitio Web
- Correo electrónico
- Bienes o servicios adquiridos
- Monto facturado anualmente
- Clasificación, esta será en base al monto que estarán facturando anualmente, se clasificarán como alto impacto o bajo impacto, esto para cumplir siempre con los requerimientos establecidos por la IVE.

En el registro realizado en el sistema se deberá agregar obligatoriamente la siguiente evidencia:

- Referencias de los representantes legales, obtenidas en los buros de crédito e información que se encuentren disponibles.

- Fotocopias de las patentes de comercio
- Fotocopias de la patente de sociedad (cuando aplique)
- Fotocopias de escritura de constitución de la empresa
- Fotocopias del nombramiento de la representación legal
- Fotocopias de inscripción del nombramiento en el Registro Mercantil vigente.
- Registro Tributario Unificado (RTU) actualizado anualmente

Todos los proveedores clasificados como alto impacto, porque facturan anualmente un monto establecido por la IVE, deberán trasladar los Estados Financieros o Estados de Resultados a la organización, estos serán analizados por el Departamento Jurídico y si presentan algún indicio que ponga en duda la solidez de la empresa, se deberá elevar el caso al Comité de Riesgos para su evaluación.

Si todo se encuentra registrado y las evaluaciones son positivas se procederá a firmar el contrato con el representante legal de la entidad financiera y el representante legal del Proveedor. El registro de los campos en el sistema se deberá realiza como mínimo anualmente o bien cuando se considere oportuno.

4.5.3. Metodología de pruebas

Adicional a los lineamientos indicados en el punto anterior, todos los proveedores relacionados a los servicios de tecnologías de la información, previo a su contratación, deberán realizar una prueba de concepto, básicamente en este tipo de ensayos, los proveedores instalan sus productos y/o servicios en un ambiente controlado y el área que custodiará el activo por parte del Departamento de Tecnologías de la Información realizará pruebas

funcionales de todo lo que el proveedor vendió u ofreció en papel. El resultado de estas pruebas garantiza que el producto que se prevé adquirir realmente satisface las necesidades por las cuales se ha buscado.

Las subgerencias del Departamento de Tecnologías de Información realizarán todas las actividades que considere oportunas para la prueba de concepto y documentará los resultados obtenidos en un formulario establecido, esto con el fin de presentarlo a quien autorizará la contratación del proveedor (Gerente del Departamento de Tecnologías de Información) y contar con la evidencia de que se realizaron las pruebas.

Si los resultados de las pruebas de concepto son los esperados entonces se procederá con el procedimiento de contratación. Para conocer el formulario empleado para validar y certificar las pruebas de concepto, véase el anexo 3.

La metodología de pruebas previo a la contratación del proveedor que apruebe positivamente las pruebas de concepto incluyen entre otros, la evaluación de los siguientes puntos:

- Precio: la evaluación se realiza a través de la verificación de precios en el mercado, en relación con el tipo de bien o servicio, es decir, de acuerdo con las propuestas económicas presentadas por los distintos proveedores y su comparación con el presupuesto que se tiene asignado.
- Experiencia en el sector: se evalúa el grado de experiencia de acuerdo a los años que posea trabajando en el sector según el tipo de bien o servicio, entre menor sea la experiencia directamente proporcional será la consideración que le será otorgada.
- Tiempo de entrega: será considerado si el tiempo de entrega o implementación se adecúa a las necesidades y al tiempo establecido

internamente.

- Garantías: en este caso, se debe evaluar la oferta de garantía por parte del proveedor, asimismo las condiciones, tiempos, coberturas, entre otros.
- Certificación de calidad: evaluar si el proveedor cuenta con certificados internacionales de calidad de servicios o procesos, los cuales garanticen la entrega exacta y puntal.
- Casos de éxito: se corroborará personalmente los casos de éxito indicados por el proveedor, si es posible se considerará realizar una reunión.
- Representación local: es preferible que los proveedores sean empresas locales o tengan representación legal dentro del país.
- Respaldo internacional: determinar si el proveedor posee un socio internacional que respaldará el bien o servicio.

El resultado de todos estos análisis deberá ser documentado y de la misma forma aprobado por el Gerente del Departamento de Tecnologías de la Información, para ello se podrá utilizar el formulario correspondiente (véase anexo 4).

4.5.4. Creación de acuerdos de nivel de servicio

Es probable que para todos los proveedores contratados y por contratar en el Departamento de Tecnologías de Información, no se pueda llegar a realizar acuerdos de nivel de servicio, sin embargo, es obligatorio indicar las razones por las cuales no fue posible.

Para los casos en los que se puedan entablar acuerdos de nivel de servicio, el custodio de los activos deberá considerar los tipos que más se adecuen a las características del bien o servicio:

- En el caso de servicios que serán medidos por la disponibilidad que se encuentren hábiles deberá ser en un porcentaje relativo al tiempo, es decir, que el proveedor se comprometerá a proporcionar el servicio por una cantidad x en horas durante el tiempo que perdure el contrato, este tipo se utiliza por ejemplo en los servicios de enlaces de datos (internet).
- En el caso de servicios relacionados con soporte y/o mantenimiento, se deberá considerar el tiempo en el que el proveedor se compromete a resolver las incidencias reportadas por la sociedad.
- Existe el tipo en el que se pueden establecer compromisos sobre bienes y/o servicios, es decir que no se pueden medir de forma cuantitativa sino más bien de forma cualitativa.

Independientemente del tipo de acuerdo de nivel de servicio que se establezca será necesario detallar los activos específicos asociados, las ubicaciones regionales y el escalonamiento. Es importante mencionar que los acuerdos de nivel de servicio que se establezcan con los proveedores deberán estar alineados a los que establece el Departamento de Tecnologías de la Información con las áreas y departamento.

4.5.5. Evaluación periódica de proveedores

En el Departamento de Tecnologías de la Información se ha designado a una persona quien tiene la responsabilidad de llevar el control de las

evaluaciones de desempeño de los proveedores, las cuales deberán realizarse mensualmente, con el objetivo de determinar si los proveedores son aptos para continuar prestando los servicios o si es necesario aplicar penalizaciones, porque no están cumpliendo con los acuerdos de nivel de servicio establecidos. Los responsables de los proveedores deberán enviar las evaluaciones realizadas a más tardar los primeros 8 días de cada mes.

Para realizar la evaluación se ha elaborado un formulario (véase anexo 5), en esta prueba únicamente se estarán evaluando los acuerdos de nivel de servicio establecidos por el proveedor del bien o servicio en relación al cumplimiento de los mismos, o bien si existen requerimientos realizados a los proveedores los cuales no han resuelto satisfactoriamente. Si se presente algún indicio de este tipo se deberá reportar al Gerente de Departamento de Tecnologías de la Información, a fin de que se pueda comunicar al representante del proveedor y analizar si corresponde realizar las penalizaciones establecidas en los contratos.

4.6. Manual de riesgo tecnológico

El Departamento de Tecnologías de la Información se sustentó en un marco de referencia desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés), el cual fue titulado Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, por sus siglas en inglés), en su versión 4.1, para la administración del riesgo tecnológico.

Las buenas prácticas establecidas por este marco de referencia se basan en el propósito de establecer recomendaciones / controles objetivos que debe considerar un buen gobierno de gestión de Tecnologías de la Información en una organización, con el fin de que se puedan apoyar en los beneficios que

estas proveen para la consecución de los objetivos trazados por cualquier tipo de empresa.

Considerando los controles propuestos por COBIT 4.1, el Departamento de Tecnologías de la Información desarrolló e implementó una herramienta que tiene la función principal de facilitar la gestión y seguimiento de los lineamientos proporcionados para identificar, analizar, determinar, priorizar y manejar los riesgos.

4.6.1. Identificación del riesgo

Básicamente el Departamento de Tecnologías de la Información podría considerar la implementación de un número infinito de buenas prácticas recomendadas por una gran variedad de metodologías, sin embargo, es por ello que al utilizar la descripción y definición de los objetivos de control incluidos en los procesos de COBIT 4.1.

La institución fundamentalmente lo que define es que, al no contar con las recomendaciones emitidas por el marco de referencia, se puede materializar un riesgo tecnológico que podría poner en peligro la consecución de los objetivos y metas trazados por la organización.

En otras palabras, COBIT 4.1 propone un control que debería existir para cierto proceso definido en la gestión de servicios de tecnologías de la información, el Departamento de Tecnologías de Información lo interpreta como la falta de existencia de un control de este tipo, podría generar la materialización de un riesgo del mismo tipo.

Bajo esta premisa se identifica en primera instancia cuales son los riesgos y como están descritos. Entonces el trabajo del coordinador y los analistas de riesgos tecnológicos de la empresa, deben indicar cuales son los controles actuales que se tienen para manejar los riesgos identificados, asimismo se deberán describir los detalles y sus posibles deficiencias.

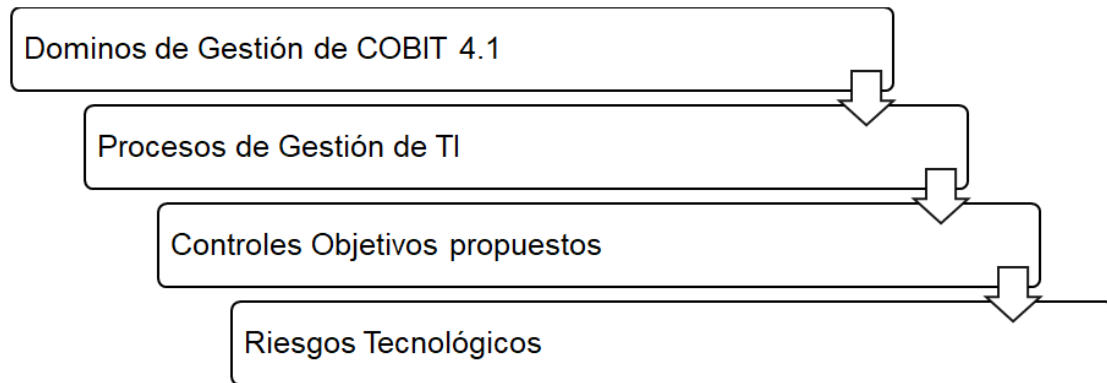
A lo que se quiere llegar con esta actividad es que El Departamento de Tecnologías de la Información debe plantearse como objetivo que sus controles implementados tengan el nivel de madurez propuesto por el marco de referencia.

Cuando se describen y son relacionados los controles con los riesgos propuestos, esto se basa principalmente en la aplicación de políticas, definición de procesos y procedimientos, solicitudes de cambios, revisiones adecuadas de documentos publicados en el repositorio compartido para este fin, adecuación de reportes y/o informes de auditorías internas y externas efectuadas a los servicios tecnológicos de Información provistos por el Departamento de Tecnologías de la Información.

Considerando el párrafo anterior, el Departamento de Tecnologías de la Información documentó un procedimiento donde define los parámetros y lineamientos para la creación e implementación de controles (planes, políticas, procedimientos, registros, validaciones manuales, automatizadas, entre otros).

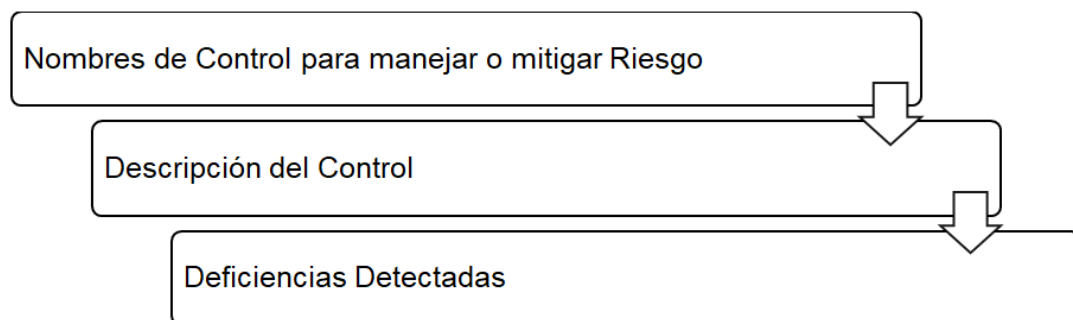
El esquema empleado para la administración del riesgo tecnológico en el cual se relacionan los riesgos en comparación con los controles implementados por el Departamento de Tecnologías de la Información, está fundamentado de la siguiente forma:

Figura 13. **Primer Nivel –Objetivos de Control de COBIT 4.1-**



Fuente: Manual de Administración de Riesgo Tecnológico, entidad financiera.

Figura 14. **Segundo Nivel –Controles Implementados por el Departamento de Tecnologías de la Información-**



Fuente: Manual de Administración de Riesgo Tecnológico, entidad financiera.

La lógica de comparación expuesta fue la misma que se empleó para desarrollar la herramienta de software interna para la administración del Riesgo Tecnológico.

4.6.2. Análisis del riesgo

El análisis de los riesgos propuestos se aborda a través de una valoración y priorización asignada con base a la información obtenida en la identificación del riesgo, así como diferentes aspectos extrínsecos e intrínsecos de la organización que podrían verse afectados o están relacionados.

Los detalles analizados para calcular el nivel de riesgo y las acciones que se van a implementar para manejar estos mismos son definidos considerando ciertos criterios a los que se debe adaptar la información resguardada en la infraestructura tecnológica para satisfacer los objetivos de negocio, por tal razón se definieron los siguientes requerimientos:

- Efectividad: se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- Eficiencia: se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- Confidencialidad: se refiere a la protección de información sensible contra divulgación no autorizada.
- Integridad: se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas de la organización.
- Disponibilidad: se refiere a la disponibilidad de la información cuando esta es requerida, también se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- Cumplimiento: se refiere al ejercicio de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocio está sujeto.
- Confiabilidad: se refiere a la provisión de la información apropiada para la

administración, con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y cumplimiento.

Los puntos anteriormente descritos pasan a definirse por el Departamento de Tecnologías de la Información como los requerimientos generales del negocio, es decir, como el negocio necesita que los recursos tecnológicos adapten la información para cumplir sus objetivos y metas trazadas.

4.6.3. Determinación del nivel de riesgo

Considerando lo expuesto por la Norma ISO 31000, en donde se hace referencia que la gestión de riesgos es un proceso estructurado y secuencial, de identificación, análisis y cuantificación de las probabilidades de ocurrencia de una determinada amenaza, cuya materialización provoca pérdidas o deterioro además de efectos secundarios; el nivel de riesgo en el Departamento de Tecnologías de la Información se expresará en términos de probabilidad e impactos.

Estos dos aspectos mencionados (probabilidad e impactos), sirvieron para traducir muchos riesgos y eventos que solo pueden expresarse cualitativamente en algunos casos y en otros solo bajo supuestos ya que nunca se han materializado en el país.

La probabilidad de ocurrencia de cierto evento puede calcularse por un sinnúmero de fórmulas, asimismo la cuantificación de los impactos que se generan por la materialización de dicho evento puede proyectarse según el grado de activos (tangibles no tangibles) que podrían resultar afectados. Por esta razón en la metodología adoptada por el Departamento de Tecnologías de la Información, se estableció que tanto la probabilidad como el impacto se pueden

expresar en términos cualitativos, no obstante, considerando factores cuantitativos como a continuación se indica:

- Para indicar la probabilidad, se asignó un número en la escala de uno (1), a cinco (5), lo cual determinará la posibilidad de que ocurra un riesgo tomando como referencia lo siguiente:
 - (5) Alta: es muy factible que un evento se materialice
 - (3) Media: es factible que el hecho se presente
 - (1) Baja: es muy poco factible que el hecho se presente

Es importante no perder el enfoque y mencionar que el Departamento de Tecnologías de la Información trabaja para implementar distintos controles que reduzcan la probabilidad de materialización de algún evento no deseado, es decir, la efectividad de los controles está directamente relacionada con la posibilidad de que se materialice un riesgo, entre más efectivo sea un control menos probable será que se materialice un riesgo y viceversa.

- Para representar la magnitud del impacto negativo que podría llegarse a derivar en caso se materializará un riesgo, se asignó de la misma forma que para la probabilidad, una escala de uno (1), a cinco (5), tomando como referencia lo siguiente:
 - (5) Alta: si el hecho llegara a presentarse, los efectos negativos que se desencadenan afectan a más del 25 % de los activos tangibles y no tangibles de la entidad financiera.
 - (3) Media: si el hecho llegara a presentarse, los efectos negativos que se desencadenan afectan a más del 15 % pero menos del 20 % de los activos tangibles y no tangibles de la entidad.

- (1) Baja: si el hecho llegara a presentarse, los efectos negativos que se desencadenan afectan menos del 5 % de los activos tangibles y no tangibles de la empresa.

El cálculo de los impactos, es decir, que cantidad se le asignará a la materialización de ciertos tipos de riesgo es un trabajo que no realiza el Departamento de Tecnologías de la Información por sí solo, estas magnitudes son asignadas a través de una encuesta que se realiza a toda la organización planteando diferentes escenarios generales y específicos, de esta forma el coordinador y analistas de riesgo tecnológico consideran las respuestas indicadas por todas las áreas y departamentos y realizan promedios.

Considerando lo indicado, entonces el impacto depende de la percepción de las áreas en cuanto a la materialización de ciertos riesgos, por otro lado, la probabilidad depende directamente del nivel de madurez y exactitud de los controles implementados por el Departamento de Tecnologías de Información. Al tener una cantidad para la probabilidad y una para el impacto entonces el nivel de exposición de riesgo tecnológico será determinado a través de la fórmula de:

$$\text{Nivel de Riesgo} = \text{probabilidad} * \text{impacto}$$

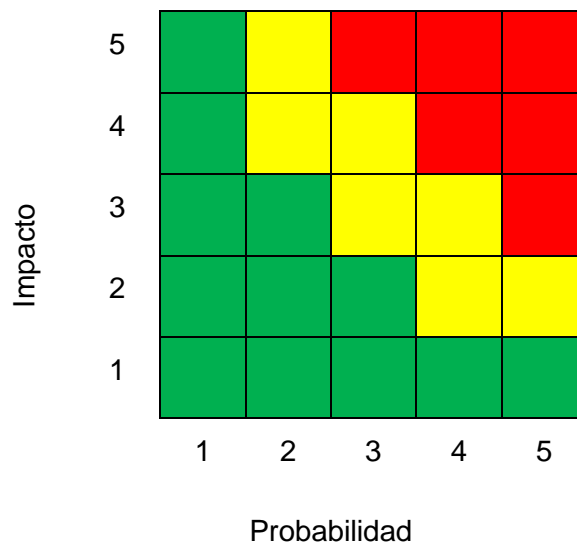
Este cálculo es realizado para cada uno de los doscientos diez (210) objetivos de control propuestos por COBIT 4.1, es decir, se asignan doscientas diez (210) probabilidades, doscientos diez (210) impactos; entonces la cartera de referencia de riesgos tecnológicos por ende será de doscientos diez (210).

4.6.4. Priorización del riesgo

Cuando el Coordinador y los analistas de riesgos tecnológicos establecieron el nivel de cada uno de los riesgos identificados, es decir, realizaron un proceso formal de evaluación de cada uno de ellos, el Departamento de Tecnologías de la Información debe priorizar los riesgos para poder focalizar correctamente los recursos que dispone en el año en curso y los que tendrá en presupuesto para el siguiente año.

Básicamente la priorización indicará visualmente cuales son aquellos riesgos que se deben atender con urgencia. La prioridad de cada riesgo no es más que el resultado de la multiplicación de la probabilidad y el impacto según la ponderación que se les haya asignado, es decir, se asigna mediante el Nivel de Riesgo indicado en la siguiente matriz:

Tabla XIV. **Matriz del Modelo de Riesgo Tecnológico**



Fuente: Manual de Administración de Riesgo Tecnológico, entidad financiera.

Tabla XV. **Matriz de Calificación del Riesgo Tecnológico**

		Rangos	
		Min	Max
	Nivel		
	Riesgo Bajo	≥ 1	< 8
	Riesgo Medio	≥ 8	< 15
	Riesgo Alto	≥ 15	

Fuente: Manual de Administración de Riesgo Tecnológico, entidad financiera.

- Riesgo Alto: cuando el riesgo tecnológico hace altamente vulnerable a la organización (Impacto y probabilidad alta con relación a los controles).
- Riesgo Medio: cuando el riesgo representa vulnerabilidades medias (impacto alto - probabilidad media y baja o impacto bajo y medio - probabilidad alta en relación a los controles).
- Riesgo Bajo: cuando el riesgo presenta vulnerabilidad baja. (impacto y probabilidad baja en relación a los controles).

4.6.5. Manejo del riesgo

En relación a la gestión de los riesgos, el Departamento de Tecnologías de Información debe analizar las posibles acciones a emprender, la cuales deben ser factibles, efectivas y sobre todo viables para las autoridades. De forma general se puede mencionar la implementación de políticas, definición de estándares, optimización de procesos y procedimientos, cambios físicos, entre otros.

Entre las acciones y alternativas que el Departamento de Tecnologías de la Información puede adoptar para manejar el riesgo, se pueden mencionar las siguientes:

- Evitar el riesgo: es siempre la primera alternativa a considerar. Se logra cuando en el interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.
- Reducir el riesgo: si el riesgo no puede ser evitado porque crea grandes dificultades operaciones, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos, políticas y la implementación de controles.
- Dispersar y fragmentar el riesgo: se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como por ejemplo la información de gran importancia se puede duplicar y almacenar en un lugar distante de ubicación segura, en vez de dejarla concentrada en un solo lugar.
- Transferir el riesgo: hace referencia a buscar respaldo y compartir con otro parte del riesgo como por ejemplo tomar pólizas de seguros, esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.

- Asumir el riesgo: luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso la Gerencia Dirección de Operaciones simplemente acepta la pérdida residual probable y el Departamento de Tecnologías de Información deberá elaborar planes de contingencia para su manejo.

Cualquier alternativa adoptada por el Departamento de Tecnologías de Información deberá ser aprobado por el Comité de Riesgos, solo así se puede dar lugar a los planes de acción.

Es importante mencionar que una vez se concreten las acciones que serán consideradas para gestionar el riesgo, se deberán manejar los planes de acuerdo a su condiciones, es decir evaluar si sólo son cambios, tareas, o bien tendrán que ser proyectos complejos.

5. SEGUIMIENTO O MEJORA

5.1. Resultados obtenidos

El coordinador y los analistas de riesgos tecnológicos deberán preparar una presentación en donde incluyan gráficos entendibles para que se pueda observar de forma clara y concisa cual es el nivel de exposición de riesgo tecnológico de la entidad financiera.

En esta presentación es recomendable hacer una gráfica para conocer cuáles son los resultados obtenidos a nivel de: Dominios de Gestión de COBIT 4.1, Procesos de Gestión de TI, e indicar todos aquellos Controles objetivos propuestos por el Marco de Referencia que muestren un nivel de riesgo alto, para estos últimos es importante describirlos e indicar las razones por las cuales se considera que están vulnerables, así mismo de una forma muy escueta cuales podrían ser las recomendaciones que se pueden implementar para manejar el riesgo.

Es recomendable representar los resultados periódicos según el tiempo en el que se hagan las evaluaciones, asimismo realizar una gráfica comparativa para determinar si han existido avances en cuanto a la gestión de riesgos o bien existen brechas en las que se debe prestar más atención. Para conocer ejemplos de las gráficas que se pueden emplear.

5.1.1. Interpretación

El Gerente de Departamento de Tecnologías de Información deberá revisar la presentación elaborada, asimismo conocer los detalles, básicamente el coordinador y los analistas de riesgos tecnológicos hacen la propuesta escueta para manejar el riesgo tecnológico, sin embargo, es el Gerente mencionado quien deberá analizar minuciosamente con su equipo de trabajo, cuáles serán las propuestas formales.

El nivel de exposición de riesgo tecnológico no solo es producto del trabajo realizado por el coordinador y los analistas de riesgos tecnológicos de la empresa. El Departamento de Tecnologías de la Información se apoya en la opinión realizada por el Departamento de Auditoría Interna y contrata los servicios de auditores externos de firmas reconocidas como KPMG; Ernst & Young, Verizon Business y Delloite para que los resultados se rectifiquen y se pueda conocer la opinión de cada uno de ellos, el resultado es que las acciones a implementar para manejar el riesgo sean objetivas y precisas.

Tanto el departamento de auditoría interna como los auditores externos contratados deberán alienarse a la misma metodología propuesta del marco de referencia de COBIT 4.1, ellos son quienes también soportan y fundamentan las cantidades colocadas en los impactos; para asignar estos datos emplean una distinta metodología, pero son generadas en las mismas escalas de acuerdo a lo definido.

El contratar distintas auditorías externas es un punto clave porque estas no solo dan un resultado efectivo si no también entregan un informe comparando el nivel de exposición de riesgo tecnológico en relación a otras instituciones financieras nacionales e internacionales.

Según la revisión y aprobación del Gerente de Departamento de Tecnologías de Información, los informes entregados por el coordinador de riesgos tecnológicos, departamento de auditoría interna y auditorías externas son consolidados y se presentan al comité de riesgos semestralmente para trasladar anualmente la información al Consejo Directivo.

5.2. Evaluaciones periódicas

La Gestión de Riesgos no es un tema que se realice una sola vez, este es un tópico continuo ya que día con día se generan nuevos riesgos y los controles se deben adaptar de tal forma que la gestión sea efectiva y eficiente.

5.2.1. Autoevaluación

Esta evaluación es a nivel interno del Departamento de Tecnologías de la Información es liderado por el Coordinador de Riesgos Tecnológicos y ejecutado por los analistas, este proceso se deberá realizar anualmente a fin de conocer los avances en las propuestas realizadas con anterioridad y si estas propuestas han apoyado en la gestión efectiva de los riesgos tecnológicos.

5.2.2. Auditorías internas

El departamento de auditoría interna participa en dos procesos de evaluación, el primero es un testeo anual empleando la misma metodología propuesta de COBIT 4.1; la segunda se basa en evaluar todos aquellos procesos y objetivos de control propuestos que consideren están por debajo del nivel deseado y que, según su percepción, las vulnerabilidades están más expuestas, este trabajo es realizado de forma esporádica, bajo demanda o bien está atado al calendario anual de este departamento.

Los informes emitidos por el departamento de auditoría interna, reflejan hallazgos que a su consideración deben ser mitigados. Estos pueden falencias en los controles implementados o bien procesos vulnerables que no tienen los controles adecuados y deben ser fortalecidos. Los resultados de estos reportes son enviados a la Gerencia General y Administración Ejecutiva.

5.2.3. Auditorías externas

El Departamento de Riesgos y el Departamento de Tecnologías de Información, con el aval de la Gerencia Dirección de Operaciones deberán contratar semestralmente una de las firmas reconocidas de auditoría, a esta se les deberá explicar cuál es la metodología propuesta por la organización, y que realicen un proceso de evaluación de acuerdo a dicho marco de trabajo. Adicional a esto también se les requiere realizar las evaluaciones que consideren oportunas con el fin de conocer los resultados que se manejan en otras organizaciones y estos se puedan comparar.

Los informes en donde se pueden visualizar los resultados de las evaluaciones realizadas por las auditorías externas son presentados directamente en las reuniones ordinarias del Consejo Directivo. En estos informes también son reflejados hallazgos que tienen que ser evaluados por el Departamento de Riesgos con el fin de indicar las formas en las cuales se estarán mitigando o bien manejando los riesgos asociados.

5.3. Medidas preventivas y correctivas

Las unidades involucradas en la gestión del riesgo tecnológico, como parte de la mejora continua en la implementación de controles, deberán interponer los planes de acción y/o medidas que prevengan la materialización de riesgos,

sobre todas aquellas acciones y/o actividades que corrijan los impactos luego de que se presente un evento negativo.

Si y solo si luego de la evaluación realizada consideran que únicamente se podrá mitigar o manejar un riesgo con acciones correctivas, esto deberá quedar justificado y de igual forma serán los controles que estarán más sujetos a revisión, con el fin de que en algún momento se puedan cambiar por medidas de prevención.

5.4. Monitoreo y estadísticas

La gestión de riesgo tecnológico es un trabajo en el que debe estar implicado un buen gobierno corporativo, es decir, debe existir un enfoque holístico de las decisiones que se hagan en relación al manejo de estos riesgos, esto se debe a que en algunos casos es importante la interrelación que existe internamente en las áreas y departamentos.

Asimismo, de decisiones importantes en el que se ven involucradas terceras partes; por esta razón las unidades definidas para su gestión, tales como, el Comité de Riesgos, la Gerencia General y Dirección Ejecutiva y el Consejo Directivo deberán periódicamente estar enterados de los niveles de exposición al riesgo tecnológico.

5.4.1. Mensual

El Gerente del Departamento de Tecnologías de la Información mensualmente se reunirá con el Coordinador de Riesgos Tecnológicos y su equipo de trabajo, con el fin de revisar la cantidad de hallazgos señalados en los informes de las auditorías, los cuales están pendientes por mitigar, se

encuentran en procesos de mitigación y los que han sido mitigados con los planes de acción propuestos, asimismo comunicará nuevas directrices en caso sea necesario y recibirá propuestas para la implementación de nuevos recursos para el manejo de riesgos. En la reunión se generará una minuta y un reporte que se traslada a la Gerencia Dirección de Operaciones para su debido control y resguardo.

En esta reunión mensual el Gerente del Departamento de Tecnologías de la Información analizará la calidad, efectividad y eficiencia de los controles que se implementaron para mitigar los hallazgos señalados.

5.4.2. Semestral

El Departamento de Riesgos comunicará semestralmente al Comité de Riesgos los reportes sobre la exposición al riesgo tecnológico, los cambios sustanciales de tal exposición y su evolución en el tiempo. Asimismo, deberá notificar sobre las desviaciones que puedan existir, con el fin de que se pueda rectificar en el menor tiempo posible y ajustarse de nuevo a lo proyectado.

5.4.3. Anual

El Departamento de Riesgos deberá analizar las estadísticas que representen anualmente los avances en los niveles de exposición al riesgo tecnológico, elaborará un informe comparativo sobre los resultados de años anteriores y evaluará los cambios que considere oportunos.

En el informe se tendrán que proponer las acciones que por su condición se consideren relevantes y de trascendencia para toda la entidad financiera, el reporte será trasladado a todos los funcionarios involucrados en el Comité de

Riesgos y se tendrá que presentar al Consejo Directivo, este último estimará y valorará las propuestas que tengan una inversión alta para determinar si son viables y autorizar el presupuesto mínimo necesario, todo esto deberá constar en un acta.

CONCLUSIONES

1. Con base a los diversos controles propuestos, específicamente con la base de datos de configuración y la evaluación de desempeño y capacidad de los activos tecnológicos, se prevé aumentar la eficiencia de los recursos tecnológicos en un 15 %.
2. Utilizando el marco de referencia de COBIT 4.1 se puede desplegar un mapa completo de todos aquellos objetivos de control que se deben implementar para mitigar los riesgos tecnológicos, siendo necesario identificar y visualizar de forma detallada cuales son los que inciden con mayor probabilidad en la consecución de los objetivos y metas organizacionales.
3. Por medio del Análisis de Impacto al Negocio (BIA), identificar los procesos y subprocesos críticos para la organización, posteriormente los recursos tecnológicos que soportan dichos procesos y subprocesos al trazar en los mapas de interdependencia tecnológica, todos estos recursos tecnológicos clasificados como críticos.
4. Crear una política de seguridad de la información que contemple todos los lineamientos que deben seguir los colaboradores para asegurar la confidencialidad de los datos de la organización.
5. Plantear políticas aprobadas por el Consejo Directivo de la institución, para gestionar el riesgo tecnológico, como resultado de que diversos riesgos se deben mitigar de forma holística en toda la organización; y

traducir las políticas en procedimientos y metodologías como parte del buen gobierno corporativo.

6. El Departamento de Tecnologías de la Información a través de la priorización de los riesgos tecnológicos, debe definir el nivel y urgencia en la implementación de los controles que mitigan dichos riesgos, para que se integren y focalicen los recursos financieros, humanos y los procesos de negocio.
7. Implementar el marco de trabajo para la gestión de riesgo tecnológico que fue diseñado en la presente investigación, permite cumplir con los requerimientos establecidos por la Resolución JM-102-2011.

RECOMENDACIONES

1. Continuar evaluando los elementos que conforman los recursos tecnológicos, que serán objeto de control de la base de datos de configuración, y en un corto plazo se deberán incluir los parámetros tales como la obsolescencia y/o la depreciación por uso de dichos recursos.
2. Evaluar e implementar los objetivos de control, proporcionados por el marco de referencia de COBIT 4.1, la entidad financiera deberá continuar con la actualización de las versiones nuevas o mejoras que se publiquen de dicho marco de referencia.
3. En la próxima revisión y/o mantenimiento del Análisis de Impacto al Negocio (BIA), es recomendable identificar y definir las variables que permitan realizar estimaciones y cálculos de los impactos financieros que se pueden generar por la interrupción de los procesos y/o subprocesos que sean catalogados como críticos.
4. Todos los estatutos incluidos en la política de seguridad de la información deben ser implementados por las áreas operativas y de negocio y que el cumplimiento de los lineamientos sea objeto de verificación por parte de la auditoría interna, contratar diversas auditorías externas que puedan asegurar de forma objetiva la efectividad de los controles definidos.
5. Que la entidad busque los estándares más actualizados a fin de que pueda utilizarlos como referencia para fortalecer el modelo de madurez

de su Gobierno Corporativo. Dichos estándares no deberán estar limitados a la mitigación de los riesgos tecnológicos, sino también a las estructuras formalmente definidas para la minimización de los riesgos operativos, legales, de crédito, liquidez y solvencia en la organización

6. Mantener el control activo y seguimiento de todo el marco de trabajo para la administración de riesgo tecnológico, el Departamento de Tecnologías de la Información deberá trabajar para mantener dicho marco de trabajo y considerar los lineamientos propuestos en la presente investigación.
7. La compañía debe evaluar a mediano plazo la implementación de un cuadro de mando integral, donde se pueda monitorear en tiempo real los indicadores de efectividad de los controles implementados para la mitigación de riesgos tecnológicos y donde la herramienta permita la generación de reportes que se trasladen a la Superintendencia de Bancos, con el fin de evidenciar el cumplimiento de los requerimientos establecidos en la Resolución JM-102-2011.

BIBLIOGRAFÍA

1. ANDER-EGG, Ezequiel. *Métodos y técnicas de investigación social*. Argentina: Rio de Plata. 2003. 175 p.
2. BANCO CENTROAMERICANO DE INTEGRACIÓN ECONÓMICA, *Tendencias & Perspectivas*. Económicas de Guatemala y Centroamérica 2010, 35 p.
3. BANCO DE GUATEMALA. *Evaluación de la Política Monetaria, Cambiaria y Crediticia*. Guatemala, 2015. 85 p.
4. BARQUERO HERRERA, Mauricio. *Globalización y Derecho Financiero: La nueva propuesta del Comité de Basilea relacionada con estándares de supervisión bancaria*. 2006. 82 p.
5. CARVAJAL O. Arturo E. *Presentación Administración de Riesgo Operacional*. 2005. 52 p.
6. ECO, Umberto. *Cómo se hace una tesis*. España: Gedisa 2009. 240 p.
7. HERNÁNDEZ, Roberto. *Metodología de la investigación*. México: McGraw-Hill. 2006. 569 p.
8. PÉREZ RAMÍREZ, Jorge; CALVO GONZÁLEZ, Javier. *Instrumentos Financieros: Análisis y valoración con una perspectiva bancaria y*

de información financiera internacional. España: Ediciones Pirámide, 2006. 615 p.

9. ROJAS-SUAREZ, Lilibiana. *Presentación La Bancarización en América Latina: Obstáculos, Avances y la Agenda Pendiente*. Bogotá. 2008. 125 p.
10. SANTIAGO GALLEGO, Ramón. *Diccionario de Economía y Finanzas. Tercera Edición*. Madrid, España: Alianza Editorial, S. A., 1996. 929 p.
11. SANTILLANA González, Juan Ramón. *Auditoría Interna Integral (Administrativa, operacional y financiera)*. International Thomson Editores, S. A. de C. V. Segunda edición, 2002. 415 p.
12. ZAPATA, Óscar. *Herramientas para elaborar tesis e investigaciones*. México: Pax. 2005. 280 p.

ANEXOS

Anexo 1. Esquema gráfico del mapa de interdependencias vista negocio

Departamento de Riesgos

FECHA DE ACTUALIZACIÓN	
CODIGO	
VERSION	

Gerencia:

Departamento:

Proceso Crítico:

C o n t i n i d o r e s	INTERNO DEL ÁREA		ÁREA O DEPARTAMENTO		OBSERVACIONES
	NOMBRE DEL PUESTO	DESCRIPCIÓN	NOMBRE DE ÁREA O DEPARTAMENTO	DESCRIPCIÓN	
RECURSO HUMANO					

PROVEEDORES	NOMBRE PROVEEDOR	DESCRIPCIÓN	OBSERVACIONES

RECURSO TECNOLÓGICO	INFORMACIÓN Y DATOS	SOFTWARE			HARDWARE		OTROS
	SISTEMAS DE INFORMACIÓN (Aplicaciones)	HERRAMIENTAS DE SOFTWARE	SISTEMAS OPERATIVOS (Servidores)	BASES DE DATOS	#	NEGOCIO	

PROCESOS	INTERNOS AL ÁREA	EXTERNOS AL ÁREA	OTROS	OBSERVACIONES

MODULARIO, EQUIPO Y MATERIALES	ESPACIO FÍSICO	MATERIALES	OTROS

Historial de Modificaciones				
No.	Fecha de Modificación	Descripción del Cambio	Persona que Realizó el Cambio	Versión Documento
1				

Fuente: Departamento de Riesgos.

Anexo 2. Esquema gráfico del mapa de interdependencias tecnológico

Logo Entidad Financiera	Nombre Entidad Financiera	Fecha	
	Área Dueña del Proceso / Sub-Proceso: (/)	Página	
Mapa de Interdependencias del Sub-Proceso de "....."			
Fuente de Información: BIA de la Entidad Financiera (Año 2015)			

Proceso	Nombre del Proceso / Subproceso	Breve descripción y alcance del proceso / subproceso				

Recursos	Recurso Humano	Infraestructura de Seguridad Infraestructura de Telecomunicaciones	Sistemas de información	Bases de Datos	Servidores (Infraestructura Tecnológica)	Storage
	Personal de Área de Negocio y/o responsables del proceso / subproceso: Personal del Departamento de Tecnologías de Información relacionado:	Equipo Necesario: -Equipo de Infraestructura de Seguridad necesario para proteger los servidores- -Equipo de Telecomunicaciones mínimo necesario-				
	Recurso Tecnológico	Equipo Complementario:				
	Características del Hardware del Equipo de Computo					
	Recurso Externo					
	Interno a la Entidad Financiera, (Áreas de soporte de la Entidad Financiera)					
	Externo, proveedores, (Directamente relacionados con el Departamento de Tecnologías de Información)					

Recurso Tecnológico actualmente no soportado en el Sitio Alterno de Datos

Departamento de Tecnologías de Información	Documento Relacionado:	Plan de Recuperación de Desastres	Responsable Documento:	Coordinación de Riesgos Tecnológicos
--	------------------------	-----------------------------------	------------------------	--------------------------------------

Fuente: Departamento de Tecnologías de la Información.

Anexo 3. Formulario de Certificación y Validación de Pruebas de Concepto (Hoja 1 / 2)

1. IDENTIFICACIÓN DEL PROYECTO / PROVEEDOR			
Fecha de Inicio del Proyecto:		Fecha de Finalización del Proyecto: (Prevista)	
Nombre del Proveedor		Nombre del Proyecto	
Breve Descripción del Proyecto:			
Alcance del Proyecto:			
2. IDENTIFICACIÓN GENERAL			
2.1 IDENTIFICACIÓN DEL LIDER DEL PROYECTO:			
Nombre:			
Puesto:			
Departamento /Subgerencia/Jefatura:		Correo electrónico:	
2.2 IDENTIFICACIÓN DEL PROVEEDOR:			
Contrato de Mantenimiento	SI: <input type="checkbox"/>	NO: <input type="checkbox"/>	Observaciones: _____
Contrato de Compra Venta:	SI: <input type="checkbox"/>	NO: <input type="checkbox"/>	Observaciones: _____
Nombre del Proveedor:			
Razón Social:		No. Teléfono:	
Nombre de Contacto Directo:		No. Teléfono:	
Correo Electrónico:		No. NIT:	
3. PRUEBAS DE CONCEPTO			
Fecha de Inicio de las Pruebas		Fecha de Finalización de las Pruebas:	
Nombre del usuario que realizó las pruebas:		Correo electrónico:	
Nombre del Sistema Evaluado:		Ambiente:	
4. CERTIFICACIÓN:			
Información retroalimentada por el área beneficiada	Observaciones:		
	¿Se recibieron manuales relacionados?	SI: <input type="checkbox"/>	No: <input type="checkbox"/> N/A: <input type="checkbox"/>
	¿Se recibió entrenamiento?	SI: <input type="checkbox"/>	No: <input type="checkbox"/> N/A: <input type="checkbox"/>
	¿Cumple con las expectativas?	SI: <input type="checkbox"/>	No: <input type="checkbox"/> N/A: <input type="checkbox"/>
			Nota: N/A: No Aplica

Anexo 3. Formulario de Certificación y Validación de Pruebas de Concepto (Hoja 2 / 2)

Información competente al Departamento de Tecnologías de Información	¿Cumple con las necesidades del Proyecto?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	Observaciones:
	¿Cumple con los tiempos programados?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	
	¿Se recibió Entrenamiento Técnico?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	
	¿Se recibió Manual Técnico?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	
	¿Se recibió Manual de Soporte y Operación?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	
	¿Se recibió Manual de Configuración?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	
	¿Cumple los Requerimientos de Seguridad de Inforr	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	
	¿Se recibió Diccionario de Datos?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	
	¿Se recibió claves de Accesos?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	
	¿Se recibió Plan de Depuración?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	
	¿Se recibió Plan de Mantenimiento?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	
¿Se recibió Diagramas de Entidad y Relación?	Si: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>		
Nota: N/A: No Aplica					
5. COMENTARIOS Y OBSERVACIÓN					
6. APROBACIÓN					
_____ Líder del Proyecto			_____ Gerente del Departamento de Tecnologías de Información		

Fuente: Departamento de Tecnologías de la Información.

Anexo 4. Registro de Evaluación de Proveedores, previo a su contratación

1. IDENTIFICACIÓN GENERAL					
1.1 IDENTIFICACIÓN DEL RESPONSABLE DEL PROVEEDOR					
Nombre:					
Puesto:					
Departamento /Subgerencia/Jefatura:		Correo electrónico:			
1.2 IDENTIFICACIÓN DEL PROVEEDOR:					
Contrato de Mantenimiento	SI: <input type="checkbox"/>	NO: <input type="checkbox"/>	Observaciones: _____		
Contrato de Compra Venta:	SI: <input type="checkbox"/>	NO: <input type="checkbox"/>	Observaciones: _____		
Nombre del Proveedor:					
Razón Social:		No. Teléfono:			
Nombre de Contacto Directo:		No. Teléfono:			
Correo Electrónico:		No. NIT:			
2. CERTIFICACIÓN:					
Calificación asignada al proveedor	¿Cumple con los tiempos de entrega?	SI: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	Observaciones: _____
	¿El precio es adecuado?	SI: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	_____
	¿Cuenta con Experiencia en el Sector?	SI: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	_____
	¿Proporciona las Garantías adecuadas?	SI: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	_____
	¿Cuenta con Certificaciones de Calidad?	SI: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	_____
	¿Cuenta con casos de éxito?, ¿Quiénes?	SI: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	_____
	¿Tiene representación local?	SI: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	_____
	¿Tiene respaldo internacional?	SI: <input type="checkbox"/>	No: <input type="checkbox"/>	N/A: <input type="checkbox"/>	_____
Nota: N/A: No Aplica					
3. RECOMENDACIONES CON BASE A LAS CALIFICACIONES ASIGNADAS					
4. APROBACIÓN					
_____ Responsable del Proveedor		_____ Gerente del Departamento de Tecnologías de Información			

Fuente: Departamento de Tecnologías de la Información.

Anexo 5. Reporte Mensual de Evaluación de Proveedores que prestan servicios directamente al Departamento de Tecnologías de la Información

Departamento de Tecnologías de Información	
Reporte correspondiente al mes de: -----	

No	Listado de Proveedores Activos	Acuerdos de Nivel de Servicios		Comentarios	Servicios Contratados
		SI	NO		
1					
2					
3					
4					
5					

Requerimientos Reportados No Resueltos		
No	Nombre Proveedor	Descripción
1		
2		
3		
4		
5		

Penalizaciones que se deben aplicar		
No	Nombre Proveedor	Incidente Relacionado
1		
2		
3		
4		
5		

Solución de Requerimientos Reportados:		
No	Nombre Proveedor	Reporte de Seguimiento
1		
2		
3		
4		
5		

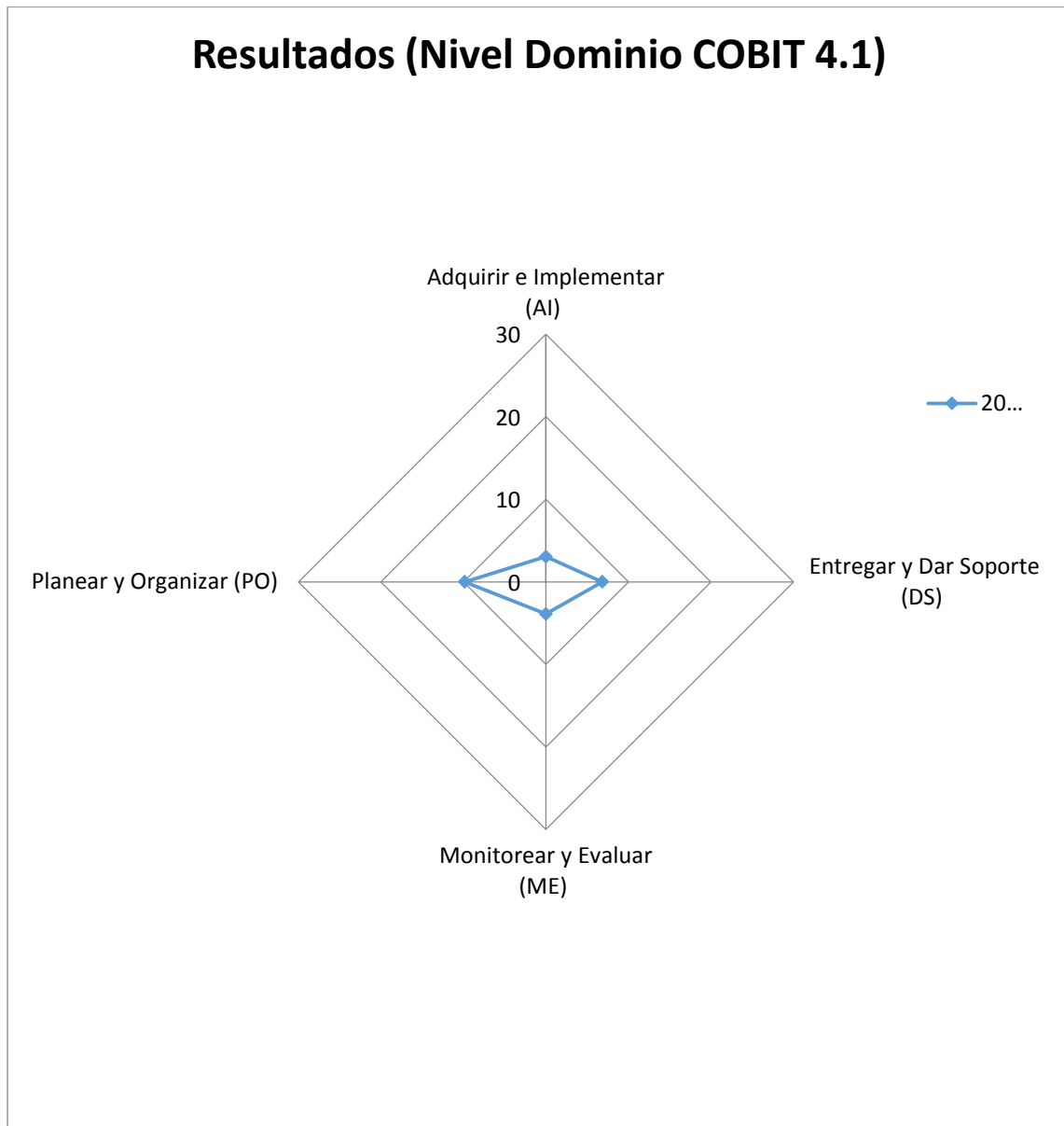
Fuente: Departamento de Tecnologías de la Información.

Anexo 6. Formato de Evaluación de Controles que mitigan el Riesgo Tecnológico

Dominio/ Proceso	No. Proceso	Objetivo de Control Propuesto por COBIT 4.1	Requerimiento de Información							Puntaje	Calificación del Riesgo	Nombre de Control Verificado <i>(Indicar la referencia de la evidencia)</i>	Observaciones del Evaluador <i>(Justificación de la nota asignada)</i>
			Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiable				
Dominio de COBIT 4.1													
Nombre del Proceso	Número del Proceso según COBIT 4.1	Control objetivo propuesto por COBIT 4.1, sin embargo en este cuadro se puede redactar dicho objetivo como la descripción del mismo y lo que podría provocar la falta de implementación.										Se indica el nombre de control implementado por el Departamento de Tecnologías de Información, asimismo se indica el nombre y tipo de evidencia que deja	Son los comentarios que dejar el evaluar en relación a la justificación de la nota que está asignando a la probabilidad.

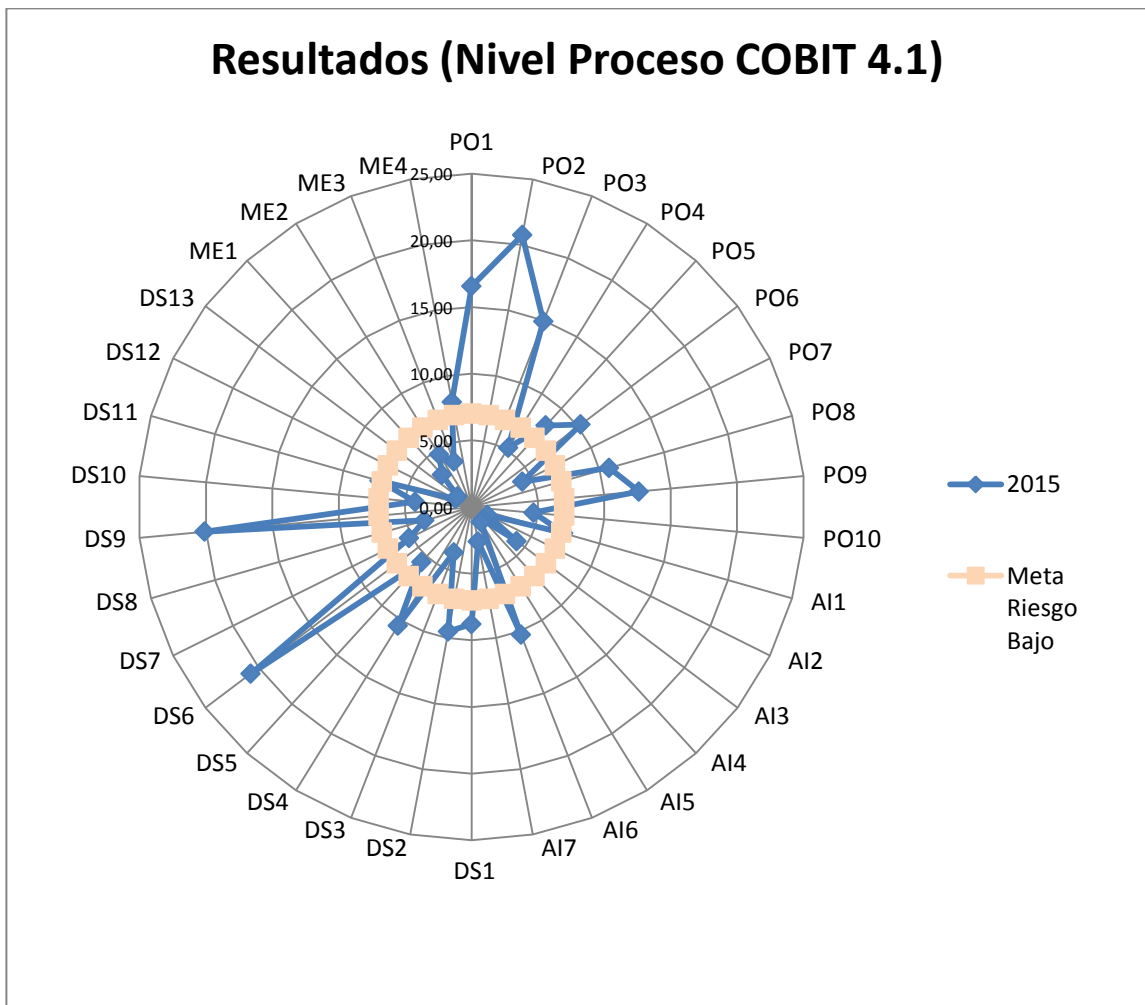
Fuente: Departamento de Tecnologías de la Información.

Anexo 7. **Gráficas que se pueden emplear para la comparación de resultados de las evaluaciones de riesgo tecnológico realizadas por dominio.**



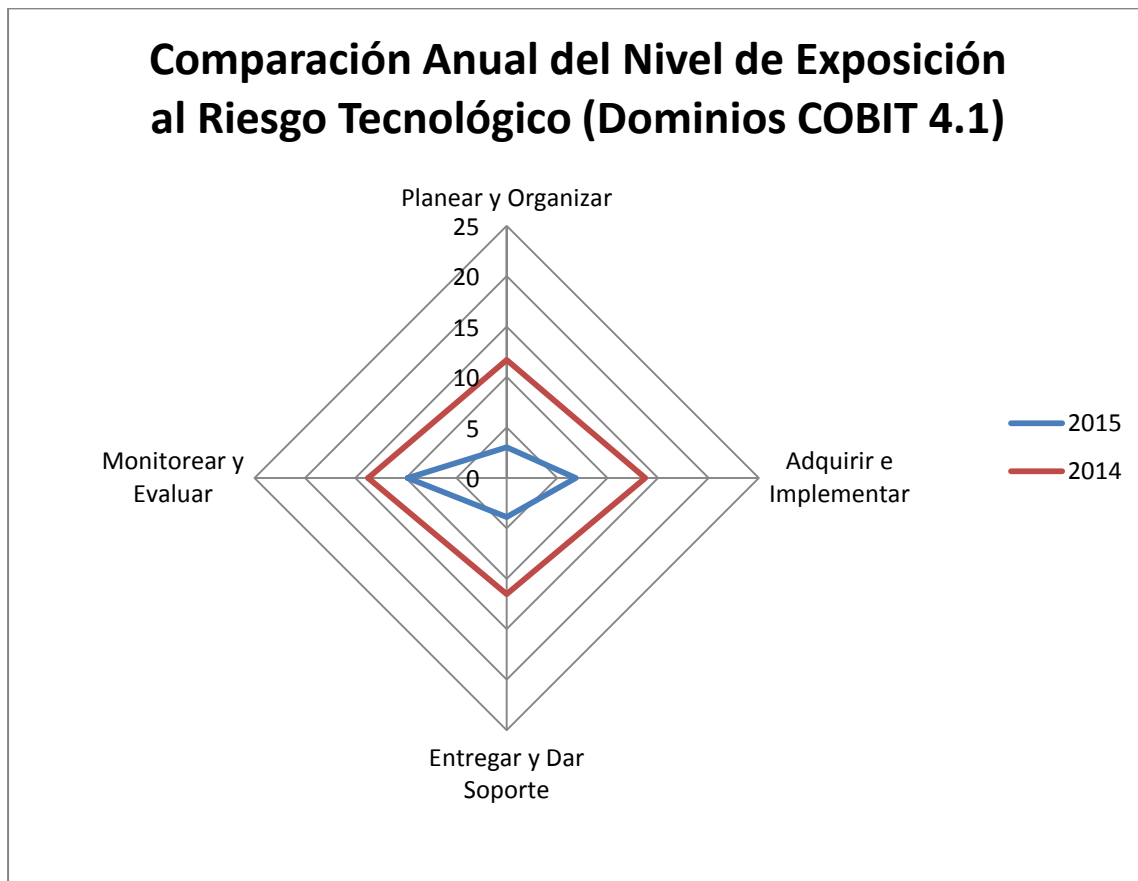
Fuente: Departamento de Tecnologías de la Información.

Anexo 8. Gráficas que se pueden emplear para la comparación de resultados de las evaluaciones de riesgo tecnológico realizadas por proceso.



Fuente: Departamento de Tecnologías de la Información.

Anexo 9. Gráficas que se pueden emplear para la comparación de resultados de las evaluaciones anuales de riesgo tecnológico realizadas por dominio.



Fuente: Departamento de Tecnologías de la Información.