ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

PROPUESTA DE UN PLAN DE CONTINGENCIA DE TI PARA LA EMPRESA LOGICIEL

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

DIANA CAROLINA PACHECO POZO
diana.pachecop@epn.edu.ec

Director: PhD. JENNY GABRIELA TORRES OLMEDO
jenny.torres@epn.edu.ec

Quito, Febrero 2016

DECLARACIÓN

Yo, Diana Carolina Pacheco Pozo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Diana Carolina Pacheco Pozo

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Diana Carolina Pacheco Pozo, bajo mi supervisión.

PhD. Jenny Gabriela Torres Olmedo
DIRECTOR

AGRADECIMIENTOS

Primero quiero agradecer a Dios, por darme las fuerzas y la capacidad para completar este trabajo.

A mis padres, por darme la vida y ser una fuente incondicional de apoyo.

A mis hermanos, por estar siempre conmigo y motivarme a seguir adelante.

A mis amigos, por su cariño y apoyo incondicional.

A mi tutora, por su constante apoyo durante el desarrollo de este trabajo.

A la empresa LOGICIEL, por todo el apoyo brindado durante la elaboración de este trabajo.

Y a cada una de las personas que pusieron un granito de arena para ayudarme a atravesar mi vida universitaria.

DEDICATORIA

Dedico este trabajo a mi mami por siempre apoyarme incondicionalmente y no permitirme darme por vencida en ningún momento.

A mi abuelita Teresa por ser un ejemplo de sacrificio, tenacidad y superación, por estar siempre conmigo.

ÍNDICE DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

El presente proyecto de Titulación tiene como finalidad elaborar una propuesta de un plan de contingencia de Tecnologías de Información (TI) mediante el desarrollo de un modelo basado en marcos de referencia enfocados en la continuidad del negocio para la empresa LOGICIEL. Para determinar que marcos de referencia se tomaron como base para el desarrollo del modelo, se realizó un proceso de discriminación entre varios marcos de referencia reconocidos internacionalmente. A continuación, con los marcos de referencia seleccionados, se procedió a realizar un análisis comparativo para poder determinar las principales etapas del proceso de planeación de contingencias. Debido a que uno de los pasos de este proceso es la evaluación de riesgos, se realizó un proceso similar al anterior para determinar los puntos clave de la evaluación de riesgos considerando varios marcos de referencia. Haciendo uso de los resultados de los análisis comparativos realizados, se logró establecer un modelo que explica en detalle cada una de las etapas que conforman el proceso de elaboración de un plan de contingencias de una manera sencilla y fácil de entender que cualquier empresa podría poner en práctica. La parte final de este trabajo incluye la validación del modelo propuesto, definiendo un plan de contingencias para la empresa LOGICIEL.

Palabras clave: Continuidad del Negocio. Plan de Contingencia. Tecnologías de Información. Evaluación de Riesgos. Análisis de Impacto en el Negocio.

ABSTRACT

This project aims to develop an Information Technology (IT) Contingency Plan through the development of a model based on frames of reference focused on business continuity for the company LOGICIEL. In order to determine which frames of reference are taken as a basis to develop this model, a process of discrimination was made between different internationally recognized frames. Then with the selected frames, we proceeded to make a comparative analysis to identify the main stages of contingency planning. Because one of the steps in this process is the risk assessment, a process similar to the above is performed to determine the key points of risk assessment, considering various frameworks. Making use of the results of the conducted comparative analysis, we are able to establish a model that explains in detail each of the steps included in the process of drawing up a contingency plan in a simple way, easy to understand and implement in any company. The final part of this work includes validation of the proposed model, defining a contingency plan for the company LOGICIEL.

Keywords: Business Continuity. Contingency Plan. Information Technology. Risk Assessment. Business Impact Analysis.

PRESENTACIÓN

Hoy en día las empresas dependen más y más de las Tecnologías de Información (TI) para lo consecución de sus objetivos estratégicos y la puesta en marcha de sus operaciones. Es por esto que, asegurar la continuidad del soporte de las TI dentro de las empresas se ha vuelto imperativo. El desarrollo e implementación de planes de contingencia es una forma de asegurar que la empresa se encuentre preparada para hacer frente a una posible interrupción del funcionamiento de las TI y de esta manera atenuar el impacto en las operaciones de la organización.

Para el desarrollo de planes de contingencia existe un sin número de estándares, metodologías, guías, legislaciones y regulaciones, lo cual puede dificultar la selección de un marco de referencia que se acople de las necesidades de la empresa y que sobre todo sea fácil de entender y poner en práctica. Es por esto que se plantea un modelo para la elaboración de planes de contingencias fácilmente adaptable a cualquier tipo de empresa y que considera los mejores aspectos de algunos marcos de referencia reconocidos internacionalmente.

El presente proyecto de titulación consta de cuatro capítulos, los mismos que contienen el marco teórico, un estudio comparativo de los marcos de referencia de evaluación de riesgos, un estudio comparativo de los marcos de referencia de continuidad del negocio y por último, el modelo propuesto para la elaboración de planes de contingencia de TI.

En el Capítulo I se definen los conceptos claves que permitirán entender de mejor manera los capítulos posteriores. Se inicia definiendo ciertos aspectos generales de la Seguridad de la Información, para finalizar explicando el concepto de un Plan de Contingencia y listando los objetivos.

El Capítulo II contiene un estudio comparativo de varios marcos de referencia orientados a la evaluación de riesgos. El estudio inicia con la elaboración de un listado de marcos de referencia de evaluación de riesgos, a partir del cual se

procederá a seleccionar las mejores prácticas para luego caracterizarlas. Luego de describir las mejores prácticas seleccionadas, se realiza un análisis comparativo a partir del cual se establece los puntos clave de la evaluación de riesgos.

En el Capítulo III se realiza un estudio comparativo de varios marcos de referencia orientados a la continuidad del negocio. El estudio parte con la elaboración de un listado de marcos de referencia de continuidad del negocio, del cual se seleccionarán las mejores prácticas para luego caracterizarlas. Luego de la caracterización de los marcos de referencia seleccionados, se realiza un análisis comparativo, el mismo que identifica los puntos clave de un plan de contingencia.

En el Capítulo IV, en base a los puntos clave de la evaluación de riesgos identificados en el Capítulo II y los puntos clave de un plan de contingencia identificados en el Capítulo III, se describe el modelo propuesto para la elaboración de planes de contingencia de TI y se realiza una validación del mismo mediante la elaboración de una propuesta de un Plan de Contingencia de TI para el caso de estudio LOGICIEL.

Finalmente, se presentan las conclusiones y recomendaciones a las que se llegaron una vez terminado el presente proyecto.

1 MARCO TEORÍCO

El presente capítulo contiene la definición de los conceptos más relevantes que servirán como fundamento teórico para el desarrollo de este proyecto.

1.1 ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se definen los conceptos relacionados con la seguridad de la información.

1.1.1 ACTIVO

Un activo es un "componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización" [1]. Como parte de los activos se considera a la información, los datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones y recursos humanos.

1.1.2 AMENAZA

El término amenaza [2] se define como cualquier circunstancia o evento con el potencial de afectar negativamente a las operaciones de la organización (misión, funciones, imagen o reputación), los activos de información o los individuos, a través del acceso no autorizado, destrucción, divulgación, modificación de la información o denegación de servicio.

También se puede definir como eventos o acciones (accidentales o deliberadas) que pueden conducir a la aparición de un riesgo causado daño a los activos de la organización, como por ejemplo un accidente, fuego, robo, etc. [3] [4].

Las amenazas a los sistemas de información pueden incluir ataques intencionales, perturbaciones ambientales, errores humanos o de máquina, fallas

estructurales, y puede resultar en daño a los intereses de seguridad e intereses económicos de la organización.

1.1.3 VULNERABILIDAD

El término vulnerabilidad [2] [3] se define como una debilidad o defecto de un sistema de información en sus procedimientos de seguridad, arquitectura, implementación o en los controles de seguridad que podrían ser explotados por una amenaza para eludir los sistemas de seguridad y acceder de manera no autorizada a la información.

La mayoría de las vulnerabilidades de los sistemas de información se pueden asociar a los controles de seguridad que, o bien no han sido implementados, o han sido implementados, pero conservan cierta debilidad.

1.1.4 RIESGO

El riesgo [3] se define como la posibilidad de que una determinada acción o actividad, en donde también se incluye la inacción, dará lugar a una pérdida o un resultado no deseado.

El riesgo es la medida del grado en que una entidad se ve amenazada por una circunstancia potencial o un evento. Por lo general se lo considera como una función de los impactos adversos que surgirían si se produce la circunstancia o acontecimiento y la probabilidad de ocurrencia de los mismos [2].

1.1.5 IMPACTO

Se denomina impacto [1] [2] a la magnitud del daño que se puede esperar sobre un activo como resultado de la materialización de una amenaza como por ejemplo, la divulgación o destrucción no autorizada de información, la pérdida de información o de la disponibilidad del sistema de información.

1.1.6 CONTROLES

Los controles de seguridad [5] son las salvaguardias (técnicas o administrativas) o las contramedidas para evitar, contrarrestar o minimizar la pérdida o falta de disponibilidad debido a las amenazas que actúan sobre las vulnerabilidades de un activo. Lo que se busca con los controles definidos para un sistema de información es proteger la confidencialidad, integridad y disponibilidad del sistema y la información del mismo [2].

1.2 ¿QUÉ ES UN PLAN DE CONTINGENCIA?

Un plan de contingencia [6] [7] es una salida del proceso de planeación de contingencias en donde se definen los procedimientos, recursos y sistemas necesarios para mantener o reestablecer las operaciones empresariales luego de una interrupción del negocio resultado de fallos de sistema o desastres. Además, proporciona información clave para la recuperación del sistema como procedimientos de recuperación, funciones y responsabilidades, procedimientos de evaluación, etc.

La planeación de contingencias es un proceso que proporciona procedimientos para permitir la recuperación rápida y eficaz de un sistema de TI después de que se produzca una falla en el mismo, una interrupción del servicio o desastre.

Este proceso está conformado generalmente por 7 pasos, que se listan a continuación [6] [8] [9]:

1. *Desarrollar la política del plan de contingencia.* Se define los objetivos de contingencia de la organización y se establece el marco de trabajo y responsabilidades para la planeación de contingencias.
2. *Realizar una evaluación de riesgos.* Se identifica y prioriza las amenazas a las que una organización puede ser vulnerable.
3. *Realizar un análisis de impacto en el negocio.* Permite determinar el daño potencial a una organización causado por una emergencia o crisis y el fallo de uno o más procesos del negocio.

4. *Desarrollar e implementar las estrategias de contingencia.* Durante este paso se identifican e implementan estrategias de continuidad que mejor satisfagan las necesidades de la organización, basándose en un análisis costo-beneficio y los resultados obtenidos de la evaluación de riesgos y el análisis de impacto en el negocio.
5. *Desarrollar y documentar el plan.* Documentar los procedimientos de respuesta, recuperación y restauración que permitan la continuidad de las operaciones del negocio.
6. *Realizar pruebas del plan y entrenamiento.* Las pruebas del plan permiten la validación y el mejoramiento continuo de las estrategias de contingencia y los procedimientos definidos. Además, permite identificar las posibles deficiencias del plan. El entrenamiento se realiza para que el personal de la empresa se familiarice con los procedimientos definidos y las acciones a tomar en caso de que ocurra una crisis.
7. *Asegurar el mantenimiento del plan.* El plan de contingencia debe ser actualizado y mantenido para que siempre refleje los requerimientos, procedimientos, estructura y políticas de la organización.

1.3 OBJETIVOS DE UN PLAN DE CONTINGENCIA

El objetivo de un plan de contingencia es permitir que una organización vuelva a sus actividades cotidianas tan pronto como sea posible después de un acontecimiento imprevisto [10]. Además, con el plan de contingencia se busca proteger los recursos, minimizar las molestias al cliente y reducir al mínimo los potenciales impactos.

Los siguientes son los objetivos generales de un plan de contingencia [11]:

- Garantizar la seguridad de todos los empleados y visitantes que se encuentren en las instalaciones en el momento de un incidente.
- Proteger la información crítica.
- Asegurar las instalaciones de la organización.

- Salvaguardar y hacer que estén disponibles los materiales, suministros y equipos necesarios para garantizar la seguridad y la rápida recuperación de las operaciones de la empresa.
- Reducir el riesgo resultado de desastres causados por errores humanos, la destrucción deliberada y las fallas de los equipos.
- Garantizar la capacidad de la organización para seguir funcionando después de un desastre.
- Recuperar la información perdida o dañada después de un desastre.

2 ESTUDIO COMPARATIVO DE MARCOS DE REFERENCIA DE EVALUACIÓN DE RIESGOS

Este capítulo contiene un estudio comparativo de diferentes marcos de referencia de evaluación de riesgos. Inicialmente, se establece un listado de los marcos de referencia a ser analizados. De este listado, en base a ciertos criterios, se seleccionarán las mejores prácticas, las mismas que serán comparadas para determinar las principales etapas de la evaluación de riesgos.

La evaluación de riesgos [12] se define como el proceso de identificar amenazas y vulnerabilidades tanto internas y externas, determinando la probabilidad de que un evento surja como resultado de dichas amenazas y vulnerabilidades y el impacto que esto implicaría.

2.1 MARCOS DE REFERENCIA A SER ANALIZADOS

En la actualidad existen varios marcos de referencia relacionados con la evaluación de riesgos de seguridad de la información. Debido a este gran número de trabajos encontrados en la literatura, la selección de uno de ellos puede resultar complicada. Para iniciar, una lista de marcos de referencia se ha establecido en base al inventario de marcos de referencia publicados por ENISA (European Network and Information Security Agency) [13], además de trabajos con una fecha de publicación entre el 2009 y la actualidad en lo que se incluye Matalobos [14], Syalim et al. [15], Shamala et al. [16], Saleh et al. [17], Behnia et al. [18], Kiran et al. [19], Ionita [20], Macedo et al. [21]; y Shukla et al. [22].

Esta lista se compone de un total de 40 marcos de referencia de evaluación de riesgos entre metodologías, guías y estándares, como se muestra a continuación en la Tabla 2-1.

Tabla 2-1 - Listado inicial de marcos de referencia de evaluación de riesgos

#	Marco de Referencia
1	AS/NZS 4360:2004
2	Austrian IT Security Handbook
3	BS 7799-3:3006
4	COBIT
5	CORAS
6	CRAMM
7	Dutch A&K Analysis
8	Ebios
9	FAIR
10	FRAP
11	GAO/AIMD-00-33
12	IS Risk Analysis Based on Business Model
13	ISAMM
14	ISF Methods (SARA, IRAM, SPRINT)
15	ISO/IEC 15408
16	ISO TR 13335: 1997
17	ISO/IEC 17799
18	ISO/IEC 27001
19	ISO/IEC 27002
20	ISO/IEC 27005:2008
21	ISRAM
22	IT System Security Assessment
23	IT-Grundschutz
24	MG-2 and MG-3
25	MAGERIT
26	Marion
27	MAR
28	MEHARI
29	Microsoft Security Management Guide
30	Migra
31	NIST SP 800-39
32	NIST SP 800-30
33	OCTAVE
34	Risk IT
35	Risk Watch
36	Security Risk Management Guide
37	Structured Risk Analysis
38	SOMAP
39	TARA
40	UNE 71504:2008

2.2 SELECCIÓN DE MARCOS DE REFERENCIA DE EVALUACIÓN DE RIESGOS

En esta sección se realiza la selección de los marcos de referencia de evaluación de riesgos a ser comparados. Primero se establece criterios de exclusión para reducir el listado inicial. A continuación, se aplican los criterios de exclusión previamente definidos y se crea un ranking en base al número de veces que el marco de referencia es citado por cada uno de los autores de los trabajos en base a los cuales se elaboró el listado inicial de marcos de referencia de evaluación de riesgos.

2.2.1 CRITERIOS DE EXCLUSIÓN

Para el análisis de todos los marcos de referencia de evaluación de riesgos listados en la Tabla 2-1, se van a considerar los siguientes Criterios de Exclusión (CE):

CE-1. Dificultad al conseguir documentación relacionada con el marco de referencia. Entre las principales causas tenemos que la documentación encontrada estaba disponible únicamente mediante pago, el marco de referencia estaba obsoleto, o no cuenta con información completa disponible.

CE-2. La documentación se encuentra disponible en otro idioma que no sea inglés o español. Las limitaciones con el idioma traen como consecuencia problemas de acceso a marcos de referencia que se encuentran en otros idiomas, puesto que imposibilita la comprensión del marco de referencia.

CE-3. El marco de referencia se encuentra inactivo, descontinuado o desactualizado, debido a que ya no cuentan con soporte.

CE-4. El marco de referencia no identifica riesgos de seguridad de la información. Ciertos marcos de referencia a pesar de enfocarse en la gestión de riesgos no necesariamente están relacionados con la seguridad de la información.

Del listado inicial se eliminarán todos los marcos de referencia que cumplan con al menos uno de los criterios de exclusión antes descritos. Con los marcos de referencia restantes se procederá a crear un ranking en base al número de veces que un marco de referencia es citado por cada uno de los autores de los trabajos

en base a los cuales se elaboró el listado inicial de marcos de referencia de evaluación de riesgos. Por cada mención se asignará un punto.

Finalmente, los marcos de referencia incluidos en el ranking se dividirán en dos grupos, los marcos más citados y los menos citados. Para determinar a qué grupo pertenece cada uno de los marcos de referencia se considerará lo siguiente:

- El número máximo de puntos que puede tener un marco de referencia es 10, en vista de que se están analizando el trabajo de 10 autores de los trabajos en base a los cuales se elaboró el listado inicial de marcos de referencia de evaluación de riesgos.
- El número mínimo de puntos que puede tener un marco de referencia es 1, ya que si se encuentra en el listado de marcos de referencia es porque es citado al menos una vez por uno de los autores de los trabajos en base a los cuales se elaboró el listado inicial de marcos de referencia de evaluación de riesgos.
- Visto que se tienen únicamente 2 grupos y 10 posibles valores, los marcos menos citados tendrán un valor entre 1 y 5 puntos, mientras que los más citados un valor entre 6 y 10.

2.2.2 APLICACIÓN DE LOS CRITERIOS DE EXCLUSIÓN

En la Tabla 2-2, se indica el criterio de exclusión que cumple o no cada uno de los marcos de referencia de evaluación de riesgos listados en la Tabla 2-1.

Tabla 2-2 – Aplicación de los criterios de exclusión en el listado inicial de marcos de referencia de evaluación de riesgos

Marco de Referencia	Criterio de exclusión	Justificación
AS/NZS 4360:2004	CE-1, CE-3	Documentación no disponible. Se encuentra obsoleto, su última versión salió en el 2004 y ha sido reemplazado por el estándar AS/NZS ISO 31000:2009.
Austrian IT Security Handbook	CE-1, CE-2	No cuenta con documentación completa disponible. La documentación disponible está en alemán.
BS 7799-3:2006	CE-1	Documentación disponible mediante

Marco de Referencia	Criterio de exclusión	Justificación
		pago.
COBIT	CE-4	No identifica riesgos relacionados con la seguridad de la información, se enfoca en el gobierno de TI y no está diseñado explícitamente para la gestión de riesgos.
CORAS		
CRAMM	CE-1	Documentación disponible mediante pago.
Dutch A&K Analysis	CE-1, CE-2, CE-3	No cuenta con documentación completa disponible. La documentación disponible está en holandés. Se encuentra obsoleto.
Ebios		
FAIR		
FRAP		
GAO/AIMD-00-33	CE-3	Se encuentra obsoleto, no ha sido actualizado desde la publicación de 1998.
IS Risk Analysis Based on a Business Model	CE-1	No cuenta con documentación completa disponible.
ISAMM	CE-1, CE-2, CE-3	No cuenta con documentación completa disponible. La documentación disponible está en otros idiomas, a pesar de que el marco de referencia está en inglés. Se encuentra obsoleto.
ISF Methods (SARA, IRAM, SPRINT)	CE-1	No cuenta con documentación completa disponible, la misma se encuentra únicamente a disposición de sus miembros.
ISO/IEC 15408	CE-1, CE-4	Documentación disponible mediante pago. No identifica riesgos relacionados con la seguridad de la información, se enfoca en la evaluación de la seguridad de los productos de TI.
ISO TR 13335: 1997	CE-1, CE-3	Documentación no disponible. Se encuentra obsoleto, de acuerdo a la página de la ISO.
ISO/IEC 17799	CE-1, CE-3	Documentación no disponible. Se encuentra obsoleto, de acuerdo a la página de la ISO.
ISO/IEC 27001	CE-1,	Documentación disponible mediante

Marco de Referencia	Criterio de exclusión	Justificación
	CE-4	pago. No identifica riesgos relacionados con la seguridad de la información, se enfoca en la gestión de la seguridad de la información.
ISO/IEC 27002	CE-1, CE-4	Documentación disponible mediante pago. No identifica riesgos relacionados con la seguridad de la información, presenta un conjunto de mejores prácticas relacionadas con la gestión de la seguridad de la información.
ISO/IEC 27005:2011	CE-1	Documentación disponible mediante pago.
ISRAM		
IT System Security Assessment	CE-1	No cuenta con documentación completa disponible.
IT-Grundschutz	CE-1, CE-3	No cuenta con documentación completa disponible. Se encuentra obsoleto, no ha sido actualizado.
MG-2 and MG-3	CE-1	No cuenta con documentación completa disponible.
MAGERIT		
Marion	CE-1, CE-2, CE-3	No cuenta con documentación completa disponible. La documentación disponible está en alemán. Se encuentra obsoleta, no ha sido mantenida desde 1998, y ha sido reemplazada por MEHARI.
MAR	CE-4	No identifica riesgos relacionados con la seguridad de la información, se enfoca en riesgos relacionados con la salud y el ambiente.
MEHARI		
Microsoft Security Management Guide		
Migra	CE-1, CE-2	No cuenta con documentación completa disponible. La norma se vende como parte de los servicios de consultoría de seguridad. La documentación disponible está en otros idiomas, a pesar de que el modelo está en inglés.

Marco de Referencia	Criterio de exclusión	Justificación
NIST SP 800-39		
NIST SP 800-30		
OCTAVE		
Risk IT	CE-4	No identifica riesgos relacionados con la seguridad de la información.
Risk Watch	CE-1	No cuenta con documentación completa disponible.
Security Risk Management Guide	CE-1	No cuenta con documentación completa disponible.
Structured Risk Analysis		
SOMAP		
TARA		
UNE 71504:2008	CE-1	Documentación disponible mediante pago.

Después de este proceso de exclusión quedan 15 marcos de referencia. A continuación, se procederá a crear un ranking, en base al número de veces que un marco es citado por cada uno de los autores de los trabajos en base a los cuales se elaboró el listado inicial de marcos de referencia de evaluación de riesgos.

Tabla 2-3 – Marcos de referencia de evaluación de riesgos

Autor / Marco de Referencia	Matalobos	Syalim et al.	Shamala et al.	Saleh et al.	ENISA	Behnia et al.	Kiran et al.	Ionita	Macedo et al.	Shukla et al.	Puntaje
CORAS	x		x			x		x		x	5
Ebios					x		x	x	x		4
FAIR	x							x			2
FRAP						x		x			2
ISRAM			x							x	2
MAGERIT	x	x			x		x	x	x		6
MEHARI		x			x		x	x	x		5
Microsoft Security Management Guide		x		x			x		x		4
NIST SP 800-39								x			1
NIST SP 800-30	x	x	x	x	x		x		x		7
OCTAVE	x		x	x	x	x	x	x	x	x	9
Structured Risk Analysis								x			1
SOMAP	x										1
TARA								x			1

De acuerdo a lo que se observa en la Tabla 2-3, los marcos de referencia más citados son OCTAVE, NIST SP 800-30 y MAGERIT que tienen entre 6 y 10 puntos. Mientras que los menos citados son CORAS, MEHARI, Ebios, Microsoft Security Management Guide, CORA, FAIR, FRARP, ISRAM, NIST SP 800-39, Structured Risk Analysis, SOMAP y TARA; cuyos valores son inferiores a 5.

2.3 ANÁLISIS COMPARATIVO DE LOS MARCOS SELECCIONADOS

En esta sección se realiza un análisis comparativo de los marcos de referencia de evaluación de riesgos seleccionados en la sección anterior. Se inicia con la descripción de cada uno de ellos, con el objetivo de determinar cuáles son las principales etapas de la evaluación de riesgos.

2.3.1 INFORMACIÓN GENERAL DE LOS MARCOS SELECCIONADOS

Los marcos de referencia de evaluación de riesgos seleccionados en la Sección 2.2, se van a describir a continuación para su posterior análisis.

2.3.1.1 OCTAVE

OCTAVE Allegro [23] es un método utilizado para evaluar las necesidades de seguridad de la información de una organización. OCTAVE Allegro es el método más recientemente desarrollado y apoyado activamente por el CERT (Community Emergency Response Team). Se trata de un método auto-dirigido, flexible y que evoluciona en el tiempo. Se centra en los activos de información. Los activos importantes de una organización se identifican y evalúan en base a los activos de información a los que se encuentran conectados.

OCTAVE Allegro consta de ocho pasos organizados en cuatro fases que son las siguientes [23] [24]:

Fase 1: Desarrollar criterios de medición del riesgo en consonancia con la misión de la organización, las metas y objetivos del negocio, y los factores críticos de éxito.

Paso 1: Establecer los criterios para la medición de riesgos: establece los criterios de medición que se utilizarán para evaluar los efectos de un riesgo para la misión y objetivos de negocio de una empresa.

Fase 2: Crear un perfil de cada uno de los activos críticos de información, en donde se establecen claramente los límites para el activo, identifica sus necesidades de seguridad, e identifica todos sus contenedores (es decir en donde la información es almacenada, procesada y transportada).

Paso 2: Desarrollar un perfil de un activo de información: un perfil es una representación de un activo de información que describe sus características únicas, cualidades y valor. Es importante que los perfiles sean claros y consistentes, que no haya una descripción inequívoca de los límites del activo, y que los requisitos de seguridad del mismo estén definidos de forma adecuada.

Paso 3: Identificar los contenedores de los activos de información: Los contenedores son los lugares en donde los activos de información son almacenados, transportados y procesados, sean estos internos o externos. Es importante identificar los contenedores debido a que los riesgos asociados a los mismos son heredados por los activos de información.

Fase 3: Identificar las amenazas de cada activo de información en el contexto de cada uno de sus contenedores.

Paso 4: Identificar las áreas de preocupación: comienza con una lluvia de ideas sobre las posibles condiciones o situaciones que pueden poner en peligro la información de activos de información de una organización. Estos escenarios se los conoce como áreas de preocupación, y pueden representar amenazas y sus correspondientes resultados indeseables.

Paso 5: Identificar situaciones de amenaza: las áreas de preocupación identificadas en el paso anterior se expanden en escenarios de amenaza, que tienen en mayor detalle las propiedades de una amenaza. En este paso también se considera la probabilidad de ocurrencia de un escenario.

Fase 4: Identificar y analizar los riesgos para los activos de información y empezar a desarrollar los enfoques de mitigación.

Paso 6: Identificar riesgos: en base a las amenazas identificadas en el paso anterior, en este paso se identifican las consecuencias que tendría para una organización si una amenaza se presenta. Una amenaza puede tener múltiples impactos en la organización.

Paso 7: Analizar riesgos: se calcula el grado en que una amenaza afecta a la organización. Esta puntuación de riesgo relativo se obtiene teniendo en cuenta el grado del impacto del riesgo de la organización respecto de la importancia relativa de las distintas áreas de impacto, y, posiblemente, la probabilidad. Dependiendo de la organización, se dará prioridad a uno u otro criterio.

Paso 8: Seleccionar un enfoque de mitigación: las organizaciones determinan cuáles de los riesgos que se han identificado requieren de mitigación, y en base a esto se desarrolla una estrategia. Éstos son priorizados base al riesgo relativo calculado en el paso anterior.

2.3.1.2 NIST SP 800-30

La metodología NIST SP 800-30 [2] provee una guía para la evaluación de riesgos de sistemas de información federales y de organizaciones. La evaluación de riesgos es parte del proceso de gestión de riesgos, el mismo que proporciona a los directivos de las empresas la información necesaria para determinar las acciones a tomar en respuesta a los riesgos identificados. De esta metodología existen 2 publicaciones, la que se encuentra vigente es la revisión 1 del 2012.

De acuerdo a la publicación del 2012 de esta metodología, el proceso de evaluación de riesgos está conformado por cuatros pasos que son [2]:

- **Preparación para la evaluación de riesgos:** este paso tiene como objetivo establecer el marco en el que se va a realizar la evaluación, es decir se debe definir el propósito, alcance, los supuestos y restricciones asociadas con la evaluación, las fuentes de información, el modelos de riesgos y los enfoques analíticos.

- **Realización de la evaluación de riesgos:** que tiene como objetivo elaborar una lista de riesgos de seguridad priorizados por el nivel de riesgo. Para lo cual en las organizaciones, se analiza las amenazas y vulnerabilidades, el impacto y la probabilidad de cada una de las amenazas y vulnerabilidades analizadas, y la incertidumbre asociada con el proceso de evaluación de riesgos.

- **Comunicar y compartir los resultados de la evaluación de riesgos a toda la organización:** el objetivo de este paso es asegurarse de que las personas que toman las decisiones dentro de la empresa cuenten con la información necesaria sobre los riesgos para orientarse en la toma de decisiones relacionadas con los riesgos.

- **Mantenimiento de la evaluación de riesgos:** tiene como objetivo mantener actual el conocimiento sobre riesgos de las organizaciones, de manera que se pueda apoyar con esto el monitoreo de la efectividad de las respuestas al riesgo, que se han implementado.

2.3.1.3 MAGERIT

MAGERIT [1] es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España. Esta metodología nace como respuesta a la percepción de que toda la sociedad depende de manera creciente de los sistemas de información para la consecución de sus objetivos.

La razón de MAGERIT se relaciona directamente con la generalización del uso de las TI, que supone beneficios evidentes para los personas; pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

La información y los servicios informáticos utilizados para tratarla son de vital importancia y tienen un gran valor para las todas las organizaciones. Mediante el

uso de MAGERIT se puede conocer cuánto valor está en juego, y a partir de esto determinar la mejor manera de protegerlo. Es imprescindible conocer el riesgo al que están sometidos los elementos de trabajo, para de esta manera poder gestionarlos de mejor manera [25].

De acuerdo a MAGERIT, el proceso de gestión de riesgos está conformado por dos actividades [25]:

- **Análisis de riesgos:** permite determinar qué tiene la organización y estimar que le podría pasar, para lo cual considera los siguientes elementos:
  - *Activos*, son los elementos del sistema de información que soportan la misión de la organización.
  - *Amenazas*, es todo aquello que puede afectar a los activos causando perjuicios a la organización.
  - *Salvaguardias*, medidas de protección que se despliegan en la organización para evitar que las amenazas causen un gran daño en la organización.

  Con estos elementos se puede estimar el impacto (la magnitud del daño) y el riesgo (posibilidad de que se materialice una amenaza). Una vez analizados todos estos elementos de forma metódica se pueden establecer conclusiones, las mismas que van a ser utilizadas en la etapa de tratamiento.

- **Tratamiento de riesgos:** permite organizar una defensa concienzuda y prudente que permita a la organización sobrevivir a los incidentes y seguir operando en las mejores condiciones. Lo que se busca es que no pase nada malo y al mismo tiempo estar preparados para actuar de manera oportuna ante una emergencia.

2.3.2 ANÁLISIS COMPARATIVO

A continuación, se muestra en la Tabla 2-4, un análisis comparativo entre los 3 marcos de referencia descritos en la Sección 2.3.1, en donde se consideran las etapas que define cada uno de los marcos de referencia a ser comparados.

Tabla 2-4 – Tabla comparativa de los marcos de referencia de evaluación de riesgos seleccionados

Características \ Marcos de referencia		OCTAVE	NIST SP 800-30	MAGERIT
Etapas	**Caracterización de la empresa**		x	
	Identificación de activos	x		x
	Valoración de activos	x		x
	Analizar los controles vigentes		x	
	Identificación de amenazas	x	x	x
	Identificación de vulnerabilidades		x	
	Determinación de la probabilidad	x	x	x
	Determinación del impacto	x	x	x
	Determinación del riesgo	x	x	x
	Selección y recomendación de contramedidas	x		x

De acuerdo a lo observado en la Tabla 2-4, se puede determinar que los puntos clave de una evaluación de riesgos son:

- Identificación de activos
- Valoración de activos
- Analizar los controles vigentes
- Identificación de amenazas
- Determinación de la probabilidad
- Determinación del impacto
- Determinación del riesgo

3 ESTUDIO COMPARATIVO DE MARCOS DE REFERENCIA DE CONTINUIDAD DEL NEGOCIO

Este capítulo contiene un estudio comparativo de marcos de referencia de continuidad del negocio. Inicialmente se establece un listado de los marcos de referencia a ser analizados. De este listado, en base a ciertos criterios, se seleccionarán las mejores prácticas de evaluación de riesgos, las mismas que serán comparadas para determinar los principales componentes de un plan de contingencia.

3.1 MARCOS DE REFERENCIA A SER ANALIZADOS

Existen varios marcos de referencia relacionados con la gestión de continuidad del negocio. Debido a la gran cantidad de marcos de referencia, la selección de uno de ellos puede resultar complicada. Para iniciar, una lista de marcos de referencia se ha establecido en base al inventario publicado por el Business Continuity Institute [26].

En la Tabla 3-1 se listan un total de 43 marcos de referencia de gestión de continuidad del negocio entre metodologías, guías, regulaciones, legislaciones y estándares, todos directamente relacionados con la continuidad del negocio y con las TI.

Tabla 3-1 – Listado inicial de marcos de referencia de gestión de continuidad del negocio

#	Marco de Referencia
1	AE/HSC 7000: 2011
2	ASIS BCM.01-2010
3	BCI Good Practice Guidelines
4	BS/ISO 22301 Societal security – business continuity management systems – (Requirements)
5	BS/ISO22313 Societal security – business continuity management systems – (Guidance)
6	BS25999-1: 2006 Code of Practice for Business Continuity Management

#	Marco de Referencia
7	BS25999-2: 2007 Specification for Business Continuity Management.
8	BSI Standard 100-4 Business Continuity Management
9	Business Continuity Management, Building Resilience in public sector entities
10	Business Continuity Standard and Guide AE/HSE/NCEMA 7000:2012
11	CAN/CSA-Z 731-03
12	CSA Z1600-08
13	DRI International : “Ten Professional Practices for Business Continuity Professionals”
14	DS 3001:2009 Organisatorisk Robusthed.
15	FFIEC BCP Handbook: Business Continuity Planning “IT Examination Handbook”
16	Generally Accepted Practices (GAP) for Business Continuity.
17	Government of Saskatchewan Business Continuity Guide
18	GTAG 10 – Business Continuity Management
19	Handbok för kontinuitetsplanering i privat-offentlig samverkan
20	HB 221:2004 Business Continuity Management Handbook
21	HB 292:2006 A practitioners guide to business continuity
22	HB 293:2006 Executive guide to business continuity management
23	HIPAA (Health Insurance Portability and Accountability Act) Final Security Rule #7. Contingency Plan (164.308 (a) (7) (i)
24	ISO 22301 Societal Security –Business Continuity Management Systems – Requirements.
25	ISO 22313 Societal Security – Business Continuity Management Systems – Guidance.
26	ISO BIA (ISO/TS 22317)
27	ISO/IEC 24762:2008 Guidelines for information and communications technology disaster recovery services.
28	ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
29	Kontinuitetsplanering – en introduktion (2006)

#	Marco de Referencia
30	NBR ISO/IEC 24762: Tecnologia da informação Técnicas de segurança - Diretrizes para os serviços de recuperação após um desastre na tecnologia da informação e de comunicação
31	NBR 15999-1: Gestão de continuidade de negócios - Parte 1: Código de prática
32	NBR 15999-2: Gestão de continuidade de negócios - Parte 2: Requisitos
33	NC nº06/IN01/DSIC/GSIPR – Gestão De Continuidade de Negócios
34	NFPA 1600 : Standard on Disaster/Emergency Management and Business Continuity Programs
35	NIST SP 800-34 Contingency Planning Guide
36	PD25222 Guidance on Supply Chain Continuity
37	PD25666 Exercising BCM (2010)
38	Samhällssäkerhet - Ledningssystem för kontinuitet - Krav (SS-EN ISO 22301:2012, IDT)
39	Samhällssäkerhet - Ledningssystem för kontinuitet - Riktlinjer (ISO 22313:2012, IDT)
40	Samhällssäkerhet — Ledningssystem för kontinuitet — Vägledning till SS-ISO 22301 (2014)
41	SS 540:2008
42	SS507:2004
43	TR19:2005

3.2 SELECCIÓN DE MARCOS DE REFERENCIA DE CONTINUIDAD DEL NEGOCIO

En esta sección se realiza la selección de los marcos de referencia de gestión de continuidad del negocio a ser comparados. Primero, se establece criterios de exclusión para reducir el listado inicial. A continuación, se aplican los criterios de exclusión previamente definidos.

3.2.1 CRITERIOS DE EXCLUSIÓN

Para el análisis de todos los marcos de referencia de gestión de continuidad del negocio listados la Tabla 3-1, se van a considerar los siguientes Criterios de Exclusión (CE):

CE-1. El marco de referencia es una legislación, puesto que una legislación es un conjunto de leyes propias de un Estado.

CE-2. Dificultad al conseguir documentación relacionada con el marco de referencia. Entre las principales causas tenemos que la documentación encontrada estaba disponible únicamente mediante pago, el marco de referencia estaba obsoleto, o no cuenta con información completa disponible.

CE-3. La documentación se encuentra disponible en otro idioma que no sea inglés o español. Las limitaciones con el idioma traen como consecuencia problemas de acceso a marcos de referencia que se encuentran en otros idiomas, dado que imposibilita la comprensión del marco de referencia.

CE-4. El marco de referencia se encuentra inactivo, discontinuado o desactualizado, pues ya no cuentan con soporte.

CE-5. El marco de referencia se encuentra en desarrollo, a consecuencia de lo cual aún no cuenta con soporte.

Del listado inicial se eliminarán todos los marcos de referencia que cumplan con al menos uno de los criterios de exclusión antes descritos.

3.2.2 APLICACIÓN DE LOS CRITERIOS DE EXCLUSIÓN

En la Tabla 3-2, se indica el criterio de exclusión que aplica o no cada uno de los marcos de referencia de gestión de continuidad del negocio listados en la tabla que se muestra a continuación, Tabla 3-2.

Tabla 3-2 – Aplicación de los criterios de exclusión en el listado inicial de marcos de referencia de gestión de continuidad del negocio

Marco de Referencia	Criterio de Exclusión	Justificación
AE/HSC 7000: 2011	CE-2	No se encontró documentación oficial relacionada con el marco de referencia.
ASIS BCM.01-2010	CE-2	Documentación disponible mediante pago.
BCI Good Practice Guidelines	CE-2	Documentación disponible mediante pago.

Marco de Referencia	Criterio de Exclusión	Justificación
BS/ISO 22301 Societal security – business continuity management systems – (Requirements)	CE-2	Documentación disponible mediante pago.
BS/ISO 22313 Societal security – business continuity management systems – (Guidance)	CE-2	Documentación disponible mediante pago.
BS 25999-1: 2006 Code of Practice for Business Continuity Management	CE-2	Documentación disponible mediante pago.
BS 25999-2: 2007 Specification for Business Continuity Management.	CE-2, CE-4	Documentación disponible únicamente para facilitar el traslado de esta norma a la norma a la BS/ISO 22301 por la cual es reemplazada. Se encuentra obsoleto.
BSI Standard 100-4 Business Continuity Management		
Business Continuity Management, Building Resilience in public sector entities		
Business Continuity Standard and Guide AE/HSE/NCEMA 7000:2012		
CAN/CSA-Z 731-03	CE-2	Documentación disponible mediante pago.
CSA Z1600-08	CE-2	Documentación disponible mediante pago, pero de la nueva versión del 2014. Se encuentra obsoleto.
DRI International : “Ten Professional Practices for Business Continuity Professionals”		
DS 3001:2009 Organisatorisk Robusthed.	CE-2	Documentación disponible mediante pago.
FFIEC BCP Handbook: Business Continuity Planning “IT Examination Handbook” (2003)	CE-4	Se encuentra obsoleta.
Generally Accepted Practices (GAP) for Business Continuity.		
Government of Saskatchewan Business Continuity Guide		

Marco de Referencia	Criterio de Exclusión	Justificación
GTAG 10 – Business Continuity Management	CE-2	Documentación disponible únicamente para los miembros del Institute of Internals Auditors.
Handbok för kontinuitetsplanering i privat-offentlig samverkan	CE-3	La documentación disponible está en sueco.
HB 221:2004 Business Continuity Management Handbook	CE-2	Documentación disponible mediante pago.
HB 292:2006 A practitioners guide to business continuity	CE-2	Documentación disponible mediante pago.
HB 293:2006 Executive guide to business continuity management	CE-2	Documentación disponible mediante pago.
HIPAA (Health Insurance Portability and Accountability Act) Final Security Rule #7. Contingency Plan 164.308 (a)(7)(i)	CE-1	Se trata de una legislación de USA.
ISO 22301 Societal Security – Business Continuity Management Systems – Requirements.	CE-2	Documentación disponible mediante pago.
ISO 22313 Societal Security – Business Continuity Management Systems – Guidance.	CE-2	Documentación disponible mediante pago.
ISO BIA (ISO/TS 22317)	CE-2, CE-5	Documentación no disponible. Se encuentra en proceso de desarrollo.
ISO/IEC 24762:2008 Guidelines for information and communications technology disaster recovery services.	CE-2, CE-4	Documentación no disponible. Se encuentra obsoleta.
ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity	CE-2	Documentación disponible mediante pago.
Kontinuitetsplanering – en introduktion (2006)	CE-2, CE-3	Documentación disponible mediante pago. La documentación disponible está en sueco.

Marco de Referencia	Criterio de Exclusión	Justificación
NBR ISO/IEC 24762: Tecnologia da informação Técnicas de segurança - Diretrizes para os serviços de recuperação após um desastre na tecnologia da informação e de comunicação	CE-2, CE-4	Documentación no disponible. Se encuentra obsoleta.
NBR 15999-1: Gestão de continuidade de negócios - Parte 1: Código de prática	CE-2, CE-3	Documentación disponible mediante pago. La documentación disponible está en portugués.
NBR 15999-2: Gestão de continuidade de negócios - Parte 2: Requisitos	CE-2, CE-4	Documentación disponible mediante pago. Se encuentra obsoleta, reemplazada por ABNT NBR ISO 22301:2013
NC nº06/IN01/DSIC/GSIPR – Gestão De Continuidade de Negócios	CE-3	La documentación disponible está en portugués.
NFPA 1600 : Standard on Disaster/Emergency Management and Business Continuity Programs	CE-2	Documentación disponible mediante pago.
NIST SP 800-34 Contingency Planning Guide		
PD25222 Guidance on Supply Chain Continuity	CE-2	Documentación disponible mediante pago.
PD25666 Exercising BCM (2010)	CE-2	Documentación disponible mediante pago.
Samhällssäkerhet - Ledningssystem för kontinuitet - Krav (SS-EN ISO 22301:2012, IDT)	CE-2	Documentación disponible mediante pago.
Samhällssäkerhet - Ledningssystem för kontinuitet - Riktlinjer (ISO 22313:2012, IDT)	CE-2	Documentación disponible mediante pago.
Samhällssäkerhet — Ledningssystem för kontinuitet — Vägledning till SS-ISO 22301 (2014)	CE-2, CE-3	Documentación disponible mediante pago. La documentación disponible está en sueco.
SS 540:2008	CE-2, CE-4	Documentación disponible mediante pago. Se encuentra obsoleto.
SS507:2004	CE-2, CE-5	Documentación disponible mediante pago. Se encuentra bajo revisión.

Marco de Referencia	Criterio de Exclusión	Justificación
TR19:2005	CE-2, CE-4	Documentación disponible mediante pago. Se encuentra obsoleta.

3.3 ANÁLISIS COMPARATIVO DE LOS MARCOS SELECCIONADOS

En esta sección se realiza un análisis comparativo de los marcos de referencia seleccionados en la Sección anterior, con la finalidad de determinar los componentes principales del proceso de elaboración de planes de contingencia de TI.

3.3.1 INFORMACIÓN GENERAL DE LOS MARCOS SELECCIONADOS

A continuación, se describen los marcos de referencia de continuidad del negocio no excluidos, para su posterior análisis.

3.3.1.1 BSI STANDARD 100-4: BUSINESS CONTINUITY MANAGEMENT

BSI Standard 100-4 describe un Sistema de Gestión de Continuidad del Negocio (SGCN) y la respuesta de continuidad del negocio. El objetivo de este estándar es señalar un método sistemático para permitir reacciones rápidas a situaciones de emergencia y crisis de todo tipo y orígenes que pueden conducir a una interrupción de las operaciones del negocio [9].

El proceso de gestión de continuidad del negocio de una empresa es un proceso complejo que está conformado por las siguientes fases [9]:

- *Iniciación de la gestión de continuidad del negocio*

  En esta primera fase se establecen las condiciones generales para que la gestión de continuidad del negocio pueda ser establecida en la organización. Está conformada por los siguientes pasos:

  - Aceptación de la responsabilidad por la gerencia, este es un paso importante ya que la gerencia es la encargada de inicializar,

desarrollar y publicar la política para gestión de continuidad del negocio que ha sido creada.

- Concepción y planificación del proceso de gestión de continuidad del negocio, durante este paso se deben definir los objetivos del proceso, se especifica el alcance, se determinan las condiciones generales y se especifica la estrategia a usarse para alcanzar los objetivos.
- El cumplimiento de los prerrequisitos organizacionales. La gestión de continuidad del negocio se puede dividir en dos áreas la planeación de contingencias (se realiza de manera proactiva) y respuesta a la continuidad del negocio (se activa sólo cuando se produce una emergencia). Durante este paso se deben establecer los roles y responsabilidades para cada una de estas áreas.
- Creación de la política de gestión de continuidad del negocio. La política define el marco de trabajo para la concepción, establecimiento y mantenimiento del SGCN.
- Proveer recursos tanto financieros como de personal para asegurar la estructura y el funcionamiento de un proceso de gestión de continuidad del negocio.
- Incluir a todos los empleados de la organización en el proceso, mediante capacitaciones y sensibilización.

- *Planeación de contingencias*

  Antes de desarrollar el concepto de planeación de contingencias se debe realizar un trabajo preparatorio que permita entender a la organización, en lo que se incluye:

  - Análisis de impacto en el negocio (BIA por sus siglas en inglés), el mismo que permite comprender cuales son los procesos importantes para mantener las operaciones del negocio, y los posibles efectos que una falla pudiera tener.

- Análisis de riesgos, sirve para identificar las amenazas que podrían conducir a la interrupción de los procesos del negocio y evaluar los riesgos asociados.
- Determinar el estado actual de las medidas de contingencia y los actuales tiempos objetivos de recuperación (RTO por sus siglas en inglés), para hacer una estimación aproximada de la acción requerida para las distintas opciones de estrategia, y de los costos asociados.
- Estrategias de continuidad, se identifican las principales alternativas de solución y luego se seleccionan las que mejor se adapten a la organización.
- Concepto de planeación de contingencias, se forma el fundamento para la implementación de las estrategias de continuidad.

- *Implementación del concepto de planeación de contingencias*

  Se describe como planear, ejecutar, supervisar y monitorear la implementación de las medidas de contingencia. En esta fase se incluye lo siguiente:

  - Estimación del tiempo y los gastos, es un paso importante debido al presupuesto que se tiene para la implementación de las medidas preventivas y las estrategias de contingencia.
  - Especificación del orden de implementación de las medidas, es un paso importante cuando el presupuesto existente no es suficiente para la implementación inmediata de todas las medidas.
  - Especificación de las tareas y responsabilidades, es importante especificar quien es requerido para poner en práctica las medidas preventivas y para cuando.
  - Medidas que acompañan a la implementación, que incluyen programas de sensibilización y capacitación. Los programas deben ilustrar el papel de los trabajadores en la gestión de continuidad del negocio.

- *Gestión de crisis*

  Esta fase incluye la identificación y el análisis de posibles situaciones de emergencia y crisis, el desarrollo de estrategias de respuesta, y la introducción y monitoreo de contramedidas.

- *Pruebas y ejercicios*

  Para asegurar la pertinencia y eficiencia del plan de contingencia y de la respuesta a emergencias o crisis, las medidas preventivas y todos los planes deben ser revisados regularmente, probados y se deben realizar ejercicios.

- *Mantenimiento y mejora continua del proceso de gestión de continuidad del negocio*

  Se debe monitorear, controlar y actualizar continuamente el proceso de gestión de continuidad del negocio y las medidas de contingencia implementadas. Las revisiones continuas de las medidas de contingencia y los planes aseguran que el proceso de continuidad del negocio siempre sea el apropiado.

3.3.1.2 BUSINESS CONTINUITY MANAGEMENT, BUILDING RESILIENCE IN PUBLIC SECTOR ENTITIES

Esta guía desarrollada por el Australian National Audit Office (ANAO), está dividida en dos secciones, la guía y el libro de trabajo. Ambas secciones se encuentran estructuradas de acuerdo a los 7 elementos definidos en las mejores prácticas para gestión de continuidad del negocio identificadas por ANAO [27].

Los 7 elementos para gestión de continuidad del negocio son [27]:

1. Gestionar la continuidad del negocio como un programa integral del trabajo.
   - Iniciación: determinación de objetivos, alcance y límites del proyecto de continuidad del negocio, un comité coordinador, y el presupuesto

asignado al proyecto. El proyecto refleja el tamaño y la complejidad de los problemas de continuidad del negocio de la entidad.

- Gestión continua: desarrollar e implementar un marco de gobernanza robusta, de manera que se integre la gestión de continuidad del negocio con el marco de gobierno existente en la entidad.

2. Incorporación de la gestión de continuidad del negocio en la cultura de la entidad, consiste en integrar la gestión de continuidad del negocio en la cultura de la entidad, para garantizar que se convierta en parte de los valores centrales de la entidad y en una costumbre en la gestión del negocio.
    - Asegurar el compromiso de la dirección para una gestión exitosa de la continuidad del negocio.
    - Integrar la gestión de continuidad del negocio dentro de la gestión de cambios. Los planes de continuidad y los análisis de impacto en el negocio deben ser actualizados cuando se hayan realizado cambios significativos.
    - Capacitación y sensibilización de las partes importantes del programa de gestión de continuidad del negocio.

3. Análisis de la entidad y su contexto, consiste en analizar las operaciones y el entorno de la entidad; lo que incluye:
    - Identificar los procesos críticos del negocio, es decir aquellos que son esenciales para lograr los objetivos del negocio.
    - Llevar a cabo un análisis de impacto en el negocio, en donde se determina y documenta el impacto de una interrupción en cada uno de los procesos críticos del negocio.

4. Diseño de un enfoque de continuidad del negocio de la entidad. Para minimizar los efectos de las interrupciones en cada proceso crítico del

negocio se debe establecer un plazo máximo tolerable de interrupción y el tiempo objetivo de recuperación. Minimizar los efecto implica:

- Identificar y evaluar las opciones para minimizar los efectos de una interrupción en el negocio.
- Seleccionar las actividades y recursos alternativos.

5. Construcción de la resiliencia de la entidad, que consiste en implementar procedimientos preparatorios y reactivos para minimizar las interrupciones del negocio. Esto incluye:
   - Implementar controles preventivos, para mitigar las consecuencias de una interrupción en el negocio a un nivel aceptable.
   - Preparar los planes de continuidad del negocio en donde se documentan los acuerdos de recuperación a ser implementados después de que se produzca una interrupción en el negocio.

6. En caso de una interrupción: activación y despliegue del plan, se deben establecer directrices claras para determinar cuándo declarar una interrupción del negocio y así poner en marcha el plan.

7. Mantenimiento del programa y del plan: Pruebas, ejercicios, actualización y revisión. Este es un punto esencial para asegurar que el plan refleje los objetivos de le entidad, los procesos y recursos críticos y una prioridad acordada para la recuperación.

3.3.1.3 BUSINESS CONTINUITY STANDARD AND GUIDE AE/HSE/NCEMA 7000:2012

AE/HSE/NCEMA 7000:2012 es un estándar y guía para la continuidad del negocio propuesta por el National Emergency Crisis and Disasters Management (NCEMA). Ha sido desarrolla para ayudar a las entidades a construir sistemáticamente sus capacidades para la continuidad del negocio durante y después de una emergencia, desastre o crisis [28].

Este estándar identifica los componentes, mecanismos y actividades usadas para establecer, implementar y mejorar continuamente la gestión de continuidad del negocio tanto para entidades del sector público como privado.

El modelo de gestión de continuidad del negocio definido por este estándar incluye [28]:

- Entender las actividades críticas de la entidad, para lo cual se debe:
  - Establecer el alcance y los objetivos, es decir definir las actividades, servicios y funciones que se deben considerar en el alcance.
  - Asegurar el compromiso de la dirección, para que se provean los recursos necesarios para implementar y mantener un programa para la gestión de continuidad del negocio.
- Determinar la estrategia, lo que incluye:
  - Realizar un análisis de impacto en el negocio, en donde se identifique el impacto que una interrupción podría tener en los servicios y actividades principales.
  - Determinar las operaciones críticas.
  - Gestionar los riesgos en donde se debe identificar, analizar y evaluar los riesgos, además de determinar las estrategias para tratamiento de los mismos.
  - Identificar los recursos de soporte.
  - Desarrollar la estrategia para gestión de continuidad del negocio, para asegurar el continuo desempeño de las principales actividades y servicios después de una interrupción.
- Crear e implementar la gestión de continuidad del negocio
  - Desarrollar los planes para gestión de continuidad del negocio, y la gestión de emergencias y desastres, los cuales deben estar debidamente documentados y deben dar soporte a la estrategia previamente desarrollada.
  - Realizar una prueba inicial del plan
- Capacitación, revisión y sostenibilidad de la gestión de continuidad del negocio

- Capacitación y concientización, desarrollar e implementar un programa para entrenamiento y concientización que soporte efectivamente los objetivos del plan de gestión de continuidad del negocio.
- Pruebas y Ejercicios, para asegurar que los planes cumplen con los fines perseguidos y que son efectivos.

3.3.1.4 DRI INTERNATIONAL: "TEN PROFESSIONAL PRACTICES FOR BUSINESS CONTINUITY PROFESSIONALS"

Estas prácticas desarrolladas por DRI International, pretenden servir tanto como una guía para el desarrollo, implementación y mantenimiento de un programa para gestión de continuidad del negocio así como una herramienta para conducir auditorías de un programa existente [29].

Las 10 prácticas para gestión de continuidad del negocio son [29]:

1. *Iniciación y gestión del programa.* El objetivo de esta práctica es obtener el apoyo de la entidad y la financiación necesaria para construir el marco organizativo para desarrollar el programa de gestión de continuidad del negocio.
2. *Evaluación y control de riesgos.* El objetivo de esta práctica es identificar amenazas y vulnerabilidades que puedan afectar adversamente a la entidad. Una vez identificadas las amenazas y vulnerabilidades se debe evaluar la probabilidad de ocurrencia y el nivel potencial del impacto.
3. *Análisis de impacto en el negocio.* Las actividades de esta práctica incluyen la identificación de la probabilidad y potencial impacto de eventos en la entidad o en sus procesos, y los criterios que serán utilizados para cualificar y cuantificar dichos impactos.
4. *Estrategia de continuidad del negocio.* La información obtenida del análisis de impacto en el negocio y de la evaluación de riegos, es usada por esta práctica para identificar las estrategias de recuperación y continuidad disponibles para las operaciones y tecnología de la entidad.
5. *Respuestas y operación de emergencia.* Esta práctica define los requerimientos para desarrollar e implementar el plan para responder ante

situaciones de emergencia que pueden afectar a los empleados, visitantes y los activos de la entidad.

6. *Implementación y documentación del plan.* En esta práctica se define el plan de gestión de continuidad del negocio, el cual es un conjunto de procesos y procedimientos documentados, que van a permitir a la entidad recuperar los procesos a un nivel aceptable.
7. *Programas de sensibilización y capacitación.* En esta práctica se debe desarrollar e implementar un programa para establecer y mantener la conciencia empresarial sobre la gestión de continuidad del negocio y para capacitar al personal para que estén preparados para responder durante un evento.
8. *Plan de ejercicio, auditoría y mantenimiento del plan de gestión de continuidad del negocio.* El objetivo de esta práctica es el de establecer un programa para ejercicios, pruebas, mantenimiento y auditoría.
9. *Comunicación de crisis.* Esta práctica provee un marco de trabajo para identificar, desarrollar, comunicar y ejercitar un plan de comunicación de crisis. El mismo que aborda la necesidad de una comunicación eficaz y oportuna entre la entidad y los stakeholders[1] afectados o involucrados en los esfuerzos de respuesta y recuperación.
10. *Coordinación con agencias externas.* Esta práctica define la necesidad de establecer políticas y procedimientos para coordinar actividades de respuesta, continuidad y recuperación con agencias externas a nivel local, regional y nacional al tiempo que se garantiza el cumplimiento de los estatutos y reglamentos aplicables.

[1] Cualquier grupo o individuo que pueda afectar o ser afectado por el logro de los propósitos de una corporación. Stakeholders incluye a empleados, clientes, proveedores, accionistas, bancos, ambientalistas, gobierno u otros grupos que puedan ayudar o dañar a la corporación [38].

3.3.1.5 GENERALLY ACCEPTED PRACTICES (GAP) FOR BUSINESS CONTINUITY

El Disaster Recovery Journal en conjunto con DRI International, desarrollaron un conjunto de 10 prácticas para la continuidad del negocio las cuales se describen a continuación [30]:

1. Iniciación y gestión del proyecto. Se establece la necesidad de un plan de continuidad del negocio (BCP por sus siglas en inglés), se obtiene el apoyo de la dirección para la gestión y organización del proyecto del BCP hasta su finalización.
2. Evaluación y control de riesgos. Se determinan los eventos que pueden afectar negativamente a la organización y sus instalaciones con una interrupción, el daño que dichos eventos pueden causar y los controles necesarios para prevenir o minimizar los efectos de una pérdida potencial.
3. Análisis de impacto en el negocio. Identifica los impactos resultantes de interrupciones y escenarios de desastre que pueden afectar a la organización y las técnicas que pueden ser usadas para calificar y cuantificar dichos impactos.
4. Desarrollo de estrategias de continuidad del negocio. Determina y guía la selección de estrategias alternativas de recuperación para recuperar el negocio y las Tecnologías de Información dentro de los tiempos objetivos de recuperación, al tiempo que se mantienen las funciones críticas de la organización.
5. Respuestas y operaciones de emergencia. Desarrolla e implementa procedimientos para responder y estabilizar la situación después de un incidente o evento.
6. Desarrollo e implementación de planes de continuidad del negocio. Incluye el diseño, desarrollo e implementación de planes para crisis y continuidad del negocio que proporcionan continuidad dentro de los tiempos y puntos objetivos de recuperación.
7. Programas de capacitación y concientización. Prepara un programa para crear y mantener conciencia empresarial y mejorar las habilidades

necesarias para desarrollar e implementar el programa o proceso de gestión de continuidad del negocio y sus actividades de apoyo.

8. Mantenimiento y ejercicio de los planes de continuidad el negocio, planificar y coordinar planes de ejercicios, y evaluar y documentar los resultados de los ejercicios. Desarrollar procesos para mantener el plan actualizado, de manera que esté de acuerdo con la dirección estratégica de la dirección.
9. Relaciones públicas y coordinación de crisis. Consiste en desarrollar, coordinar, evaluar y preparar planes para comunicarse con stakeholders internos (empleados, gerencia, etc.) y externos (vendedor, compradores, proveedores, etc.).
10. Coordinación con entidades públicas. Establece procedimientos y políticas para coordinar actividades de respuesta, continuidad y restauración con agencias externas al tiempo que se garantiza el cumplimiento de leyes o regulaciones aplicables.

3.3.1.6 NIST SP 800-34 CONTINGENCY PLANNING GUIDE

La guía NIST SP 800-34 provee instrucciones, recomendaciones y consideraciones para planeación de contingencias. Esta guía define 7 pasos para el proceso de planeación de contingencias, los cuales son [6]:

1. Desarrollar la política de planificación de contingencias, la misma que proporciona la orientación necesaria para desarrollar un plan de contingencia efectivo.
2. Realizar un análisis de impacto en el negocio, que ayude a identificar y priorizar los sistemas de información y componentes críticos que soportan los procesos del negocio de la organización.
3. Identificación de controles preventivos, es decir las medidas adoptadas para reducir los efectos de las interrupciones de manera que pueda aumentar la disponibilidad del sistema y reducir los costos.
4. Crear estrategias de contingencia o recuperación, que garanticen que el sistema se pueda recuperar rápida y efectivamente después de una interrupción.

5. Desarrollo del plan de contingencia, que debería contener una guía y procedimientos detallados para restaurar un sistema afectado de acuerdo al nivel de impacto y los requisitos de recuperación.
6. Asegurar las pruebas del plan, la capacitación y los ejercicios. Las pruebas validan las capacidades de recuperación, mientras que la capacitación prepara al personal para la activación del plan y los ejercicios identifican lagunas dentro de la planificación. La combinación de estas actividades mejoran la efectividad del plan.
7. Asegurar el mantenimiento del plan. El plan debe ser actualizado regularmente para que se mantenga al corriente con los cambios organizacionales.

3.3.2 ANÁLISIS COMPARATIVO

A continuación, se muestra en la Tabla 3-3, un análisis comparativo entre los 6 marcos de referencia descritos en la Sección 3.3.1, en donde se consideran los componentes de un plan de continuidad [31].

Tabla 3-3 – Tablas comparativas de los marcos de referencia de gestión de continuidad del negocio seleccionados

Marco de Referencia / Componentes del Plan de Contingencia	BSI Standard 100-4	Business Continuity Management, Building Resilience in public sector entities	Business Continuity Standard and Guide AE/HSE/NCEMA 7000:2012	DRI International "Ten Professional Practices for Business Continuity Professionals"	Generally Accepted Principles for Business Continuity	NIST SP 800-34
Gestión del Proceso						
Establece un comité coordinador.				x	x	x
Define los objetivos del plan.	x	x	x	x	x	x
Define el alcance del plan.	x	x	x	x	x	x
Define horarios y documenta los eventos de prueba y mantenimiento.	x		x	x	x	x
Evaluación de riesgos						
Identifica legislaciones y regulaciones.	x		x	x	x	

Marco de Referencia / Componentes del Plan de Contingencia	BSI Standard 100-4	Business Continuity Management, Building Resilience in public sector entities	Business Continuity Standard and Guide AE/HSE/NCEMA 7000:2012	DRI International "Ten Professional Practices for Business Continuity Professionals"	Generally Accepted Principles for Business Continuity	NIST SP 800-34
Define un proceso formal de evaluación de riesgos, es decir identificar vulnerabilidades, amenazas, probabilidad, impacto.	x		x	x	x	x
Evalúa los controles de mitigación vigentes.	x			x	x	x
Análisis de impacto en el negocio						
Identifica los procesos clave del negocio.	x	x	x	x	x	x
Identifica los tiempos objetivos de recuperación específicos de cada proceso. (RTO)	x	x	x	x	x	x
Identifica los requerimientos mínimos para restaurar las operaciones del negocio a un nivel aceptable.	x	x	x	x	x	x
Prioriza los esfuerzos de recuperación en base a los RTO establecidos.	x		x	x	x	x
Revisa los acuerdos de nivel de servicio establecidos entre la empresa y socios externos.			x	x	x	
Estrategias de recuperación						
Identifica sitios alternos de recuperación para todos los procesos críticos del negocio.	x	x	x	x	x	x
Establece un procedimiento para contactar con vendedores en caso de requerir adquirir recursos críticos frente a un eventual desastre.	x			x	x	x
Identifica y documenta la información de contacto de las autoridades locales.			x	x	x	

Marco de Referencia / Componentes del Plan de Contingencia	BSI Standard 100-4	Business Continuity Management, Building Resilience in public sector entities	Business Continuity Standard and Guide AE/HSE/NCEMA 7000:2012	DRI International "Ten Professional Practices for Business Continuity Professionals"	Generally Accepted Principles for Business Continuity	NIST SP 800-34
Lleva a cabo un análisis costo beneficio para determinar la ubicación y costos asociados con los sitios alternos de recuperación y la distancia del sitio principal.	x	x	x	x	x	x
Procedimiento para la gestión de continuidad del negocio						
Define procedimientos de respuesta, recuperación y restauración, planes de comunicación, etc.	x	x	x	x	x	x
Desarrolla y documenta procedimientos para reubicar y recuperar los procesos críticos del negocio basándose en RTO aprobados por la gerencia.	x		x	x	x	x
Documenta respuestas de emergencia y recuperación de procedimientos del negocio y de TI.	x		x	x	x	x
Define los nombres de los miembros del equipo de respuesta a emergencia y recuperación, junto con su información de contacto.	x	x	x	x	x	x
Crea actividades de respuesta, recuperación y restauración que tengan en cuenta la seguridad del personal, además de la seguridad física y a nivel de TI.	x			x	x	x
Documenta los procedimientos de comunicación de crisis.	x		x	x	x	x
Identifica un coordinador de comunicación de crisis.				x	x	x

Marco de Referencia / Componentes del Plan de Contingencia	BSI Standard 100-4	Business Continuity Management, Building Resilience in public sector entities	Business Continuity Standard and Guide AE/HSE/NCEMA 7000:2012	DRI International "Ten Professional Practices for Business Continuity Professionals"	Generally Accepted Principles for Business Continuity	NIST SP 800-34
Plan de capacitación y concientización						
Desarrolla y documenta planes de entrenamiento. La capacitación debe producirse sobre una base regular definida.	x	x	x	x	x	x
Procedimientos de prueba del plan						
Asigna, documenta y comunica roles y responsabilidades para probar el plan.	x		x	x		x
Utiliza numerosos tipos de enfoque de pruebas (simulacros, simulaciones de desastres y pruebas completas del plan).	x	x	x	x	x	x
Implementa análisis posteriores de los reportes de las pruebas y revisión de los procesos.				x	x	x
Auditoría y Mantenimiento del plan						
Define y documenta los plazos específicos para la actualización del plan.	x	x		x	x	x
Audita el proceso de BCM de forma periódica para asegurar el cumplimiento de la normas de la empresa.	x	x	x	x	x	x

De acuerdo a lo observado en la Tabla 3-3 y tomando en consideración los pasos del proceso de planeación de contingencias definidos en la Sección 1.2, se puede determinar que los principales pasos para la elaboración de un plan de contingencia son:

- *Política de planificación de contingencias,* se define los objetivos, el alcance y el marco de trabajo para el proceso de elaboración del plan de contingencia.

- *Evaluación de riesgos,* en donde se identifica las amenazas que afectan a los activos de la empresa, y se determina el nivel de riesgo de cada una de las amenazas encontradas en base a su probabilidad e impacto.
- *Análisis de impacto en el negocio,* en donde se debe identificar los tiempos objetivos de recuperación (RTO) y los requerimientos mínimos de recuperación. Además, de priorizar los esfuerzos de recuperación.
- *Desarrollo de las estrategias de contingencia,* en donde se define los procedimientos a considerar para la recuperación y restauración de las operaciones del negocio y de las TI. Además, de incluir un análisis de costos para determinar que estrategias son viables para la organización.
- *Documentación del plan,* en donde se documentan todas las estrategias de contingencia que se van a considerar para la organización.
- *Concientización y capacitaciones,* en donde se define planes de entrenamiento para los empleados de la organización.
- *Pruebas del plan,* se definen los parámetros a considerar al momento de probar el plan de contingencia.
- *Mantenimiento del plan de contingencia,* en donde se define y documenta los plazos específicos para la actualización del plan.

4 MODELO PROPUESTO

Este capítulo contiene la descripción del modelo propuesto basado en los marcos de referencia de gestión de continuidad del negocio analizados en el estudio comparativo realizado en el Capítulo III y tomando en consideración los componentes principales de un plan de contingencia definidos en la Sección 3.3.2 del mismo capítulo.

Una vez definido el modelo propuesto se va a realizar la validación del mismo elaborando una propuesta de un plan de contingencia de TI para la empresa LOGICIEL.

4.1 DESCRIPCIÓN DEL MODELO PROPUESTO

El modelo propuesto a continuación, parte del supuesto de que la organización está basada en procesos, en la Figura 4-1, se indica el ciclo del modelo propuesto para realizar un Plan de Contingencias de TI.

Figura 4-1 – Ciclo del modelo propuesto

A continuación, se describen cada una de las fases que se van a contemplar en el modelo propuesto:

4.1.1 ESTUDIO DE RECONOCIMIENTO EMPRESARIAL

Esta fase permite conocer el entorno en el que se encuentra envuelta la organización, para en base a esto poder desarrollar un plan de contingencia conforme al tipo de empresa y la situación actual de la misma.

4.1.1.1 CARACTERIZACIÓN DE LA EMPRESA

Con este paso se busca conocer la empresa para la cual se va a desarrollar el plan de contingencia. Para esto es necesario describir sus principales características, misión, visión, objetivos estratégicos, descripción de la cadena de valor y de la estructura organizacional.

4.1.1.2 SITUACIÓN ACTUAL DE LAS TI

En este paso se determina la situación actual de las TI en la organización, para lo cual se debe:

- Describir la Infraestructura de TI[2], en donde se debe indicar los dispositivos físicos, aplicaciones de software y servicios que se utilizan en la empresa.
- Describir el perímetro de seguridad de la organización, es decir firewalls, zonas desmilitarizadas, sistemas de detección y prevención de intrusos, etc.
- Detallar las seguridades implementadas en la empresa a nivel de:
    - *Sistema*, lo que incluye todo lo relacionado con los equipos, redes, aplicaciones, sistemas operativos y la información manejada por las computadoras y la red.
    - *Recurso humano*, si bien todas las políticas están relacionadas con el recurso humano, en vista de que son quienes ponen en práctica

[2] La infraestructura de TI consiste en un conjunto de dispositivos físicos y aplicaciones de software que se requieren para operar toda la empresa. También se la puede definir como un conjunto de servicios a lo largo y ancho de la empresa, presupuestados por la administración, que abarcan capacidades tanto humanas como técnicas [36].

las políticas de seguridad y trabajan directamente con los sistemas, existen algunas políticas que se pueden considerar exclusivamente a este nivel.

- Describir los planes de contingencia levantados actualmente en la empresa, en el caso de no tener un plan de contingencia se deben especificar las medidas de contingencia con las que se cuente en la empresa.

4.1.2 PRIORIZACIÓN DE LOS PROCESOS DEL NEGOCIO

Partiendo de la premisa de que existen procesos del negocio que son más críticos que otros, debido a que tienen una mayor influencia en la consecución de los objetivos estratégicos, se los debe priorizar para determinar que procesos van a considerarse para el desarrollo del plan de contingencia [32]. Para realizar la priorización, se debe identificar el nivel de participación que tiene cada uno de los procesos de la cadena de valor de la empresa sobre el logro de los objetivos estratégicos establecidos por la misma, los cuales se detallaron en la fase de Estudio de reconocimiento empresarial. Además, se debe analizar el valor agregado que da el proceso al cliente.

Para el análisis del impacto de los procesos organizacionales en la estrategia del negocio y del valor agregado con respecto al cliente se va a tomar en consideración la escala de valoración que se encuentra en la Tabla 4-1.

Tabla 4-1 – Escala de valoración de los procesos del negocio

Escala	Valor
Muy Alto	5
Alto	4
Medio	3
Bajo	2
Muy Bajo	1

Una vez establecido el impacto total de cada proceso en la estrategia del negocio y analizado el valor agregado respecto al cliente, se procede a multiplicar estos valores. En base a este total se establece el nivel de criticidad de los procesos.

Los niveles de prioridad a considerarse son Crítico, Alto, Medio y Bajo. Para establecer los intervalos de valores que van a determinar el nivel de prioridad se va a considerar lo siguiente:

1. El proceso más crítico, es decir aquel que tiene un impacto muy alto en cada uno de los objetivos estratégicos y un muy alto valor agregado con respecto al cliente.
2. El proceso menos crítico, es decir aquel que tiene un impacto muy bajo en cada uno de los objetivos estratégicos y un muy bajo valor agregado con respecto al cliente.
3. El rango entre el proceso más crítico y el menos crítico, es decir la diferencia entre sus puntos totales.
4. El ancho de cada intervalo se calcula dividiendo el rango calculado en el punto anterior para el número de niveles de criticidad a considerar.
5. Los intervalos resultantes para cada nivel de prioridad, se deben calcular como sigue:
    a. Intervalo 1:
        i. Límite inferior 1 = valor mínimo
        ii. Límite superior 1= Límite inferior 1 + ancho del intervalo -1
    b. Intervalo 2:
        i. Límite inferior 2 = límite superior 1 + 1
        ii. Límite superior 2 = límite inferior 2 + ancho del intervalo -1
    c. Intervalo 3:
        i. Límite inferior 3 = límite superior 2 + 1
        ii. Límite superior 3 = límite inferior 3 + ancho del intervalo -1
    d. Intervalo 4:
        i. Límite inferior 2 = límite superior 3 + 1
        ii. Límite superior 2 = valor máximo

Para realizar la priorización se va a considerar la matriz que se muestra en la Tabla 4-2.

Tabla 4-2 – Matriz de priorización de procesos del negocio

Lista de procesos	Objetivos estratégicos							Total por impacto del proceso en la estrategia del negocio	Análisis del valor agregado respecto al cliente	TOTAL
	Objetivo 1	Objetivo 2	Objetivo 3	…	…	…	Objetivo n			
Proceso 1										
Proceso 2										
Proceso 3										
…										
…										
…										
Proceso n										

4.1.3 EVALUACIÓN DE LOS ACTIVOS

En esta fase se busca identificar los activos de información que participan dentro de los procesos que tengan una prioridad crítica y alta, y valorarlos conforme al aporte a los atributos que dan valor a la información que representan.

4.1.3.1 IDENTIFICACIÓN DE ACTIVOS

En esta sección se van a identificar los activos involucrados en cada proceso con prioridad crítica y alta. Para esto, será necesario realizar entrevistas con los responsables de cada uno de los procesos objeto de evaluación. Para cada activo se va a detallar la siguiente información [32]:

- **ID Activo:** número único con el que se va a identificar a cada activo dentro del inventario.
- **Nombre del activo:** nombre con el que se conoce al activo dentro de la empresa.
- **Tipo de activo:** se identifica si el activo pertenece a uno de los siguientes grupos:
    - **Información:** toda fuente de información física o electrónica (bases de datos, documentación del sistema, etc.).

- **Aplicación:** todos los componentes de software de los sistemas de información, software del sistema, herramientas de software y utilidades.
- **Infraestructura:** todas las instalaciones y dispositivos físicos (equipos de computación, de comunicaciones, discos duros removibles y otros dispositivos) requeridos para la ejecución de un proceso.
- **Persona:** personas naturales que por su conocimiento, habilidades experiencia y criticidad para el proceso, son considerados activos de información. Se incluye personal de la organización, personal subcontratado, clientes y usuarios
- **Servicio:** todo servicio propio o suministrado por terceros (agua, energía eléctrica, telecomunicaciones, sistemas de extinción de incendios, aire acondicionado, mantenimiento de hardware, software e infraestructura).

- **Descripción:** detalles importantes del activo.

Durante la identificación de activos se debe llenar la matriz que se muestra en la Tabla 4-3.

Tabla 4-3 – Matriz de inventario de activos

ID ACTIVO	NOMBRE ACTIVO	TIPO ACTIVO					DESCRIPCIÓN
		Información	Aplicación	Infraestructura	Persona	Servicio	

4.1.3.2 VALORACIÓN DE ACTIVOS

Una vez identificados los activos involucrados en cada proceso con prioridad crítica y alta, se debe identificar que tan significativo es el aporte de cada activo a los atributos de la información que representan y que se definen a continuación:

Confidencialidad: se debe evaluar el impacto que tendría si el activo fuera accedido por personas, procesos o entidades no autorizadas. Para valorar la confidencialidad se debe considerar los criterios establecidos en la Tabla 4-4.

Tabla 4-4 – Valoración de la Confidencialidad

Escala	Valor	Criterio
Muy Alto	5	El conocimiento o divulgación no autorizada de la información que gestiona el activo impacta negativamente a toda la organización.
Alto	4	El conocimiento o divulgación no autorizada de la información que gestiona el activo impacta negativamente de manera leve a la organización. Además, impacta al proceso evaluado y a los otros procesos de la organización.
Medio	3	El conocimiento o divulgación no autorizada de la información que gestiona el activo impacta negativamente al proceso evaluado.
Bajo	2	El conocimiento o divulgación no autorizada de la información que gestiona el activo impacta negativamente de manera leve al proceso evaluado.
Muy Bajo	1	El conocimiento o divulgación no autorizada de la información que gestiona el activo no impacta negativamente al proceso.

El impacto que tendría la pérdida de confidencialidad sobre el activo de información, de acuerdo a su tipo se especifica en la Tabla 4-5 que se muestra a continuación.

Tabla 4-5 – Impacto por pérdida de Confidencialidad de acuerdo al tipo de activo

Tipo de activo	Impacto
Información	Individuo, entidad o proceso no autorizado que accede al activo de información.
Aplicación	Individuo, entidad o proceso no autorizado que conoce la existencia o parametrización del activo.
Infraestructura	Alguien que conoce que existe el elemento, su configuración o accede al activo sin autorización.
Persona	Se hace uso inadecuado de la información privilegiada a la

Tipo de activo	Impacto
	cual tiene acceso por el cargo o función que desempeña.
Servicio	Alguien que conoce su existencia, configuración o hace uso no autorizado del activo.

Integridad: se debe evaluar el impacto que tendría si la precisión, calidad, veracidad, imparcialidad y completitud de la información fuera alterada. Para valorar la integridad se debe considerar los criterios establecidos en la Tabla 4-6.

Tabla 4-6 – Valoración de la Integridad

Escala	Valor	Criterio
Muy Alto	5	La pérdida de exactitud, precisión y completitud del activo impacta negativamente a la organización.
Alto	4	La pérdida de exactitud, precisión y completitud del activo impacta negativamente de manera leve a la organización. Además, impacta al proceso evaluado y a los otros procesos de la organización.
Medio	3	La pérdida de exactitud, precisión y completitud del activo impacta negativamente al proceso evaluado.
Bajo	2	La pérdida de exactitud, precisión y completitud del activo impacta negativamente de manera leve al proceso evaluado.
Muy Bajo	1	La pérdida de exactitud, precisión y completitud del activo no impacta negativamente al proceso.

El impacto que tendría la pérdida de la integridad sobre el activo de información, de acuerdo a su tipo se especifica en la Tabla 4-7 que se muestra a continuación.

Tabla 4-7 – Impacto por pérdida de Integridad de acuerdo al tipo de activo

Tipo de activo	Impacto
Información	Se pierde la completitud, exactitud o precisión del activo de información.
Aplicación	Se valora la completitud, exactitud o precisión de la parametrización del activo.
Infraestructura	El activo no efectúa las actividades de procesamiento o su función correctamente; o es alterada su configuración indebidamente.
Persona	La persona produce datos errados o incompletos; o de acuerdo con su rol toma decisiones equivocadas, por capacidades o aptitudes inadecuadas para desempañar el rol o función.
Servicio	Se valora la completitud, exactitud o precisión del servicio.

Disponibilidad: se debe evaluar el impacto que tendría si los usuarios autorizados no tuvieran acceso a los activos de información en el momento que lo requieran. Para valorar la disponibilidad se debe considerar los criterios establecidos en la Tabla 4-8.

Tabla 4-8 – Valoración de la Disponibilidad

Escala	Valor	Criterio
Muy Alto	5	La falta o no disponibilidad del activo impacta negativamente a la organización.
Alto	4	La falta o no disponibilidad del activo impacta negativamente de manera leve a la organización. Además, impacta al proceso evaluado y a los otros procesos de la organización.
Medio	3	La falta o no disponibilidad del activo impacta negativamente al proceso evaluado.
Bajo	2	La falta o no disponibilidad del activo impacta negativamente de manera leve al proceso evaluado.
Muy Bajo	1	La falta o no disponibilidad del activo no impacta negativamente al proceso.

El impacto que tendría la pérdida de la disponibilidad sobre el activo de información, de acuerdo a su tipo se especifica en la Tabla 4-9 que se muestra a continuación.

Tabla 4-9 – Impacto por pérdida de Disponibilidad de acuerdo al tipo de activo

Tipo de activo	Impacto
Información	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado.
Aplicación	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado.
Infraestructura	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado.
Persona	La persona no se encuentra disponible para el proceso.
Servicio	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado.

Para valorar los activos listados en el inventario resultado de la Identificación de activos, se debe llenar una matriz como la que se muestra a continuación en la Tabla 4-10.

Tabla 4-10 – Matriz de valoración de activos

ID ACTIVO	NOMBRE ACTIVO	Proceso Crítico 1			Proceso Crítico 2			…			Proceso crítico N			VALOR ACTIVO
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	

Una vez completa la Matriz de valoración de activos, se debe proceder a calcular el valor total de cada activo, para lo cual se debe sumar los valores asignados para la confidencialidad, integridad y disponibilidad por cada proceso crítico, los cuales se determinaron durante la fase de priorización de los procesos del negocio.

Debido a que el número de activos involucrados en los procesos críticos puede ser muy alto, se sugiere continuar la evaluación de riesgos con los activos de mayor valor. En base al valor total se va a establecer el nivel de criticidad de los activos.

Los niveles de prioridad a considerarse son Crítico, Alto, Medio y Bajo. Para establecer los intervalos de valores que van a determinar el nivel de prioridad se va a considerar lo siguiente:

1. El activo más crítico, es decir aquel que tiene un valor muy alto para la confidencialidad, integridad y disponibilidad por cada proceso crítico.
2. El activo menos crítico, es decir aquel que tiene valor muy bajo para la confidencialidad, integridad y disponibilidad por cada proceso crítico.
3. El rango entre el proceso más crítico y el menos crítico, es la diferencia entre sus valores totales.

4. El ancho de cada intervalo se calcula dividiendo el rango calculado en el punto anterior dividido para el número de niveles de criticidad a considerar.
5. Los intervalos resultantes para cada nivel de prioridad, se deben calcular como sigue:
   a. Intervalo 1:
      i. Límite inferior 1 = valor mínimo
      ii. Límite superior 1= Límite inferior 1 + ancho del intervalo -1
   b. Intervalo 2:
      i. Límite inferior 2 = límite superior 1 + 1
      ii. Límite superior 2 = límite inferior 2 + ancho del intervalo -1
   c. Intervalo 3:
      i. Límite inferior 3 = límite superior 2 + 1
      ii. Límite superior 3 = límite inferior 3 + ancho del intervalo -1
   d. Intervalo 4:
      i. Límite inferior 2 = límite superior 3 + 1
      ii. Límite superior 2 = valor máximo

4.1.4 DESARROLLO DE LA POLÍTICA DE PLANIFICACIÓN DE CONTINGENCIAS

En esta fase se busca desarrollar la política de planificación de contingencias. La política debe definir el marco de trabajo y las responsabilidades para la concepción, establecimiento y mantenimiento del plan de contingencia [12], de manera que se pueda definir y potencialmente mejorar la habilidad de continuar con las operaciones del negocio durante y después de una interrupción [9].

Es importante definir la política en base a las características de la organización, sus productos, servicios, ubicación y ambiente operativo, sus stakeholders, obligaciones y activos.

La política debe ser [9] [12]:

- Lo suficientemente clara para que pueda ser entendida por todos los interesados.

- Aprobada por la gerencia.
- Comunicada y estar disponible para todas las personas involucradas (empleados y potenciales grupos de interés) en el proceso de planeación de contingencias.
- Revisada a intervalos definidos y cuando se produzcan cambios significativos en las condiciones generales, los objetivos del negocio, tareas o estrategias.

Los elementos clave que debe incluir la política son [6]:

- Propósito
- Alcance
- Intención
- Requerimientos de capacitación / entrenamiento
- Programa de ejercicios y pruebas
- Programa de mantenimiento del plan
- Frecuencia mínima de respaldo y almacenamiento de los medios de respaldo.

En el Anexo A, se define un modelo de política de planeación de contingencias, en donde se describe en mayor detalle cada uno de los elementos clave previamente listados.

4.1.5 EVALUACIÓN DE RIESGOS

En esta fase se busca estimar el riesgo asociado a los activos críticos identificados en la fase de Evaluación de los activos, partiendo de la identificación de amenazas y vulnerabilidades.

4.1.5.1 IDENTIFICACIÓN DE RIESGOS

En este paso se determinan las amenazas que pueden afectar a cada activo con prioridad crítica y alta que se valoraron en la fase anterior. Para facilitar la identificación de las amenazas, se presenta un listado de posibles amenazas basadas en el catálogo propuesto por MAGERIT [33].

De cada posible amenaza se detalla la siguiente información:

- **ID:** número único con el que se va a identificar a cada amenaza dentro del listado.
- **Nombre de la Amenaza:** nombre con el que se conoce a la amenaza.
- **Origen:** se identifican cada uno de los orígenes de las amenazas que pueden ser los siguientes [1]:
    - **De origen natural:** se incluyen los accidentes naturales como terremotos, inundaciones, etc.
    - **Del entorno (de origen industrial):** se incluyen los desastres industriales como contaminación, fallos eléctricos, etc.
    - **Defectos de las aplicaciones:** se incluyen los problemas que nacen directamente en el equipamiento por defectos en su diseño o implementación.
    - **Causadas por las personas de forma accidental:** se incluyen problemas no intencionados causados por personas con acceso al sistema de información, típicamente por error u omisión.
    - **Causadas por las personas de forma deliberada:** se incluyen problemas intencionados causados por personas con acceso al sistema de información, generalmente con el ánimo de beneficiarse o causar daños y perjuicios a la organización.
- **Tipo de Activo:** se identifican los tipos de activos que se pueden ver afectados por la amenaza. Se consideran los tipos previamente definidos en la Sección 4.1.3.1.
- **Criterios Afectados:** se identifican los atributos de información que se pueden ver afectados por la amenaza.
- **Descripción:** se detalla más la amenaza, incluyendo lo que le puede ocurrir al activo.

En la Tabla 4-11 se encuentra el listado de posibles amenazas [33]:

Tabla 4-11 – Listado de posibles amenazas

ID	Nombre de la Amenaza	Origen					Tipo de Activo					Criterios afectados			Descripción
		Natural (accidental)	Entorno (accidental)	Defecto de las Aplicaciones	Humano (accidental)	Humano (deliberado)	Información	Aplicación	Infraestructura	Persona	Servicio	Confidencialidad	Integridad	Disponibilidad	
1	Abuso de privilegios de acceso					x	x	x	x		x	x	x	x	Cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia.
2	Acceso no autorizado					x	x	x	x		x	x	x		El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. (Uso ilícito del hardware)
3	Alteración de la información				x	x	x	x			x		x		Alteración accidental o deliberada de la información.
4	Alteración de secuencia					x		x	x		x		x		Alteración del orden de los mensajes transmitidos. Con el objetivo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando la integridad de los datos afectados.
5	Análisis de tráfico					x			x			x			El atacante, sin necesidad de analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.

ID	Nombre de la Amenaza	Origen					Tipo de Activo					Criterios afectados			Descripción
		Natural (accidental)	Entorno (accidental)	Defecto de las Aplicaciones	Humano (accidental)	Humano (deliberado)	Información	Aplicación	Infraestructura	Persona	Servicio	Confidencialidad	Integridad	Disponibilidad	
6	Ataque destructivo					x			x					x	Destrucción del hardware o de soportes, vandalismo, terrorismo, etc.
7	Avería de tipo físico o lógico		x		x	x	x	x	x					x	Se incluyen fallos en los equipos o en los programas.
8	Caída del sistema por agotamiento de recursos				x						x			x	Caída del sistema por carencia de recursos suficientes cuando la carga de trabajo es desmesurada. (Saturación del sistema informático)
9	Condiciones inadecuadas de temperatura o humedad		x		x	x			x					x	Fallas en la climatización de los locales (excesivo calor, frío, humedad, etc.)
10	Contaminación electromagnética		x		x	x	x		x		x			x	Se incluyen interferencias de radio, campos magnéticos, luz ultravioleta, etc.
11	Contaminación mecánica		x		x	x	x		x		x			x	Se incluyen vibraciones, polvo, suciedad, etc.
12	Corrupción de la información					x	x						x		Degradación intencionada de la información, con ánimo de obtener un beneficio o causar un perjuicio.
13	Corte de suministro eléctrico		x		x	x			x					x	Constituye la pérdida del suministro de energía.
14	Daños por agua / Inundaciones	x	x		x	x	x		x		x			x	Posibilidad de que el agua acabe con recursos del sistema.

ID	Nombre de la Amenaza	Origen					Tipo de Activo					Criterios afectados			Descripción
		Natural (accidental)	Entorno (accidental)	Defecto de las Aplicaciones	Humano (accidental)	Humano (deliberado)	Información	Aplicación	Infraestructura	Persona	Servicio	Confidencialidad	Integridad	Disponibilidad	
15	Deficiencias en la organización				x					x				x	No se tienen claros los roles y responsabilidades del personal, por lo que no se tiene claro qué hacer y cuándo hacerlo.
16	Degradación de la información				x		x						x		Degradación accidental de la información.
17	Degradación de los soportes de almacenamiento de la información		x		x	x	x		x					x	Se incluye la avería y la falla del funcionamiento del hardware como consecuencia del paso del tiempo.
18	Denegación de servicio					x			x		x			x	Saturación del sistema informático, la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
19	Desastres industriales		x		x	x	x		x		x			x	Se incluyen incidentes como explosiones, derrumbes, etc. (Se excluyen los incendios e inundaciones.)
20	Desastres naturales	x	x		x	x	x		x		x			x	Se incluyen incidentes como rayos, tormentas eléctricas, terremotos, ciclones, avalanchas, deslaves, etc. (Se excluyen los incendios e inundaciones.)
21	Destrucción deliberada de información					x	x							x	Pérdida intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.

ID	Nombre de la Amenaza	Origen					Tipo de Activo					Criterios afectados			Descripción
		Natural (accidental)	Entorno (accidental)	Defecto de las Aplicaciones	Humano (accidental)	Humano (deliberado)	Información	Aplicación	Infraestructura	Persona	Servicio	Confidencialidad	Integridad	Disponibilidad	
22	Destrucción accidental de información				x		x	x			x			x	Pérdida accidental de información.
23	Difusión de software dañino				x	x		x				x	x	x	Propagación inocente o intencionada de virus, spyware, gusanos, etc.
24	Divulgación de información					x	x					x			Revelación intencional de información.
25	Errores de (re)encaminamiento				x	x		x			x	x			Envío de información a través de rutas incorrectas que lleve la información a donde no es debido o a las manos indebidas.
26	Errores de configuración				x		x	x	x		x	x	x	x	Introducción de datos de configuración erróneos.
27	Errores de mantenimiento / actualizaciones de equipos (Hardware)				x				x					x	Defectos en los procedimientos de actualización que permite que sigan utilizándose los equipos más allá del tiempo nominal de uso.
28	Errores de mantenimiento / actualizaciones de programas (Software)				x			x					x	x	Defectos en los procedimientos de actualización, lo cual permite que sigan utilizándose programas con defectos conocidos y provoca fallas en el funcionamiento del software.
29	Errores de monitorización (log)				x		x	x			x		x		Inadecuado registro de actividades, falta de registros, registros incompletos, registros fechados incorrectamente, etc.

ID	Nombre de la Amenaza	Origen					Tipo de Activo					Criterios afectados			Descripción
		Natural (accidental)	Entorno (accidental)	Defecto de las Aplicaciones	Humano (accidental)	Humano (deliberado)	Información	Aplicación	Infraestructura	Persona	Servicio	Confidencialidad	Integridad	Disponibilidad	
30	Errores de secuencia				x			x			x		x		Alteración accidental del orden de los mensajes transmitidos.
31	Errores de usuarios				x		x	x			x	x	x	x	Errores de uso de servicios, datos, etc.
32	Errores del administrador				x		x	x	x		x	x	x	x	Equivocaciones de personas con responsabilidades de instalación y operación.
33	Extorsión					x				x		x	x	x	Presión mediante amenazas que se ejerce sobre alguien para obligarle a obrar en determinado sentido.
34	Fallo de servicios de comunicaciones		x		x	x					x			x	Pérdida de los medios de telecomunicación y cese de la capacidad de transmitir datos de un sitio a otro.
35	Fuego / Incendios	x	x		x	x	x		x		x			x	Posibilidad de que el fuego acabe con recursos del sistema.
36	Fugas de información				x		x	x		x	x	x			Revelación por indiscreción o incontinencia verbal la información.
37	Indisponibilidad accidental del personal				x					x				x	Ausencia del personal por enfermedad, alteraciones del orden público, etc.
38	Indisponibilidad del personal					x				x				x	Ausencia del personal por huelgas, absentismo, bajas no justificadas, etc.
39	Ingeniería social					x				x		x	x	x	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

ID	Nombre de la Amenaza	Origen					Tipo de Activo					Criterios afectados			Descripción
		Natural (accidental)	Entorno (accidental)	Defecto de las Aplicaciones	Humano (accidental)	Humano (deliberado)	Información	Aplicación	Infraestructura	Persona	Servicio	Confidencialidad	Integridad	Disponibilidad	
40	Inserción de información incorrecta				x	x	x						x		Inserción accidental o deliberada de información incorrecta.
41	Intercepción de información					x	x	x				x			El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
42	Interrupción de otros servicios y suministros esenciales		x		x	x					x			x	Otros servicios o recursos de los que depende la operación de los equipos (tóner, papel para impresiones, etc.)
43	Manipulación de equipos					x			x			x		x	Alteración intencionada del funcionamiento de los equipos, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. (Sabotaje del hardware)
44	Manipulación de la configuración					x	x	x	x		x	x	x	x	Manipulación deliberada de la configuración de los activos (privilegios de acceso, etc.).
45	Manipulación de los registros de actividad (log)					x	x						x		Manipulación deliberada de los registros de actividad.
46	Manipulación de programas					x		x				x	x		Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
47	Modificación deliberada de la información					x	x	x			x		x		Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

ID	Nombre de la Amenaza	Origen					Tipo de Activo					Criterios afectados			Descripción
		Natural (accidental)	Entorno (accidental)	Defecto de las Aplicaciones	Humano (accidental)	Humano (deliberado)	Información	Aplicación	Infraestructura	Persona	Servicio	Confidencialidad	Integridad	Disponibilidad	
48	Ocupación no autorizada					x			x			x		x	Cuando las instalaciones han sido invadidas por personas no autorizadas y se carece de control sobre los medios de trabajo.
49	Pérdida de equipos				x				x			x		x	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios.
50	Repudio					x	x				x		x		Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.
51	Robo					x	x		x		x	x		x	Robo de soportes o documentos, o del hardware.
52	Suplantación de la identidad del usuario					x	x	x			x	x	x	x	Cuando un atacante consigue hacerse pasar por un usuario autorizado.
53	Uso no previsto					x		x	x		x	x	x	x	Utilización de recursos del sistema para fines no previstos (juegos, programas personales, etc.)
54	Vulnerabilidades de los programas			x	x	x		x				x	x	x	Defectos en el código de los programas que generan operaciones defectuosas que pueden afectar la integridad de los datos y su capacidad de operar.

4.1.5.2 VALORACIÓN DE CONTROLES EXISTENTES

En este paso se busca identificar los controles o salvaguardias que se encuentran implementadas para mitigar las amenazas previamente identificadas. Una vez identificados los controles existentes se deben evaluar la eficiencia de los mismos, para lo cual se debe considerar los criterios que se muestran en la Tabla 4-12 [32].

Tabla 4-12 – Evaluación de la efectividad de los controles existentes

Escala	Valor	Criterio
Muy Adecuado	5	El control existente disminuye casi toda la probabilidad de ocurrencia y el impacto de la amenaza.
Adecuado	4	El control existente disminuye en gran medida la probabilidad de ocurrencia y el impacto de la amenaza.
Moderado	3	El control existente disminuye de manera moderada la probabilidad de ocurrencia y el impacto de la amenaza.
Débil	2	El control existente disminuye levemente la probabilidad de ocurrencia y el impacto de la amenaza.
Muy débil	1	El control existente no ayuda a disminuir la probabilidad de ocurrencia y el impacto de la amenaza.

4.1.5.3 VALORACIÓN DE RIESGOS

En este paso se debe determinar, para cada una de las amenazas identificadas para los activos críticos, la probabilidad de ocurrencia de las amenazas y el impacto que tendrían en la organización en caso de que lleguen a materializarse.

4.1.5.3.1. Determinación de la Probabilidad

Para determinar la probabilidad de ocurrencia se deben considerar los criterios que se muestran en la Tabla 4-13 [2].

Tabla 4-13 – Valoración de la Probabilidad

Escala	Valor	Criterio
Muy Alta	5	Es casi seguro que la amenaza (error, accidente o acto de la naturaleza) ocurra.
Alta	4	Es altamente probable que la amenaza (error, accidente o acto de la naturaleza) ocurra.
Media	3	Es algo probable que la amenaza (error, accidente o acto de la naturaleza) ocurra.
Baja	2	Es improbable que la amenaza (error, accidente o acto de la naturaleza) ocurra.

Escala	Valor	Criterio
Muy Baja	1	Es altamente improbable (raro) que la amenaza (error, accidente o acto de la naturaleza) ocurra.

4.1.5.3.2. Determinación del Impacto

Para determinar el impacto potencial se deben considerar los criterios que se muestran en la Tabla 4-14 [2].

Tabla 4-14 – Valoración del Impacto

Escala	Valor	Criterio
Muy Alto	5	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar múltiples efectos adversos graves o catastróficos en las operaciones, activos o individuos de la organización.
Alto	4	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso grave o catastrófico en las operaciones, activos o individuos de la organización.
Medio	3	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un serio efecto adverso en las operaciones, activos o individuos de la organización.
Bajo	2	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso limitado en las operaciones, activos o individuos de la organización.
Muy Bajo	1	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso insignificante en las operaciones, activos o individuos de la organización.

Un *efecto adverso grave o catastrófico* significa que la amenaza puede [2]:

- Detener las principales funciones de la organización.
- Provocar daños graves a los bienes de la organización.
- Producir un gran perjuicio económico.
- Provocar daños graves o catastróficos para las personas (amenaza la vida).

Un *serio efecto adverso* significa que la amenaza puede [2]:

- Afectar la eficacia de las principales funciones de la organización.
- Dar lugar a daños significativos a los bienes de la organización.
- Provocar importantes pérdidas económicas.
- Provocar daños significativos a las personas (sin amenazar la vida).

Un *efecto adverso limitado* significa que la amenaza puede [2]:

- Reducción insignificante de la efectividad de las funciones de la organización.
- Provocar daños menores en los activos de la organización.
- Provocar pérdidas económicas de menor importancia.
- Resultar en un daño menor a los individuos.

4.1.5.3.3. Determinación del Nivel de Riesgo

Para determinar el nivel de riesgo se deben multiplicar los valores establecidos por activo tanto para la probabilidad como para el impacto, de acuerdo a esto se tendría lo que se muestra en la Tabla 4-15.

Tabla 4-15 – Valoración del Riesgo

Impacto / Probabilidad		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		1	2	3	4	5
Muy Bajo	1	1	2	3	4	5
Bajo	2	2	4	6	8	10
Medio	3	3	6	9	12	15
Alto	4	4	8	12	16	20
Muy Alto	5	5	10	15	20	25

En base a los valores mostrados en la Tabla 4-15 se va a establecer los niveles de riesgo que son Muy Alto, Alto, Medio, Bajo y Muy Bajo. Para establecer los intervalos de valores que van a determinar el nivel de riesgo se va a considerar lo siguiente:

1. Un riesgo muy alto, es decir aquel que tiene un impacto muy alto y una probabilidad muy alta, tendría una valoración de 25.
2. Un riesgo muy bajo, es decir aquel que tiene un impacto muy bajo y una probabilidad muy baja, tendría una valoración de 1.
3. El rango entre un riesgo muy alto y uno muy bajo, es decir, la diferencia entre sus puntos totales es 24.
4. El ancho de cada intervalo se calcula dividiendo el rango calculado en el punto anterior para el número de niveles de criticidad a considerar, es decir $24/5 \approx 5$.

En la Tabla 4-16 [2], se encuentran los intervalos resultantes para cada nivel de riesgo y la descripción de cada uno de ellos.

Tabla 4-16 – Nivel de Riesgo

Escala	Valor	Criterio
Muy Alto	21 – 25	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar múltiples efectos adversos graves o catastróficos en las operaciones, activos o individuos de la organización.
Alto	16 – 20	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso grave o catastrófico en las operaciones, activos o individuos de la organización.
Medio	11 – 15	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un serio efecto adverso en las operaciones, activos o individuos de la organización.
Bajo	6 – 10	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso limitado en las operaciones, activos o individuos de la organización.
Muy Bajo	1 – 5	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso insignificante en las operaciones, activos o individuos de la organización.

4.1.6 ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)

Esta fase es una parte importante del proceso de planeación de contingencias puesto que es el procedimiento utilizado para determinar el impacto que una interrupción tendría en cada uno de los procesos críticos del negocio [9] [12]. Además, el BIA es usado para especificar los puntos de recuperación de los procesos críticos del negocio y los intervalos de tiempo en que deben ser restaurados. Adicionalmente, permite asignar las prioridades de recuperación e identificar los recursos mínimos requeridos para que cada proceso opere a un nivel mínimo aceptable [9].

Los resultados obtenidos después de realizar el BIA sirven como base para definir estrategias de contingencia [28].

4.1.6.1 DETERMINACIÓN DEL IMPACTO DE UNA INTERRUPCIÓN

En esta sección se va a determinar el impacto que tendría una interrupción en cada uno de los procesos críticos del negocio. La determinación del impacto de una interrupción se debe valorar en base a las siguientes categorías [29]:

- **Impacto al cliente**, en la Tabla 4-17 se muestran los criterios a considerar en esta categoría.

Tabla 4-17 – Valoración del Impacto al Cliente

Escala	Valor	Criterio
Severo	3	La interrupción puede ocasionar que el que el nivel de servicio se vea completamente comprometido, haciendo que el cliente opte por contratar a otra empresa.
Moderado	2	La interrupción puede ocasionar que el nivel de servicio se vea altamente comprometido.
Mínimo	1	La interrupción puede ocasionar que el nivel de servicio se vea levemente comprometido.

- **Impacto Financiero**, en la Tabla 4-18 se muestran los criterios a considerar en esta categoría.

Tabla 4-18 – Valoración del Impacto Financiero

Escala	Valor	Criterio
Severo	3	La interrupción puede ocasionar que se vean comprometidas las ventas futuras.
Moderado	2	La interrupción puede ocasionar que se tengan pérdidas de ingresos.
Mínimo	1	La interrupción puede ocasionar que se tenga que pagar multas o sanciones por incumplimiento de contrato.

- **Impacto Operacional**, en la Tabla 4-19 se muestran los criterios a considerar en esta categoría.

Tabla 4-19 – Valoración del Impacto Operacional

Escala	Valor	Criterio
Severo	3	La interrupción puede ocasionar que no se puedan cumplir con los plazos establecidos.
Moderado	2	La interrupción puede ocasionar que se reduzca el nivel de servicio ofrecido.
Mínimo	1	La interrupción puede ocasionar que se vea interrumpido el flujo de trabajo de la organización.

- **Impacto Reputacional**, en la Tabla 4-20 se muestran los criterios a considerar en esta categoría.

Tabla 4-20 – Valoración del Impacto Reputacional

Escala	Valor	Criterio
Severo	3	La interrupción puede ocasionar que se tenga atención negativa de los medios de comunicación.
Moderado	2	La interrupción puede ocasionar que se pierda la confianza de los accionistas.
Mínimo	1	La interrupción puede ocasionar que el competidor tome ventaja de la atención negativa que tiene la empresa.

Para determinar el impacto en la organización si las operaciones de los procesos críticos del negocio se vieran interrumpidas, se debe considerar la Tabla 4-21 [6].

Tabla 4-21 – Matriz de impacto de una interrupción en los procesos críticos del negocio

Proceso del Negocio	Impacto				Total
	Al Cliente	Financiero	Operacional	Reputacional	

4.1.6.2 DETERMINACIÓN DE LOS PARÁMETROS DE RECUPERACIÓN

En esta sección se deben especificar el máximo tiempo de inactividad, el tiempo objetivo de recuperación y el punto objetivo de recuperación [6] de cada uno de los procesos del negocio, en base a la secuencia cronológica de los acontecimientos perjudiciales y la cantidad de daño a esperar.

- **Tiempo Máximo de Inactividad (MTD, por sus siglas en inglés):** representa la cantidad total de tiempo que un proceso crítico del negocio puede estar inactivo (interrumpido) antes de que haya efectos perjudiciales para la organización. La determinación de MTD es importante porque ayuda en la selección de un método de recuperación apropiada, y permite determinar la profundidad del detalle que se requiere en el desarrollo de los procedimientos de recuperación.

- **Tiempo Objetivo de Recuperación (RTO, por sus siglas en inglés):** define la cantidad máxima de tiempo en el que un recurso debe reanudar su operación antes de que haya un impacto inaceptable en otros recursos del sistema, procesos del negocio soportados y el MTD. La determinación

del RTO de los recursos del sistema de información es importante para la selección de las tecnologías que son los más adecuadas para el cumplimiento de los MTD.

- **Puntos Objetivos de Recuperación (RPO, por sus siglas en inglés):** representa el punto en el tiempo a partir del cual se va a iniciar la recuperación de los datos del proceso del negocio (por ejemplo: una hora antes, un día antes, una semana antes de que se produzca la interrupción). A diferencia del RTO, RPO no se considera como parte del MTD. Más bien, es un factor de la cantidad de datos perdidos que el proceso del negocio puede tolerar durante el proceso de recuperación.

El RTO debe asegurarse de que no se exceda el MTD, por lo que el RTO debe normalmente ser más corto que el MTD. Por ejemplo, una interrupción del sistema puede impedir que un determinado proceso se complete, y porque se necesita tiempo para volver a procesar los datos, el tiempo de procesamiento adicional se debe agregar a la RTO para mantenerse dentro del límite de tiempo establecido por el MTD [6].

En la Tabla 4-22 se deben identificar el MTD, RTO y RPO para los procesos críticos del negocio. Los valores que se asignen al MTD, RTO y RPO deben ser intervalos de tiempo específicos, identificados en incrementos de una hora (por ejemplo, 8 horas, 36 horas, 97 horas, etc.).

Tabla 4-22 – Matriz de parámetros de recuperación de los procesos del negocio

Procesos del negocio	MTD	RTO	RPO

4.1.6.3 IDENTIFICAR LOS RECURSOS MÍNIMOS REQUERIDOS

En esta sección se deben identificar los recursos mínimos requeridos para restaurar los procesos críticos del negocio lo más pronto posible. En la Tabla 4-23

se deben listar los recursos tanto de hardware, software y otros recursos como archivos de datos.

Tabla 4-23 – Inventario de recursos mínimos requeridos

Id Recurso	Nombre Recurso	Descripción

Se debe considerar que los recursos listados en la Tabla 4-23, son aquellos que soportan los procesos críticos del negocio.

4.1.6.4 IDENTIFICAR LAS PRIORIDADES DE RECUPERACIÓN DE LOS RECURSOS

En esta sección se debe listar el orden en que se van a recuperar los recursos. En la Tabla 4-24 se debe listar los recursos en orden de prioridad, identificando el tiempo esperado de recuperación de cada uno de los recursos.

Tabla 4-24 – Matriz de priorización de recuperación de recursos

Id Recurso	Nombre Recurso	RTO

4.1.7 DESARROLLO E IMPLEMENTACIÓN DE ESTRATEGIAS DE CONTINGENCIA

En esta fase se deben establecer estrategias de contingencia para prevenir, prepararse, mitigar, responder y recuperarse de interrupciones del negocio. La información recolectada en la evaluación de riesgos y el BIA se usan en esta fase para identificar las estrategias de contingencia para las operaciones de la organización y la tecnología [12].

Para establecer las estrategias de contingencia se debe considerar el RTO y RPO identificados para cada uno de los procesos críticos durante la fase del BIA. Los

siguientes pasos se deben tomar en cuenta para establecer las estrategias de contingencia [29]:

1. Identificar las estrategias de continuidad que mejor se adapten a las necesidades de la empresa.
2. Determinar los roles y responsabilidades para la correcta implementación de las estrategias.
3. Establecer los parámetros a considerar para la activación del plan de contingencia.

4.1.7.1 ESTRATEGIAS DE CONTINGENCIA

Para establecer las estrategias de contingencia se debe identificar tanto medidas preventivas como medidas de mitigación. Las medidas preventivas permiten a todos los miembros de la organización estar preparados para hacer frente a los posibles riesgos que se presenten. Por otro lado, las medidas de mitigación permiten atenuar los potenciales impactos causados por un riesgo.

Para las *medidas preventivas* se debe detallar la siguiente información:

- **Medida Preventiva:** en donde se especifica el nombre de la medida preventiva que se va a describir. Cada medida preventiva debe ser enumerada.
- **Riesgos que contrarresta:** se debe listar los riesgos que se verán reducidos por la medida preventiva descrita.
- **Medidas Técnicas / Organizativas / Humanas:** se debe listar las acciones a nivel técnico, organizativo o humano de acuerdo a la medida preventiva descrita.

Para las *medidas de mitigación o recuperación* se debe detallar la siguiente información:

- **Contingencia:** nombre de la contingencia cuyas medidas de mitigación o recuperación se van a describir.
- **Factores de riesgo:** listado de las posibles fuentes de amenaza que pueden terminar en la contingencia.

- **Plan de Acción:** listado de medidas de mitigación o recuperación a considerar en el caso de que la contingencia se presente en la organización.

Las potenciales estrategias de contingencia incluyen pero no se limitan a las que se detallan a continuación:

Personas

Las personas son el recurso vital para asegurar la continuidad del negocio, por lo que una pérdida inesperada de personal clave o experimentado puede tener consecuencias significativas en el cumplimiento de los objetivos de la organización [27].

Entre las estrategias enfocadas en las personas se incluyen [27]:

- Estrategias de comunicación: en donde se debe especificar los canales de comunicación por los que se enviarán los mensajes a las personas interesadas durante una interrupción.
- Estrategias para reemplazo y capacitación del personal a corto plazo.

Instalaciones

En el caso de una interrupción, puede que sea necesario restaurar las operaciones en un sitio alterno por lo que se debe incluir en el plan de contingencia el tipo de sitio alterno a implementar, su ubicación y los costos que implicaría en caso de ser necesario [6]. Este tipo de estrategias ayudarán a la organización en la restauración oportuna de los procesos de negocio críticos que se requieran mover o reubicar en nuevas instalaciones para asegurar la continuidad del negocio [27].

Hay tres tipos de sitios alternativos, los cuales se describen a continuación [6]:

- **Cold sites:** son locaciones que tienen la infraestructura básica (cableado eléctrico, aire acondicionado, etc.), pero no equipos de computación o de telecomunicaciones.

- **Warm sites:** son locaciones que tienen la infraestructura básica de un cold site, pero que además tienen instalado y disponible el suficiente equipo computacional y de telecomunicaciones para ejecutar las operaciones de la empresa. Sin embargo, los equipos no se encuentran cargados con el software o los datos requeridos para una rápida recuperación de los sistemas y es necesaria una configuración previa.
- **Hot sites:** son locaciones con el equipo en pleno funcionamiento y la capacidad para retomar rápidamente las operaciones de la empresa después de la pérdida de las instalaciones primarias.

La Tabla 4-25 [6] resume los criterios que pueden ser usados para determinar qué tipo de sitio alterno cumple con los requerimientos de la organización.

Tabla 4-25 – Tipos de sitos alternos

Tipo	Costo	Equipamiento	Telecomunicaciones	Tiempo de configuración
Cold Site	Bajo	Ninguno	Ninguno	Prolongado
Warm Site	Medio	Parcial	Parcial/Completo	Medio
Hot Site	Medio/ Alto	Completo	Completo	Corto

La selección de un tipo de sitio alterno se debe realizar considerando los impactos en el negocio y los parámetros de recuperación definidos en el BIA.

Tecnología (sistemas de información y aplicaciones)

Los sistemas de información y las aplicaciones gestionan los datos e información de la organización. Algunas estrategias relacionadas con la tecnología incluyen:

- **Protección de recursos**

Parte del éxito de la planeación de contingencias es hacer los recursos más resistentes al entorno y fallas de los componentes que podrían causar interrupciones en las operaciones del negocio. Hay varios métodos para hacer el hardware y software más resistentes. Los resultados de la evaluación de riesgos permiten determinar los métodos más apropiados para la protección de los recursos [6].

El uso de UPS es un método que permite la protección de los recursos de la empresa ante las fallas de energía eléctrica, de manera que el hardware crítico de la empresa (servidores) así como los sistemas y datos contenidos en el mismo no se vean corrompidos. Los UPS también protegen a los recursos de las fluctuaciones de energía [6].

- **Reemplazo de equipos**

En caso de que los recursos se vean afectados por una interrupción o las instalaciones primarias están comprometidas por una interrupción, puede ser preciso configurar y adquirir el hardware y software necesario para restaurar las operaciones. Existen tres alternativas para prepararse para el reemplazo de equipos, las cuales se detallan a continuación [2]:

- **Acuerdos con proveedores:** esta alternativa implica el establecimiento de acuerdos de nivel de servicio (SLA, por sus siglas en inglés) con los proveedores de hardware y software.
- **Inventario de equipos:** incluye la adquisición previa de equipos de respaldo, que se encuentren debidamente almacenados en una locación segura.
- **Equipo existente:** implica el uso de equipos redundantes similares y compatibles a los que actualmente son usados y ocupados en la organización.

Al momento de evaluar que alternativa es la más adecuada para la organización, hay que considerar que la compra de equipos durante una contingencia aunque puede ser rentable puede aumentar el tiempo de recuperación al esperar el envío de los documentos y proceder con la correspondiente configuración de los mismos. Por otro lado, el almacenamiento de equipos en desuso es costoso, pero permite una recuperación más rápida de las operaciones.

Información

La información debe ser respaldada regularmente. Se deben establecer políticas en donde se especifique la frecuencia mínima y el alcance de los respaldos o

copias de seguridad basándose en la criticidad de la información y la frecuencia con la que la nueva información es introducida [6]. Dentro de las políticas se debe especificar el lugar en donde se almacenará la información, el formato de etiquetado de los respaldos, la forma en que se transportarán, etc.

Los respaldos de información deben estar almacenados en una locación segura fuera de la organización, de manera que puedan estar disponibles para ser restaurados durante una contingencia. Hay tres principales métodos para realizar los respaldos de información [6]:

- **Respaldo Completo:** captura todos los archivos de un disco o de la carpeta seleccionada para el respaldo. Este método puede facilitar la búsqueda de archivos, pero el tiempo necesario para realizar este tipo de respaldos puede ser muy largo dependiendo del volumen de información. Además, mantener este tipo de respaldos puede resultar excesivo si los archivos no cambian frecuentemente, pues implicaría el uso innecesario de los medios de almacenamiento.

- **Respaldo Incremental:** captura los archivos que fueron creados o cambiados desde el último respaldo realizado. Este método permite un uso más eficiente de los medios de almacenamiento y los tiempos de respaldo se ven reducidos.

- **Respaldo Diferencial:** almacena los archivos que fueron creados o cambiados desde el último respaldo completo que se ha realizado. De manera que si un archivo es modificado después del último respaldo completo, el respaldo diferencial guardará el archivo hasta que el siguiente respaldo completo se realice.

Dependiendo de la configuración del sistema y de los requisitos de recuperación, puede ser necesaria una combinación de los tres tipos de respaldos.

Adicionalmente, es importante asegurar la integridad y seguridad de la información. Hay varios métodos disponibles para mantener la integridad y la seguridad de los datos almacenados [6].

La integridad de los datos implica mantener los datos seguros y precisos en los dispositivos en donde son almacenados. Entre los métodos utilizados para asegurar la integridad se encuentran procesos de redundancia y tolerancia a fallos [6], lo que consiste en almacenar los datos en más de una unidad, para de esta forma eliminar la pérdida de datos por fallas en unidades individuales de almacenamiento.

Por otro lado, la seguridad de los datos implica la protección de los mismos del acceso o uso no autorizado. El cifrado es un método común para asegurar los datos. La encriptación es más eficaz cuando se aplica tanto al dispositivo de almacenamiento de datos, como a las copias de seguridad (respaldos).

4.1.7.2 ROLES Y RESPONSABILIDADES

Una vez seleccionadas las estrategias de continuidad se deben definir y documentar claramente los roles, responsabilidades y equipos apropiados para asegurar la implementación de las estrategias, prevenir malos entendidos (especialmente durante un incidente) y evitar tareas duplicadas o sin atender [12]. Cada equipo debe ser capacitado y debe estar listo para responder en caso de que un evento requiera la activación del plan de contingencia. El principal objetivo de cada uno de los equipos es devolver las operaciones del negocio a su estado normal [6]. Para esto, cada miembro de los equipos necesita entender claramente las responsabilidades que llevará a cabo y como éstas pueden afectar al éxito de la implementación de las estrategias.

4.1.7.3 ACTIVACIÓN DEL PLAN

En este paso se debe establecer un procedimiento para la activación del plan de contingencia una vez que un desastre ha ocurrido. Este procedimiento debe detallar las actividades a realizarse para poner mitigar la incidencia y recuperar

los procesos del negocio. Entre las principales actividades se encuentran las que se describen a continuación:

- *Verificación de la Incidencia*. Revisión inicial de los daños causados por la incidencia para en base a esto poder realizar la correspondiente notificación.
- *Notificación Inicial de la incidencia*. Se notifica al líder del equipo de respuesta ante incidencias, para que sea él quien proceda con la ejecución del resto de actividades para la correcta activación del plan.
- *Escalamiento de notificaciones*. Determinar en caso de ser necesario las notificaciones adicionales que tienen que ser enviadas en base a la severidad de la situación.
- *Activación del equipo de recuperación*. Determinar que miembros del equipo son requeridos de acuerdo a la medida de mitigación seleccionada por el líder.
- *Evaluación de daños*. Conducir una inspección en el sitio donde se produjo la incidencia, con el objetivo de determinar la extensión del daño, las áreas afectadas y la mejor forma de acción para solucionar la incidencia.
- *Seguimiento del evento de contingencia.* Mantener un registro de las actividades de respuesta y recuperación realizadas para contrarrestar el incidente.

4.1.8 DESARROLLO Y DOCUMENTACIÓN DEL PLAN DE CONTINGENCIA

La capacidad para manejar rápida y efectivamente una emergencia depende principalmente de la documentación disponible [9]. La disponibilidad de la documentación también juega un papel decisivo, además de su calidad y cuan al día se encuentre.

La documentación debe ser revisada y actualizada en una base regular, sin embargo, en caso de que se produzcan cambios significativos en la organización o en los procesos del negocio la actualización del documento deberá abordarse con prontitud.

El documento del plan de contingencia debe contener principalmente [9]:

- Alcance
- Roles y responsabilidades
- Resultados de la evaluación de riesgos
- Resultados del análisis de impacto en el negocio
- Estrategias de contingencia

En el Anexo B, se define un modelo del documento del plan de contingencias de TI, en donde se describe en mayor detalle cada uno de los elementos clave previamente listados.

4.1.9 PRUEBAS Y EJERCICIOS

Una vez se tengan establecidas claramente las estrategias de contingencia y se haya documentado el plan, la organización debe hacer pruebas y ejercicios que permitan asegurar la pertinencia y eficiencia del plan de contingencia.

Los ejercicios demuestran si la documentación del plan de contingencia es útil, si los implicados son capaces de realizar las tareas que asignadas y si se cumple todo lo definido en el plan [9] [27] [28]. Mientras que las pruebas evalúan la disponibilidad, usabilidad y adecuación de las herramientas, tecnologías, instalaciones e infraestructura requeridas para la implementación del plan. Las pruebas también permiten identificar las deficiencias del plan [6] [28].

Los ejercicios además permiten entrenar al personal en los procedimientos descritos en los planes, permitiéndoles realizar las acciones necesarias de manera rutinaria, mejorando así el tiempo de reacción de los empleados frente a una emergencia [12].

Una vez finalizadas las pruebas y ejercicios, se debe realizar un análisis posterior de los resultados obtenidos para identificar mejoras o revisiones que se necesitan hacer en el plan de contingencia.

Previa la realización de las pruebas del plan de contingencia se debe definir un plan de pruebas, para lo cual se debe considerar el modelo definido en el Anexo C.

Para la realización de los ejercicios del plan de contingencia se debe establecer el escenario para la realización del ejercicio, para lo cual se debe llenar el modelo definido en el Anexo D. Una vez finalizado el ejercicio, se debe llenar un informe considerando el modelo definido en el Anexo E, en donde se especifican los principales resultados y recomendaciones obtenidas luego de la realización del ejercicio.

4.1.10 CONCIENTIZACIÓN Y CAPACITACIONES

En este paso se busca concientizar a los empleados de la organización con respecto a la importancia del plan de contingencia [9] [28]. Las capacitaciones se usan para asegurar que todos los empleados de la organización conocen el plan de contingencia, su importancia, la forma en que pueden ayudar en la exitosa implementación del mismo y cómo deben responder en caso de emergencia [28].

Previa la realización de concientización y capacitaciones del plan de contingencia se debe establecer un plan de capacitación que considere el número de personas a ser capacitadas, su disponibilidad de tiempo, grado de habilidad, conocimientos y tipos de actitudes. El plan de capacitación debe hacerse en base al modelo definido en el Anexo F.

4.1.11 MANTENIMIENTO DEL PLAN DE CONTINGENCIA

El plan de contingencia debe ser revisado a intervalos planificados (al menos una vez al año) y cuando se produzcan cambios significativos, para asegurar su idoneidad, exactitud y efectividad [12] [28]. La organización debe revisar el análisis de impacto en el negocio, el análisis de riesgos, las estrategias de contingencia y el plan de contingencia.

La revisión permite determinar si los documentos son válidos y consistentes con los objetivos estratégicos de la organización. Esta revisión debe incluir la evaluación de oportunidades de mejora. Los resultados obtenidos de la revisión se los debe documentar para un posterior análisis, para lo cual se debe llenar la plantilla definida en el Anexo G.

4.2 VALIDACIÓN DEL MODELO PROPUESTO EN LA EMPRESA LOGICIEL

Tomando como referencia lo establecido en la descripción del modelo propuesto, en esta sección se va proceder con la validación del mismo, para lo cual se va a elaborar una propuesta de un plan de contingencia de TI para la empresa LOGICIEL.

4.2.1 ESTUDIO DE RECONOCIMIENTO EMPRESARIAL DE LOGICIEL

Aplicando lo definido en la Sección 4.1.1, se va a describir el contexto de la empresa LOGICIEL, para en base a esto realizar el plan de contingencias.

4.2.1.1 CARACTERIZACIÓN DE LA EMPRESA LOGICIEL

LOGICIEL es una compañía de responsabilidad limitada, fundada en el mes de mayo del año 2000. La empresa entrega soluciones integradas con las Tecnologías de la Información (TI), es decir productos y servicios informáticos, los cuales apoyan a las empresas de producción y servicio en la consecución de sus metas críticas superando sus expectativas y necesidades. Adicionalmente, buscan que la calidad de vida y los valores compartidos sean el eje para el desarrollo tanto personal de sus empleados y usuarios, así como de las organizaciones relacionadas [34].

LOGICIEL se enfoca fundamentalmente en el segmento financiero-bancario (bancos, cooperativas, administradoras de cartera, etc.), sin embargo cubre otros segmentos siempre que el análisis de mercado demuestre que se pueden ofrecer

precios aceptables de sus productos y servicios [35]. A continuación, se lista en orden de prioridad los segmentos del negocio a los que se enfoca la empresa:

- Segmento financiero: bancos, administradoras de cartera, mutualistas, cooperativas, cajas de ahorro.
- Empresas industriales, de comercialización y servicio, medianas y grandes, que permitan a la empresa tener ingresos y beneficios cercanos a los obtenidos con los clientes de la Banca.
- Organizaciones sociales.
- Investigación: se considera la elaboración de una herramienta informática en el área de Biotecnología y conservación con el medio ambiente.

Su principal actividad económica es el desarrollo de aplicaciones flexibles y dinámicas en la parametrización de los productos, fácilmente adaptables a las políticas, estrategias y condiciones de trabajo de sus clientes [35].

Entre los principales servicios ofertados por la empresa se encuentran los siguientes [34]:

- Desarrollo y mantenimiento de sistemas de información
- Implantación de soluciones informáticas integradas
- Asesoría y consultoría en tecnologías de la información
- Comercialización de licencias de uso de paquetes de software
- Arrendamiento (outsourcing) de sistemas de información
- Desarrollo de modelos de score

4.2.1.1.1. Objetivos Estratégicos

Para finales del año 2015, LOGICIEL espera cumplir con los siguientes objetivos estratégicos [35]:

1. Aumentar la dedicación de las actividades de marketing y ventas de 10% a 12%.
2. Ampliar el catálogo de clientes en al menos 2 clientes nuevos.
3. Mantener y fortalecer la relación con los clientes principales de LOGICIEL: Grupo Pichincha, BIESS, Originarsa, Cooprogreso; para de esta manera

permitir que los ingresos se mantengan, al menos, en un monto similar a los ingresos obtenidos en el año 2014 por estos servicios.

4. Realizar ventas de los productos disponibles, para alcanzar un incremento en los ingresos anuales, que permitan cumplir con la meta establecida para el periodo.
5. Disponer de un 60% de la funcionalidad de su Core Bancario (LOGICORBA).
6. Aplicación de las mejoras de procesos establecidas en la implementación del modelo/técnica ITMark.
7. Capacitación e incentivos al personal.

4.2.1.1.2. Cadena de Valor de LOGICIEL

En la cadena de valor se contemplan los procesos primarios relacionados con la generación de los productos y servicios ofertados por la empresa y de los procesos de apoyo a los procesos primarios. En la Figura 4-2 [35] se presenta la cadena de valor de LOGICIEL, en la cual se identifican los siguientes grupos de procesos [35]:

- **Procesos Estratégicos y Administrativos**
  - **Planeación estratégica y del negocio:** análisis de la situación actual de la empresa y planificación de la estrategia del negocio.
  - **Gestión financiera y administrativa:** actividades de administración contable así como la gestión del personal y soporte administrativo.

- **Procesos Primarios (principales)**
  - **Implementación de paquetes de software:** gestión de requerimientos, planificación de proyectos, desarrollo, monitoreo y control. Se lo ejecuta por un desarrollo proactivo, que no nace de una necesidad formal de algún cliente externo. El levantamiento se lo hace en un comité interno de la empresa.
  - **Implementación de aplicaciones:** gestión de requerimientos, planificación de proyectos, desarrollo, monitoreo y control, para proyectos que satisfagan las necesidades de clientes externos.

- **Implantación de soluciones informáticas:** instalación de los sistemas implementados en los ambientes de los clientes (pruebas, producción), capacitaciones, pruebas de aceptación.
- **Mantenimiento de software:** gestión de requerimientos, planificación del proyecto, desarrollo, monitoreo y control. Cuando los usuarios reportan alguna necesidad nueva que desean incluir o notifican alguna funcionalidad que no se esté ejecutando correctamente en los sistemas implantados en sus ambientes.
- **Gestión de la calidad de software:** administración de la calidad de software, gestión de versiones, verificación de estándares, pruebas y análisis de métricas.
- **Marketing, venta y post-venta:** planificación y organización de eventos y promociones, prospección de clientes, venta, seguimiento en la implementación y post-venta de las aplicaciones desarrolladas.

➢ **Procesos de Soporte:**

- **Gestión de la seguridad de la información:** administración de la seguridad y administración de respaldos.
- **Investigación y desarrollo:** investigación de avances tecnológicos que se acoplan a las nuevas tendencias del mercado.
- **Administración de recursos computacionales:** administración de redes y comunicaciones, de base de datos y de software base.

Figura 4-2 – Cadena de valor de LOGICIEL

4.2.1.1.3. Estructura Organizacional

La estructura organizacional de la empresa LOGICIEL se encuentra basada en una división técnica del trabajo, en donde se definen perfiles y funciones de acuerdo a los servicios de software prestados y a las TI con las que cuenta la empresa.

En la Figura 4-3 [35] se especifica cada una de las áreas que tiene la empresa:

- Gerencia de Desarrollo
- Gerencia de Gestión de la Calidad del Software (SQM)
- Gerencia de Producto
- Gerencia de Investigación y Desarrollo (I&D)
- Gerencia de Marketing
- Área Financiera y Administrativa

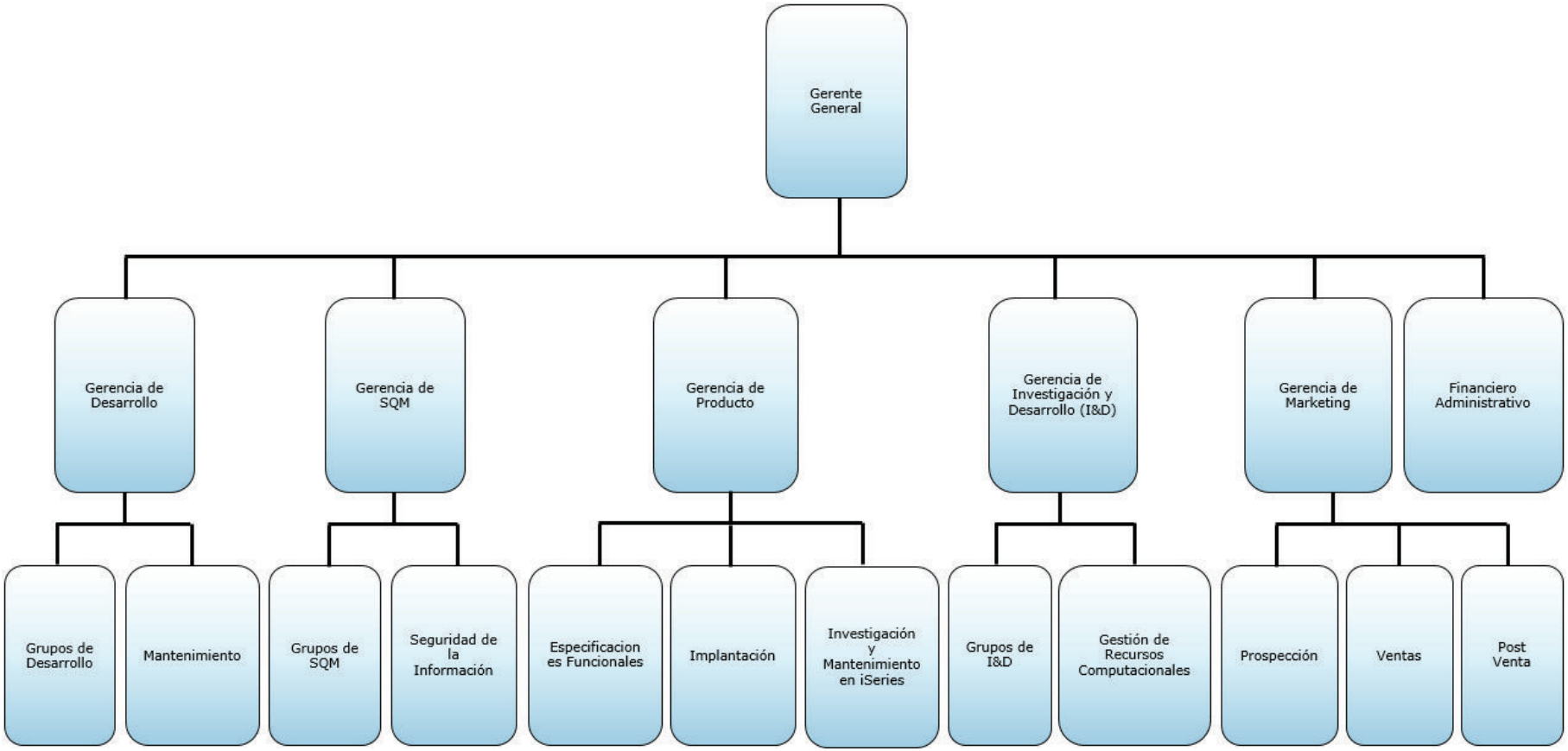

Figura 4-3 – Estructura organizacional de LOGICIEL

4.2.1.2 SITUACIÓN ACTUAL DE LAS TI EN LOGICIEL

A continuación, se describe la situación actual de las TI en la empresa LOGICIEL.

4.2.1.2.1. Infraestructura de TI de LOGICIEL

En la Figura 4-4 y Figura 4-5, se muestra el diagrama de red detallado de los dos pisos en donde funciona la empresa. La empresa cuenta con una sola LAN, y un backbone que conecta los segmentos de red de ambos pisos. De acuerdo a lo especificado en estas figuras se puede ver que la empresa posee:

- 7 servidores físicos y 3 servidores virtuales.
- 24 computadores de escritorio: 11 en el 4° piso y 13 en el 9° piso.
- 9 computadores portátiles: 5 en el 4° piso y 4 en el 9° piso.
- 4 switches: 1 en el 9° piso y 3 en el 4° piso.
- 2 impresoras

En cada uno de los pisos existe un cuarto de telecomunicaciones, en donde se encuentran ubicados los servidores de la empresa. Uno de los servidores cuenta con el sistema operativo Asterisk y el resto de servidores tienen como sistema operativo Microsoft Server 2008 R2. Los computadores de escritorio y equipos portátiles tienen como sistema operativo Microsoft Windows 7, 8 y 8.1.

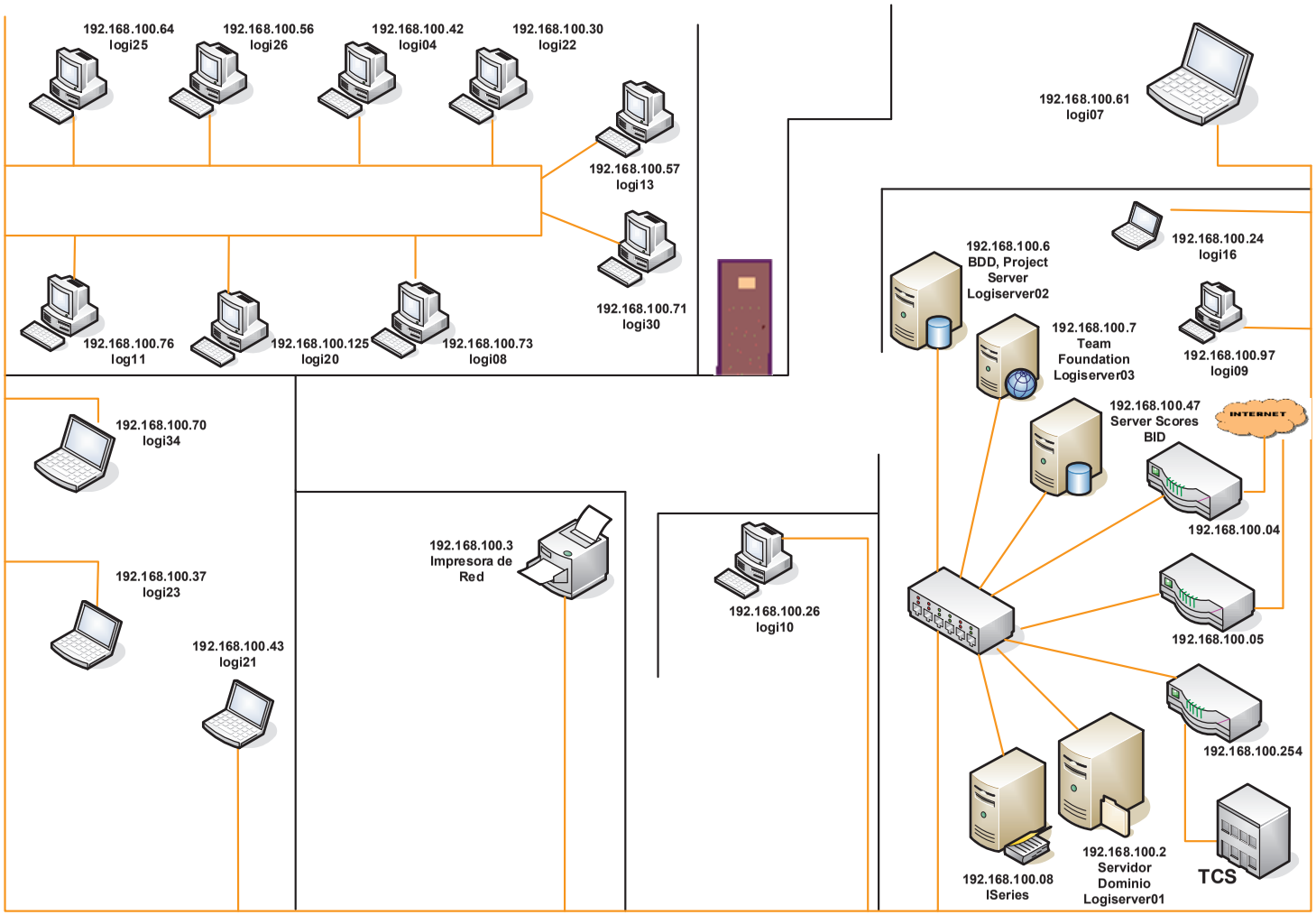

Figura 4-4 – Diagrama de red detallado del cuarto piso

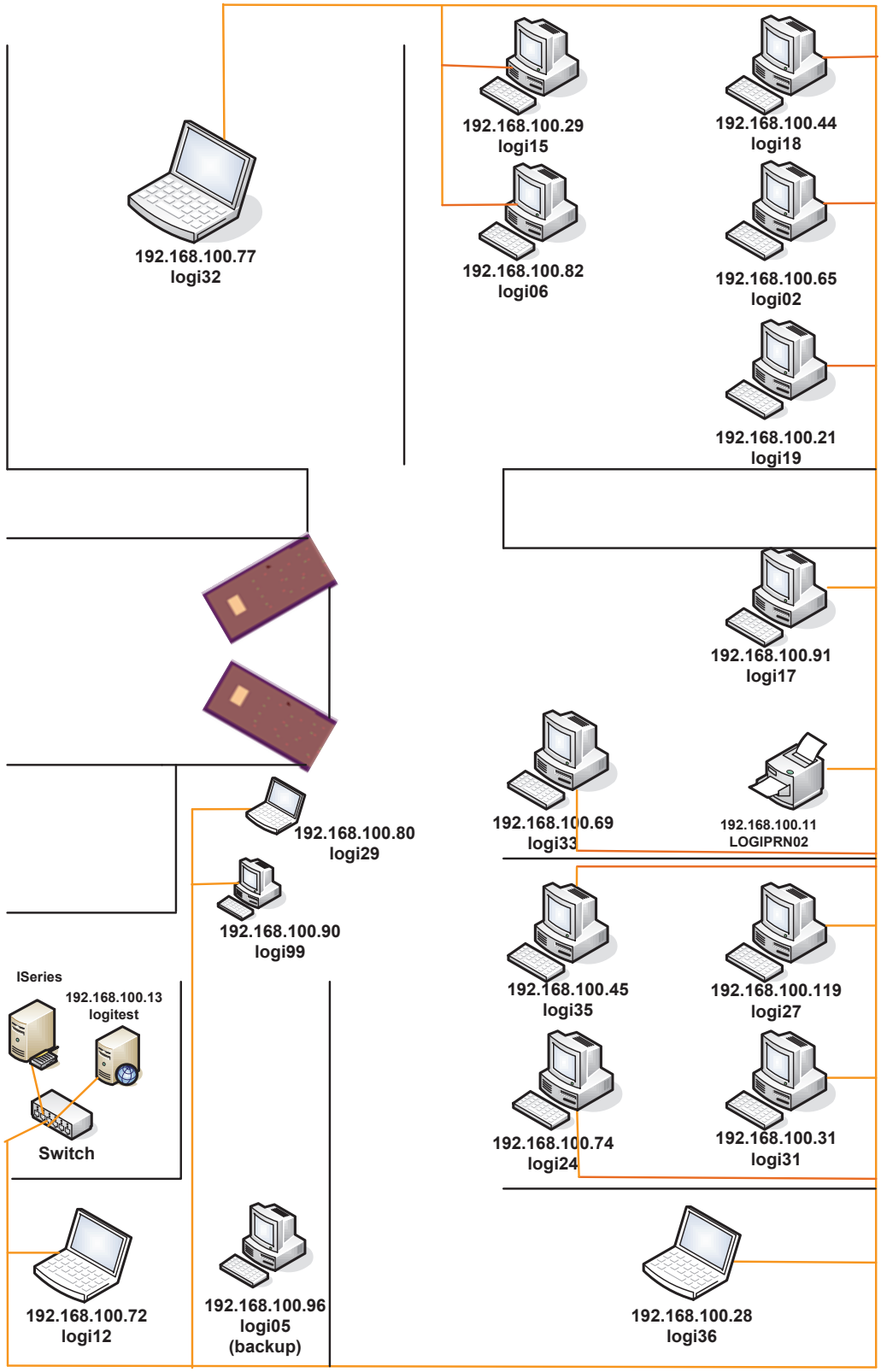

Figura 4-5 – Diagrama de red detallado del noveno piso

Los servidores contienen los siguientes servicios levantados:

- **Logiserver01,** servidor físico que tiene alojado los siguientes servicios:
  - Active Directory
  - DHCP
  - DNS principal
  - VPN

- **Logiserver02,** servidor físico que tiene alojado los siguientes servicios:
  - DNS secundario
  - Virtualización de los servidores:
    - **Logiserver03:** Team Foundation
    - **Logidesa01:** Servidor de Aplicaciones del Ambiente de Desarrollo
  - Sistemas de Score (Ambiente de Test)
  - Project Server 2010 y su interfaz web Project Web App (PWA)
  - Sharepoint 2010 de LOGICIEL

- **Logihypervi01,** servidor físico que tiene alojado lo siguiente:
  - Virtualización del servidor:
    - **Logiserver04:** Servidor de aplicaciones del ambiente de TEST.

- **Logihypervi02,** servidor físico que tiene alojado lo siguiente:
  - Ambiente LOGICIEL de producción
  - Ambiente de Test de algunos clientes
  - Servidor de aplicaciones de tratamiento de incidencias

- **Logitest,** servidor físico que tiene alojado los siguientes servicios:
  - Servidor de Base de Datos del Ambiente de Test
  - Servicio PRTG.

- **Servidores iSeries,** se cuenta con dos servidores físicos. Uno que se encuentra físicamente en la empresa, y sirve para el manejo de la contabilidad de la misma. El segundo no se encuentra en la empresa, y sirve para dar servicios de outsourcing a los clientes.

- **Servidor Asterisk,** servidor físico que tiene alojado el servicio de Telefonía IP.

La empresa cuenta con dos proveedores de Internet:

- Uno residencial, que lo provee TVCable, y es utilizado a nivel gerencial dentro de la empresa.
- Otro corporativo, que lo provee Telconet, y es utilizado por el resto de funcionarios de la empresa.

La persona encargada de la administración de la infraestructura de TI en la empresa es el *administrador de recursos computacionales*.

4.2.1.2.2. Perímetro de Seguridad de LOGICIEL

a) Nivel físico

Se cuenta con un cuarto de telecomunicaciones en cada uno de los pisos en donde opera la empresa, a los cuales tiene acceso únicamente el personal autorizado.

b) Nivel Lógico

Se cuenta con dos firewalls que controlan el acceso no autorizado a la red a través de Internet. Uno de ellos controla el Internet Corporativo y está implementado en el IOS del router Cisco (192.168.100.4), mientras que el segundo controla la conexión residencial a Internet, mediante el firewall que se encuentra instalado en el router Dlink (192.168.100.5).

Para el escaneo de las conexiones que se realizan desde afuera de la empresa, se utilizan los logs que se guardan en los equipos que hacen de firewall, es decir

el router Cisco y router Dlink. Adicionalmente se usa el monitor de red PRTG, que también controla la utilización del ancho de banda.

Como política de seguridad, se ha establecido que en todos los equipos de la empresa, sean estos servidores, computadores de escritorio o portátiles, se mantenga levantado el firewall de Windows o el firewall proporcionado por el antivirus. Las licencias de antivirus con las que cuentan los equipos son Symantec.

Finalmente, se tienen bien establecidos los puertos que se encuentran abiertos y los protocolos con los que se puede acceder a cada uno de ellos, de manera que se limiten al máximo el número de accesos no permitidos.

4.2.1.2.3. Seguridades Implementadas en LOGICIEL

Dentro de la empresa se manejan Políticas y Procedimientos de Seguridad que cubren principalmente dos aspectos importantes: *seguridad a nivel de sistema*, y a *nivel de recurso humano*.

a) Seguridades a nivel de sistema

Entre las políticas a nivel sistema se tiene:

- Políticas para la clasificación y etiquetado de la información.
- Controles de seguridad administrativos, en donde se consideran los siguientes aspectos:
    - Propiedad exclusiva del material desarrollado
    - Acceso a Internet
- Controles para el acceso a la información y los servicios, y la protección en contra de robos.
- Políticas para la protección en contra de software malicioso, en donde se contempla la prevención y eliminación de virus.
- Políticas relacionadas con la seguridad de la red, lo que incluye:
    - Conexiones de red interna
    - Conexiones de red externa

- Cambios en la red
- Trabajo remoto

- Políticas para la asignación de propietarios de los activos con los que cuenta la empresa.
- Políticas de seguridad física, en donde se incluye:
  - Seguridad de servidores y racks de comunicación
  - Controles físicos de entrada
  - Suministro de energía eléctrica
  - Exposición al fuego
  - Mantenimiento de equipos
  - Seguridad en el área de trabajo
  - Difusión de los procedimientos y de las políticas de seguridad del personal
- Mecanismos para la eliminación segura de información
  - Medios de almacenamiento
  - Selección de la información a destruir
  - Mecanismos de destrucción de la información según su clasificación
- Políticas para la actualización de las estaciones de trabajo (computadores de escritorio y equipos portátiles) y servidores.
- Procedimientos para la generación, administración y restauración de respaldos.
- Procedimientos para verificar la correcta realización de respaldos.

b) Seguridad a nivel de recurso humano

Entre las políticas a nivel de recurso humano se tiene:

- Controles de seguridad técnicos, en donde se contempla:
  - Identificación y autenticación de usuario
  - Administración de cuentas de usuario
  - Políticas para las contraseñas implementadas
- Políticas con respecto al cumplimiento de las políticas y procedimientos de seguridad, además de las legislaciones y regulaciones definidas dentro de la empresa.

- Políticas para la asignación de roles y responsabilidades de acuerdo a las seguridades de información establecidas.
- Políticas para la definición de los acuerdos de confidencialidad con los empleados.
- Política para el uso aceptable de los servicios.
- Política para el uso aceptable de los contenidos.

4.2.1.2.4. Planes de Contingencia levantados en LOGICIEL

La empresa no cuenta con un plan formal para tratar las contingencias relacionadas con las TI. Dentro de las políticas y procedimientos de seguridad definidas en la empresa, se contemplan aspectos relacionados con esta temática como son la administración de respaldos, suministros de energía eléctrica, exposición al fuego, etc. Las cuales no se encuentran lo suficientemente detalladas.

4.2.2 PRIORIZACIÓN DE LOS PROCESOS DEL NEGOCIO DE LOGICIEL

Aplicando lo definido en la Sección 4.1.2, primero se deben establecer los intervalos de valores que van a determinar el nivel de prioridad, para lo cual se va a considerar lo siguiente:

1. Se tienen 7 objetivos críticos, los cuales se listaron previamente en la Sección 4.2.1.1.1.
2. El proceso más crítico y el menos crítico, serían igual a lo indicado en la Tabla 4-26:

Tabla 4-26 – Cálculo del valor de los procesos más y menos críticos

LISTA DE PROCESOS	Objetivos Estratégicos							Total por impacto del proceso en la estrategia del negocio	Análisis del valor agregado respecto al cliente	TOTAL
	Objetivo 1	Objetivo 2	Objetivo 3	Objetivo 4	Objetivo 5	Objetivo 6	Objetivo 7			
Proceso más critico	5	5	5	5	5	5	5	35	5	**175**
Proceso menos crítico	1	1	1	1	1	1	1	7	1	**7**

3. El rango entre el proceso más crítico y el menos crítico, es decir la diferencia entre sus puntos totales, es 168.

4. El ancho de cada intervalo se calcula dividiendo el rango calculado en el punto anterior dividido para el número de niveles de criticidad a considerar, es decir: 168 / 4, que daría como resultado 42.

En la Tabla 4-27, se encuentran los intervalos resultantes para cada nivel de prioridad.

Tabla 4-27 – Intervalos de valores por cada nivel de prioridad

Nivel de prioridad	Intervalos de valores
Crítico	133 – 175
Alto	91 – 132
Medio	49 – 90
Bajo	7 – 48

Para priorizar los procesos, es decir analizar el impacto de los procesos organizacionales en la estrategia del negocio y el valor agregado con respecto al cliente se va a tomar en consideración la escala de valoración establecida anteriormente la Tabla 4-1, que se muestra a continuación.

Escala	Valor
Muy Alto	5
Alto	4
Medio	3
Bajo	2
Muy Bajo	1

En la Tabla 4-28 se muestra la matriz de priorización de los procesos del negocio, ordenados en base al total, en donde se tiene que:

- Los procesos de prioridad crítica (señalados en rojo) son:
  - Implementación de paquetes de software
- Los procesos de prioridad alta (señalados en anaranjado) son:
  - Gestión de la calidad del software
  - Mantenimiento de software
  - Implementación de aplicaciones
  - Implantación de soluciones informáticas
  - Investigación y desarrollo

- Los procesos de prioridad media (señalados en amarillo) son:
    - Gestión financiera y administrativa
    - Administración de recursos computacionales
    - Gestión de la seguridad de la información
    - Marketing, venta y post-venta
- Los procesos de prioridad baja (señalados en verde) son:
    - Planeación estratégica y del negocio

De acuerdo a esto, los procesos organizacionales que van a ser objeto de aseguramiento y que requieren que sus activos y riesgos asociados sean identificados y valorados son aquellos con prioridad crítica y alta.

Tabla 4-28 – Matriz de priorización de procesos del negocio de LOGICIEL

LISTA DE PROCESOS	Objetivos Estratégicos							Total por impacto del proceso en la estrategia del negocio	Análisis del valor agregado respecto al cliente	TOTAL
	Objetivo 1	Objetivo 2	Objetivo 3	Objetivo 4	Objetivo 5	Objetivo 6	Objetivo 7			
Implementación de paquetes de software	1	5	5	1	5	5	5	27	5	**135**
Gestión de la calidad del software (SQM)	1	1	4	1	5	5	5	22	5	**110**
Mantenimiento de software	1	1	5	1	3	5	5	21	5	**105**
Implementación de aplicaciones	1	4	4	5	1	5	1	21	5	**105**
Implantación de soluciones informáticas	1	1	5	4	1	4	5	21	5	**105**
Investigación y desarrollo	1	5	4	1	5	4	5	25	4	**100**
Gestión financiera y administrativa	4	1	4	4	3	1	5	22	4	**88**
Administración de recursos computacionales	1	1	4	1	4	5	5	21	3	**63**
Gestión de la seguridad de la información	1	1	4	1	4	5	5	21	3	**63**
Marketing, venta y post-venta	3	3	3	3	1	1	5	19	3	**57**
Planeación estratégica y del negocio	2	4	3	1	3	3	5	21	2	**42**

4.2.3 EVALUACIÓN DE LOS ACTIVOS DE LOGICIEL

Aplicando lo establecido en la Sección 4.1.3, se va a proceder a identificar y valorar a los activos de la empresa LOGICIEL.

4.2.3.1 IDENTIFICACIÓN DE ACTIVOS

En la Tabla 4-29 se encuentra un inventario de todos los activos involucrados en cada proceso con prioridad crítica y alta.

Tabla 4-29 – Inventario de activos de LOGICIEL

ID ACTIVO	IDENTIFICACIÓN		TIPO ACTIVO					COMENTARIO
	Nombre Activo	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	
1	Acceso Remoto	Administrador de Recursos Computacionales					x	Es un servicio que se ofrece a aquellos empleados que requieran acceder a los recursos de la empresa desde afuera de la misma.
2	Administrador de Recursos Computacionales	Gerente de Desarrollo				x		Se encarga de la administración de bases de datos, sistemas operativos, redes y comunicaciones.
3	Antivirus	Administrador de Recursos Computacionales		x				Se encarga de detectar la presencia de virus informáticos en los computadores para posteriormente eliminarlos.
4	Aplicaciones de ofimática	Administrador de Recursos Computacionales		x				Se incluyen aplicaciones como Microsoft Office, Microsoft Project, Microsoft Visio, Bizagi, Dr. Explain, etc.
5	Aplicaciones desarrolladas por LOGICIEL	Gerente de Desarrollo		x				Se incluyen las siguientes aplicaciones: LOGICORBA, FASTrade, GAF, LogiFlow, GP, LogiScore, LOGISEG, LogiFTP, LogiSiEx, LogiNotificador y LogiGenDocs.
6	Aplicaciones utilizadas para el desarrollo de software	Administrador de Recursos Computacionales		x				Se incluyen las siguientes aplicaciones: Microsoft Visual Studio 2012, Team Foundation Server 2010, Power Designer, Kendo, Altova Umodel, Microsoft Sql Server 2008, etc.
7	Asistente de Gerencia	Gerente General, Gerente de Marketing				x		Se encarga del seguimiento de compromisos y negociaciones de la gerencia con los clientes.

ID ACTIVO	IDENTIFICACIÓN		TIPO ACTIVO					COMENTARIO
	Nombre Activo	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	
8	Bases de Datos	Administrador de Recursos Computacionales	x					Se incluyen las bases de datos tanto del ambiente de desarrollo como del ambiente de test.
9	Cableado de datos	Administrador de Recursos Computacionales			x			Permite la conexión y comunicación entre los distintos equipos que conforman la red.
10	Código fuente de las aplicaciones	Gerente de Desarrollo	x					Consiste en el conjunto de líneas de código con las instrucciones que debe seguir la computadora para ejecutar un programa.
11	Computadoras de Escritorio	Administrador de Recursos Computacionales			x			Se incluyen todos los equipos de escritorio utilizados por los empleados de la empresa.
12	Computadoras Portátiles	Administrador de Recursos Computacionales			x			Se incluyen todos los equipos portátiles utilizados por los empleados de la empresa.
13	Correo Electrónico	Administrador de Recursos Computacionales					x	Permite el intercambio de mensajes entre los empleados de la empresa y con los clientes.
14	Documentación de las aplicaciones	Gerente de Desarrollo	x					Se incluyen todos los entregables generados durante el proceso de desarrollo de las aplicaciones.
15	Documentación de las pruebas de software	Gerente de SQM	x					Contiene información detallada sobre las pruebas que se llevaron a cabo en las diferentes aplicaciones.

ID ACTIVO	IDENTIFICACIÓN		TIPO ACTIVO					COMENTARIO
	Nombre Activo	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	
16	Equipo de climatización	Administrador de Recursos Computacionales			x			En donde se incluyen los ventiladores y equipos de aire acondicionado utilizados para evitar el sobrecalentamiento de los servidores.
17	Equipo de desarrollo	Gerente de Desarrollo				x		Conformado por el líder de proyecto y los analistas programadores asignados a un proyecto de desarrollo.
18	Equipo de SQM	Gerente de SQM				x		Conformado por el líder de SQM y analistas de SQM asignados a un proyecto.
19	Equipos de telecomunicaciones	Administrador de Recursos Computacionales			x			Se cuenta con dos routers uno utilizado a nivel gerencia y otro a nivel corporativo. Además de switches para permitir la conexión entre equipos.
20	Firewall	Administrador de Recursos Computacionales		x				Se cuenta con dos firewalls que controlan el acceso no autorizado a la red a través de Internet.
21	Fuentes de Alimentación (UPS)	Administrador de Recursos Computacionales			x			Permite evitar que los equipos no se dañen cuando hay una interrupción de energía, se tiene uno en cada piso.
22	Gerente de Desarrollo	Gerente General				x		Define el modelo de desarrollo de software a aplicarse en los proyectos y lidera los proyectos de desarrollo de software.
23	Gerente de Producto	Gerente General				x		Define el alcance funcional de las aplicaciones a ser desarrolladas.
24	Gerente de SQM	Gerente General				x		Define las políticas, estándares, procedimientos, entregables y plantillas a ser utilizadas en los proyectos de desarrollo, de software para garantizar la calidad de los productos.

ID ACTIVO	IDENTIFICACIÓN		TIPO ACTIVO					COMENTARIO
	Nombre Activo	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	
25	Gerente General	Directorio de la Empresa				x		Se encarga de negociar con los clientes las propuestas presentadas y establecer los acuerdos para lograr la firma de contratos.
26	Impresoras	Administrador de Recursos Computacionales			x			Se cuenta con dos impresoras, una en cada piso.
27	Internet	Administrador de Recursos Computacionales					x	Permite la conexión con otras redes.
28	Políticas, estándares y procedimientos	Asistente de Gerencia	x					Se definen los lineamientos para el seguimiento, evaluación y gestión de los proyectos de desarrollo de software.
29	Red LAN	Administrador de Recursos Computacionales			x			Red local que comunica a todos los dispositivos de la empresa.
30	Red WLAN	Administrador de Recursos Computacionales			x			Red local inalámbrica.
31	Respaldos de las Bases de Datos	Administrador de Recursos Computacionales	x					Copias de seguridad de las bases de datos de la empresa, se extraen una vez al mes.
32	Servidor de Aplicaciones	Administrador de Recursos Computacionales			x			Se cuenta con dos servidores de aplicaciones uno para el ambiente de desarrollo y otro para el ambiente de test.

ID ACTIVO	IDENTIFICACIÓN		TIPO ACTIVO					COMENTARIO
	Nombre Activo	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	
33	Servidor de Base de Datos	Administrador de Recursos Computacionales			x			Se cuenta con dos servidores de bases de datos una para el ambiente de desarrollo y otro para el ambiente de test.
34	Share Point	Administrador de Recursos Computacionales					x	Repositorio en donde se tiene almacenada información relacionada con la empresa.
35	Telefonía IP	Administrador de Recursos Computacionales					x	Permite integrar en la misma red las comunicaciones de voz y datos.

4.2.3.2 VALORACIÓN DE ACTIVOS

Una vez valorados los activos identificados en la sección anterior de acuerdo a los atributos de la información definidos en la Sección 4.1.3.2 se deben establecer los intervalos de valores que van a determinar el nivel de criticidad de cada uno de los activos, para lo cual se va a considerar lo siguiente:

1. Se tienen 6 procesos críticos.
2. El activo más crítico y el menos crítico, serían igual a lo indicado en la Tabla 4-30:

Tabla 4-30 – Cálculo del valor de los activos más y menos críticos

ID ACTIVO	NOMBRE ACTIVO	Implementación de paquetes de Software			Gestión de la calidad de software			Mantenimiento de software			Implementación de Aplicaciones			Implantación de soluciones informáticas			Investigación y desarrollo			VALOR ACTIVO
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
1	Activo más crítico	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	90
2	Activo menos crítico	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	18

3. El rango entre el proceso más crítico y el menos crítico, es decir la diferencia entre sus puntos totales, es 72.
4. El ancho de cada intervalo se calcula dividiendo el rango calculado en el punto anterior dividido para el número de niveles de criticidad a considerar, es decir: 72 / 4, que daría como resultado 18.

En la Tabla 4-31, se encuentran los intervalos resultantes para cada nivel de prioridad.

Tabla 4-31 – Intervalos de valores por cada nivel de prioridad

Nivel de prioridad	Intervalos de valores
Crítico	72 – 90
Alto	54 – 71
Medio	36 – 53
Bajo	18 – 35

Para valorar los activos, se debe identificar que tan significativo es el aporte de cada activo a los atributos de la información que representan y que son los siguientes:

- **Confidencialidad**, para valorar este atributo se debe considerar los criterios establecidos anteriormente en la Tabla 4-4, la cual se muestra a continuación.

Escala	Valor	Criterio
Muy Alto	5	El conocimiento o divulgación no autorizada de la información que gestiona el activo impacta negativamente a toda la organización.
Alto	4	El conocimiento o divulgación no autorizada de la información que gestiona el activo impacta negativamente de manera leve a la organización. Además, impacta al proceso evaluado y a los otros procesos de la organización.
Medio	3	El conocimiento o divulgación no autorizada de la información que gestiona el activo impacta negativamente al proceso evaluado.
Bajo	2	El conocimiento o divulgación no autorizada de la información que gestiona el activo impacta negativamente de manera leve al proceso evaluado.
Muy Bajo	1	El conocimiento o divulgación no autorizada de la información que gestiona el activo no impacta negativamente al proceso.

El impacto que tendría la pérdida de confidencialidad sobre el activo de información de acuerdo a su tipo, se especifica anteriormente en la Tabla 4-5, la cual se muestra a continuación.

Tipo de activo	Impacto
Información	Individuo, entidad o proceso no autorizado que accede al activo de información.
Aplicación	Individuo, entidad o proceso no autorizado que conoce la existencia o parametrización del activo.
Infraestructura	Alguien que conoce que existe el elemento, su configuración o accede al activo sin autorización.

Tipo de activo	Impacto
Persona	Se hace uso inadecuado de la información privilegiada a la cual tiene acceso por el cargo o función que desempeña.
Servicio	Alguien que conoce su existencia, configuración o hace uso no autorizado del activo.

- **Integridad**, para valorar este atributo se debe considerar los criterios establecidos anteriormente en la Tabla 4-6, la cual se muestra a continuación.

Escala	Valor	Criterio
Muy Alto	5	La pérdida de exactitud, precisión y completitud del activo impacta negativamente a la organización.
Alto	4	La pérdida de exactitud, precisión y completitud del activo impacta negativamente de manera leve a la organización. Además, impacta al proceso evaluado y a los otros procesos de la organización.
Medio	3	La pérdida de exactitud, precisión y completitud del activo impacta negativamente al proceso evaluado.
Bajo	2	La pérdida de exactitud, precisión y completitud del activo impacta negativamente de manera leve al proceso evaluado.
Muy Bajo	1	La pérdida de exactitud, precisión y completitud del activo no impacta negativamente al proceso.

El impacto que tendría la pérdida de la integridad sobre el activo de información de acuerdo a su tipo, se especifica anteriormente en la Tabla 4-7, la cual se muestra a continuación.

Tipo de activo	Impacto
Información	Se pierde la completitud, exactitud o precisión del activo de información.
Aplicación	Se valora la completitud, exactitud o precisión de la parametrización del activo.
Infraestructura	El activo no efectúa las actividades de procesamiento o su función correctamente o es alterada su configuración indebidamente.
Persona	La persona produce datos errados o incompletos o de acuerdo con su rol toma decisiones equivocadas, por capacidades o aptitudes inadecuadas para desempañar el rol o función.
Servicio	Se valora la completitud, exactitud o precisión del servicio.

- **Disponibilidad**, para valorar este atributo se debe considerar los criterios establecidos anteriormente en la Tabla 4-8, la cual se muestra a continuación.

Escala	Valor	Criterio
Muy Alto	5	La falta o no disponibilidad del activo impacta negativamente a la organización.
Alto	4	La falta o no disponibilidad del activo impacta negativamente de manera leve a la organización. Además, impacta al proceso evaluado y a los otros procesos de la organización.
Medio	3	La falta o no disponibilidad del activo impacta negativamente al proceso evaluado.
Bajo	2	La falta o no disponibilidad del activo impacta negativamente de manera leve al proceso evaluado.
Muy Bajo	1	La falta o no disponibilidad del activo no impacta negativamente al proceso.

El impacto que tendría la pérdida de la disponibilidad sobre el activo de información de acuerdo a su tipo, se especifica anteriormente en la Tabla 4-9 que se muestra a continuación.

Tipo de activo	Impacto
Información	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado.
Aplicación	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado.
Infraestructura	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado.
Persona	La persona no se encuentra disponible para el proceso.
Servicio	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado.

En la Tabla 4-32 se muestra la matriz de valoración de activos, ordenados en base al valor total del activo, en donde se tiene que:

- Los activos de prioridad crítica se encuentran señalados en rojo.
- Los activos de prioridad alta se encuentran señalados en anaranjado.
- Los activos de prioridad media se encuentran señalados en amarillo.
- Los activos de prioridad baja se encuentran señalados en verde.

De acuerdo a esto, los activos con prioridad crítica y alta son aquellos que se considerarán para los posteriores análisis a realizarse.

Tabla 4-32 – Matriz de valoración de activos de LOGICIEL

ID ACTIVO	NOMBRE ACTIVO	Implementación de paquetes de software			Gestión de la calidad de software			Mantenimiento de software			Implementación de aplicaciones			Implantación de soluciones informáticas			Investigación y desarrollo			VALOR ACTIVO
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
8	Bases de Datos	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	2	2	1	80
5	Aplicaciones desarrolladas por LOGICIEL	5	5	5	4	5	5	5	5	5	2	5	5	5	5	5	1	2	1	75
10	Código fuente de las aplicaciones	5	5	5	5	5	1	5	5	4	5	5	4	5	5	1	2	2	1	70
20	Firewall	5	4	2	5	4	2	5	4	2	5	4	2	5	4	2	5	4	1	65
32	Servidor de Aplicaciones	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	1	3	1	64
33	Servidor de Base de Datos	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	1	3	1	64
2	Administrador de Recursos Computacionales	5	4	3	5	4	3	5	4	3	3	4	3	4	4	3	2	2	2	63
13	Correo Electrónico	5	3	3	5	3	3	5	3	3	5	3	3	5	3	3	2	3	1	61
34	Share Point	3	4	3	3	4	3	3	4	3	3	4	3	3	4	3	3	4	3	60
14	Documentación de las aplicaciones	4	4	3	4	4	3	4	4	3	4	4	3	4	4	3	1	1	1	58

ID ACTIVO	NOMBRE ACTIVO	Implementación de paquetes de software			Gestión de la calidad de software			Mantenimiento de software			Implementación de aplicaciones			Implantación de soluciones informáticas			Investigación y desarrollo			VALOR ACTIVO
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
15	Documentación de las pruebas de software	4	4	3	4	4	3	4	4	3	4	4	3	4	4	3	1	1	1	58
17	Equipo de desarrollo	4	4	4	3	4	3	4	4	4	4	4	4	3	4	1	1	2	1	58
18	Equipo de SQM	3	4	3	4	4	4	4	4	4	3	4	3	3	4	4	1	1	1	58
11	Computadoras de Escritorio	4	3	3	4	3	3	4	3	3	4	3	3	4	3	2	4	3	1	57
22	Gerente de Desarrollo	4	4	3	3	4	3	3	4	3	4	4	3	3	4	3	2	2	1	57
7	Asistente de Gerencia	4	5	1	4	5	1	4	5	1	4	5	1	4	5	3	1	2	1	56
31	Respaldos de las Bases de Datos	4	5	2	4	4	2	3	5	2	4	5	2	2	5	2	1	2	2	56
23	Gerente de Producto	4	4	3	2	4	3	2	4	3	4	4	3	2	4	3	2	2	1	54
9	Cableado de datos	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3	53
25	Gerente General	2	5	1	2	5	1	2	5	1	2	5	1	4	5	3	1	5	1	51
24	Gerente de SQM	3	4	1	4	4	3	3	4	3	3	4	1	3	4	3	1	1	1	50
29	Red LAN	3	2	3	3	2	3	3	2	3	3	2	3	3	2	3	3	2	3	48
12	Computadoras Portátiles	2	3	3	2	3	1	3	3	3	2	3	3	3	3	1	2	3	1	44

ID ACTIVO	NOMBRE ACTIVO	Implementación de paquetes de software			Gestión de la calidad de software			Mantenimiento de software			Implementación de aplicaciones			Implantación de soluciones informáticas			Investigación y desarrollo			VALOR ACTIVO
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
19	Equipos de telecomunicaciones	3	2	3	2	2	2	3	2	3	3	2	2	3	2	2	1	1	1	39
27	Internet	1	2	2	1	2	2	3	2	3	1	2	2	2	2	3	2	2	3	37
16	Equipo de climatización	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	36
28	Políticas, estándares y procedimientos	1	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	3	2	36
6	Aplicaciones utilizadas para el desarrollo de software	1	3	3	1	2	1	1	3	3	1	2	3	1	2	1	1	3	3	35
1	Acceso Remoto	4	2	1	2	2	1	2	2	2	2	2	1	2	2	2	1	1	1	32
3	Antivirus	2	2	1	2	2	1	2	2	1	2	2	1	2	2	1	2	2	1	30
4	Aplicaciones de ofimática	1	2	2	1	2	2	1	2	2	1	2	2	1	2	2	1	2	2	30
35	Telefonía IP	1	1	1	1	1	1	2	2	2	1	2	2	2	2	2	1	1	1	26
21	Fuentes de Alimentación (UPS)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	18
26	Impresora	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	18
30	Red WLAN	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	18

4.2.4 POLÍTICA DE PLANIFICACIÓN DE CONTINGENCIAS

La política de planificación de contingencias de LOGICIEL se la debe hacer en base al modelo de política definido en la Sección 4.1.8 (Anexo A).

4.2.5 EVALUACIÓN DE RIESGOS

En esta fase se busca estimar el riesgo asociado a los activos críticos. Para cada una de las amenazas identificadas para cada uno de los activos críticos se debe valorar los siguientes aspectos:

- **Efectividad de controles existentes**, para valorar este punto se debe considerar los criterios establecidos anteriormente en la Tabla 4-12, la cual se muestra a continuación.

Escala	Valor	Criterio
Muy Adecuado	5	El control existente disminuye casi toda la probabilidad de ocurrencia y el impacto de la amenaza.
Adecuado	4	El control existente disminuye en gran medida la probabilidad de ocurrencia y el impacto de la amenaza.
Moderado	3	El control existente disminuye de manera moderada la probabilidad de ocurrencia y el impacto de la amenaza.
Débil	2	El control existente disminuye levemente la probabilidad de ocurrencia y el impacto de la amenaza.
Muy débil	1	El control existente no ayuda a disminuir la probabilidad de ocurrencia y el impacto de la amenaza.

- **Probabilidad**, para valorar este punto se debe considerar los criterios establecidos anteriormente en la Tabla 4-13, la cual se muestra a continuación.

Escala	Valor	Criterio
Muy Alta	5	Es casi seguro que la amenaza (error, accidente o acto de la naturaleza) ocurra.
Alta	4	Es altamente probable que la amenaza (error, accidente o acto de la naturaleza) ocurra.
Media	3	Es algo probable que la amenaza (error, accidente o acto de la naturaleza) ocurra.
Baja	2	Es improbable que la amenaza (error, accidente o acto de la naturaleza) ocurra.
Muy Baja	1	Es altamente improbable (raro) que la amenaza (error, accidente o acto de la naturaleza) ocurra.

- **Impacto**, para valorar este punto se debe considerar los criterios establecidos anteriormente en la Tabla 4-14, la cual se muestra a continuación.

Escala	Valor	Criterio
Muy Alto	5	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar múltiples efectos adversos graves o catastróficos en las operaciones, activos o individuos de la organización.
Alto	4	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso grave o catastrófico en las operaciones, activos o individuos de la organización.
Medio	3	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un serio efecto adverso en las operaciones, activos o individuos de la organización.
Bajo	2	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso limitado en las operaciones, activos o individuos de la organización.
Muy Bajo	1	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso insignificante en las operaciones, activos o individuos de la organización.

- **Nivel de riesgo**, se debe multiplicar los valores establecidos tanto para la probabilidad como para el impacto, y clasificar el resultado obtenido en base a los criterios establecidos anteriormente en la Tabla 4-16, la cual se muestra a continuación.

Escala	Valor	Criterio
Muy Alto	21 – 25	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar múltiples efectos adversos graves o catastróficos en las operaciones, activos o individuos de la organización.
Alto	16 – 20	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso grave o catastrófico en las operaciones, activos o individuos de la organización.
Medio	11 – 15	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un serio efecto adverso en las operaciones, activos o individuos de la organización.
Bajo	6 – 10	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso limitado en las operaciones, activos o individuos de la organización.
Muy Bajo	1 – 5	La amenaza (error, accidente o acto de la naturaleza) puede ocasionar un efecto adverso insignificante en las operaciones, activos o individuos de la organización.

A continuación, se indica el nivel de riesgo de cada una de las amenazas identificadas para cada uno de ellos ordenado por el nivel de criticidad de cada activo.

ID Activo: 8

Nombre Activo: Base de datos

Nivel de Criticidad: Crítico

En la Tabla 4-33 se muestran los riesgos relacionados con la base de datos ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel medio, que puede tener un serio efecto adverso en el activo.
- 7 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 16 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-33 – Evaluación de riesgos Base de datos

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
7	Avería de tipo físico o lógico			3	4	12
14	Daños por agua / Inundaciones			3	4	12
20	Desastres naturales			2	5	10
13	Corte de suministro eléctrico	x	4	3	3	9
17	Degradación de los soportes de almacenamiento de la información	x	5	3	3	9
31	Errores de usuarios	x	4	3	3	9
32	Errores del administrador			3	3	9
35	Fuego / Incendios	x	2	2	4	8
26	Errores de configuración			2	3	6
1	Abuso de privilegios de acceso	x	5	2	2	4
52	Suplantación de la identidad del usuario	x	5	2	2	4
3	Alteración de la información	x	4	1	1	1
12	Corrupción de la información			1	1	1

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
16	Degradación de la información			1	1	1
22	Destrucción accidental de información			1	1	1
21	Destrucción deliberada de información			1	1	1
24	Divulgación de información			1	1	1
29	Errores de monitorización (log)	x	5	1	1	1
40	Inserción de información incorrecta	x	4	1	1	1
41	Intercepción de información	x	5	1	1	1
44	Manipulación de la configuración	x	5	1	1	1
45	Manipulación de los registros de actividad (log)	x	4	1	1	1
47	Modificación deliberada de la información			1	1	1
50	Repudio	x	5	1	1	1
51	Robo	x	3	1	1	1

ID Activo: 5

Nombre Activo: Aplicaciones desarrolladas por LOGICIEL

Nivel de Criticidad: Crítico

En la Tabla 4-34 se muestran los riesgos relacionados con las aplicaciones desarrolladas por LOGICIEL ordenados por el nivel de riesgo, en donde se puede observar:

- 2 riesgos de nivel medio, que pueden tener un serio efecto adverso en el activo.
- 6 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 6 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-34 – Evaluación de riesgos Aplicaciones desarrolladas por LOGICIEL

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
7	Avería de tipo físico o lógico			3	4	12
54	Vulnerabilidades de los programas	x	5	3	4	12
31	Errores de usuarios	x	4	5	2	10
26	Errores de configuración			3	3	9
32	Errores del administrador			3	3	9
28	Errores de mantenimiento / actualizaciones de programas (Software)			2	4	8
44	Manipulación de la configuración	x	5	2	4	8
29	Errores de monitorización (log)	x	5	2	3	6
1	Abuso de privilegios de acceso	x	5	1	4	4
2	Acceso no autorizado	x	5	1	4	4
3	Alteración de la información	x	4	1	4	4
46	Manipulación de programas	x	4	1	4	4
47	Modificación deliberada de la información			1	4	4
52	Suplantación de la identidad del usuario	x	5	1	3	3

ID Activo: 10

Nombre Activo: Código fuente de las aplicaciones

Nivel de Criticidad: Alto

En la Tabla 4-35 se muestran los riesgos relacionados con el código fuente de las aplicaciones ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel medio, que puede tener un serio efecto adverso en el activo.
- 8 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 13 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-35 – Evaluación de riesgos Código fuente de las aplicaciones

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
14	Daños por agua / Inundaciones			3	4	12
20	Desastres naturales			2	5	10
7	Avería de tipo físico o lógico			3	3	9
13	Corte de suministro eléctrico	x	4	3	3	9
17	Degradación de los soportes de almacenamiento de la información	x	5	3	3	9
31	Errores de usuarios	x	4	3	3	9
35	Fuego / Incendios	x	2	2	4	8
1	Abuso de privilegios de acceso		5	2	3	6
32	Errores del administrador			3	2	6
51	Robo	x	3	1	5	5
26	Errores de configuración			2	2	4
12	Corrupción de la información			1	3	3
21	Destrucción deliberada de información			1	3	3
24	Divulgación de información			1	3	3
29	Errores de monitorización (log)	x	5	1	3	3
47	Modificación deliberada de la información			1	3	3
3	Alteración de la información	x	4	1	2	2
41	Intercepción de información	x	5	1	2	2
44	Manipulación de la configuración	x	4	1	2	2
45	Manipulación de los registros de actividad (log)	x	4	1	2	2
50	Repudio	x	5	1	2	2
52	Suplantación de la identidad del usuario	x	5	1	1	1

ID Activo: 20

Nombre Activo: Firewall

Nivel de Criticidad: Alto

En la Tabla 4-36 se muestran los riesgos relacionados con el Firewall ordenados por el nivel de riesgo, en donde se puede observar:

- 3 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.

- 3 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-36 – Evaluación de riesgos Firewall

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
7	Avería de tipo físico o lógico			3	3	9
26	Errores de configuración			3	3	9
28	Errores de mantenimiento / actualizaciones de programas (Software)			3	3	9
29	Errores de monitorización (log)	x	5	3	2	6
32	Errores del administrador			3	2	6
44	Manipulación de la configuración			2	3	6

ID Activo: 32

Nombre Activo: Servidor de aplicaciones

Nivel de Criticidad: Alto

En la Tabla 4-37 se muestran los riesgos relacionados con el servidor de aplicaciones ordenados por el nivel de riesgo, en donde se puede observar:

- 3 riesgos de nivel medio, que pueden tener un serio efecto adverso en el activo.
- 8 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 5 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-37 – Evaluación de riesgos Servidor de aplicaciones

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
7	Avería de tipo físico o lógico			3	4	12
14	Daños por agua / Inundaciones			3	4	12
17	Degradación de los soportes de almacenamiento de la información	x	5	3	4	12
51	Robo	x	3	2	5	10
13	Corte de suministro eléctrico	x	4	3	3	9
26	Errores de configuración			3	3	9
20	Desastres naturales			2	4	8
35	Fuego / Incendios	x	2	2	4	8
9	Condiciones inadecuadas de temperatura o humedad	x	4	2	3	6
27	Errores de mantenimiento / actualizaciones de equipos (Hardware)	x	4	2	3	6
32	Errores del administrador			3	2	6
6	Ataque destructivo			1	4	4
43	Manipulación de equipos	x	3	1	4	4
49	Pérdida de equipos	x	5	1	4	4
53	Uso no previsto	x	4	2	2	4
2	Acceso no autorizado	x	3	1	3	3

ID Activo: 33

Nombre Activo: Servidor de base de datos

Nivel de Criticidad: Alto

En la Tabla 4-38 se muestran los riesgos relacionados con el servidor de base de datos ordenados por el nivel de riesgo, en donde se puede observar que:

- 3 riesgos de nivel medio, que pueden tener un serio efecto adverso en el activo.
- 8 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.

- 4 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-38 – Evaluación de riesgos Servidor de base de datos

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
7	Avería de tipo físico o lógico			3	5	15
17	Degradación de los soportes de almacenamiento de la información	x	5	3	5	15
14	Daños por agua / Inundaciones			3	4	12
51	Robo	x	3	2	5	10
13	Corte de suministro eléctrico	x	4	3	3	9
26	Errores de configuración			3	3	9
32	Errores del administrador			3	3	9
20	Desastres naturales			2	4	8
35	Fuego / Incendios	x	2	2	4	8
9	Condiciones inadecuadas de temperatura o humedad	x	4	2	3	6
27	Errores de mantenimiento / actualizaciones de equipos (Hardware)	x	4	2	3	6
2	Acceso no autorizado	x	3	1	4	4
6	Ataque destructivo			1	4	4
43	Manipulación de equipos	x	3	1	4	4
49	Pérdida de equipos	x	5	1	4	4
53	Uso no previsto	x	4	2	2	4

ID Activo: 2

Nombre Activo: Administrador de recursos computacionales

Nivel de Criticidad: Alto

En la Tabla 4-39 se muestran los riesgos relacionados con el Administrador de recursos computacionales ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 3 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-39 – Evaluación de riesgos Administrador de recursos computacionales

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
37	Indisponibilidad accidental del personal			3	3	9
36	Fugas de información	x	5	1	3	3
38	Indisponibilidad deliberada del personal			1	3	3
39	Ingeniería social			1	2	2

ID Activo: 13

Nombre Activo: Correo electrónico

Nivel de Criticidad: Alto

En la Tabla 4-40 se muestran los riesgos relacionados con el Correo electrónico ordenados por el nivel de riesgo, en donde se puede observar:

- 3 riesgos de nivel medio, que pueden tener un serio efecto adverso en el activo.
- 5 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 13 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-40 – Evaluación de riesgos Correo electrónico

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
14	Daños por agua / Inundaciones			3	4	12
34	Fallo de servicios de comunicaciones			3	4	12
53	Uso no previsto	x	3	4	3	12
20	Desastres naturales			2	5	10
36	Fugas de información	x	3	3	3	9
42	Interrupción de otros servicios y suministros esenciales			3	3	9
35	Fuego / Incendios	x	2	2	4	8
44	Manipulación de la configuración	x	4	2	3	6
18	Denegación de servicio			2	2	4
26	Errores de configuración			2	2	4
3	Alteración de la información	x	4	1	3	3
22	Destrucción accidental de información			1	3	3
25	Errores de (re)encaminamiento			1	3	3
30	Errores de secuencia			1	3	3
47	Modificación deliberada de la información			1	3	3
50	Repudio	x	5	1	3	3
52	Suplantación de la identidad del usuario	x	5	1	3	3
8	Caída del sistema por agotamiento de recursos	x	3	1	2	2
29	Errores de monitorización (log)	x	5	2	1	2
32	Errores del administrador			2	1	2
31	Errores de usuarios	x	4	1	1	1

ID Activo: 24

Nombre Activo: Sharepoint

Nivel de Criticidad: Alto

En la Tabla 4-41 se muestran los riesgos relacionados con el Sharepoint ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel medio, que puede tener un serio efecto adverso en el activo.
- 7 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.

- 13 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-41 – Evaluación de riesgos Sharepoint

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
14	Daños por agua / Inundaciones			3	4	12
20	Desastres naturales			2	5	10
34	Fallo de servicios de comunicaciones			3	3	9
36	Fugas de información	x	3	3	3	9
42	Interrupción de otros servicios y suministros esenciales			3	3	9
35	Fuego / Incendios	x	2	2	4	8
26	Errores de configuración			2	3	6
44	Manipulación de la configuración	x	4	2	3	6
18	Denegación de servicio			2	2	4
32	Errores del administrador			2	2	4
1	Abuso de privilegios de acceso	x	5	1	3	3
3	Alteración de la información	x	4	1	3	3
47	Modificación deliberada de la información			1	3	3
22	Destrucción accidental de información			1	2	2
29	Errores de monitorización (log)	x	5	2	1	2
31	Errores de usuarios	x	4	1	2	2
51	Robo	x	3	1	2	2
8	Caída del sistema por agotamiento de recursos	x	3	1	1	1
25	Errores de (re)encaminamiento			1	1	1
30	Errores de secuencia			1	1	1
52	Suplantación de la identidad del usuario	x	5	1	1	1

ID Activo: 14

Nombre Activo: Documentación de las aplicaciones

Nivel de Criticidad: Alto

En la Tabla 4-42 se muestran los riesgos relacionados con la Documentación de las aplicaciones ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel medio, que puede tener un serio efecto adverso en el activo.
- 6 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 11 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-42 – Evaluación de riesgos Documentación de las aplicaciones

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
14	Daños por agua / Inundaciones			3	4	12
20	Desastres naturales			2	5	10
13	Corte de suministro eléctrico	x	4	3	3	9
17	Degradación de los soportes de almacenamiento de la información	x	5	3	3	9
31	Errores de usuarios	x	4	3	3	9
35	Fuego / Incendios	x	2	2	4	8
7	Avería de tipo físico o lógico			3	2	6
51	Robo	x	3	1	5	5
12	Corrupción de la información			1	4	4
3	Alteración de la información	x	4	1	3	3
21	Destrucción deliberada de información			1	3	3
24	Divulgación de información			1	3	3
29	Errores de monitorización (log)	x	5	1	2	2
47	Modificación deliberada de la información			1	2	2
50	Repudio	x	5	1	2	2
1	Abuso de privilegios de acceso		5	1	1	1
41	Intercepción de información	x	5	1	1	1
45	Manipulación de los registros de actividad (log)	x	4	1	1	1

ID Activo: 15

Nombre Activo: Documentación de las pruebas de software

Nivel de Criticidad: Alto

En la Tabla 4-43 se muestran los riesgos relacionados con la Documentación de las pruebas de software ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel medio, que puede tener un serio efecto adverso en el activo.
- 6 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 11 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-43 – Evaluación de riesgos Documentación de las pruebas de software

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
14	Daños por agua / Inundaciones			3	4	12
20	Desastres naturales			2	5	10
13	Corte de suministro eléctrico	x	4	3	3	9
17	Degradación de los soportes de almacenamiento de la información	x	5	3	3	9
31	Errores de usuarios	x	4	3	3	9
35	Fuego / Incendios	x	2	2	4	8
7	Avería de tipo físico o lógico			3	2	6
51	Robo	x	3	1	5	5
12	Corrupción de la información			1	4	4
3	Alteración de la información	x	4	1	3	3
21	Destrucción deliberada de información			1	3	3
24	Divulgación de información			1	3	3
29	Errores de monitorización (log)	x	5	1	2	2
47	Modificación deliberada de la información			1	2	2
50	Repudio	x	5	1	2	2
1	Abuso de privilegios de acceso		5	1	1	1
41	Intercepción de información	x	5	1	1	1
45	Manipulación de los registros de actividad (log)	x	4	1	1	1

ID Activo: 17

Nombre Activo: Equipo de desarrollo

Nivel de Criticidad: Alto

En la Tabla 4-44 se muestran los riesgos relacionados con el equipo de desarrollo ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 3 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-44 – Evaluación de riesgos Equipo de desarrollo

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
37	Indisponibilidad accidental del personal			3	3	9
36	Fugas de información	x	5	1	4	4
39	Ingeniería social			1	3	3
38	Indisponibilidad deliberada del personal			1	2	2

ID Activo: 18

Nombre Activo: Equipo de SQM

Nivel de Criticidad: Alto

En la Tabla 4-45 se muestran los riesgos relacionados con el Equipo de SQM ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 3 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-45 – Evaluación de riesgos Equipo de SQM

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
37	Indisponibilidad accidental del personal			3	3	9
36	Fugas de información	x	5	1	4	4
39	Ingeniería social			1	3	3
38	Indisponibilidad deliberada del personal			1	2	2

ID Activo: 11

Nombre Activo: Computadoras de escritorio

Nivel de Criticidad: Alto

En la Tabla 4-46 se muestran los riesgos relacionados con las computadoras de escritorio ordenados por el nivel de riesgo, en donde se puede observar:

- 4 riesgos de nivel medio, que pueden tener un serio efecto adverso en el activo.
- 5 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 7 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-46 – Evaluación de riesgos Computadoras de escritorio

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
7	Avería de tipo físico o lógico			3	4	12
13	Corte de suministro eléctrico	x	4	3	4	12
14	Daños por agua / Inundaciones			3	4	12

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
17	Degradación de los soportes de almacenamiento de la información	x	5	3	4	12
32	Errores del administrador			3	3	9
20	Desastres naturales			2	4	8
35	Fuego / Incendios	x	2	2	4	8
51	Robo	x	3	2	4	8
26	Errores de configuración			3	2	6
9	Condiciones inadecuadas de temperatura o humedad	x	4	2	2	4
27	Errores de mantenimiento / actualizaciones de equipos (Hardware)	x	4	2	2	4
49	Pérdida de equipos	x	5	1	4	4
53	Uso no previsto	x	4	2	2	4
6	Ataque destructivo			1	3	3
43	Manipulación de equipos	x	3	1	3	3
2	Acceso no autorizado	x	3	1	2	2

ID Activo: 22

Nombre Activo: Gerente de desarrollo

Nivel de Criticidad: Alto

En la Tabla 4-47 se muestran los riesgos relacionados con el gerente de desarrollo ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel medio, que puede tener un serio efecto adverso en el activo.
- 3 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-47 – Evaluación de riesgos Gerente de desarrollo

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
31	Indisponibilidad accidental del personal			3	4	12
21	Fugas de Información	x	5	1	5	5
54	Ingeniería social			1	4	4
52	Indisponibilidad del personal			1	3	3

ID Activo: 7

Nombre Activo: Asistente de gerencia

Nivel de Criticidad: Alto

En la Tabla 4-48 se muestran los riesgos relacionados con el asistente de gerencia ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 3 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-48 – Evaluación de riesgos Asistente de gerencia

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
37	Indisponibilidad accidental del personal			3	2	6
36	Fugas de información	x	5	1	5	5
39	Ingeniería social			1	3	3
38	Indisponibilidad deliberada del personal			1	2	2

ID Activo: 31

Nombre Activo: Respaldos de las bases de datos

Nivel de Criticidad: Alto

En la Tabla 4-49 se muestran los riesgos relacionados con los Respaldos de las Bases de datos ordenados por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel medio, que puede tener un serio efecto adverso en el activo.
- 7 riesgos de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 15 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-49 – Evaluación de riesgos Respaldos de las bases de datos

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
14	Daños por agua / Inundaciones			3	4	12
20	Desastres naturales			2	5	10
7	Avería de tipo físico o lógico			3	3	9
17	Degradación de los soportes de almacenamiento de la información	x	5	3	3	9
35	Fuego / Incendios	x	2	2	4	8
13	Corte de suministro eléctrico	x	4	3	2	6
31	Errores de usuarios	x	4	3	2	6
32	Errores del administrador			3	2	6
12	Corrupción de la información			1	4	4
24	Divulgación de información			1	4	4
26	Errores de configuración			2	2	4
51	Robo	x	3	1	4	4
16	Degradación de la información			1	3	3
21	Destrucción accidental de información			1	3	3
22	Destrucción deliberada de información			1	3	3
47	Modificación deliberada de la información			1	3	3
1	Abuso de privilegios de acceso	x	5	2	1	2
41	Intercepción de información	x	5	1	2	2

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
44	Manipulación de la configuración	x	4	1	2	2
52	Suplantación de la identidad del usuario	x	5	2	1	2
29	Errores de monitorización (log)	x	5	1	1	1
45	Manipulación de los registros de actividad (log)	x	4	1	1	1
50	Repudio	x	5	1	1	1

ID Activo: 2

Nombre Activo: Gerente de producto

Nivel de Criticidad: Alto

En la Tabla 4-50 se muestran los riesgos relacionados con el Gerente de producto por el nivel de riesgo, en donde se puede observar:

- 1 riesgo de nivel bajo, cuyo efecto puede ser limitado en el activo.
- 3 riesgos de nivel muy bajo, cuyo efecto puede resultar insignificante para el activo.

Tabla 4-50 – Evaluación de riesgos Gerente de producto

AMENAZA		Controles existentes		Riesgos		
ID	NOMBRE	Tiene un control	Efectividad del control	Probabilidad	Impacto	Nivel de Riesgo
37	Indisponibilidad accidental del personal			3	2	6
36	Fugas de información	x	5	1	5	5
39	Ingeniería social			1	3	3
38	Indisponibilidad deliberada del personal			1	2	2

4.2.6 ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)

En esta paso se busca determinar el impacto que una interrupción tendría en cada uno de los procesos críticos de LOGICIEL.

4.2.6.1 DETERMINACIÓN DEL IMPACTO DE UNA INTERRUPCIÓN

La determinación del impacto de una interrupción se debe valorar en base a las siguientes categorías:

- **Impacto al cliente**, en esta categoría se deben considerar los criterios establecidos anteriormente en la Tabla 4-17, la cual se muestra a continuación:

Escala	Valor	Criterio
Severo	3	La interrupción puede ocasionar que el que el nivel de servicio se vea completamente comprometido, haciendo que el cliente opte por contratar a otra empresa.
Moderado	2	La interrupción puede ocasionar que el nivel de servicio se vea altamente comprometido.
Mínimo	1	La interrupción puede ocasionar que el nivel de servicio se vea levemente comprometido.

- **Impacto Financiero**, en esta categoría se deben considerar los criterios establecidos anteriormente en la Tabla 4-18, la cual se muestra a continuación:

Escala	Valor	Criterio
Severo	3	La interrupción puede ocasionar que se vean comprometidas las ventas futuras.
Moderado	2	La interrupción puede ocasionar que se tengan pérdidas de ingresos.
Mínimo	1	La interrupción puede ocasionar que se tenga que pagar multas o sanciones por incumplimiento de contrato.

- **Impacto Operacional**, en esta categoría se deben considerar los criterios establecidos anteriormente en la Tabla 4-19, la cual se muestra a continuación:

Escala	Valor	Criterio
Severo	3	La interrupción puede ocasionar que no se puedan cumplir con los plazos establecidos.
Moderado	2	La interrupción puede ocasionar que se reduzca el nivel de servicio ofrecido.

Escala	Valor	Criterio
Mínimo	1	La interrupción puede ocasionar que se vea interrumpido el flujo de trabajo de la organización.

- **Impacto Reputacional**, en esta categoría se deben considerar los criterios establecidos anteriormente en la Tabla 4-20, la cual se muestra a continuación:

Escala	Valor	Criterio
Severo	3	La interrupción puede ocasionar que se tenga atención negativa de los medios de comunicación.
Moderado	2	La interrupción puede ocasionar que se pierda la confianza de los accionistas.
Mínimo	1	La interrupción puede ocasionar que el competidor tome ventaja de la atención negativa que tiene la empresa.

En la Tabla 4-51 se va a determinar el impacto que tendría una interrupción en cada uno de los procesos críticos del negocio identificados en la Sección 4.2.2, en donde se encuentran ordenados por el valor total del impacto.

Tabla 4-51 – Impacto de una interrupción en los procesos críticos de LOGICIEL

Proceso del Negocio	Impacto				Total
	Al Cliente	Financiero	Operacional	Reputacional	
Implantación de soluciones informáticas	3	3	3	2	11
Mantenimiento de software	2	3	3	1	9
Implementación de aplicaciones	2	3	3	1	9
Implementación de paquetes de software	2	2	2	2	8
Gestión de la calidad del software (SQM)	2	1	2	1	6
Investigación y desarrollo	1	1	2	1	5

4.2.6.2 DETERMINACIÓN DE LOS PARÁMETROS DE RECUPERACIÓN

En la Tabla 4-52 se especifica el tiempo máximo de inactividad (MTD), el tiempo objetivo de recuperación (RTO) y el punto objetivo de recuperación, para cada uno de los procesos críticos del negocio identificados en la Sección 4.2.2.

Tabla 4-52 – Parámetros de recuperación de los procesos críticos de LOGICIEL

Procesos del Negocio	MTD	RTO	RPO
Implementación de paquetes de software	48 horas	24 horas	12 horas
Gestión de la calidad del software (SQM)	36 horas	18 horas	6 horas
Mantenimiento de software	36 horas	18 horas	6 horas
Implementación de aplicaciones	48 horas	24 horas	12 horas
Implantación de soluciones informáticas	24 horas	12 horas	6 horas
Investigación y desarrollo	72 horas	48 horas	24 horas

4.2.6.3 IDENTIFICAR LOS RECURSOS MÍNIMOS REQUERIDOS

En la Tabla 4-53 que se muestra a continuación, se listan los recursos mínimos requeridos para restaurar los procesos críticos del negocio de LOGICIEL lo más pronto posible.

Tabla 4-53 – Inventario de recursos mínimos requeridos

ID	Nombre Recurso	Descripción
1	Aplicaciones de ofimática	Se incluyen aplicaciones como: Microsoft Office, Microsoft Project, Microsoft Visio, Bizagi, Dr. Explain, etc.
2	Aplicaciones desarrolladas por LOGICIEL	Se incluyen las siguientes aplicaciones: LOGICORBA, FASTrade, GAF, LogiFlow, GP, LogiScore, LOGISEG, LogiFTP, LogiSiEx, LogiNotificador y LogiGenDocs.
3	Aplicaciones utilizadas para el desarrollo de software	Se incluyen las siguientes aplicaciones: Microsoft Visual Studio 2012, Team Foundation Server 2010, Power Designer, Kendo, Altova Umodel, Microsoft Sql Server 2008, etc.
4	Bases de Datos	Se incluyen las Bases de Datos tanto del ambiente de desarrollo como del ambiente de test.
5	Cableado de datos	Permite la conexión y comunicación entre los distintos equipos que conforman la red.
6	Código fuente de las aplicaciones	Consiste en el conjunto de líneas de código con las instrucciones que debe seguir la computadora para ejecutar un programa.
7	Computadoras de Escritorio	Se incluyen todos los equipos de escritorio utilizados por los empleados de la empresa.
8	Documentación de las aplicaciones	Se incluyen todos los entregables generados durante el proceso de desarrollo de las aplicaciones.
9	Documentación de las pruebas de software	Contiene información detalla sobre las pruebas que se llevaron a cabo en las diferentes aplicaciones.
10	Equipo de climatización	En donde se incluyen los ventiladores y equipos de aire acondicionado utilizados para evitar el sobrecalentamiento de los servidores.

ID	Nombre Recurso	Descripción
11	Equipo de desarrollo	Conformado por el líder de proyecto y los analistas programadores asignados a un proyecto de desarrollo.
12	Equipo de SQM	Conformado por el líder de SQM y analistas de SQM asignados a un proyecto.
13	Equipos de telecomunicaciones	Se cuenta con dos routers uno utilizado a nivel gerencia y otro a nivel corporativo. Además de switches para permitir la conexión entre equipos.
14	Firewall	Se cuenta con dos firewalls que controlan el acceso no autorizado a la red a través de Internet.
15	Fuentes de Alimentación (UPS)	Permite evitar que los equipos no se dañen cuando hay una interrupción de energía, se tiene uno en cada piso.
16	Internet	Permite la conexión con otras redes.
17	Red LAN	Red local que comunica a todos los dispositivos de la empresa.
18	Respaldos de las Bases de Datos	Copias de seguridad de las bases de datos de la empresa, se extraen una vez al mes.
19	Servidor de Aplicaciones	Se cuenta con dos servidores de aplicaciones uno para el ambiente de desarrollo y otro para el ambiente de test.
20	Servidor de Base de Datos	Se cuenta con dos servidores de bases de datos una para el ambiente de desarrollo y otro para el ambiente de test.
21	Share Point	Repositorio en donde se tiene almacenada información relacionada con la empresa.

4.2.6.4 IDENTIFICAR LAS PRIORIDADES DE RECUPERACIÓN DE LOS RECURSOS

En la Tabla 4-54 se listan los recursos en el orden en que se deben recuperar de acuerdo al tiempo objetivo de recuperación definido para cada uno de los recursos identificados en la Sección 4.2.6.3.

Tabla 4-54 – Orden de priorización de recuperación de recursos mínimos requeridos

Orden		Nombre Recurso	RTO
1	1	Cableado de datos	12 horas
		Equipos de telecomunicaciones	12 horas
		Red LAN	12 horas
	2	Servidor de Aplicaciones	12 horas
		Servidor de Base de Datos	12 horas
	3	Aplicaciones desarrolladas por LOGICIEL	12 horas
		Bases de Datos	12 horas

Orden		Nombre Recurso	RTO
	4	Internet	12 horas
	5	Código fuente de las aplicaciones	12 horas
2	1	Firewall	24 horas
	2	Computadoras de Escritorio	24 horas
	3	Equipo de climatización	24 horas
	4	Aplicaciones utilizadas para el desarrollo de software	24 horas
	5	Equipo de desarrollo	24 horas
		Equipo de SQM	24 horas
3	1	Fuentes de Alimentación (UPS)	48 horas
	2	Share Point	48 horas
	3	Respaldos de las Bases de Datos	48 horas
	4	Aplicaciones de ofimática	48 horas
	5	Documentación de las aplicaciones	48 horas
		Documentación de las pruebas de software	48 horas

4.2.7 DESARROLLO E IMPLEMENTACIÓN DE ESTRATEGIAS DE CONTINGENCIA

En este paso se busca establecer las estrategias de contingencia que mejor se adapten a las necesidades de la empresa, para lo cual se va a usar los resultados obtenidos de la evaluación de riesgos y del BIA.

4.2.7.1 ESTRATEGIAS DE CONTINGENCIA

Las potenciales estrategias de contingencia incluyen pero no se limitan a las medidas preventivas y medidas de mitigación que se describen a continuación.

4.2.7.1.1. Medidas Preventivas

Las medidas preventivas que se describen a continuación permitirán que todo el personal esté preparado para hacer frente a los posibles riesgos que se presenten en la organización.

Medida Preventiva 1: Control de Acceso a la red de datos

Riesgos que contrarresta: Acceso no autorizado (2), Avería de origen físico o lógico (7), Caída del sistema por agotamiento de recursos (8), Difusión de software dañino (23), Errores en la configuración (26), Errores de mantenimiento /

actualizaciones de programas (software) (28), Errores del administrador (32), Manipulación de la configuración (44), Uso no previsto (53)

Medidas Técnicas:

- Las conexiones del backbone de red deberán mantener redundancia para su rápida sustitución en caso de emergencia.
- Establecer una política que indique que los puertos de red que no están siendo ocupados deberán estar desactivados para evitar accesos no autorizados a la red de datos.
- Los puntos de red que no estén siendo usados deben estar desconectados.
- Mantener actualizados los diagramas de red.
- Mantener los puertos de diagnóstico y configuración remota desactivados, y activarlos sólo cuando se requiera hacer alguna tarea de mantenimiento en los equipos.
- Disponer de un servidor DHCP redundante que entre en funcionamiento cuando el servidor principal sufra algún daño.

Medidas Organizativas:

- Establecer políticas para regular los accesos de usuarios remotos.

Medida Preventiva 2: Control de la temperatura de los equipos informáticos

Riesgos que contrarresta: Condiciones inadecuadas de Temperatura o Humedad (9)

Medidas Técnicas:

- Asegurar que los servidores que se encuentran en los cuartos de telecomunicaciones, tengan la ventilación necesaria para asegurar que tengan un funcionamiento óptimo.
- Tomar las medidas necesarias para que la temperatura en los cuartos de telecomunicaciones se encuentren dentro de los límites aceptables, para lo cual se sugiere la utilización de un sistema de monitorización de temperatura.

- Configurar el BIOS de los servidores, para que se monitoree la temperatura interna de los mismos y el correcto funcionamiento de sus ventiladores, y se notifique en caso de que la temperatura supere los límites marcados.

Medida Preventiva 3: Disponibilidad de los equipos computacionales

Riesgos que contrarresta: Acceso no autorizado (2), Avería de origen físico o lógico (7), Caída del sistema por agotamiento de recursos (8), Difusión de software dañino (23), Errores en la configuración (26), Errores de mantenimiento / actualizaciones de programas (software) (28), Errores del administrador (32), Manipulación de la configuración (44), Uso no previsto (53)

Medidas Técnicas:

- Mantener un inventario actualizado de los equipos computacionales, en donde se especifique el responsable, las características básicas, la ubicación física, etc.
- Disponer de al menos 2 PC´s y 1 laptop para reemplazo de equipo crítico de la empresa.
- Disponer de un stock mínimo de componentes computacionales cuyo daño sea más frecuente como discos duros, monitores, etc.
- Realizar mantenimientos periódicos de los equipos computacionales.
- Mantener registros de todo el mantenimiento preventivo o correctivo que se realice a los equipos.

Medidas Organizativas:

- Establecer una política que indique que sólo el personal autorizado puede llevar a cabo las reparaciones y mantenimientos a los equipos.

Medida Preventiva 4: Disponibilidad de los respaldos de información

Riesgos que contrarresta: Alteración de la Información (3), Degradación de Información (16), Destrucción deliberada o accidental de información (21, 22), Introducción de Información incorrecta (40)

Medidas Organizativas:

- Mantener los respaldos de información almacenados fuera de las instalaciones principales en una locación segura.
- Probar los respaldos de información de manera regular para asegurar de que funcionen correctamente.
- Establecer una política en donde se indique el tipo de respaldo a realizar, la frecuencia con la que se debe extraer los respaldos, el responsable, etc.
- Asignar a una persona responsable de la extracción de los respaldos de información.
- Establecer un periodo de retención de los respaldos de información.

Medida Preventiva 5: Gestión del cambio de los sistemas de información

Riesgos que contrarresta: Errores de configuración (26), Errores del administrador (32), Acceso no autorizado (2), Manipulación de la configuración (44), Errores de mantenimiento / actualizaciones de programas (software) (28), Uso no previsto (53)

Medidas Técnicas:

Establecer controles de seguridad que cubran los siguientes puntos:

- Mantener un control de las versiones de todas las actualizaciones de software.
- Asegurar que la documentación de las aplicaciones esté actualizada al completar cada cambio y que la documentación antigua se archive o se elimine de manera adecuada.
- Mantener un registro de auditoría de todas las solicitudes de cambio y de los cambios que se han realizado.
- Analizar el impacto de los cambios antes de realizar alguno.
- Asegurar que todos los cambios han sido probados antes de ser implementados en el ambiente de producción.

Medida Preventiva 6: Operatividad de los sistemas de información

Riesgos que contrarresta: Avería de origen físico o lógico (7), Caída del sistema por agotamiento de recursos (8), Difusión de software dañino (23), Errores en la configuración (26), Errores del administrador (32), Acceso no autorizado (2), Manipulación de la configuración (44), Errores de mantenimiento / actualizaciones de programas (software) (28), Uso no previsto (53)

Medidas Técnicas:

- El software crítico deberá tener documentado los parámetros, procedimientos, detalles de configuración y software de soporte.
- El software crítico deberá disponer de estrategias de roll back antes de implementar cualquier cambio.
- Mantener versiones previas del software como una medida de contingencia en caso de que la nueva versión presente errores.
- Establecer parámetros o criterios para poder determinar si el sistema se comporta de manera eficiente.
- Tener documentados las interdependencias con otros sistemas para en caso de que se presente un error poder identificar más fácilmente los procesos y sistemas del Core Bancario que se verán afectados.

Medidas Organizativas:

- Disponer de procedimientos de monitoreo del funcionamiento de los sistemas críticos de la empresa para asegurar un funcionamiento eficiente de los mismos.
- Mantener documentados los procedimientos de los sistemas críticos de la empresa como bases de datos, servidor de aplicaciones, servidor de bases de datos, respaldos de la información, etc.
- Tener documentados los datos de las personas de soporte a las cuales contactar en caso de que se presenten dificultades operacionales o técnicas inesperadas.
- Tener identificados los responsables y claramente establecidas las funciones a desarrollar para cada uno de los sistemas críticos de la empresa.

Medidas Humanas:

- Elaborar un programa de vacaciones que asegure la presencia permanente del personal para vigilar el correcto funcionamiento de los sistemas.

Medida Preventiva 7: Seguridad contra desastres naturales

Riesgos que contrarresta: Desastres Naturales (20)

Medidas Organizativas:

- Crear un plan de evacuación del hardware que permita transportar a los equipos críticos a un sitio alterno, en donde se considere la importancia que tiene cada uno de los equipos de acuerdo a la información almacenada en los mismos, de forma que los equipos y datos más importantes sean evacuados primero.
- Etiquetar a cada uno de los activos de acuerdo a su nivel de criticidad, en donde:
  - Los activos con prioridad crítica tendrán una etiqueta de color rojo.
  - Los activos con prioridad alta una de color anaranjado.
  - Los activos con prioridad media una de color amarillo.
  - Y los de prioridad baja una de color verde.
- Se dará prioridad a la evacuación de datos corporativos como datos de la empresa, datos de facturación y contabilidad, de los empleados, clientes y proveedores.

Medidas Humanas:

- Dar a conocer al personal sobre el plan de evacuación del hardware.

Medida Preventiva 8: Seguridad contra incendios

Riesgos que contrarresta: Fuegos/Incendios (35)

Medidas Técnicas:

- Tener un extintor de incendios tipo C en cada uno de los pisos en donde funciona LOGICIEL, el mismo que debe ser inspeccionado al

menos una vez al mes para asegurar que siempre funcione óptimamente. Es importante recargarlos una vez al año cuando no han sido usados, y en un plazo de hasta 72 horas en caso de haya sido requerido su uso. Se debe mantener un registro fuera de los extintores con las fechas de la última y próxima recarga.

- Realizar mantenimientos periódicos de las instalaciones eléctricas, por lo menos una vez cada seis meses, para prevenir cortocircuitos.

Medidas Organizativas:

- Establecer un procedimiento con las consideraciones a tener en cuenta en caso de incendio.
- Tener a mano los números telefónicos de emergencia, en un lugar que sean fácilmente visibles.
- Contar con un procedimiento para la realización de respaldos de todos los sistemas críticos de la empresa.
- Establecer un procedimiento para la adquisición o alquiler de equipos informáticos y el establecimiento de sitios alternos.

Medidas Humanas:

- Dar a conocer al personal la forma de actuar en caso de incendio.
- Capacitar al personal en el uso de los extintores de incendios, para que cualquiera de los empleados sea capaz de utilizarlos si así se lo requiere.
- Asignar roles y responsabilidades para la realización de respaldos.

Medida Preventiva 9: Seguridad contra inundaciones o daños por agua

Riesgos que contrarresta: Daños por agua /Inundaciones (14)

Medidas Técnicas:

- Colocar en los cuartos de telecomunicaciones sensores para la detección de inundaciones a ras del suelo, los mismos que se encuentren conectados a un sistema de alarmas.
- Evitar colocar los CPU´s directamente en el suelo.

- Disponer de cobertores o bolsas plásticas para proteger a los equipos, servidores y documentos importantes que pueden verse afectados por el agua.

Medidas Organizativas:

- Realizar periódicamente mantenimientos (por lo menos dos veces al año) a las instalaciones de la organización en lo que se incluya revisión de goteras, filtraciones de agua, ductos de agua y drenaje.
- Establecer un procedimiento con las consideraciones a tener en cuenta para proteger a los equipos contra el agua.

Medida Preventiva 10: Seguridad de los procesos de usuario

Riesgos que contrarresta: Acceso no autorizado (2), Avería de origen físico o lógico (7), Caída del sistema por agotamiento de recursos (8), Difusión de software dañino (23), Errores en la configuración (26), Errores de mantenimiento / actualizaciones de programas (software) (28), Errores del administrador (32), Manipulación de la configuración (44), Uso no previsto (53)

Medidas Técnicas:

- Establecer un mecanismo para cerrar los sistemas después de unos minutos de inactividad, en donde para volver a activar la sesión se requiera el ingreso de una clave de usuario.
- Capacitar a los usuarios en el manejo de las diferentes aplicaciones que estén a su cargo.

Medidas Organizativas:

Crear una política en donde se establezca que los usuarios deben:

- Respaldar la información que almacenan en sus equipos, definiendo en donde se van a guardar dichos respaldos y cada cuanto se deben realizar los mismos.
- Resguardar las claves de acceso a los servicios y equipos que administran.
- Evitar la instalación de software ilegal en los equipos que administran.

- Bloquear las sesiones activas en los equipos, lo que no incluye solo apagar la pantalla de la computadora. Esto se hace para evitar que haya equipos de usuario desatendidos.

Medida Preventiva 11: Seguridad Física

Riesgos que contrarresta: Acceso no autorizado (2), Avería de tipo físico o lógico (7), Fallo de Servicios de telecomunicaciones (34), Manipulación de la configuración (44), Robo (51)

Medidas Técnicas:

- Software:
  - Mantener un inventario actualizado del software disponible en la empresa, el mismo que debe contener una breve descripción del software, los equipos en donde se encuentran instalados, ubicación física, etc.
  - Instaurar un procedimiento para registrar el ingreso y salida del software.
  - Establecer que documentación se debe tener de cada uno de los aplicativos desarrollados en la empresa, la cual debe estar almacenada de manera segura en donde solo tenga acceso personal autorizado.
  - Determinar los procedimientos a seguirse para la extracción de respaldos del código fuente y los ejecutables del software y aplicativos de LOGICIEL, que garanticen su disponibilidad en caso de una contingencia.
  - Restringir al mínimo los permisos de accesos a la documentación de los aplicativos.
- Hardware
  - Establecer una política para el control de acceso a los cuartos de telecomunicaciones, de manera que se permita el acceso solo al personal autorizado. En caso de que una persona ajena a la organización requiera el acceso a la cuarto de

telecomunicaciones, una persona deberá acompañarla permanentemente.
    - Verificar periódicamente (por lo menos cada 6 meses) el inventario de activos.
- Cableado
    - Mantener un acceso controlado a los cuartos de cableado.
- Documentación
    - Mantener los archivos impresos y digitales, en un lugar aislado y seguro.

Medidas Organizativas:

- Software
    - Instaurar políticas y procedimientos de seguridad para la protección y el uso del software de la organización.
    - Crear una política para regular el ingreso y salida del software.
    - Establecer una política de control de acceso al código fuente de los aplicativos desarrollados en la empresa.
- Hardware
    - Mantener los cuartos de telecomunicaciones cerrados con llave para evitar accesos no autorizados.
    - Los dispositivos y servidores situados fuera de los cuartos de telecomunicaciones deben ser protegidos y almacenados en armarios o tener seguros para proteger los mismos.
    - Mantener un registro de los visitantes que han accedido a los cuartos de telecomunicaciones.

Medida Preventiva 12: Separación de ambientes de desarrollo y producción de los sistemas de información

Riesgos que contrarresta: Acceso no autorizado (2), Errores en la configuración (26), Errores de mantenimiento/actualizaciones de programas (software) (28), Errores del administrador (32), Manipulación de la configuración (44), Uso no previsto (53)

Medidas Organizativas:

- Establecer el procedimiento a seguir para asegurar que todo el software desarrollado cumple con los requisitos identificados al inicio del proceso de desarrollo.
- Asignar personal debidamente calificado para definir y verificar los criterios de aceptación para el traspaso del software del ambiente de desarrollo y pruebas al ambiente de producción.
- Establecer el procedimiento a seguir para la aceptación del paso de un nuevo sistema del ambiente de desarrollo y pruebas al ambiente de producción.
- Crear una política para la extracción de respaldos del código fuente y ejecutable de cada una de las aplicaciones desarrollas por la empresa.
- Designar un administrador por aplicación que asigne los permisos de acceso al ambiente de desarrollo y pruebas.

4.2.7.1.2. Medidas de Mitigación o Recuperación

Las medidas de mitigación que se describen a continuación permitirán atenuar los potenciales impactos causados por un riesgo.

Contingencia 1: Daño de un equipo de comunicación del backbone de la institución

Fuentes de riesgo: Hardware, Software, Instalaciones, Otro equipo

Plan de Acción:

- Determinar si el daño es producto de deficiencias en la red eléctrica o un problema de hardware.
- En caso de que se trate de un problema eléctrico, se debe proceder de acuerdo a la contingencia correspondiente.
- En caso de que se trate de un problema de hardware, se debe proceder con la reparación del equipo en caso de que sea un daño menor.
- En caso de que se trate un daño mayor, se debe reparar el equipo y reemplazarlo por un equipo temporal.

Contingencia 2: Daño de una conexión del backbone de la institución
Fuentes de riesgo: Hardware, Software, Instalaciones, Otro equipo
Plan de Acción:

- Identificar la parte en donde se ha producido el daño.
- En caso de que se trate de un problema de conectividad, se debe monitorear y comprobar que enlaces y áreas de trabajo han sido afectadas, para lo cual se debe revisar el diagrama de red y determinar cuan grave es el daño.
- Proceder a contactarse con el personal técnico especializado para que repare el daño.

Contingencia 3: Daño de PC´s de usuario
Fuentes de riesgo: Hardware, Software, Instalaciones, Otro equipo
Plan de Acción:

- El usuario responsable del equipo debe reportar el problema al Administrador de Recursos Computacionales.
- El Administrador de Recursos Computacionales debe verificar si el daño es producido por un problema de hardware o software.
- En caso de que se trate de un problema de hardware, se debe considerar si el equipo puede ser reparado o si debe ser reemplazado.
- En caso de que se trate de un problema con un componente del equipo pero sus aplicaciones siguen funcionando normalmente, se debe dar por terminada la contingencia.
- En caso de no poder acceder directamente al disco, se debe proceder a respaldar la información del mismo, para proceder a formatearlo y poder reinstalar el software.

Contingencia 4: Daños en las bases de datos corporativas

Fuentes de riesgo: Hardware, Software

Plan de Acción:

- Determinar la causa del problema hardware, configuración, instalación y datos.
- En caso de que se trate de un problema de hardware, se debe verificar que los discos de respaldos entren en funcionamiento para mitigar la contingencia.
- En caso de que se trate de un problema de configuración, se debe verificar los parámetros de configuración y ajustar el motor de base de datos de acuerdo al procedimiento documentado de recuperación y guardar registro de los errores y problemas corregidos, durante el evento.
- En caso de que se trate de un problema de instalación, se debe reinstalar el motor de base de datos y recuperar los últimos respaldos de acuerdo al proceso de recuperación de base de datos. Se debe guardar un registro de las acciones y problemas que se presentaron durante la instalación para que sirva para solucionar posibles problemas futuros.
- En caso de que se trate de un problema con los datos, se debe corregirlos directamente o mediante una modificación de los datos.

Contingencia 5: Humedad o Inundación

Fuentes de riesgo: Hardware, Software, Instalaciones, Otro equipo

Plan de Acción:

- Comunicar al Coordinador del Plan de Contingencia sobre el evento ocurrido y proceder a activar el plan de contingencia y los procedimientos de recuperación establecidos.
- Apagar los equipos computacionales, iniciando por los más críticos.
- Cubrir con bolsas plásticas y ubicar en lugares seguros el hardware, software y documentos importantes que puedan mojarse.
- Apagar la caja principal de corriente.

Contingencia 6: Incendio o Fuego

Fuentes de riesgo: Hardware, Software, Instalaciones, Otro equipo

Plan de Acción:

- Comunicar al coordinador del plan de contingencia sobre el evento ocurrido y proceder a activar el plan de contingencia y los procedimientos de recuperación establecidos.
- Verificar que el sistema contra incendios esté operativo.
- Intentar sofocar el fuego si se conoce el manejo de los extintores. En el caso de que el fuego sea considerable, pedir ayuda y no tratar de extinguirlo con los propios medios.
- Activar el sistema de alarmas.
- Llamar a los números de emergencia.
- Respetar los señalamientos de las rutas de evacuación.
- En caso de ser necesario, utilizar lámparas de emergencia con batería.
- Apagar los servidores si el tiempo lo permite.
- Apagar la caja principal de corriente.

Contingencia 7: Sistemas Corporativos fuera de servicio

Fuentes de riesgo: Hardware, Software, Instalaciones, Otro equipo

Plan de Acción:

- Determinar la causa del problema hardware, software o conectividad.
- En caso de que trate de un problema de hardware, se debe comprobar la disponibilidad del fluido eléctrico. Si el problema es por daño en los componentes, se debe establecer contacto con el proveedor para coordinar el reemplazo o reparación de los mismos.
- En caso de que trate de un problema de software, se deben revisar el sistema operativo, aplicaciones, bases de datos y demás procesos que intervengan en el funcionamiento de los sistemas corporativos.
- En caso de que trate de un problema de conectividad, se debe comprobar la disponibilidad de los enlaces y accesos de red.

- Considerar la utilización de un servidor alterno para restituir servicios críticos, en caso de que la solución de los problemas de hardware o software requiera un tiempo superior a 1 día.

Contingencia 8: Suspensión del servicio de Internet
Fuentes de riesgo: Hardware, Software, Instalaciones, Otro equipo
Plan de Acción:

- Determinar la causa del problema conectividad, hardware o problema de configuración.
- En caso de que trate de un problema de conectividad, se debe monitorear y comprobar que los enlaces con el proveedor están funcionando. Si se comprueba la suspensión del servicio, contactar al proveedor para consultar el motivo de la falla del servicio.
- En caso de que trate de un problema de hardware, se debe comprobar el correcto funcionamiento de los equipos de conexión y revisar los indicadores para determinar el fallo. Una vez identificado el fallo se debe contactar con el proveedor para coordinar el cambio, reemplazo o reparación del equipo.
- En caso de que trate de un problema de configuración, se debe revisar la configuración actual del servicio de Internet con ayuda de un manual en caso de ser posible, el diagrama de red actualizado y el registro de las últimas modificaciones realizadas, para en base a esto identificar y corregir la falla.

Contingencia 9: Suspensión del servicio eléctrico
Fuentes de riesgo: Hardware, Software
Plan de Acción:

- En caso de que en los 5 minutos posteriores a un apagón no retorna el servicio eléctrico, el personal de la empresa debe guardar la información sobre la que estaban trabajando y apagar sus equipos para posteriormente

apagar los UPS. Una vez restaurado el servicio se debe encender el UPS y el personal podrá continuar con su trabajo normal.

4.2.7.2 ROLES Y RESPONSABILIDADES

Para la adecuada gestión del plan de contingencia, es necesario tener claramente definidos los roles que se harán cargo de las actividades del plan y las responsabilidades de los mismos.

A continuación, se presenta un organigrama de cómo se debería estructurar el equipo de tratamiento de incidencias:

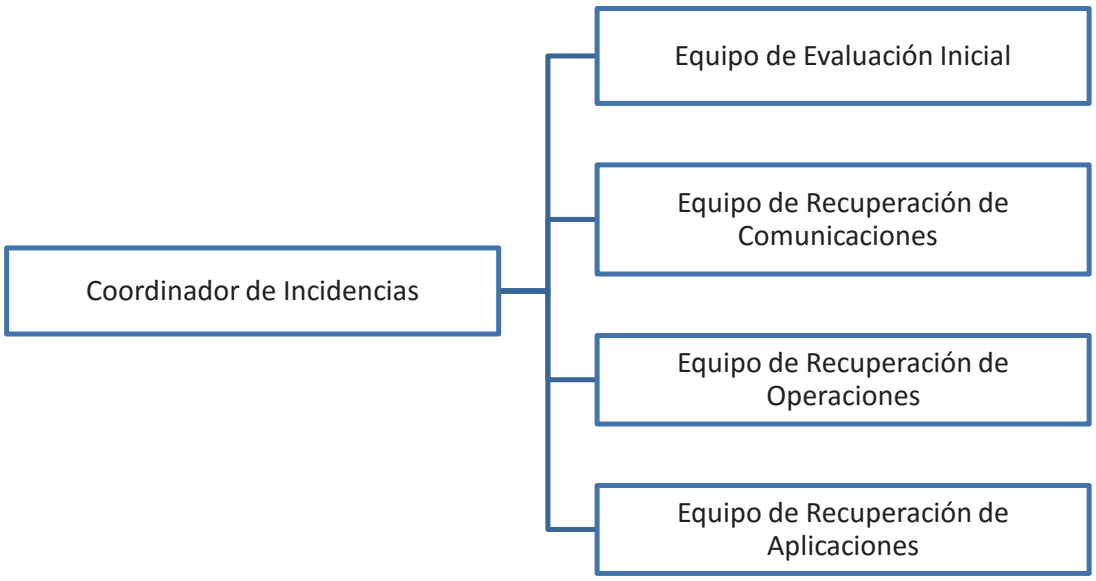

Figura 4-6 – Organigrama del equipo de tratamiento de incidencias

Las responsabilidades de los roles definidos en la Figura 4-6 se detallan a continuación:

Coordinador de Incidencias: coordina todos los esfuerzos de recuperación con los equipos de evaluación inicial y recuperación, desde el momento en que se realiza la notificación inicial y se activa el plan de contingencia. Entre sus responsabilidades están las siguientes:

- Activar el plan de contingencia
- Coordinar con los equipos de evaluación inicial y recuperación la ejecución del plan de contingencia.
- Monitorear y dar seguimiento a las actividades de recuperación durante la ejecución del plan.

Equipo de Evaluación Inicial: evalúa el incidente y sugiere o no al coordinador de incidencias la activación del plan de contingencia. Entre sus responsabilidades están las siguientes:

- Evaluar el incidente notificado.
- Definir el nivel de riesgo y el impacto del incidente en las personas, instalaciones y operaciones de la empresa.
- Asesorar al coordinador de incidencias sobre la activación o no del plan de contingencias.

Equipo de Recuperación de Comunicaciones: mantiene la continuidad y recupera las comunicaciones durante una contingencia. Entre sus responsabilidades están las siguientes:

- Informar al coordinador de incidencias la interrupción en el servicio y el avance en la recuperación del mismo.
- Ejecutar la medida de recuperación definida por la empresa.
- Determinar el daño en la red de comunicaciones.
- Coordinar la instalación del software o hardware necesario para restaurar las comunicaciones.
- Coordinar con los proveedores en caso de que se requiera el reemplazo de equipos.
- Probar que las comunicaciones se han reestablecido correctamente.
- Monitorear el funcionamiento de las comunicaciones durante una contingencia.
- Documentar y registrar el incidente.

Equipo de Recuperación de Operaciones: mantiene la continuidad y recupera las operaciones críticas de la empresa durante una contingencia. Entre sus responsabilidades están las siguientes:

- Informar al coordinador de incidencias la interrupción de las operaciones y el avance en la recuperación de las mismas.
- Ejecutar la medida de recuperación definida por la empresa.
- Asegurar la disponibilidad de los respaldos necesarios para la recuperación.
- Restaurar los equipos, archivos, sistemas, servicios, etc. Necesarios para el correcto funcionamiento de las operaciones críticas.
- Monitorear el funcionamiento de las operaciones durante una contingencia.
- Coordinar con los proveedores en caso de que se requiera el reemplazo de equipos.
- Coordinar la instalación del hardware necesario para restaurar las operaciones.
- Documentar y registrar el incidente.

Equipo de Recuperación de Aplicaciones: mantiene la continuidad y restaura las aplicaciones críticas de la empresa durante una contingencia. Entre sus responsabilidades están las siguientes:

- Informar al coordinador de incidencias la interrupción de las aplicaciones y el avance en la recuperación de las mismas
- Ejecutar la medida de recuperación definida por la empresa.
- Reconstruir el ambiente de operación de las aplicaciones.
- Soportar el esfuerzo de los usuarios para actualizar los datos de la aplicación una vez que las aplicaciones se han restaurado.
- Monitorear el funcionamiento de las aplicaciones durante una contingencia.
- Documentar y registrar el incidente.

Se debe designar un líder por cada uno de los equipos, el mismo que debe tener la capacidad de tomar decisiones durante el proceso de recuperación. Además,

se debe contar con un suplente tanto para el coordinador de incidencias como para los líderes de los equipos, para que asuman las responsabilidades de los roles principales en caso de que los mismos no se encuentren disponibles.

Los miembros de los equipos son quienes se encargan de ejecutar las medidas de recuperación. Es importante evitar asignar las actividades de recuperación a individuos específicos, dado que las actividades se ejecutan usualmente por múltiples personas.

4.2.7.3 ACTIVACIÓN DEL PLAN

A continuación, se describen los pasos a considerar para la activación del plan de contingencia de TI, en caso de que se presente una incidencia.

Verificación de la Incidencia

Para la verificación de la incidencia se debe considerar si se tiene acceso al lugar de la incidencia, en caso de que así sea, se debe realizar una inspección de los siguientes aspectos para evaluar el daño:

1. Evaluar si el equipo computacional está destruido, es fácil de recuperar o está disponible para ser utilizado.
2. Verificar el estado de los registros vitales como manuales, documentación, información, etc. para poder determinar las medidas de recuperación a implementar.
3. Evaluar el estado de los equipos de oficina.
4. Analizar el estado de las operaciones en el momento del desastre.
5. Identifique si se han perdidos datos críticos.
6. Evaluar si es necesario utilizar los respaldos de información para restaurar los datos.

Notificación Inicial

Una vez se ha verificado la incidencia es momento de notificarla, para lo cual se debe considerar lo siguiente:

1. Realizar la notificación al coordinador de incidencias.

2. La notificación debe contener lo siguiente
    a. Fecha y hora de la notificación
    b. Nombre de la persona que realiza la notificación.
    c. Descripción del evento o contingencia que se va a notificar.
    d. Reporte preliminar de los daños ocasionados.
    e. Consideraciones especiales a tener en cuenta.

Escalamiento de Notificaciones

En base a la severidad de incidencia, se debe considerar lo siguiente para el escalamiento de notificaciones:

1. Si la incidencia se ha manejado correctamente y no se requieren notificaciones adicionales, dar por terminada la situación de emergencia.
2. Si la incidencia involucra daños a la propiedad, daños a personas y/o una interrupción del negocio que exceda un día de trabajo, se deben enviar notificaciones adicionales.
3. Si se han producido daños al personal, se deben enviar notificaciones a los familiares.

Activación del equipo de recuperación

Una vez que el coordinador de incidencias ha activado el plan de contingencias, se debe proceder con la activación del equipo de recuperación seleccionado. Para realizar esta tarea el líder del equipo debe:

1. Determinar que miembros del equipo son requeridos para:
    a. Cumplir con los objetivos de recuperación.
    b. Asistir en los esfuerzos de recuperación.
    c. Dar soporte temporal a las áreas afectadas por la incidencia.
2. Elaborar un listado del personal requerido para iniciar con las actividades de recuperación.
3. Contactar con los miembros del equipo y proveerles toda la información relevante relacionada con la incidencia.

Evaluación de daños

El equipo de evaluación inicial debe inspeccionar el sitio en donde ocurrió la incidencia, con el objetivo de determinar la extensión del daño y las áreas afectadas. Durante la evaluación, se debe contar con al menos un representante de las áreas afectadas para determinar las condiciones del sitio y de los equipos computacionales. Además, tomar en cuenta las siguientes consideraciones:

1. Si las instalaciones han sido afectadas por la incidencia, se debe:
    a. Esperar a que sea seguro ingresar a las instalaciones para poder realizar la evaluación.
    b. Determinar y adquirir todo el equipo de emergencia necesario para los miembros del equipo de evaluación inicial y el representante de las áreas afectadas. Para los equipos de emergencia se sugiere lo siguiente:
        i. Cascos y ropa de seguridad
        ii. Linternas
        iii. Cámara fotográfica
        iv. Libretas y lápices
2. Antes de realizar la evaluación, se debe brindar toda la información disponible de la incidencia al personal que evaluará las áreas afectadas. Asimismo, se debe revisar los procedimientos de seguridad a tomar en cuenta durante la evaluación.
3. Se debe evaluar cuidadosamente la magnitud del daño de los siguientes aspectos:
    a. Infraestructura (accesos y áreas de trabajo)
    b. Comunicaciones
    c. Cableado y conexiones de red
    d. Servicio eléctrico
    e. Equipos computacionales
    f. Aplicaciones
    g. Medios de almacenamiento

Seguimiento del evento de contingencia

Una vez se ha iniciado la ejecución de la medida de recuperación adecuada para la solución de la incidencia, se debe dar seguimiento al evento de contingencia para lo cual se debe tomar en cuenta lo siguiente:

1. Se debe verificar el estado de la incidencia y dar seguimiento a las actividades de mitigación y recuperación realizadas por los miembros del equipo de recuperación.
2. Para controlar el estado de la incidencia hay que considerar lo siguiente:
    a. El tipo de incidencia
    b. Las áreas afectadas
    c. Las actividades planeadas para la mitigación y recuperación de la incidencia.
3. Llevar un registro cronológico del avance de las tareas planeadas para la mitigación y recuperación de la incidencia.
4. Solucionar prontamente cualquier problema que pudiera obstaculizar la ejecución de las acciones de mitigación y recuperación.

4.2.8 DESARROLLO Y DOCUMENTACIÓN DEL PLAN DE CONTINGENCIA

El documento del plan de contingencia de TI de LOGICIEL se lo debe hacer en base al modelo de documento definido en la Sección 4.1.8 (Anexo B).

4.2.9 PRUEBAS Y EJERCICIOS

Todas las pruebas del plan de contingencia de TI deben hacerse tomando en consideración el plan de pruebas definido, el cual debe hacerse en base al modelo de plan de pruebas definido en la Sección 4.1.9 (Anexo C).

Por otro lado, los ejercicios del plan de contingencia deben hacerse tomando en consideración establecer el escenario del ejercicio, el cual debe considerar el modelo definido en la Sección 4.1.9 (Anexo D). Una vez finalizado el ejercicio, se debe llenar un informe considerando el modelo definido en el la Sección 4.1.9 (Anexo E).

4.2.10 CONCIENTIZACIÓN Y CAPACITACIONES

Las capacitaciones del plan de contingencia a realizarse deben hacerse tomando en cuenta el plan de capacitación, el cual debe hacerse en base al modelo de plan de capacitación definido en la Sección 4.1.10 (Anexo F).

4.2.11 MANTENIMIENTO DEL PLAN DE CONTINGENCIA

El mantenimiento del plan de contingencia se debe realizar de manera anual, teniendo en consideración los informes de seguimiento de las contingencias ocurridas durante el año y los resultados de las pruebas y ejercicios del plan.

En caso de que se haya producido cambios significados en la organización, los activos de información, el entorno de la operación, o se hayan encontrado problemas significativos durante la ejecución, la implementación, o las pruebas del plan de contingencia, se debe proceder con la actualización del plan de contingencia.

De los cambios a considerarse para el mantenimiento del plan de contingencia se debe llevar un registro, para el cual se debe el formulario para solicitud de cambios definido en la Sección 4.1.11 (Anexo G).

CONCLUSIONES Y RECOMENDACIONES

A continuación, se describen las conclusiones y recomendaciones a las que se llegaron una vez terminado el presente proyecto.

CONCLUSIONES

Del presente proyecto podemos concluir diferentes puntos relacionados a la importancia de la elaboración de un plan de contingencias. Entre estos tenemos:

- La planificación de contingencias es un componente esencial de cualquier estrategia del negocio, puesto que permite asegurar la continuidad de las operaciones del negocio.
- Es de vital importancia que en las empresas se desarrollen e implementen planes de contingencia para asegurar la continuidad de las operaciones de negocio.
- Tener un buen conocimiento del entorno en que se encuentra envuelta la organización permite desarrollar un plan de contingencia que se adapte a la situación actual de la misma y que esté conforme al tipo de organización.
- El éxito en la implementación de un plan de contingencia está relacionado con el nivel de compromiso de los directivos de la organización y de cada uno de los empleados de la misma, debido a que son los directivos quienes facilitarán los recursos necesarios para la implementación del plan y son los empleados quienes en caso de presentarse una incidencia pondrán en marcha el plan.
- La disponibilidad de la documentación juega un papel decisivo en la implementación del plan de contingencia, además de su calidad y cuan al día se encuentre la misma.

Se lograron concretar los objetivos establecidos para el presente proyecto, creando un modelo para el desarrollo de un plan de contingencia de Tecnologías de Información (TI), en donde se analizaron varios marcos de referencia enfocados en la continuidad del negocio. Para reducir el listado inicial de 43

marcos de referencia se aplicaron 5 criterios de exclusión, quedando de este proceso de discriminación, 6 marcos de referencia. Se compararon los 6 marcos de referencia para determinar los principales pasos del proceso de planeación de contingencias.

Además, en vista de que la evaluación de riesgos es uno de los pasos del proceso de planeación de contingencias, se analizaron también marcos de referencia enfocados en la evaluación de riesgos para de esta forma determinar la mejor manera de llevar a cabo este proceso. El análisis se inició con un listado de 40 marcos de referencia. Para reducir este listado se aplicaron 4 criterios de exclusión y se creó un ranking en base al número de veces que es citado un marco de referencia en los trabajos considerados para la elaboración del listado. De este proceso de discriminación quedaron 3 marcos de referencia, que al ser comparados determinaron los puntos clave de la evaluación de riesgos.

Una vez comparados los 6 marcos de referencia de continuidad del negocio y los 3 marcos de referencia de evaluación de riesgos, se conformó un modelo para la elaboración de planes de contingencia de TI. El modelo propuesto constituye un ciclo compuesto por 11 etapas, entre las que se incluye la evaluación de riesgos. Dentro de la descripción del modelo, se explica en detalle como ejecutar cada una de las etapas que conforman el ciclo de una manera sencilla y fácil de entender con el fin de que cualquier empresa pueda ponerlo en práctica. Con el modelo propuesto se logró simplificar el proceso de elaboración de planes de contingencias de TI, de manera que las empresas que requieran desarrollar un plan de contingencia de TI ya no tendrán que adentrarse en la complejidad de los marcos de referencia que se encuentran orientados a la continuidad del negocio.

Finalmente, mediante la elaboración de una propuesta de un plan de contingencia de TI para la empresa LOGICIEL se hizo la validación del modelo. Para lo cual se desarrollaron cada una de las etapas definidas en el modelo propuesto. En base a la priorización de los procesos del negocio de LOGICIEL, se pudo determinar el alcance que tendría el proceso de elaboración del plan de contingencias de TI.

Con los activos críticos de los procesos determinados como prioritarios se realizó la evaluación de riesgos. Los resultados de la evaluación de riesgos y del análisis de impacto en el negocio, permitieron determinar las estrategias de contingencia que mejor se adaptan a las necesidades de la empresa.

RECOMENDACIONES

Debido a la importancia que tienen las Tecnologías de Información (TI) en las operaciones de la mayoría de organizaciones, es recomendable que en las empresas ecuatorianas se desarrollen e implementen planes de contingencia de TI para asegurar la continuidad de las operaciones en caso de que las TI se vean afectadas por algún tipo de incidente, interrupción o catástrofe.

Antes de iniciar con el desarrollo de un plan de contingencia de TI, es recomendable contar con el apoyo y total compromiso no solo de la dirección de la organización sino también de cada uno de los empleados de la misma, en vista de que son ellos quienes van a poner en práctica lo descrito en el plan en caso de que una incidencia se presente en la empresa.

Para la empresa para la que se desarrolló la propuesta de plan de contingencia de TI, se recomienda considerar los costos que representaría la implementación del plan de contingencia en la organización no como un gasto sino como una inversión. Los beneficios económicos para la organización se verán reflejados cuando no sea necesario detener las operaciones en caso de que algún tipo de incidente se presente.

Se recomienda que en el caso de hacer un trabajo similar, se consideren también modelos de referencia que sean de pago para el análisis comparativo de los modelos de referencia tanto de continuidad del negocio como de evaluación de riesgos. Debido a que es probable que entre los modelos de referencia de pago se encuentre un modelo que merezca ser incluido como base para la definición de un modelo para el desarrollo de un plan de contingencia de TI.

REFERENCIAS

[1] Ministerio de Hacienda y Administraciones Públicas, MAGERIT - versión 3.0 Libro I - Método, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[2] NIST, NIST SP800-30 r1 Guide for Conducting Risk Assessment, Gaithersburg: NIST, 2012.

[3] E. R. Stroie y A. C. Rusu, «Security Risk Management - Approaches and Methodology,» Bucharest, 2011.

[4] CLUSIF, «Risk Management - Concepts and Methods,» CLUSIF, Paris, 2009.

[5] SANS Technology Institute, «http://www.sans.edu,» 1 Septiembre 2009. [En línea]. Available: http://www.sans.edu/research/security-laboratory/article/security-controls. [Último acceso: 21 Octubre 2015].

[6] NIST, NIST SP 800-34 rev. 1 Contingengy Planning Guide for Federal Information Systems, 2010.

[7] Griffith University, «Business Continuity Management Framework,» Griffith University, 2013.

[8] Protiviti, «Guide to Business Continuity Management: Frequently Asked Questions,» Protiviti.

[9] Federal Office for Information Security, «BSI Standard 100-4 Business Continuity Managemente,» Federal Office for Information Security, Boon, 2009.

[10] D. Chinn y Demand Media, «http://smallbusiness.chron.com,» [En línea]. Available: http://smallbusiness.chron.com/purpose-contingency-planning-24864.html. [Último acceso: 10 Octubre 2015].

[11] University of Missouri System, «https://www.umsystem.edu,» 9 Marzo 2011. [En línea]. Available: https://www.umsystem.edu/ums/fa/management/records/disaster-guide-information. [Último acceso: 22 Octubre 2015].

[12] ASIS International and British Standards Institution, «Business Continuity Management Systems: Requirements with Guidance for Use,» ASIS International , 2010.

[13] European Network and Information Security Agency, «http://rm-inv.enisa.europa.eu,» Febrero 2013. [En línea]. Available: http://rm-inv.enisa.europa.eu/methods. [Último acceso: 22 Abril 2015].

[14] J. M. Matalobos Veiga, «Análisis de riesgos de seguridad de la información,» Universidad Politécnica de Madrid, Madrid, 2009.

[15] A. Syalim, Y. Hori y K. Sakurai, «Comparison of Risk Analysis Methods: Mehari, MAGERIT, NIST800-30 and Microsoft's Security and Management Guide,» IEEE, Fukuoka, 2009.

[16] P. Shamala, R. Ahmada y M. Yusoff, «A conceptual framework of info structure for information security risk assessment (ISRA),» ELSEVIER, Melaka, 2013.

[17] M. S. Saleh y A. Alfantookh, «A new comprehensive framework for enterprise information security risk management,» ELSEVIER, 2011.

[18] A. Behnia, R. A. Rashid y J. A. Chaudhry, «A Survey of Information Security Risk Analysis Methods,» Smart Computing Review, Qatar, 2012.

[19] K. V. D. Kiran, S. Mukkamala, A. Katragadda y L. Reddy, «Performance And Analysis Of Risk Assessment Methodologies In Information Security,» International Journal of Computer Trends and Technology, Vaddeswaram, 2013.

[20] D. Ionita, «Current Established Risk Assessment Methodologies and Tools,» University of Twente, 2013.

[21] F. Macedo y M. Mira da Silva, «Comparative Study of Information Security Risk Assessment Models,» Universidad Técnica de Lisboa, Lisboa.

[22] N. Shukla y S. Kumar, «A Comparative Study on Information Security Risk Analysis Practices,» Special Issue of International Journal of Computer Applications, India, 2012.

[23] CERT, «http://www.cert.org,» [En línea]. Available: http://www.cert.org/resilience/products-services/octave/. [Último acceso: 7 Abril 2015].

[24] Software Engineering Institute, Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Pittsburgh, 2007.

[25] Ministerio de Hacienda y Administraciones Públicas , «http://administracionelectronica.gob.es,» [En línea]. Available: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VSL3j-FSJ5p. [Último acceso: 5 Abril 2015].

[26] The Business Continuity Institute, «BCM Legislations, Regulations, Standards and Good Practices,» The Business Continuity Institute, 2015.

[27] Australian Nacional Audit Office, Business Continuity Managemente Building resilience in public sector entities, 2009.

[28] National Emergency Crisis and Disasters Management Authority, Business Continuity Management Standard and Guide AE/HSC/NCEMA 7000: 2012, 2012.

[29] DRI Internacional, Professional Practices for Business Continuity Practitioners, 2012.

[30] Disaster Recovery Journal and DRI Internacional, Generally Accepted Practices for Business Continuity Practitioners, 2007.

[31] B. Zawanda y J. Schwartz, Business Continuity Management Standards - A side by side comparison, ISACA, 2003.

[32] F. Caviedes Sanabria y B. A. Prado Urrego, «Modelo unificado para identificación y valoración de los riesgos de activos de información de una organización,» Universidad ICESI, Santiago de Cali, 2012.

[33] Ministerio de Hacienda y Administraciones Públicas, «MAGERIT - versión 3.0 Libro II - Catálogo de Elementos,» Ministerio de Hacienda y Administraciones Públicas, Madrid, 2012.

[34] LOGICIEL CIA LTDA., «http://www.logiciel-ec.com,» 2012. [En línea]. Available: http://www.logiciel-ec.com. [Último acceso: 17 03 2015].

[35] LOGICIEL CIA. LTDA., «Planificación Estratégica,» Quito, 2014.

[36] K. C. Laudon y J. P. Laudon, Sistemas de Información Gerencial, Pearson Educación de Mexico, 2012.

[37] TREsPASS Consortium, Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security D5.2.1, Ben Fetler, itrust consulting, 2014.

[38] IESE Business School University of Navarra, «La Evolución del Concepto de Stakeholders en los escritos de Ed Dreeman,» 2009.

[39] National Institute of Standards and Technology, «Contingency Planning Guide for Federal Information Systems,» NIST, Gaithersburg,, 2010.

ANEXOS

ANEXO A - Modelo de la Política de Planificación de Contingencias

POLÍTICA DE PLANIFICACIÓN DE CONTINGENCIAS

<Nombre de la empresa> está comprometida con sus clientes, empleados, accionistas y proveedores. Para asegurar la efectiva disponibilidad de los productos y servicios esenciales, <Nombre de la empresa> ofrece esta política planificación de contingencias para la continuidad del negocio, la prevención de desastres y la recuperación total del negocio.

Propósito

Esta política establece la Política de Contingencias Empresarial, para gestionar los riesgos que implican la interrupción, falla y desastres relacionados con los activos de información mediante el establecimiento de un programa de planificación de contingencias eficaz. El programa de planificación de contingencias ayuda a <Nombre de la empresa> en la implementación de mejores prácticas de seguridad con respecto a la continuidad del negocio y la recuperación ante desastres.

Alcance

El alcance de esta política es aplicable a todos los recursos de Tecnología de la Información (TI) propiedad u operados por <Nombre de la empresa>. Cualquier información, no específicamente identificada como propiedad de otras partes, que se transmite o se almacena en los recursos de TI de <Nombre de la empresa> (incluyendo correo electrónico, mensajes y archivos) es propiedad de <Nombre de la empresa>. Todos los usuarios (empleados, contratistas, proveedores u otros) de los recursos de TI son responsables del cumplimiento de esta política.

Intención

Es la intención de esta política el establecer la capacidad de planificación de contingencias a lo largo de <Nombre de la empresa> para ayudar a la organización a implementar mejores prácticas de seguridad con respecto a la continuidad del negocio y ante recuperación de desastres.

Política

Las siguientes subsecciones describen las normas de planificación de contingencias que constituyen la política de <Nombre de la empresa>. Todo empleado de <Nombre de la empresa> está obligado a cumplir con esta política.

- ***CP1 – Procedimientos de planificación de contingencias:*** Se debe desarrollar, adoptar o cumplir con un procedimiento de planificación de contingencias formal y documentado que incluya el propósito, el alcance, los roles, responsabilidades, el compromiso de la dirección y las estrategias de contingencia.

- ***CP2 - Plan de contingencia:*** Se debe desarrollar un plan de contingencia para los activos de información de la empresa que:
    - Identifique las funciones del negocio esenciales y los requisitos de contingencia asociados.
    - Proporcione los objetivos de recuperación, las prioridades de restauración y las métricas.
    - Incluya los roles, las responsabilidades y los individuos asignados con su información de contacto.
    - Busque mantener las funciones del negocio esenciales a pesar de la interrupción o falla de los activos de información.
    - El plan de contingencia debe ser revisado y aprobado por los funcionarios designados dentro de la organización.
    - El plan de contingencia debe ser informado y distribuido a todos los miembros de la organización.
    - El plan de contingencia debe ser revisado al menos una vez al año y cuando se realicen cambios en la organización, los activos de información, o el entorno de la operación. También en caso de que se hayan encontrado problemas durante la ejecución del plan de contingencia, la implementación, o las pruebas del mismo.

- En caso de que el plan de contingencia cambie, se debe comunicar dichos cambios a todos los miembros de la organización.

- ***CP3 – Capacitaciones:*** Se debe capacitar al personal en sus funciones y responsabilidades de contingencia asignadas y ofrecer cursos de actualización sobre una base anual.

- ***CP4 – Programa de Pruebas y Ejercicios:*** Se debe probar y realizar ejercicios del plan de contingencia por lo menos una vez al año, para determinar la eficacia del plan y la disposición de la organización para ejecutar el plan. Además, se deben revisar los resultados obtenidos de las pruebas o ejercicios realizados e iniciar con las correspondientes acciones correctivas.

- ***CP5 – Telecomunicaciones:*** Se debe establecer servicios alternativos de telecomunicaciones incluidos los acuerdos necesarios para permitir la reanudación de las operaciones dentro de los tiempos de recuperación definidos y los puntos de recuperación establecidos cuando las capacidades de telecomunicaciones primarias no están disponibles.

- ***CP6 – Respaldos de información:*** Se debe realizar respaldos de información a nivel de usuario, a nivel de sistema, y de la documentación de los activos de información (incluida la documentación relacionada con la seguridad). Además, se debe proteger la confidencialidad e integridad de la información de los respaldos en el lugar de almacenamiento.

- ***CP7 – Recuperación y reconstitución:*** Se debe ayudar en la recuperación y reconstitución de los activos de información a un estado conocido después de una interrupción, o fallo de los mismos.

ANEXO B – Modelo del Documento del Plan de Contingencia de TI

PLAN DE CONTINGENCIA

Alcance

Definir el alcance del plan de contingencia tomando en consideración la priorización de los procesos del negocio realizada para la empresa

Roles y responsabilidades

Definir claramente los roles que se harán cargo de las actividades del plan y las responsabilidades de los mismos. Considerar los roles y responsabilidades definidos durante la etapa de desarrollo e implementación de estrategias.

Además, se debe establecer a que empleados de la empresa se les va a asignar los roles e incluir su información de contacto. Para la asignación de roles se debe tener en cuenta la disponibilidad de tiempo, grado de habilidad, conocimientos y tipos de actitudes de cada uno de los empleados.

Evaluación de riesgos

Incluir un resumen que contenga los aspectos más importantes de la evaluación de riesgos como los resultados, las amenazas con un nivel de riesgo más alto, los activos críticos más afectados, etc. También se debe especificar como acceder al informe que contiene todos los aspectos de la evaluación de riesgos.

Análisis de impacto en el negocio

Incluir un resumen que contenga los aspectos más importantes del análisis de impacto en el negocio como los parámetros de recuperación definidos para cada uno de los procesos críticos de la empresa, los recursos mínimos requeridos y el orden de recuperación de los activos críticos. Asimismo se debe especificar como acceder al informe completo del análisis de impacto en el negocio.

Estrategias de contingencia

Incluir todas las estrategias definidas para la prevención y mitigación de las posibles incidencias que se puedan suceder en la empresa, con los enlaces a la documentación que sustente dichas estrategias como políticas, inventarios, etc.

ANEXO C - Modelo del Plan de Pruebas

PLAN DE PRUEBAS

ALCANCE DE LA PRUEBA

Fecha y hora de la prueba

Fecha y hora de inicio	
Fecha y hora de finalización	

Estrategias de contingencia a ser probadas

Nombre de las estrategias de contingencia	Alcance de la ejecución

Objetivos de la prueba

Objetivos

ESCENARIO DE EJECUCIÓN

Premisas básicas de la prueba

(Equipo, procedimientos o condiciones necesarias para conducir la prueba.)

No.	Premisas básicas de la prueba
1	
2	
3	
…	

Suposiciones de la ejecución de la prueba

(Describir las consideraciones a ser tomadas como ciertas al momento de conducir la prueba.)

No.	Suposiciones
1	
2	
3	
…	

Escenario de prueba

(El evento o incidencia considerada para la prueba puede ser tan simple como una falla tecnológica o tan compleja como una gran crisis. Esta sección prepara a los participantes para la prueba, contiene una visión general del escenario de prueba.

Se debe describir:

- El tiempo, ubicación y extensión del daño.
- Secuencia de eventos.
- Informe de daños inicial.
- Condiciones climáticas.)

Instrucciones a los participantes

(Se debe describir que se espera de los participantes de la prueba.)

Directorio de comunicaciones

(Se debe incluir los números de teléfono, fax y/o correo electrónico de todos los contactos con los que los participantes deben comunicarse.)

Nombre	Celular	Teléfono de contacto
Miembros del Equipo		
Vendedores		
Otros		

ANEXO D – Modelo del Plan de Ejercicios

PLAN DEL EJERCICIOS

Sistema:		**Fecha:**	
Tipo de ejercicio:		**Planificador:**	

Facilitador(es) del ejercicio

Nombre del facilitador 1
Nombre del facilitador 2
Nombre del facilitador 3

Participantes del ejercicio

Nombre	Rol
Nombre 1	Rol 1
Nombre 2	Rol 2
Nombre 3	Rol 3

Líneas de tiempo

Tiempo real del ejercicio:
Tiempo del ejercicio:

Objetivos del ejercicio

(Los objetivos deben estar relacionados con el RTO, RPO, MTD, la validación de las estrategias de contingencia y la identificación de las debilidades del plan de contingencia)

Objetivo 1
Objetivo 2
Objetivos adicionales en caso de ser necesario

Escenario del ejercicio

Incidente:	
Impacto al sistema:	
Impacto a las operaciones:	

Suministros y documentación necesaria para el ejercicio

Supuestos

Supuesto 1
Supuesto 2
Supuesto 3

Condiciones

Condición 1
Condición 2
Condición 3

Limitaciones

Limitación 1
Limitación 2
Limitación 3

Lecciones aprendidas

Cumplimento de los objetivos

Objetivo 1	Este objetivo se /no se cumplió. Específicamente, …
Objetivo 2	Este objetivo se /no se cumplió. Específicamente, …
Objetivos Adicionales	A medida que sea necesario

Hojas de evaluación

Objetivo 1:
Comentarios:

Objetivo 2:
Comentarios:
Objetivo n:
Comentarios:

ANEXO E – Modelo del Informe después del ejercicio

INFORME DESPUÉS DEL EJERCICIO

Un ejercicio del plan de contingencia de TI de <nombre de la empresa> se llevó a cabo el <fecha en que se realizó el ejercicio>. Los participantes y sus funciones asignadas se listan a continuación:

Nombre	Rol/Responsabilidad	Telf. de Contacto
	Facilitador del Ejercicio	
	Coordinador de Incidencias	
	Recolector de Información del Ejercicio	
	Líder del Equipo de Recuperación	
	Miembro del Equipo de Recuperación	

El ejercicio del plan de contingencia de TI de <nombre de la empresa> se realizó en base al plan del ejercicio del <fecha del plan del ejercicio>. El plan del ejercicio se realizó en base al siguiente escenario:

<Incluir un resumen del escenario>

El ejercicio fue desarrollado para determinar lo siguiente <listar los objetivos del ejercicio a continuación>:

- Determinar las debilidades del plan de contingencia de TI
- Objetivo 2
- Objetivo 3
- Añadir objetivos adicionales a medida que sea necesario

El ejercicio del plan de contingencia de TI de <Nombre de la Empresa> permitirá identificar la información obsoleta para realizar las correspondientes actualizaciones a medida que sea necesario. El plan del ejercicio y los resultados detallados del ejercicio se encuentran en el Apéndice de este reporte.

1. Resumen de resultados del Ejercicio

Los resultados más significativos del ejercicio fueron:

- Resultado 1

- Resultado 2
- Resultado 3
- Etc.

2. Recomendaciones

Las siguientes recomendaciones se proporcionan como resultado del ejercicio:

- Recomendación 1
- Recomendación 2
- Etc.

3. Áreas de mejora

Las siguientes áreas de mejora se proponen como resultado del ejercicio:

- Área de mejora 1
- Área de mejora 2
- Etc.

4. Fortalezas

Las siguientes fortalezas se encontraron durante la realización del ejercicio:

- Fortaleza 1
- Fortaleza 2
- Etc.

5. Problemas

Los siguientes problemas se encontraron durante la realización del ejercicio:

- Problema 1
- Problema 2
- Problema 3
- Etc.

ANEXO F – Modelo del Plan de Concientización y Capacitaciones

PLAN DE CONCIENTIZACIÓN Y CAPACITACIONES

Objetivos

Objetivo General

Debe expresar lo que se aspira una vez se hayan concluidos la capacitación, se debe responder a las siguientes preguntas: ¿qué se pretende?, ¿dónde, con quién o con qué?, ¿cómo se pretende? Y ¿para qué?

Objetivos Específicos

Listar los logros parciales que se buscan alcanzar durante la capacitación, los mismos que deben apoyar a la consecución del objetivo general.

Alcance

Delimitar la profundidad o extensión de la capacitación a realizar, describiendo de manera detallada los temas a tratar en las capacitaciones y como se las va a realizar. Además, de especificar la duración.

Justificación

Exponer, basándose en argumentos, el por qué es importante realizar la capacitación. Para la redacción se debe pensar en el "para qué se va a hacer la capacitación" y posteriormente responder a las preguntas: ¿con qué?, ¿cómo?, ¿dónde? y ¿cuándo se va a realizar?".

Temas de la capacitación

Detallar los temas y subtemas que serán tratados durante la capacitación.

Recursos

Especificar los recursos humanos y materiales necesarios para llevar a cabo la capacitación. En los recursos humanos se debe listar los participantes, facilitadores y expositores. En cambio en los recursos materiales se debe listar la infraestructura, mobiliario, equipos y documentación.

Presupuesto

Detallar los costos que implicarán llevar a cabo las capacitaciones.

Cronograma

Listar todas las actividades a realizar y las fechas previstas para el inicio y el fin de cada una de las actividades.

ANEXO G – Formulario para Solicitud de Cambios

FORMULARIO PARA SOLICITUD DE CAMBIOS

Solicitado por:	<Nombre de la persona que solicita el cambio>
Fecha de solicitud:	
Descripción del cambio	
<Describir el cambio solicitado.>	
Justificación para el cambio	
<Exponer, basándose en argumentos, el por qué es importante realizar la capacitación. Para la redacción se debe pensar en el "para qué se va a hacer la capacitación".>	
Aprobado por:	<Nombre de la persona que aprueba el cambio>
Fecha de aprobación:	
Fecha en que se hace efectivo:	
Alternativas consideradas	
<Especificar los aspectos del cambio solicitado que se van a considerar para la actualización del plan de contingencia.>	
Alternativas eliminadas	
<Especificar los aspectos del cambio solicitado que no se van a considerar para la actualización del plan de contingencia, con la respectiva justificación de porque se van a eliminar.>	

Firma del Solicitante **Firma del Aprobador**