TEC | Tecnológico de Costa Rica

Área Académica de Administración de Tecnologías de Información.

Propuesta de plan de continuidad de TI para el Área de Tecnologías de Información y Comunicación de JASEC.

Trabajo Final de Graduación para optar por el grado de Licenciatura en Administración de Tecnología de Información.

Elaborado por: Cristian Navarro Martínez.

Prof. Tutor: MAE. Gonzalo Delgado Leandro.

Cartago, Costa Rica.
Noviembre, 2018.

Nota Aclaratoria.

Genero:

La actual tendencia al desdoblamiento indiscriminado del sustantivo en su forma masculina y femenina va contra el principio de economía del lenguaje y se funda en razones extralingüísticas. Por tanto, deben evitarse estas repeticiones, que generan dificultades sintácticas y de concordancia, que complican innecesariamente la redacción y lectura de los textos.

Este documento se redacta de acuerdo con las disposiciones actuales de la Real Academia Española con relación al uso del “género inclusivo”. Al mismo tiempo se aclara que estamos a favor de la igualdad de derechos entre los géneros.

TEC | Tecnológico de Costa Rica

ÁREA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

GRADO ACADÉMICO: LICENCIATURA

Los miembros del Tribunal Examinador del Área de Administración de Tecnologías de Información, recomendamos que el siguiente Trabajo Final de Graduación del estudiante Cristian Navarro Martínez sea aceptado como requisito parcial para obtener el grado académico de Licenciatura en Administración de Tecnología de Información.

Gonzalo Delgado Leandro, MAE.
Profesor Tutor.

Ing. Carlos Luis Mata Montero.
Profesor Lector.

Ing. Luis Chavarría Sánchez. M.Ed.
Coordinador de la carrera.

Ing. Sonia Mora González. MBA.
Coordinadora del Trabajo Final de Graduación.

Pág. iv | xxi

Dedicatoria.

A las personas que han forjado lo que soy hoy, mis más grandes maestros y creadores de todas las oportunidades que la vida me ha brindado, a Josefina Martínez y Virgilio Navarro.

Sin ustedes nada hubiese sido posible, las palabras y las enseñanzas que siempre han tenido para mí, me ayudaron a recorrer un camino que para nada fue fácil.

Mamá, papá; esto les pertenece tanto a ustedes como a mí, para ustedes siempre serán todos los triunfos que alcancé en mi vida.

Agradecimientos.

A Dios, por demostrarme que en la vida todo tiene un propósito, cuando no entendía los andares de la vida, siempre me demostró el porqué de los caminos.

A mis queridos padres, quienes siempre estuvieron para mí y me brindaron todo lo que necesité para alcanzar aquello que un día, vimos lejos.

A mis hermanos, Yuliana Navarro y Gerald Navarro por todo el apoyo, que el esfuerzo realizado, sirva de motivación para soñar y luchar en la vida.

A Valery Picado, por su apoyo, su comprensión y muy especialmente por su entendimiento en muchos momentos durante estos años.

A Gaudy Araya por el cariño, el apoyo, la comprensión y todas esas conversaciones y risas que ayudaron a alivianar mi estadía en el TEC.

A Eddy Martínez, por brindar su apoyo siempre que lo necesité.

A Isela Murillo, Christopher Seas e Ignacio Aguilera por la cálida amistad que los años poco a poco fortificaron.

A las familias Navarro Montero y Picado Ureña por las palabras, los pensamientos y las oraciones tan importantes para mi durante este proceso.

A Luis Javier Chavarría, a Sonia Mora y a Gonzalo Delgado por la motivación, el apoyo y la confianza brindada en muchos momentos claves durante este proceso.

No existen palabras suficientes que manifiesten mi agradecimiento, sin ustedes la alegría que existe en mi corazón por concluir esta etapa no sería posible.

Resumen.

Este trabajo final de graduación se centra en el desarrollo de un plan de continuidad de TI para el área de TIC de JASEC. El planteamiento de la metodología implementada dentro de la investigación tomó como base el modelo PDCA y el manual para la elaboración de un plan de continuidad creado por la Caja Costarricense del Seguro Social (CCSS).

El modelo PDCA permitió estructurar la metodología por medio de etapas globales que permitió ordenar de forma secuencial las actividades que debían ser desarrolladas para alcanzar los insumos necesarios para la creación del plan de continuidad de TI. Con respecto al manual creado por la CCSS, permitió tener la base de referencia para formular las actividades que comprendieron cada etapa principal de la metodología implementada.

A nivel global, como parte de la metodología de este trabajo final de graduación se desarrolló lo siguiente:

- Análisis del contexto actual de la organización: Entendimiento de la organización, respecto al área de TIC.
- Análisis de impacto de negocio: Identificación de activos que gestiona el área de TIC para soportar los procesos críticos del negocio.
- Análisis de riesgo: Identificación de los riesgos que pueden afectar la continuidad de operación del área de TI.
- Desarrollo de estrategias de continuidad: Establecimiento de las estrategias que garanticen la operación continua de los procesos críticos de negocio soportados por activos de TI.
- Pruebas: Una vez creadas las estrategias de continuidad de TI, se realizaron pruebas que probaran y aseguraran su correcto funcionamiento.

Palabras claves: Activo critico de TI, riesgos, continuidad de operaciones, impacto de negocio, estrategia de continuidad.

Abstract.

This final graduation project focuses on the development of an IT continuity plan for the IT area of JASEC. The approach of the methodology implemented within the research was based on the PDCA model and the manual to development an IT continuity plan created by the Costa Rican Social Security Fund (CCSS).

The PDCA model made it possible to structure the methodology by means of global stages that made it possible to sequentially order the activities that had to be developed to reach the necessary inputs for the creation of the IT continuity plan. With respect to the manual created by the CCSS, it allowed to have the base of reference to formulate the activities that included each main stage of the implemented methodology.

At the global level, as part of the methodology of this final graduation work, the following was developed:

- Analysis of the current context of the organization: Understanding of the organization, regarding the IT area.
- Business impact analysis: Identification of assets managed by the IT area to support critical business processes
- Risk analysis: Identification of the risks that may affect the continuity of operation of the IT area.
- Development of continuity strategies: Establishment of strategies that guarantee the continuous operation of critical business processes supported by IT assets.
- Testing: Once the IT continuity strategies have been created, tests are carried out to prove and ensure correct operation.

Keywords: IT critical asset, risk, continuity of operations, business impact, continuity strategy.

Índice General.

Índice de Ilustraciones.

Índice de Tablas.

Índice de Gráficos.

1. Capítulo I: Introducción.

1.1. Antecedentes.

Este apartado presenta un conjunto de aspectos relevantes a modo de resumen, con el objetivo de contextualizar el entorno de desarrollo de este trabajo final de graduación.

Primeramente, se resume la descripción de la organización, se detalla algunos puntos claves como la misión, la visión y la propuesta de valor que mantiene como organización.

Seguidamente se menciona los aspectos referentes a la estructura organizativa tanto de JASEC como del área de Tecnologías de Información y Comunicación (en adelante TIC), igualmente se especifica las funciones de cada departamento del área de TIC.

Además, se detalla los proyectos realizados dentro de la organización, esto con el propósito de contextualizar esta investigación.

1.1.1. Descripción de la organización.

La organización donde se enfoca el desarrollo de este trabajo final de graduación es la Junta Administrativa Servicio Eléctrico de Cartago (en adelante JASEC), quien es la principal responsable de dotar a la provincia de Cartago del servicio de fluido eléctrico, el cual permita a todos sus usuarios contar con un servicio eficiente y confiable.

Asimismo, a partir del año 2015, JASEC diversifica la gama de servicios que brinda en la provincia de Cartago, añadiendo a su catálogo el servicio de internet por medio de una red de fibra óptica.

1.1.2. Misión.

La misión de JASEC es la siguiente:

“Contribuimos a mejorar la calidad de vida de nuestros clientes mediante la prestación eficiente de servicios de interés público, con los más altos principios éticos que procuran la igualdad de oportunidades, el desarrollo sostenible y la responsabilidad social” (JASEC, 2018).

1.1.3. Visión.

La visión de JASEC es la siguiente:

“Brindamos a nuestros clientes servicios de interés público caracterizados por la disponibilidad y continuidad, siendo reconocidos por nuestra eficiencia, tecnología e innovación, que contribuyen al desarrollo de Cartago” (JASEC, 2018).

1.1.4. Propuesta de valor.

Como propuesta de valor, JASEC dentro de su filosofía mantiene los siguientes valores:

- Compromiso: Es la actitud que identifica la lealtad y la dedicación personal, organizacional y ambiental de los colaboradores y cuerpos directivos; es

sentir y vivir como propios los objetivos y metas organizacionales, responsabilizándose por el logro de estos.

- Honestidad: Es un valor que procura siempre anteponer la verdad en sus pensamientos, expresiones y acciones.
- Solidaridad: Es el compromiso manifiesto de los funcionarios con las necesidades de los grupos de interés, los usuarios y sociedad en general.

1.1.5. Sobre la organización.

A continuación, se detalla el contexto histórico alrededor de la creación de JASEC, su actualidad y la filosofía de valor que mantiene.

1.1.5.1. Contexto histórico.

Según se detalla dentro su historia, JASEC menciona lo siguiente.

> Durante el mes de noviembre de 1961, se generan aumentos en las tarifas eléctricas, las cuales se unen al reclamo que tienen los cartagineses de la época por poseer mejores instalaciones eléctricas en diferentes sectores de la provincia de Cartago, todo esto genera la huelga llamada “Huelga de pagos eléctricos”.
>
> Dicha huelga, apoyada por el medio de comunicación Radio Victoria, que ayuda con la divulgación de los distintos aumentos desmedidos por el pago del servicio eléctrico que sufren distintos sectores del comercio cartaginés, crea un plasmado fervor cívico a plantear soluciones a la situación que vive para entonces el pueblo de Cartago, este movimiento es el más significativo a nivel popular.
>
> La huelga ya se prolonga por más de dos años y la improvisación de manifestaciones sin horas programadas con ayuda de volantes,

> comunicados de radio y alto civismo demostrado por los cartagineses, contribuye decididamente a que la Asamblea Legislativa agilice el proyecto de ley para la creación de una junta administradora del servicio eléctrico en la provincia de Cartago (JASEC, 2016).

Todo este movimiento realizado por los cartagineses, contribuye a que el 12 de octubre de 1964 nazca la Junta Administrativa Servicio Eléctrico de Cartago.

1.1.6. Estructura de la organización.

La estructura organizativa de JASEC se encuentra establecida por una estructura organizativa mixta (Véase Ilustración 1).

El trabajo final de graduación se desarrolla en el área de TIC, tomando en consideración distintas áreas que gestionan procesos críticos del negocio dentro de JASEC.

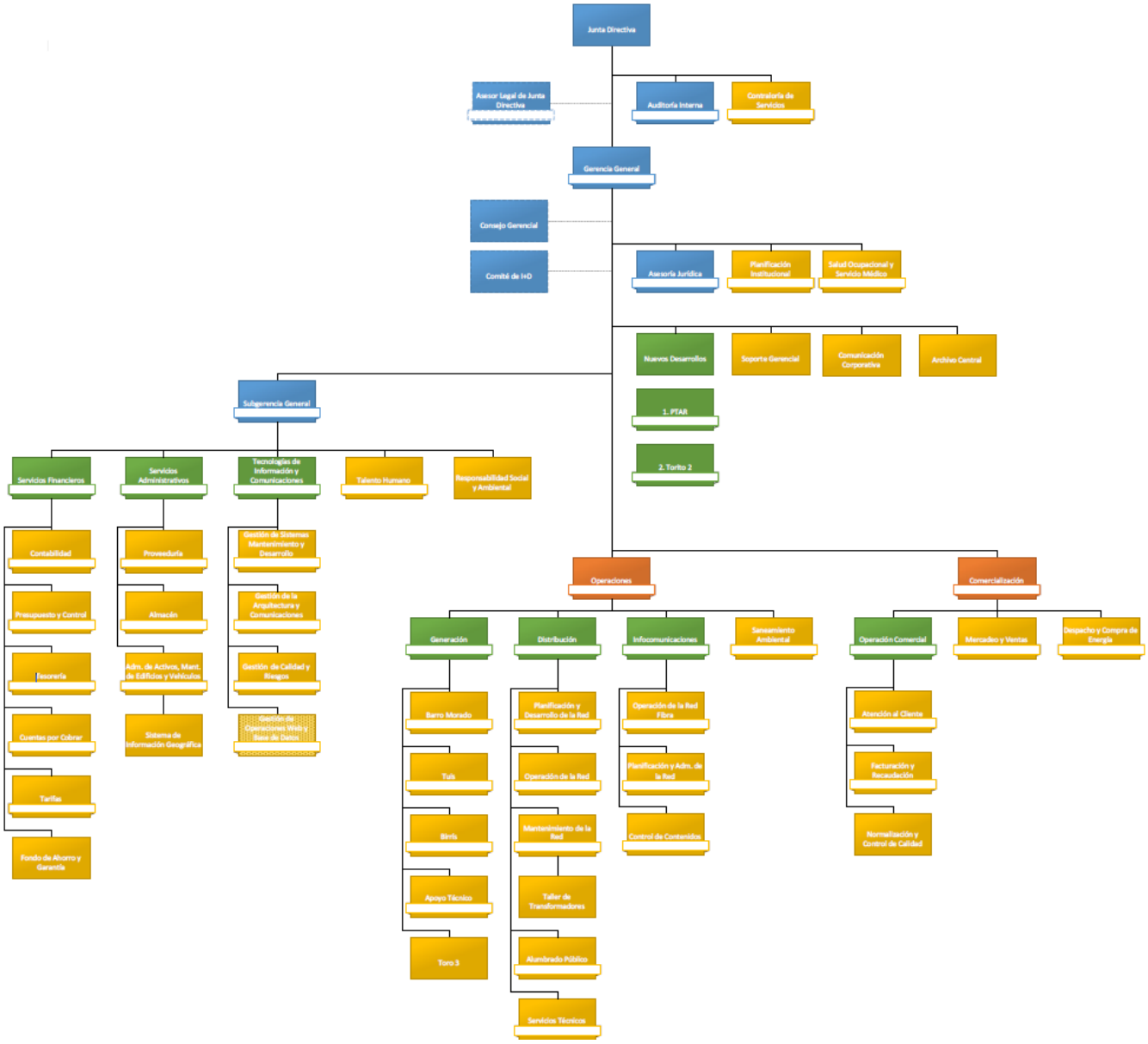


Ilustración 1 - Organigrama de JASEC.

Fuentes JASEC (2018)

1.1.7. Área de tecnología de información y comunicación.

A continuación, se presenta brevemente, información sobre el área de TIC con su respectiva estructura organizacional.

1.1.7.1. Descripción del área.

El área de TIC de JASEC está conformada por un equipo que se encarga de brindar soporte a las operaciones relacionadas con Tecnología de Información (en adelante TI) y brinda soporte a las operaciones de las demás unidades de negocio.

Dicha área está liderada por un jefe de área, que se encarga de velar por el alineamiento del área, de acuerdo con los objetivos de la organización, además de coordinar los esfuerzos realizados entre los departamentos que la conforman (Véase Tabla 1).

Tabla 1 - Departamentos y funciones del área TIC.

Departamento	Funciones
Gestión de la arquitectura y comunicaciones.	• Mantener la operación y dar asistencia a la red de comunicaciones de JASEC. • Brindar mantenimiento tanto a hardware como a hardware de la organización. • Realizar gestiones de respaldo, recuperación y restauración de bases de datos. • Administración de la seguridad informática dentro de la organización.
Gestión de calidad y riesgos.	• Realizar investigaciones para determinar factibilidad de proyectos para su diseño, desarrollo, implantación y mantenimiento. • Gestionar reportes de control. • Realizar documentación relacionada con sistemas de información a nivel técnico como de usuario.

	• Capacitaciones al personal. • Brindar mantenimiento a los sistemas de información y efectuar los ajustes necesarios.
Gestión de sistemas, mantenimiento y desarrollo.	• Elaborar estándares y procedimientos para el desarrollo de sistemas de información. • Administrar los sistemas de información. • Asesorar las dependencias de JASEC referente a los sistemas de información. • Adquisición de licencias de desarrollo.

Fuente: Elaboración propia

1.1.7.2. Estructura del área.

En el caso de la JASEC, el área de tecnologías de TIC se encuentra estructurada por medio de departamentos funcionales (Véase Ilustración 2).

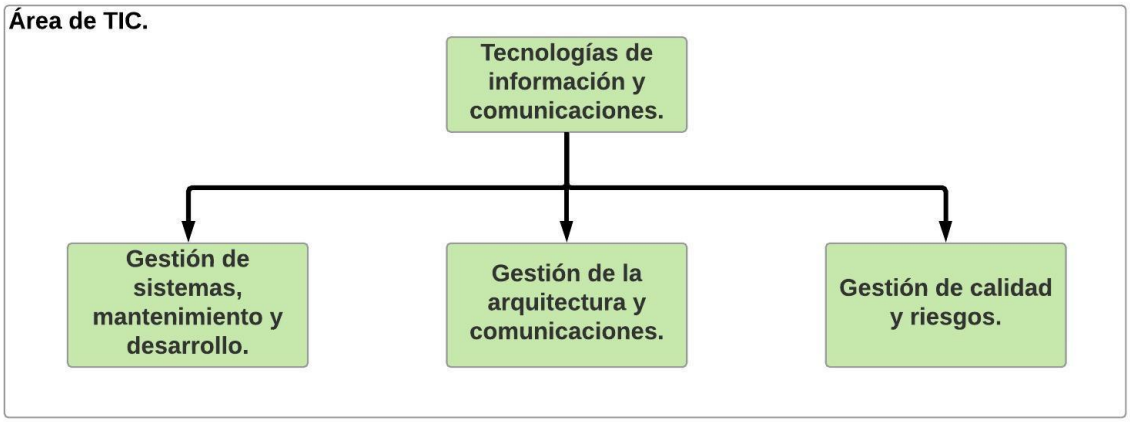


Ilustración 2- Áreas funcionales - Área de TIC.

Fuente: JASEC (2018)

1.1.8. Proyectos similares.

A continuación, se detallan los proyectos realizados dentro de la organización y mantienen relación con respecto al desarrollo de este trabajo final de graduación.

1.1.8.1. Plan de continuidad de la plataforma tecnológica.

Como JASEC es una entidad pública, debe acoger y acatar diferentes lineamientos planteados por las entidades regulatorias del país; un ejemplo de ellas es la Contraloría General de la República (en adelante CGR), quien en el 2007 aprueba las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, donde establece criterios de control, los cuales deben ser aplicados dentro de la gestión de las tecnologías de información de todo ente público del país.

En dichas normas, se menciona que toda organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad (Contraloría de la República de Costa Rica, 2007, p 11).

Con el fin cumplir con tal normativa en el año 2014, JASEC contrata una empresa consultora con el objetivo de desarrollar un plan de continuidad de la plataforma tecnológica.

De acuerdo con lo anterior, como parte de los proyectos similares realizados dentro de la organización de JASEC, se encuentra el plan de continuidad de la plataforma tecnológica desarrollado por la empresa consultora.

1.2. Planteamiento del problema

En esta sección se presenta la situación problemática que se desea abordar con el desarrollo de este trabajo final de graduación; además, los beneficios esperados con la implementación del plan de continuidad de TI.

1.2.1. Situación problemática.

En la actualidad, las organizaciones deben cumplir con las exigencias del mercado, ofreciendo operaciones continuas que permitan generar valor a sus usuarios, garantizando que los procesos y la información que utilizan, permanezcan disponibles continuamente para los usuarios que lo requieran.

Aunque JASEC cuenta con un plan de continuidad de TI, ese mantiene información desactualizada tanto a nivel operativo como administrativo; además, hace referencia a departamentos dentro del área de TIC que dentro de la nomenclatura organizativa actual no corresponden; igualmente, dentro del plan de continuidad de TI se hace referencia a la Unidad Estratégica de Negocio de Tecnología de Información, cuando actualmente está denominada como Área de Tecnología de Información y Comunicación, provocando que por los aspectos mencionados, el plan de continuidad existente no corresponda.

De igual forma, el plan de continuidad de TI con el que cuenta JASEC está basado en un inventario de activos de TI desactualizado, pues el inventario de activos de TI actual no corresponde al considerado en el 2014 para la elaboración del plan de continuidad de TI, dado que con el pasar de los años, el área de TIC ha realizado la adquisición de equipos nuevos y ha desarrollado nuevos sistemas informáticos; esto ha provocado que los procedimientos recomendados dentro del plan de continuidad de TI actual no apliquen en su totalidad.

Otro aspecto importante dentro de la situación problemática a considerar, es que el plan de continuidad de TI desarrollado por la empresa consultora no se encuentra apoyado por un análisis de riesgos, que logre brindar un respaldo sólido que justifique los procedimientos documentados dentro del plan de continuidad actual.

Con la creación de un plan de continuidad, tanto el área de TIC como la organización logra contar con conocimiento sobre los riesgos que pueden impactar la continuidad de las operaciones de aquellos activos que soportan procesos críticos de JASEC y su correspondiente plan de acción.

1.2.2. Problema.

La inexistencia de un plan que asegure la continuidad de TI para los activos que soportan los procesos críticos de JASEC y, que además logre responder a lo establecido dentro de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la CGR, genera la siguiente pregunta de investigación:

¿Cuál es el plan que asegura la continuidad de los activos de TI que soportan los procesos críticos de negocio de JASEC?

1.2.3. Definición del proyecto.

Este proyecto tiene como finalidad proponer el desarrollo de un plan de continuidad de TI, mediante el uso de normativas y mejores prácticas, que permita asegurar la operación continua de los activos de TI que soportan los procesos críticos del negocio de JASEC.

1.3. Beneficios esperados del trabajo.

Dentro de los beneficios que se espera alcanzar con la creación del plan de continuidad para los activos críticos de TI, se encuentra los siguientes:

- Implementación de un plan que permita mantener la continuidad de las operaciones de procesos críticos de negocio soportados por el área TIC, cuando sean afectadas por un evento que interrumpa sus operaciones normales.
- Identificación de recursos y procedimientos claves para brindar la continuidad de los activos críticos de TI, en caso de la materialización de un evento que interrumpa las actividades propias de sus operaciones.
- Identificación y clasificación de personal responsable y sus respectivas tareas por desarrollar dentro del plan de continuidad.
- Minimizar el impacto generado por la afectación de un evento dentro de las operaciones de procesos críticos de negocio soportados por los activos de TI.
- Cumplimiento de los requisitos regulatorios interpuestos por la CGR, con respecto a la continuidad de los procesos críticos soportados por activos de TI.

1.4. Objetivos

Esta sección enuncia los objetivos planteados para el desarrollo del trabajo final de graduación. Plantea primeramente el objetivo general, seguido por los objetivos específicos.

1.4.1. Objetivo general.

El objetivo general del trabajo final de graduación es el siguiente.

- Desarrollar un plan de continuidad de TI para los activos que soportan procesos críticos de negocio de JASEC.

1.4.2. Objetivos específicos.

Los objetivos específicos del trabajo final de graduación son los siguientes:

- Identificar los procesos críticos de negocio de JASEC y su relación con los activos de TI.
- Determinar los riesgos asociados a los activos de TICde JASEC con su respectivo nivel probabilidad de ocurrencia e impacto.
- Preparar las estrategias de respuesta y recuperación necesarias dentro el plan de continuidad para los activos de TI que soportan procesos críticos de negocio de JASEC.
- Validar mediante la ejecución de una prueba la efectividad del plan de continuidad para los activos de TI.

1.5. Alcance

El alcance de este proyecto final de graduación es que, se encuentre demarcado por el desarrollo del plan de continuidad para los activos de TI que soportan procesos críticos de negocio de JASEC.

Sin embargo, existen actividades necesarias para alcanzar dicho objetivo, las cuales deben ser consideras al momento de definir el alcance de este trabajo final de graduación, se detallan a continuación.

- Análisis y actualización de la documentación de TI.
- Identificación de activos críticos.
- Análisis de riesgos de TI.
- Identificación de estrategias para la continuidad de TI.
- Ejecución de una prueba para validar el plan de continuidad de TI.

1.5.1. Limitaciones del alcance.

En este apartado, se describe aspectos que no son tomados en cuenta en el desarrollo de este trabajo final de graduación; dichos aspectos no forman parte de los resultados esperados ni de los entregables del proyecto.

Es importante destacar que el plan de continuidad de TI está enfocado únicamente en los activos de TI que soportan procesos críticos del negocio de JASEC.

Del mismo modo, no se incluye los siguientes aspectos dentro del desarrollo de este trabajo final de graduación:

- Plan de mitigación de riesgos para el área de TIC.
- Plan de recuperación contra desastres.
- Plan de continuidad para los demás activos de TI de JASEC.

1.6. Entregables

En esta sección se presenta los principales entregables que se genera como parte del desarrollo de este proyecto. Para ello se contempla tres categorías, los entregables académicos, entregables de producto y entregables de gestión.

1.6.1. Entregables académicos.

Los entregables académicos están dirigidos al Tecnológico de Costa Rica, específicamente a la coordinación del trabajo final de graduación y al profesor tutor asignado. Estos entregables se dividen en:

- Avances solicitados por el profesor tutor o por la coordinación.

Evidencia de las actividades realizadas dentro del desarrollo del trabajo final de graduación, acotado en periodos específicos y que muestra evidencia tanto del estatus como el avance del proyecto.

- Informe final del trabajo de graduación.

Informe académico que documenta los resultados obtenidos producto de la investigación realizada como parte del trabajo final de graduación.

1.6.2. Entregables de producto.

Los entregables de producto representan el resultado del trabajo final de graduación, estos son los que se entregan a la organización y generan valor por su contenido. Para este proyecto los entregables para la organización son los siguientes:

- Documentación de TI actualizada.

Mediante un análisis de la situación actual del área de TIC de JASEC, se realiza una verificación de la documentación actual referente a TIC, con respecto a inventario de activos de TI, manual de puestos, manual operativo.

La documentación referente a inventario de activos de TI y el manual de puestos se actualiza, puesto que existe un desfase entre lo documentado y lo existente.

- Plan de continuidad de TI.

Documento que establece las estrategias necesarias para garantizar la continuidad de operaciones, los activos de TI que fungen como soporte para las operaciones críticas del negocio dentro de JASEC. Además, presenta los roles y responsabilidades establecidos a los colaboradores del área de TIC de JASEC para la ejecución del plan de continuidad.

- Documentación relacionada con pruebas realizadas.

Documentación resultante de la prueba realizada al plan de continuidad, dicha prueba es ejecutada con el fin de validar las estrategias establecidas para garantizar la continuidad de operación de activos críticos que soportan procesos críticos de negocio dentro de JASEC.

1.6.3. Entregables de gestión.

Los entregables de gestión representan un conjunto de documentos que se genera durante el proyecto y pretenden brindar información sobre los acuerdos, cambios y estados relacionados con el desarrollo y gestión del proyecto.

Los principales entregables de gestión son los presentados a continuación.

- Minutas de reunión.

Como parte del desarrollo de este trabajo final de graduación, se realiza minutas que documentan aspectos discutidos dentro de las reuniones, acuerdos alcanzados y las personas participantes de las reuniones. Toda esta información con el propósito de respaldar lo abordado y objetivos propuestos dentro del avance del proyecto.

- Solicitudes de cambio.

Permiten mantener control sobre las modificaciones realizadas dentro del proyecto, referente tanto al alcance como en actividades o entregables propios del desarrollo del proyecto. Las solicitudes de cambio detallan el cambio realizado, su impacto y la razón que lo justifica.

1.7. Supuestos.

Como parte de los supuestos contemplados para el desarrollo de este trabajo final de graduación se encuentran:

- Acceso a información de la organización requerida para el desarrollo del plan de continuidad de TI.
- Disposición de los colaboradores tanto del área de TIC como de la organización en general.
- Información actualizada de los activos de TI que gestionan los colaboradores del área de TIC.

1.8. Limitaciones.

Como parte de las limitaciones presentes dentro de este trabajo final de graduación se encuentran:

- Dentro del informe se limita la divulgación de información al público referente a la organización y al área de TIC.
- La organización al no contar con un sitio alterno, limito el ámbito de acción con respecto al desarrollo de estrategias de continuidad para el plan de continuidad de TI.

2. Capítulo II: Marco teórico

El presente capítulo contiene la base teórica para el sustento y entendimiento necesario en el desarrollo de esta investigación.

Primeramente, se introduce el concepto de análisis de impacto de negocio y otros aspectos relacionados que son de importancia para el desarrollo tanto de la investigación como para la propuesta de solución para la organización.

Más adelante se contempla el análisis de riesgos, así como definiciones que contextualiza dicho análisis. Además, se aborda mejores prácticas, normas y marcos de referencia relevantes tanto para el análisis de riesgos como para la investigación.

Finalmente, se aborda conceptos relacionados con la continuidad del negocio; además, se considera normas y modelos necesarios para el desarrollo e implantación de un plan de continuidad de TI.

2.1. Procesos de negocio.

Un proceso de negocio consiste en una unidad de un sistema que inicia y termina transacciones con los clientes en un determinado tiempo, cumpliendo un objetivo completo y agrega valor (Bravo, 2009).

De acuerdo con el Consejo de Auditoría Interna General del Gobierno de Chile, quien cita la Norma Internacional ISO 9000 (2005), un proceso corresponde a un conjunto de actividades mutuamente relacionadas o que interactúan y transforman elementos de entrada en resultados.

Igualmente, un proceso puede pasar por distintos cargos, por tal motivo los procesos alcanzan a toda una organización y la cruzan horizontalmente y puede ser divido tanto en macroprocesos como procesos operativos (Bravo, 2009).

2.1.1. Análisis de impacto de negocio.

Un análisis de impacto de negocio (en adelante BIA), corresponde a un análisis que brinda insumos que permiten identificar los activos críticos necesarios para la creación del plan de continuidad de TI y con ello, dedicar los esfuerzos necesarios para garantizar la continuidad de operaciones en aquellos procesos críticos del negocio que son soportados por el área de TI.

2.1.1.1. Definición.

Un BIA es un análisis que permite estimar la afectación generada por la ocurrencia de un desastre o incidente dentro de una organización.

Según Livingstone (2010), un BIA es un proceso metodológico utilizado para identificar los procesos críticos del negocio y analizar el alcance del impacto en caso de una posible interrupción.

Además, Kirvan (2013) menciona que un BIA es parte clave del proceso de continuidad de negocio, puesto que permite analizar las funciones de negocio críticas e identifica el impacto que tendría una organización por la pérdida de esas funciones.

Livingstone (2010) menciona que un conjunto de resultados que generan un BIA, que por su importancia son considerados dentro del desarrollo de esta investigación, se detallan a continuación:

- Criticidad de cada proceso necesario para la operación del negocio.
- Funciones de negocio a nivel departamental.
- Dependencias entre procesos y recursos.
- Tiempo máximo que la organización puede continuar sin un proceso determinado.
- Conocimiento sobre los recursos disponibles para reestablecer la operación de un proceso.
- Insumos disponibles para la creación de planes de continuidad, según necesidades del negocio.

Dado que un BIA conlleva un esfuerzo que requiere el involucramiento de diferentes áreas de la organización, varios requisitos deben ser considerados para un correcto desarrollo.

Los requisitos necesarios según Livingstone (2010), son los siguientes:

- Mantener el BIA lo más simple posible.
- Establecer una propuesta para el desarrollo del BIA que logre generar valor a la gerencia.
- Explicar el proceso que conlleva un BIA y los beneficios que brinda, con el afán de generar una cultura de aceptación y cooperación dentro de la organización.

Dentro del desarrollo de un BIA, es necesario desarrollar un conjunto de procesos clave para la creación de un plan de continuidad de TI, los cuales seguidamente se detallan.

2.1.1.2. Recolección de datos.

La recolección de datos es un paso clave dentro del análisis BIA. Livingstone (2010) recomienda ciertos aspectos importantes para realizar la recolección de datos, se detallan a continuación.

2.1.1.2.1. Información necesaria.

Durante la recolección de datos necesaria en la elaboración de un análisis BIA, la información a recolectar debe cubrir lo siguiente:

- Procesos de negocio de cada departamento de la organización.
- Recursos necesarios por proceso para funcionar correctamente.
- Relación entre procesos de negocio.
- Impactos sobre la organización en caso de interrupción de los procesos.
- Tiempos máximos de interrupción.

2.1.1.3. Valoración de impacto.

Dentro de un BIA, es necesario valorar el nivel de impacto que genera una posible interrupción de los procesos identificados por medio de la etapa anterior dentro de la organización.

Según Livingstone (2012), la valoración del impacto no está relacionada directamente con la causa de la interrupción, la valoración se aplica al impacto de no contar con un proceso de negocio con un correcto funcionamiento.

2.1.1.3.1. Categorías de impacto.

El impacto de la interrupción de un proceso dentro de la organización puede representar una afectación que es posible categorizar, la Caja Costarricense del Seguro Social (2007) (En adelante CCSS), dentro de su manual para elaborar un plan de continuidad las definió en cuatro categorías (Véase Tabla 2).

Tabla 2 - Categorías de Impactó.

Categoría	Descripción.
Operacional.	Afectación operativa dentro de la organización.
Legal o regulatorio.	Afectación por medio de una sanción de carácter legal o regulatorio.
Financiero.	Afectación en las finanzas de la organización.
Reputación.	Afectación a nivel de imagen de la organización.

Fuente: CCSS (2017).

2.1.1.3.2. Escenarios de impacto.

Existe escenarios en que se presenta durante la interrupción de un proceso y por consiguiente generan un determinado impacto, según Livingstone (2008) se clasifica en tres tipos de escenarios (Véase Ilustración 3).

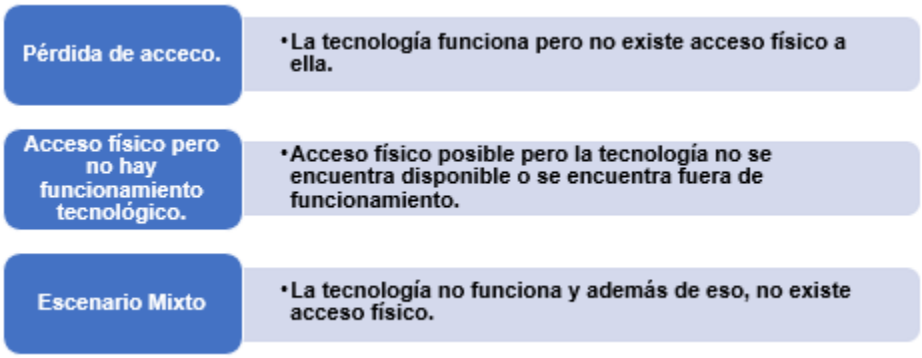


Ilustración 3 - Escenarios de Impacto.
Fuente: Livingstone (2008).

2.1.1.4. Dependencias entre procesos.

La interrupción de un proceso puede generar afectación a otros procesos, por ello es importante definir la dependencia existente entre procesos.

Esta consideración brinda la posibilidad de realizar una estimación más acertada del impacto real que genera la interrupción de un proceso con su correspondiente reacción en cadena, en caso de existir dependencias entre procesos.

2.1.1.5. Requerimientos de recuperación.

Definir y entender los requerimientos de recuperación es un proceso clave dentro del análisis BIA, los requerimientos hacen referencia a métricas de tiempo, son generadas al momento de analizar el impacto generado por una interrupción (Véase Ilustración 4).

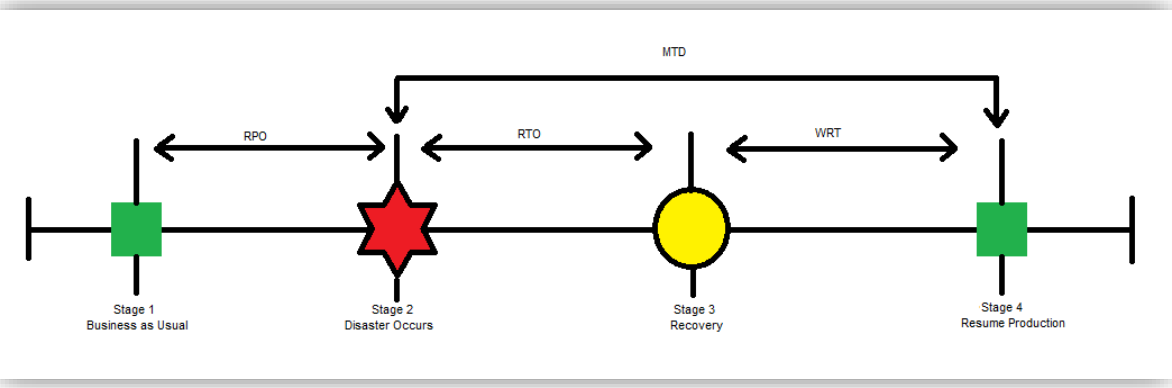


Ilustración 4 - Métricas de recuperación.
Fuente: Default Reasoning (2013).

Según detalla MINTIC (2015), dentro de su guía técnica para la elaboración de un BIA, los requerimientos de recuperación son los siguientes:

- RTO (Tiempo de recuperación objetivo): Corresponde al tiempo transcurrido entre una interrupción y la recuperación de las operaciones del proceso. Indica el tiempo para recuperar los sistemas y recursos interrumpidos.
- RPO (Punto de recuperación objetivo): Rango de tolerancia que una organización puede tener sobre la pérdida de datos.
- WRT (Tiempo de trabajo de recuperación): Es el tiempo invertido en realizar las correcciones o reparaciones necesarias y recuperación de datos perdidos.
- MTD (Tiempo máximo de inactividad tolerable): Espacio de tiempo que durante un proceso puede permanecer inoperable hasta que la organización empiece a generar pérdidas.

2.2. Riesgos.

Para contextualizar el término de riesgo, Fiorito (2006) lo define como situaciones que involucran incertidumbre, en el sentido de que el rango de posibles resultados para una determinada acción es en cierta medida significativo.

Además, es importante agregar que el riesgo hace referencia a la probabilidad de que una determinada amenaza logre materializarse en un evento, localizado en el tiempo que supere la capacidad de atención de una organización con sus recursos habituales. (Soldano, 2009, p 2).

Tomando en consideración el abordaje dado por los anteriores autores respecto al concepto de riesgo, se entiende que el riesgo tiene relación directa con respecto a la incertidumbre. Sin embargo, para Cienfuegos (2013), el riesgo puede ser considerado como no tener seguridad de aquello que va a suceder, además la

incertidumbre puede ser considerada como no tener conocimiento ni siquiera de la probabilidad de aquello que va a suceder.

Por lo tanto, la incertidumbre no puede ser medida ni calculada, mientras que el riesgo puede ser medido a través de una fórmula donde se considere la probabilidad y el impacto (Cienfuegos, 2013).

2.2.1. Riesgos de TI.

Las tecnologías de información y comunicación dentro de una organización no se encuentran ajenas a diferentes situaciones asociadas con el uso de tecnologías de información, como lo son los riesgos de TI.

Por tal motivo, los riesgos de TI dentro de una organización se encuentran relacionados con la incertidumbre que existe dentro de sus operaciones, la probabilidad de pérdidas que puede generar (Kumsuprom, 2010).

Los riesgos de TI pueden ocasionar periodos de inactividad de operaciones dentro de una organización, provocando desde la pérdida de productividad, la exposición de información de clientes por pérdida de seguridad hasta la inadecuada gestión de registros (Alvarado & Zumba, 2015).

2.2.2. Análisis de riesgos.

El análisis de riesgos es una metodología que tiene como finalidad establecer tanto la probabilidad de ocurrencia de un riesgo, como su nivel de impacto y sus respectivas consecuencias, logrando establecer un nivel de riesgo proporcional a su realidad (Tellez, 2015).

A su vez, dentro de la norma internacional ISO 31010 (2009), se define el análisis de riesgos como un proceso estructurado que logra identificar cómo pueden ser afectados los objetivos de una organización por la materialización de un riesgo, igualmente permite generar una visión del riesgo en término de consecuencias y de su respectiva probabilidad con el objetivo y, generar los criterios necesarios para la toma de decisiones proactivas que logren prevenirlos o mitigarlos.

La importancia del análisis de riesgos dentro del desarrollo de un plan de continuidad de TI, está comprendida por la identificación real del riesgo que puede afectar las operaciones dentro de una organización y con esto, lograr desarrollar estrategias dirigidas a contrarrestar dichos riesgos.

2.2.2.1. Categorización del riesgo.

Dentro de la sección de análisis de riesgos, se categoriza los riesgos (Véase Tabla 3), tomando como referencia lo indicado dentro del manual para elaborar un plan de continuidad creado por la CCSS (2007).

Tabla 3 - Categorías de riesgo.

Categoría de riesgo
Interrupción eléctrica.
Fallos en hardware.
Fallos en software.
Desastres naturales.
Incendio.
Fallos en respaldos.
Virus.
Violaciones en la seguridad física.
Intrusión.
Recurso humano.

Fuente: CCSS (2007).

Igualmente, dentro de dicho manual son considerados un conjunto de aspectos mínimos, que ayudan a militar la materialización de un riesgo asociado con cada categoría (Véase Tabla 4).

Tabla 4 - Consideraciones mínimas.

Categoría de riesgo	Consideraciones mínimas.
Interrupción eléctrica.	• Fuentes alternas de generación eléctrica: UPS y plantas eléctricas. • Mantenimiento de las fuentes alternas de generación eléctrica. • Estado de la instalación y capacidad eléctricas instalada. • Lámparas de emergencia. • Señalamiento iluminado de salidas y puertas de emergencia.
Fallos en Hardware.	• Equipo de cómputo utilizado y obsolescencia. • Capacidad de redundancia entre servidores. • Monitoreo de problemas en los servidores. • Contratos de mantenimiento preventivo y correctivo. • Condiciones físicas y ambientales (limpieza, humedad, temperatura).
Fallos en Software.	• Desarrollo local de aplicaciones (metodologías/ estándares). • Cambios y configuración en aplicaciones. • Trascendencia de los sistemas incluidos en el estudio.
Fallos en comunicaciones	• Soporte técnico de los equipos utilizados.

Categoría de riesgo	Consideraciones mínimas.
	• Mantenimiento preventivo y correctivo de los equipos de comunicación.
Desastres naturales.	• Pólizas de seguro vigentes. • Brigadas de atención ante situaciones de emergencia. • Capacitación al personal. • Rutas de evacuación. • Iluminación de pasillos y puertas y salidas de emergencia.
Incendio.	• Pólizas vigentes de seguro. • Sistemas automáticos y manuales contra incendio. • Uso de materiales retardantes del fuego. • Almacenamiento de material combustible. • Detectores de humo revisados regularmente.
Fallos en respaldos.	• Procedimientos para respaldo y recuperación de información, fuentes, objetos, documentación y configuración de los sistemas. • Periodicidad de los respaldos. • Facilidades y protección para el almacenamiento dentro y fuera de sitio. • Configuración de los discos duros de los servidores. • Documentación actualizada sobre procedimientos de respaldo y recuperación.
Virus.	• Programa antivirus instalado en computadoras y servidores. • Configuración y actualización del software antivirus. • Consultas regulares de fuentes de información para actualizaciones sobre virus.

Categoría de riesgo	Consideraciones mínimas.
	• Capacitación al personal para identificar potenciales fuentes de ataque de virus. • Políticas para el ataque de virus.
Violaciones a la seguridad física.	• Seguridad física para el ingreso al edificio, oficinas y cuartos de servidores y equipos de comunicación. • Capacitación al personal para detectar situaciones que puedan representar riesgo o cuestionar la presencia de personas desconocidas o sin identificación. • Sistemas de seguridad: circuitos cerrados de televisión, sensores de movimiento, alarmas. • Revisión y control de salida e ingreso de equipo de cómputo. • Utilización de bitácoras para el registro de ingresos.
Intrusión.	• Procedimientos para otorgamiento de acceso a las aplicaciones y políticas de acceso lógico. • Procedimientos para el acceso a los recursos tecnológicos (redes y aplicaciones). • Administración y configuración de “firewalls”. • Monitoreo de los accesos tanto legítimos como ilegítimos. • Disponibilidad de herramientas para el monitoreo de la seguridad.
Recurso humano.	• Dependencia en el personal. • Capacitación. • Documentación de las funciones del personal.

Fuente CCSS (2007)

2.2.2.2. Nivel de probabilidad.

En el manual para la elaboración de un plan de continuidad anteriormente mencionado, contiene dentro de la guía para la elaboración del análisis de riesgos, que brinda una clasificación que facilita calcular el nivel de probabilidad de los riesgos (Véase Tabla 5).

Tabla 5 - Nivel de probabilidad.

Nivel de probabilidad		Ocurrencia
Muy probable.	10	Es muy probable que ocurra un evento en un periodo de 3 meses.
Probable	7	Es poco probable que ocurra un evento en un periodo de 3 a 6 meses.
Moderada	5	El evento ocurrirá en algún momento en un periodo de 6 meses a 1 año.
Poco probable	3	Es poco probable que el evento suceda, pero podría suceder en un periodo de 1 año a 2 años.
Muy poco probable.	1	Es muy poco probable que el evento se presente en un periodo de 2 años.

Fuente: CCSS (2007).

2.2.2.3. Nivel de impacto.

Igualmente, en el manual para la elaboración de un plan de continuidad elaborado por la CCSS, dentro de la guía para la elaboración del análisis de riesgos, especifica la clasificación para el nivel de impacto de los riesgos (Véase Tabla 6).

Tabla 6 - Nivel de impacto.

Nivel de impacto		Descripción.
Crítico.	10	El evento provoca una interrupción completa dentro de las operaciones del área de TIC de JASEC. Provoca una afectación total de los procesos críticos del negocio.
Significativo.	7	El evento provoca una interrupción entre completa y parcial dentro de las operaciones del área de TIC de JASEC. Provoca una afectación parcial de los procesos críticos del negocio.
Moderado.	5	El evento provoca una interrupción en las operaciones del área de TIC de JASEC. Las actividades críticas de negocio no se ven afectadas.
Menor.	3	El evento provoca un impacto leve en las operaciones del área de TIC de JASEC sin generar interrupciones dentro de las operaciones.
Insignificante.	1	El evento no provoca un impacto dentro de las operaciones del área de TIC de JASEC.

Fuente: CCSS (2007).

2.2.2.4. Matriz de probabilidad versus impacto.

Con el objetivo de determinar el nivel de riesgo asociado según el nivel de probabilidad e impacto identificado para cada uno de los riesgos, se multiplica cada valor asignado. La asignación del nivel se realiza ubicando el valor obtenido entre los rangos especificados (Véase Tabla 7).

Tabla 7 - Matriz de rangos de riesgo.

Riesgo.	Rango Inferior.	Rango Superior.
Muy alto.	70	100
Alto.	35	69
Medio.	16	34
Bajo.	6	15
Muy Bajo.	1	5

Fuente: CCSS (2007)

2.2.2.4.1. Matriz de calor de riesgos.

Una matriz de calor de riesgos es una herramienta que permite a una organización visualizar datos relacionados con riesgos relacionados, facilitando su identificación y priorización. De igual forma, permite mejorar la compresión que tiene una organización respecto al riesgo, su nivel de probabilidad de ocurrencia y de impacto (Rouse, 2018).

Dentro del manual para elaborar un plan de continuidad creado por la CCSS (2007), establece una matriz de calor de riesgos (Véase Tabla 8), en la cual se ubican los riesgos según el nivel de probabilidad e impacto que alcanzan.

Tabla 8 - Matriz de calor.

Probabilidad.	**Impacto.**				
	10	30	50	70	100
	7	21	35	49	70
	5	15	25	35	50
	3	9	15	21	30
	1	3	5	7	10

Fuente: CCSS (2007).

2.3. Continuidad de negocio.

Con el propósito de contextualizar el término de continuidad del negocio, se hace referencia a lo indicado dentro del estándar internacional ISO 22301 (2012), donde enmarca que, la continuidad del negocio es la capacidad de continuar entregando un producto o brindando un servicio dentro de niveles previamente definidos, después de un evento alterador que interrumpa la continuidad de sus operaciones.

Por lo tanto, tomando en consideración la definición anterior, garantizar la continuidad de las operaciones y servicios de un negocio, requiere mantener en un estado óptimo los niveles de servicios, considerando aplicaciones, accesos a red, servidores e infraestructura.

Dada la importancia del papel que desempeña TI dentro de una organización de acuerdo con la definición, contar con un plan de continuidad permite a los colaboradores del área o departamento que gestiona TI, contar con estrategias que permitan garantizar ante cualquier interrupción, la continuidad de las operaciones del negocio que son soportadas por TI.

2.3.1. Plan de continuidad.

Un plan de continuidad se compone de procedimientos debidamente documentados que permiten guiar a la organización a reanudar y restablecer los niveles de operación luego de sufrir una interrupción de sus procesos.

Dentro de sus objetivos, un plan de continuidad del negocio se enfoca en sostener las funciones del negocio durante y después de una interrupción a los procesos críticos de la organización, identifica las amenazas potenciales y los impactos a las operaciones que esas amenazas podrían causar si se llegaran a materializar (Filippi (2012).

Filippi (2012) también mencionan que el éxito de un plan de continuidad de negocio depende de la correcta identificación de roles, asignación de responsabilidades y entrenamiento dentro de los colaboradores de la organización.

Además, un proceso de planeación para el desarrollo de un plan de continuidad de negocio según Cerullo y Cerullo (2004), debe alcanzar los siguientes objetivos:

- Identificar los mayores riesgos de interrupción del negocio.
- Desarrollo de un plan para reducir el impacto de los riesgos identificados.
- Probar la efectividad del plan de continuidad.
- Capacitar a los colaboradores en la ejecución del plan de continuidad.

Es importante detallar que dentro de una organización, un plan de continuidad es un componente clave para garantizar las operaciones críticas del negocio, por tal importancia, un plan de continuidad debe ser respaldado por normas que garanticen las estrategias adecuadas a aplicar dentro del plan.

2.3.2. Información requerida.

Para la creación de un plan de continuidad, Livingstone (2010) recomienda que un plan de continuidad de TI debe comprender las siguientes secciones:

- Descripción funcional: Definición de las funciones del proceso.
- Dependencias: Procesos requeridos para el funcionamiento de un proceso crítico.
- Contactos de recuperación: Contactos de líderes del equipo encargado del plan de recuperación.
- Procesos de recuperación: Proceso paso a paso necesarios para alcanzar la recuperación del proceso.

2.3.3. Tipo de estrategias.

Dentro de un plan de continuidad según Huércano (s.f), especifican dentro del libro *ITIL Service Design* que se debe combinar estrategias proactivas y reactivas con el objetivo de gestionar ya sea una posible interrupción o su materialización.

Las estrategias proactivas tienen dos objetivos principales:

- Reducir las consecuencias de una interrupción.
- Impedir la materialización de una interrupción.

Igualmente, las estrategias reactivas tienen como objetivo reanudar el servicio lo más pronto posible.

2.3.4. Organización y administración del plan de continuidad de TI.

Como parte de la administración del plan de continuidad de TI, es necesario la definición de un equipo de trabajo que se encargue de su administración, coordinación, ejecución y desarrollo (CCSS, 2007).

Dentro de los roles que pueden existir dentro del equipo encargado del plan de continuidad, se encuentran.

2.3.4.1. Coordinador del plan.

El coordinador del plan de continuidad es responsable de supervisar y coordinar todas las actividades de recuperación establecidas dentro del plan de continuidad de TI.

Igualmente, es responsable de acumular y administrar toda la información generada una vez iniciado el plan de continuidad.

2.3.4.2. Líder de equipo.

Debe ser una persona con liderazgo y con capacidad de tomar decisiones durante un periodo de recuperación. Deberán realizar las siguientes tareas:

- Participar en las sesiones de trabajo programadas.
- Aportar en el proceso de análisis y diseño de los procedimientos de recuperación.
- Liderar la recuperación del proceso de negocios a su cargo.
- Identificar e implantar mejoras al plan de continuidad.
- Mantenimiento de la información del estado de recuperación
- Coordinar con otros equipos de recuperación.

2.3.4.3. Suplente del líder de equipo.

El suplente del líder de equipo asignado cubre su lugar en caso de imposibilidad del líder para administrar el equipo. Debe contar con el mismo perfil que el líder y cumplir con las mismas responsabilidades.

2.3.4.4. Miembros de equipo.

Los miembros de equipo son responsables de ejecutar las acciones de recuperación. Debido a que las actividades son usualmente desarrolladas por múltiples personas, estos pueden variar dependiendo de las circunstancias y recursos disponibles.

2.3.4.5. Equipos para la continuidad.

Para la gestión de un plan de continuidad de TI, es necesario la conformación de equipos que logren brindar su soporte. Como parte de la organización dentro de un plan de continuidad de TI, se pueden definir los cuatro equipos con un respectivo alcance y responsabilidades (CCSS, 2007).

2.3.4.5.1. Equipo de tecnología de información.

Equipo encargado de supervisar y coordinar todas las acciones internas de recuperación y monitorea el avance de las acciones realizadas por los equipos de operaciones, comunicaciones y aplicaciones respectivamente (CCSS, 2007).

Dentro de las responsabilidades del equipo de tecnología de información se encuentran:

- Analizar los reportes de daños.
- Reportar el estado de la recuperación y cualquier otro problema que se presente.
- Servir de punto focal para las consultas planteadas por el personal de recuperación.
- Habilitar el sitio alterno para la recuperación de las aplicaciones.

2.3.4.5.2. Equipo de comunicación.

El equipo de comunicación se encarga de todas las acciones de recuperación de las comunicaciones y debe brindar informes al líder del área de tecnología de información.

Dentro de las responsabilidades del equipo de comunicaciones se encuentran:

- Desarrollar y documentar las configuraciones de las comunicaciones.
- Determinar el daño en la red de comunicaciones.
- Ordenar e instalar el *hardware* necesario para establecer la comunicación entre las oficinas.
- Coordinar con entes externos para restaurar el servicio de comunicaciones.
- Comprobar que las comunicaciones se hayan establecido correctamente.

2.3.4.5.3. Equipo de operación.

El equipo de operación debe asegurar el avance de la restauración de las operaciones de las plataformas críticas y debe brindar informes al líder del área de tecnología de información.

Dentro de las responsabilidades del equipo de operación se encuentran:

- Asegurar la disponibilidad de los respaldos.
- Restaurar archivos y sistemas operativos.
- Ordenar e instalar el hardware requerido para el procesamiento normal de las operaciones.

2.3.4.5.4. Equipo de aplicaciones.

El equipo de aplicaciones supervisa la restauración de las aplicaciones que residen dentro de los distintos ambientes existentes. Además debe coordinar y brindar informes al líder del área de tecnología de información.

Dentro de las responsabilidades del equipo de aplicaciones se encuentran:

- Coordinar la recuperación de las aplicaciones.

- ❖ Reconstruir el ambiente de operación de las aplicaciones que residen en los servidores.
- ❖ Desarrollar un plan de trabajo detallado para el traslado de operaciones del sitio principal al sitio alterno.

2.3.4.6. Habilidades requeridas por el personal.

Dentro del manual para elaborar un plan de continuidad creado por la CCSS (2007), recomienda establecer un conjunto de actividades específicas que debe contar cada posición dentro de los equipos para la continuidad (Véase Tabla 9).

Tabla 9 - Habilidades requeridas por el personal.

Nombre.	Habilidades Generales.	Habilidades Específicas.
Coordinador del plan de continuidad de TI.	• Capacidad de trabajo en equipo y coordinación con miembros de los demás equipos.	• Conocimiento de la plataforma tecnológica.
Líder del equipo de comunicación.		• Conocimiento técnico en la infraestructura de comunicaciones.
Líder del equipo de operaciones.		• Conocimiento de las plataformas tecnológicas.
Líder del equipo de sistemas.		• Conocimiento del portafolio de sistemas de la organización.

Nombre.	Habilidades Generales.	Habilidades Específicas.
Miembros de los equipos de recuperación.	• Capacidad de trabajo en equipo.	• Conocimiento técnico de la plataforma, sistemas y comunicaciones.

Fuente: CCSS (2007).

2.4. Normas, guías y manuales.

En esta sección se presentan de forma resumida, una serie de guías, normas y modelos que complementan el marco de conocimiento considerado para la investigación que soporta este trabajo final de graduación.

2.4.1. Guía para realizar el análisis de impacto de negocio.

Corresponde a un documento generado por el ministerio de TIC del gobierno colombiano, el cual presenta los lineamientos a cumplir en un BIA como parte del desarrollo del plan de continuidad de TI.

Dentro de la guía, MINTIC (2015) definió un conjunto de pasos para identificar los impactos de las interrupciones y con esto, facilitar la toma de decisiones respecto a los procesos críticos de la organización que afectan directamente en las operaciones.

Más específicamente, el proceso metodológico utilizado para el desarrollo del BIA según MINTIC (2015), tomando en consideración el alcance establecido para este trabajo final de graduación.

2.4.1.1. Identificación de funciones y procesos.

Se identifica las funciones de cada departamento dentro del negocio, las cuales son útiles para alcanzar los objetivos plantados dentro de la investigación.

Este paso tiene como resultado identificar todos los procesos de negocio, que sirven como base de análisis para los siguientes pasos del BIA.

2.4.1.2. Evaluación de impacto.

Una vez identificados los procesos del negocio, se requiere evaluar el impacto de una posible interrupción dentro de las operaciones diarias.

La evaluación del impacto debe permitir evaluar el nivel negativo que genera una interrupción hacia la organización, tomando en consideración aspectos relacionados al negocio.

2.4.1.3. Identificación de procesos críticos.

Se identifican los procesos críticos del negocio, considerando como base la clasificación de los impactos operacionales dentro de la organización. Dicha identificación permite conocer cuáles procesos son esenciales dentro del negocio y su respectiva relación con el área de TI y los activos que gestiona.

2.4.1.4. Identificación de recursos.

Las actividades consideradas dentro de la función crítica del negocio deben ser valoradas como vitales cuando apoyan los procesos críticos del negocio; por lo tanto, la identificación de los recursos dentro del área TIC que soportan los procesos

críticos del negocio, permite la toma las decisiones con respecto al impacto que estos tienen dentro del negocio.

2.4.1.5. Generación de informe de impacto de negocio.

Corresponde al paso final del proceso, es necesario generar un informe de impacto de negocio que contemple los siguientes puntos:

- Procesos críticos.
- Impactos ante una posible interrupción.
- Recursos críticos.

2.4.2. Norma ISO 31000.

La norma ISO 31000 en la versión 2009 provee un conjunto de buenas prácticas utilizadas dentro de la industria relacionadas con la gestión de riesgos, lo cual enmarca su importancia al considerarse dentro del marco teórico de esta investigación (International Organization for Standardization.,2009).

Según se menciona dentro de la norma ISO 31000, una correcta gestión de riesgos según lo que establece, permite a una organización lo siguiente:

- Aumentar la probabilidad de lograr los objetivos organizacionales.
- Fomentar una gestión proactiva.
- Concientización de la necesidad de identificar y tratar los riesgos.
- Mejorar la identificación de oportunidades y amenazas.
- Cumplimiento de exigencias legales y reglamentarias.
- Mejora la confianza de los interesados.
- Gestión eficaz de recursos para el tratamiento de los riesgos.
- Mejor eficiencia operacional.
- Mejor prevención de pérdidas y gestión de incidentes.

El proceso que recomienda la norma ISO 31000 (Véase Ilustración 5), debe ser parte integral de la gestión como tal, estar incluido dentro de las prácticas y cultura y, por último, estar adaptado a los procesos de negocio de la organización (International Organization for Standardization, 2009).

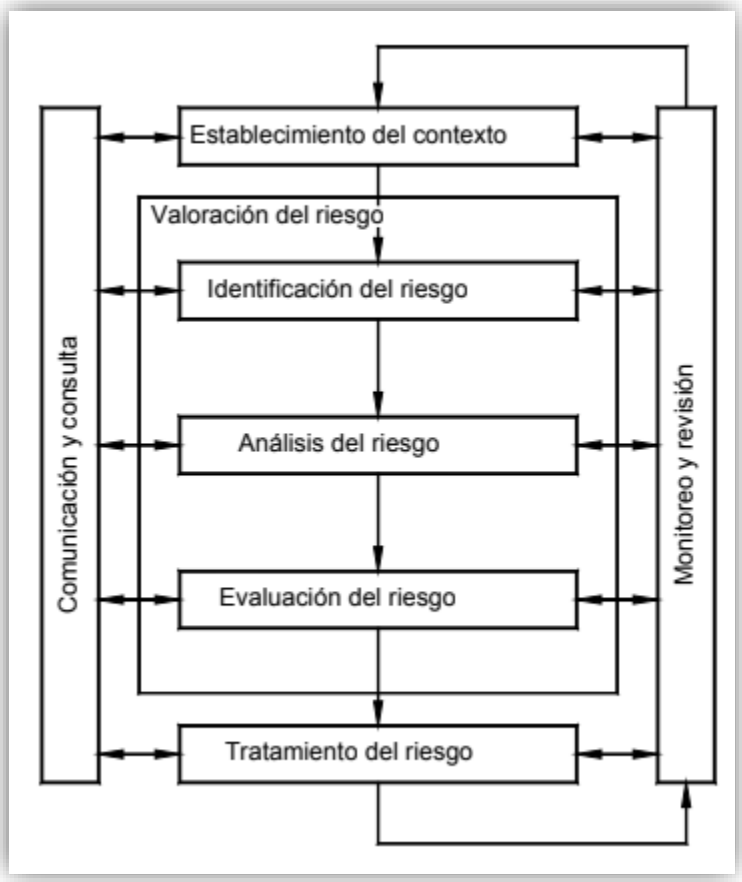


Ilustración 5 - Proceso gestión de riesgos.

Fuente: ICONTEC (2009).

Más específicamente, cada actividad del proceso para la gestión de riesgos corresponde a lo siguiente:

2.4.2.1. Comunicación y consulta

La comunicación y consulta entre las partes interesadas es una actividad importante dentro de cualquier proceso que se desarrolle dentro de una organización y específicamente dentro del proceso de la gestión de riesgos, esta actividad promueve abordar aspectos como causas, consecuencias y medidas de mitigación (International Organization for Standardization, 2009).

Importante resaltar que esta actividad, dentro del proceso de gestión de riesgos, facilita los intercambios de información de forma veraz, precisa y fácil de entender (International Organization for Standardization, 2009).

Dentro de la gestión de riesgos, esta actividad ayuda a alcanzar lo siguiente:

1. Garantiza que los riesgos se identifiquen correctamente.
2. Definición adecuada de criterios sobre riesgos.
3. Gestión del cambio dentro del proceso de gestión de riesgos.

2.4.2.2. Establecimiento del contexto.

Estableciendo el contexto del proceso de gestión de riesgos, la organización logra articular sus objetivos y definir los parámetros internos y externos necesarios para gestionar el riesgo, su alcance y criterios del riesgo necesarios para el resto de las actividades del proceso.

2.4.2.3. Valoración de riesgo.

Dicha actividad se encuentra comprendida por subactividades, las cuales son la identificación, análisis y evaluación del riesgo (Véase Ilustración 6).

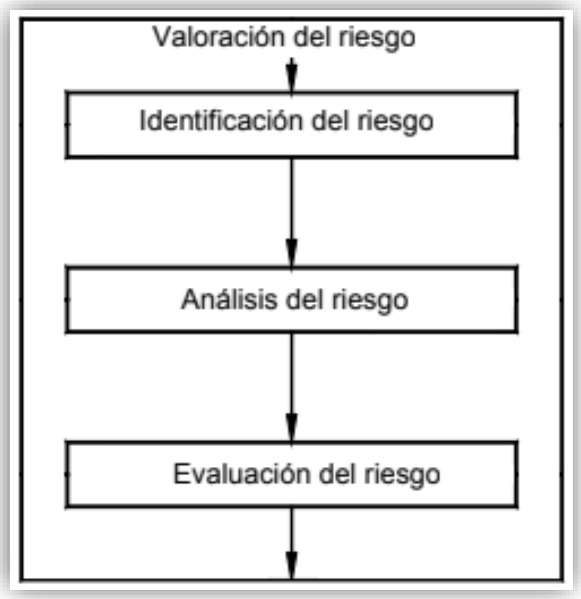


Ilustración 6 - Valoración del riesgo.
Fuente: ISO 31000.

La identificación del riesgo tiene como objetivo la generación de una lista de riesgos en los cuales se considere aspectos como las fuentes de riesgo, las áreas de impacto, causas y consecuencias, dado que son aspectos necesarios dentro de la gestión de los riesgos.

Con respecto al análisis del riesgo, esta subactividad es clave para la toma de decisiones sobre el tratamiento de los riesgos; además, considera las causas y fuentes de riesgo, consecuencias y la probabilidad de ocurrencia.

En dicha actividad, el grado de detalle considerado depende del riesgo, el propósito del análisis y los datos, información y recursos disponibles; ya que el análisis del riesgo puede realizarse cualitativa, semicuantitativa o cuantitativamente.

Por último, la evaluación del riesgo compara el nivel de riesgo observado durante el desarrollo del análisis del riesgo, esto para decidir cuáles riesgos necesitan tratamiento y la prioridad de su implementación.

Cualquier decisión que conlleve la evaluación del riesgo, considera la tolerancia existente a cada uno de los riesgos y además los requisitos legales y reglamentos existentes.

Dentro del proceso de gestión de riesgos, según lo recomendado dentro de la normativa ISO 31000, existen dos actividades extras las cuales corresponden al tratamiento del riesgo y monitoreo y revisión, dichas actividades no son abordadas dado al alcance de la investigación.

2.4.3. Norma ISO 22301.

La norma ISO 22301, en su versión 2012, es una norma internacional que contiene un conjunto de requerimientos con el objetivo de planear, establecer, implementar, gestionar, revisar y mantener efectivamente un sistema de gestión de continuidad del negocio.

Según la ISO 22301, un sistema de gestión de continuidad permite lo siguiente:

- Comprender la continuidad y la necesidad de preparar y establecer políticas de gestión de continuidad.
- Implementar y operar controles y medidas para gestionar los riesgos.
- Monitorear y revisar el desempeño del sistema de gestión de continuidad del negocio.
- Mejora continua basada en mediciones objetivas.

La norma se encuentra conformada por diferentes clausuras, específicamente dentro de la clausura seis de la norma, que se enfoca en la planeación, especifica que la organización debe asegurar que el sistema de gestión de continuidad logre alcanzar los resultados intencionados y permitir el mejoramiento continuo.

Además, dentro de la clausura de operación, se especifica las actividades que se debe realizar para aplicar correctamente dicha norma dentro de una organización.

2.4.3.1. Planeamiento operacional y control.

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con requerimientos e implementar las acciones necesarias. Igualmente, debe mantener información actualizada para garantizar que los procesos y actividades sean desarrollados conforme lo planificado.

2.4.3.2. Análisis de impacto del negocio y evaluación del riesgo.

La organización debe procurar la gestión del BIA y la evaluación del riesgo dentro de un proceso documentado y formal, donde se cumpla con las siguientes condiciones:

- Definición de criterios adecuados para los análisis.
- Establecer un contexto adecuado para su desarrollo.
- Definición de los resultados esperados.

2.4.3.2.1. Análisis de impacto.

La organización es responsable de establecer, implementar y mantener la documentación necesaria dentro de este proceso de evaluación. Se debe evaluar el impacto que genera una interrupción en las actividades de los servicios de la organización.

El proceso del BIA debe alcanzar lo siguiente:

- Identificación de las actividades que apoyan el abastecimiento de servicios a la organización.
- Evaluación de tiempos e impacto de no ejecutar actividades críticas.
- Establecer tiempos para reanudar las actividades dentro de un tiempo mínimo aceptable.
- Identificación de dependencias y recursos de apoyo existente en las actividades.

2.4.3.2.2. Evaluación del riesgo.

La organización es responsable de establecer, implementar y mantener la documentación necesaria para que la evaluación del riesgo logre identificar, analizar y evaluar los riesgos de interrupciones a las actividades críticas.

Dentro de la evaluación del riesgo debe alcanzar un conjunto de requerimientos:

- Identificar los riesgos que puede generar una interrupción dentro de las actividades críticas o priorizadas de la organización.
- Evaluar el tratamiento adecuado que requiere cada riesgo según la interrupción que genera.
- Identificar tratamientos alineados con los objetivos de recuperación.

Se detalla dentro de la norma, la recomendación de desarrollar este proceso según lo especificado dentro del ISO 31000.

2.4.3.3. Estrategia de continuidad del negocio.

La organización debe determinar y seleccionar las estrategias que permitan proteger, estabilizar, reanudar y recuperar las actividades críticas o priorizadas con

el objetivo de mitigar y gestionar el impacto que puede generar la materialización de un riesgo.

Es importante detallar que los riesgos deben ser tratados mediante medidas proactivas, que permitan la reducción de la probabilidad de interrupción, disminuyan el posible tiempo de interrupción y su impacto.

Además, como parte del establecimiento de las estrategias de continuidad, es necesario determinar los recursos requeridos para su implantación, deben ser considerados recursos como personas e información hasta equipos y tecnologías de información.

2.4.3.4. Estableciendo e implementando procedimientos para continuidad.

La organización debe establecer, implementar y mantener procedimientos para la continuidad del negocio, que le permita gestionar cualquier evento alterador y garantizar la continuidad de las operaciones.

Los procedimientos generados para el plan de continuidad deben:

- Establecer protocolos de comunicación.
- Especificar los pasos a seguir en caso de una interrupción.
- Flexibilidad a responder en caso de un escenario de amenaza y cambios.
- Focalizarse en el impacto de eventos que puedan interrumpir las operaciones de la organización.
- Efectividad en minimizar las consecuencias de implantar estrategias para la continuidad.

Con respecto a la estructura de respuesta que debe mantener el plan de continuidad, esta debe alcanzar lo siguiente:

- Identificar el impacto que justifica la iniciación de una respuesta formal del plan de continuidad.
- Evaluar la naturaleza y extensión del evento alterador.
- Contar con procedimientos de activación, operación, coordinación y comunicación de respuesta apropiados.

2.4.3.5. Ejercicios y ensayos.

La organización debe ejercitar y ensayar los procedimientos de continuidad para asegurar su consistencia, esto se logra por medio de:

- Consistencia con el alcance y objetivos del plan de continuidad.
- Escenarios apropiados y planificados con respectivos propósitos y objetivos.
- Minimizar el riesgo de alterar las operaciones.
- Generar informes luego de los ejercicios que contengan resultados o recomendaciones de mejora.
- Promover la mejora continua.

La norma ISO 22301 toma como base para su desarrollo el modelo PDCA, por ello se detalla a continuación.

2.4.4. Modelo PDCA.

El modelo PDCA (del inglés *plan-do-check-act*, correspondiente a planificar-hacer-verificar-actuar) o ciclo Deming, este corresponde a un modelo de mejora continua de la calidad, que consta de una secuencia de cuatro pasos repetitivos que apoyan la mejora continua y el aprendizaje.

Los cuatro pasos que comprenden el modelo PDCA son planear, hacer, verificar y actuar (Véase Ilustración 7), los cuales permiten a las organizaciones mejorar integralmente a nivel de competitividad, calidad, productividad y rentabilidad.

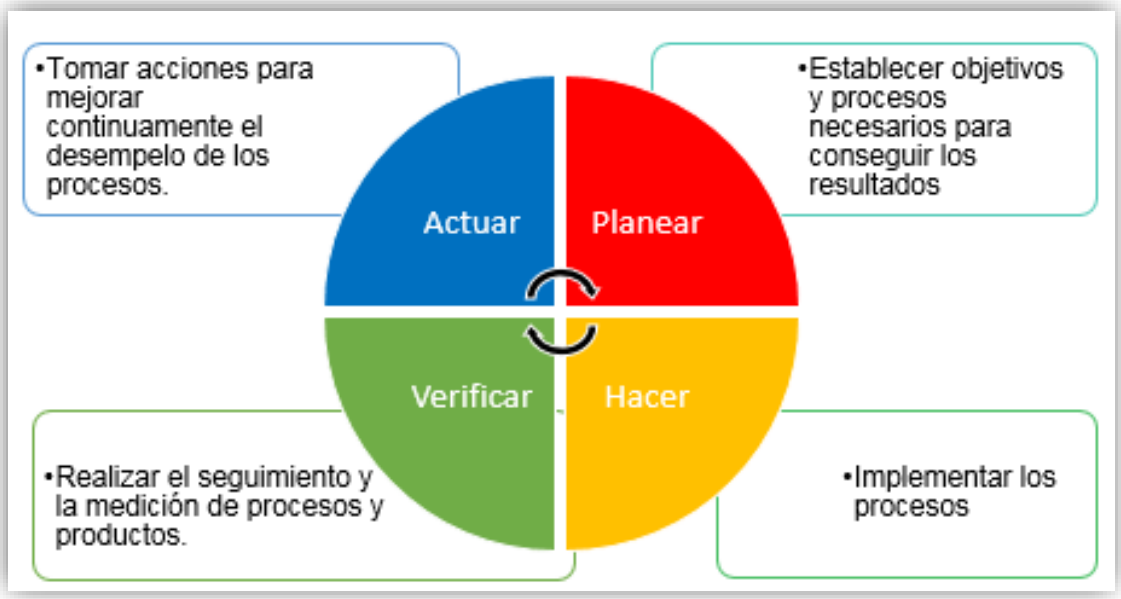


Ilustración 7 - Modelo PDCA.

Fuente: Elaboración propia.

Dentro de la normativa ISO 22301, se propone el modelo PDCA para la mejora continua de un sistema de gestión de la continuidad (Véase Ilustración 8), utilizando insumos de las partes interesadas y los requerimientos para la continuidad. Además, funciona como generador de insumos para la gestión de la continuidad del negocio y sus interesados.

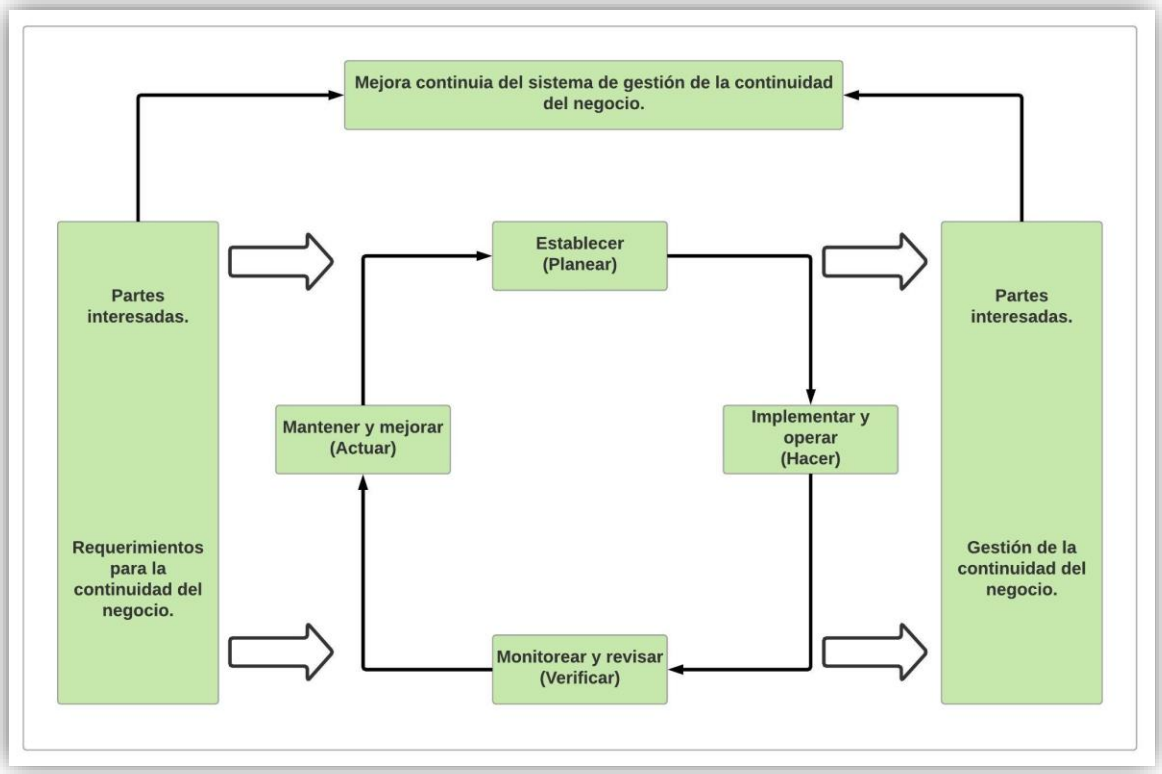


Ilustración 8 - Ciclo PDCA aplicado al proceso de continuidad del negocio.

Fuente: International Organization for Standardization. (2012).

Dentro de la normativa ISO 22301, cada uno de los cuatro pasos del modelo PDCA plantea un objetivo específico (Véase Tabla 10) que apoya tanto el desarrollo como la gestión de un sistema de gestión de continuidad de negocio.

Tabla 10 - Modelo PDCA-ISO 22301.

Modelo PDCA.	ISO 22301.
Planear	Establecer una política de continuidad del negocio, objetivos, metas y procedimientos relevantes para la mejorar de la continuidad del negocio.

Modelo PDCA.	ISO 22301.
Hacer	Implementar y operar la política de continuidad de negocio, controles, procesos y procedimientos.
Verificar	Monitorear y evaluar el desempeño de la política de continuidad del negocio. Determinar y autorizar acciones de remediación y mejora.
Actuar	Mantener y mejorar el sistema de gestión de continuidad de negocio mediante acciones correctivas, basadas en resultados de evaluaciones gerenciales.

Fuente: International Organization for Standardization. (2012).

2.4.5. Manual para elaborar un plan de continuidad de la gestión en tecnología de información y comunicación.

El departamento de TI de la CCSS crea un manual para la elaboración de los planes de continuidad de la gestión en TIC dentro de las unidades regionales que cuenta.

Según la CCSS (2007), el enfoque que debe mantener un plan de continuidad debe ser la recuperación de las operaciones de los procesos de una organización, dentro de un tiempo determinado y buscando equilibrio entre costo y viabilidad.

2.4.5.1. Etapas mínimas para elaborar un plan de continuidad de TI.

Dentro del manual se especifica un conjunto de etapas mínimas para alcanzar con éxito la elaboración de un plan de continuidad (Véase Ilustración 9).

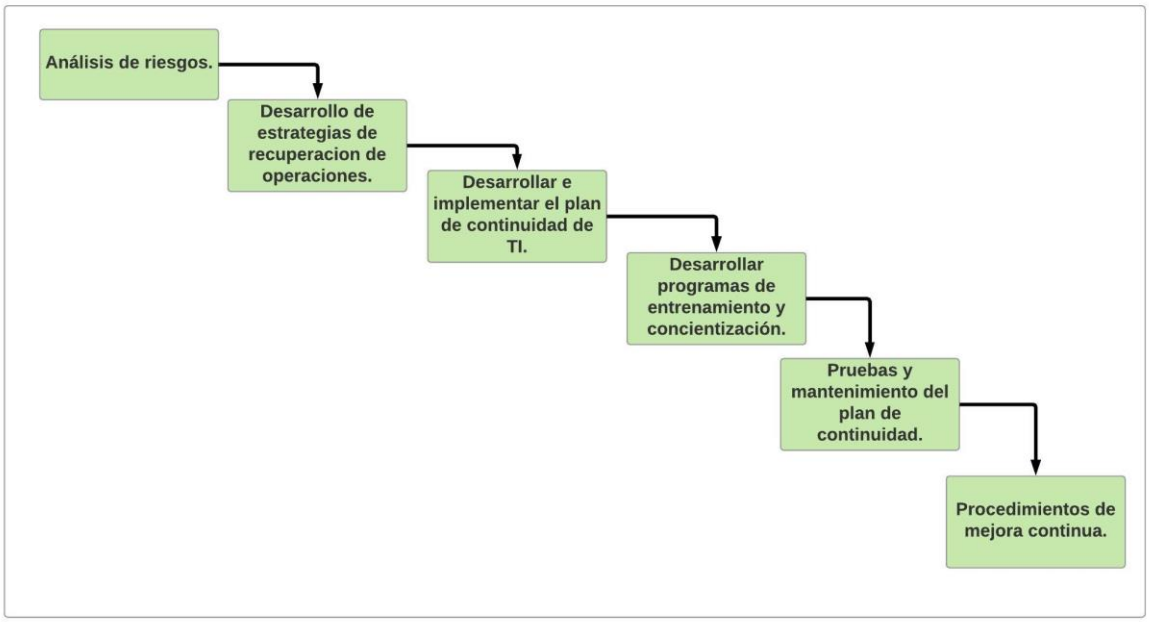


Ilustración 9 - Etapas mínimas para elaborar un plan de continuidad de TI.

Fuente: CCSS (2007).

2.4.5.1.1. Análisis de riesgos.

Según el manual elaborado por la CCSS (2007), con un análisis de riesgos se busca determinar eventos y situaciones externas como una interrupción o un desastre, que permita afectar la organización y su infraestructura. Además, evalúa los controles requeridos para prevenir y minimizar los efectos de una potencial materialización.

Mediante el análisis de riesgos, el manual pretende alcanzar lo siguiente:

- Evaluar y controlar los riesgos.
- Determinar la exposición de la organización a pérdidas potenciales.
- Identificar y evaluar la efectividad de los controles para prevenir y mitigar pérdidas por la materialización de un riesgo.

Igualmente, el manual recomienda desarrollar un BIA, dado que permite identificar lo siguiente:

- Información general de las áreas funcionales.
- Información de los niveles de impacto.
- Información de las funciones críticas de cada área funcional.
- Los requerimientos de recursos por área funcionan.

2.4.5.1.2. Desarrollo de estrategias de recuperación de las operaciones.

Esta etapa busca establecer las estrategias orientadas a la recuperación según los objetivos de recuperación establecidos.

El manual especifica que dentro de esta etapa se debe realizar lo siguiente:

- Identificar requerimientos estratégicos para la recuperación.
- Valorar la oportunidad de estrategias alternativas.
- Preparar un análisis de costo/beneficio de las estrategias.
- Seleccionar posibles sitios alternos de operación y respaldo de datos.

2.4.5.1.3. Desarrollar e implementar el plan de continuidad de TI.

Diseñar, desarrollar e implementar el plan de continuidad de TI es el objetivo de esta etapa, plan necesario para recuperar las operaciones de TI dentro del tiempo establecido.

Para alinear el plan de continuidad de TI con los objetivos planeados, se debe realizar lo siguiente:

- Determinar los requerimientos del plan de continuidad de TI.

- Determinar la estructura del plan de continuidad de TI.
- Diseñar dicho plan.
- Definir y documentar los procedimientos de recuperación.
- Desarrollar los requerimientos de documentos a utilizar tanto durante como después de la interrupción.
- Establecer pruebas y procedimientos de control, capacitación y mejora continua del plan.

2.4.5.1.4. Procedimientos de recuperación.

Los procedimientos de recuperación son documentos que apoyan el proceso de recuperación posterior a la manifestación de un evento que afecta de forma parcial o total las operaciones de la organización (CCSS, 2007).

Estos procedimientos de recuperación deben responder a los elementos o recursos necesarios para mantener la operación de los procesos críticos del negocio identificados. Además, deben mantener la información necesaria para alcanzar la recuperación desde cero de cualquier recurso de la plataforma crítica del negocio en caso de ser necesario.

2.4.5.1.5. Desarrollo de programas de entrenamiento y concienciación.

Esta etapa tiene como objetivo un programa orientado a crear y mantener conciencia en el negocio y con esto, mejorar las habilidades requeridas para gestionar el plan de continuidad.

Para alcanzar dicho objetivo, como parte del desarrollo de un plan de continuidad de TI es necesario lo siguiente:

- Definir objetivos de los entrenamientos.
- Desarrollar programas diversos de entrenamiento.
- Identificar oportunidades de educación.

2.4.5.1.6. Pruebas y dar mantenimiento al plan.

Como parte de las pruebas y mantenimiento del plan de continuidad de TI, esta etapa pretende probar con antelación y documentar los resultados obtenidos, con el afán de lograr una adecuada recuperación de las operaciones de TI.

Esta etapa pretende realizar lo siguiente:

- Establecer y ejercitar el plan de continuidad.
- Desarrollar escenarios y realizar para las pruebas.
- Preparar reportes y procedimientos de control.
- Obtener retroalimentación de los resultados obtenidos dentro de las pruebas.

2.4.5.1.7. Procedimiento de mejora continua.

La mejora continua del plan de continuidad de TI es un proceso clave, por ello dentro de esta etapa se recomienda considerar los siguientes elementos:

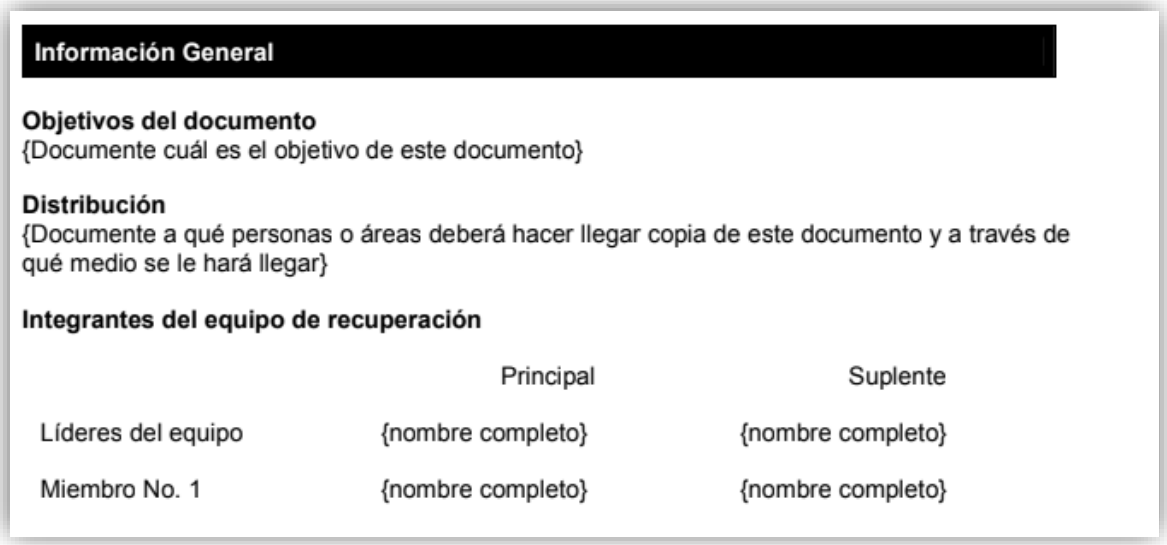
- Administración del cambio dentro de la organización y su impacto dentro del plan de continuidad.
- Capacitación del personal, fomentando su ejecución una vez al año.
- Ensayos del plan de continuidad de TI, contando con el compromiso del personal relacionado al plan.

- Revisión constante de la organización, su proceso y actividades, con el objetivo de actualizar el plan de continuidad en caso de existir cambios sustanciales.

Para la creación de un plan de continuidad, la CCSS (2007) utiliza un conjunto de plantillas para documentar los procesos de recuperación de los activos de TI, las cuales son utilizadas como base para la creación del plan de continuidad de TI.

2.4.5.2. Plantillas de control.

Dentro del manual, la CCSS (2007) establece plantillas con el objetivo de gestionar el control y documentación de los procedimientos de recuperación aplicados dentro de la organización (Véase Ilustración 10).



Información General

Objetivos del documento
{Documente cuál es el objetivo de este documento}

Distribución
{Documente a qué personas o áreas deberá hacer llegar copia de este documento y a través de qué medio se le hará llegar}

Integrantes del equipo de recuperación

	Principal	Suplente
Líderes del equipo	{nombre completo}	{nombre completo}
Miembro No. 1	{nombre completo}	{nombre completo}

Ilustración 10 - Información general del documento.
Fuente: CCSS (2007).

Además, gestiona una plantilla con información general sobre las versiones generadas del plan de continuidad de TI, donde detalla el responsable a cargo de

la aprobación y los ensayos realizados que respaldan dicho plan (Véase Ilustración 11).

Control de revisión y aprobación del documento

Historial de revisiones

Versión	Autor	Fecha	Revisión

Control de aprobación

	Responsable	Firma	Fecha de Aprobación
1			
2			
3			
4			
5			

Control de ensayos

	Responsable	Fecha	Resultados
1			
2			
3			
4			
5			

Ilustración 11 - Control de revisión y aprobación del documento.
Fuente: CCSS (2007).

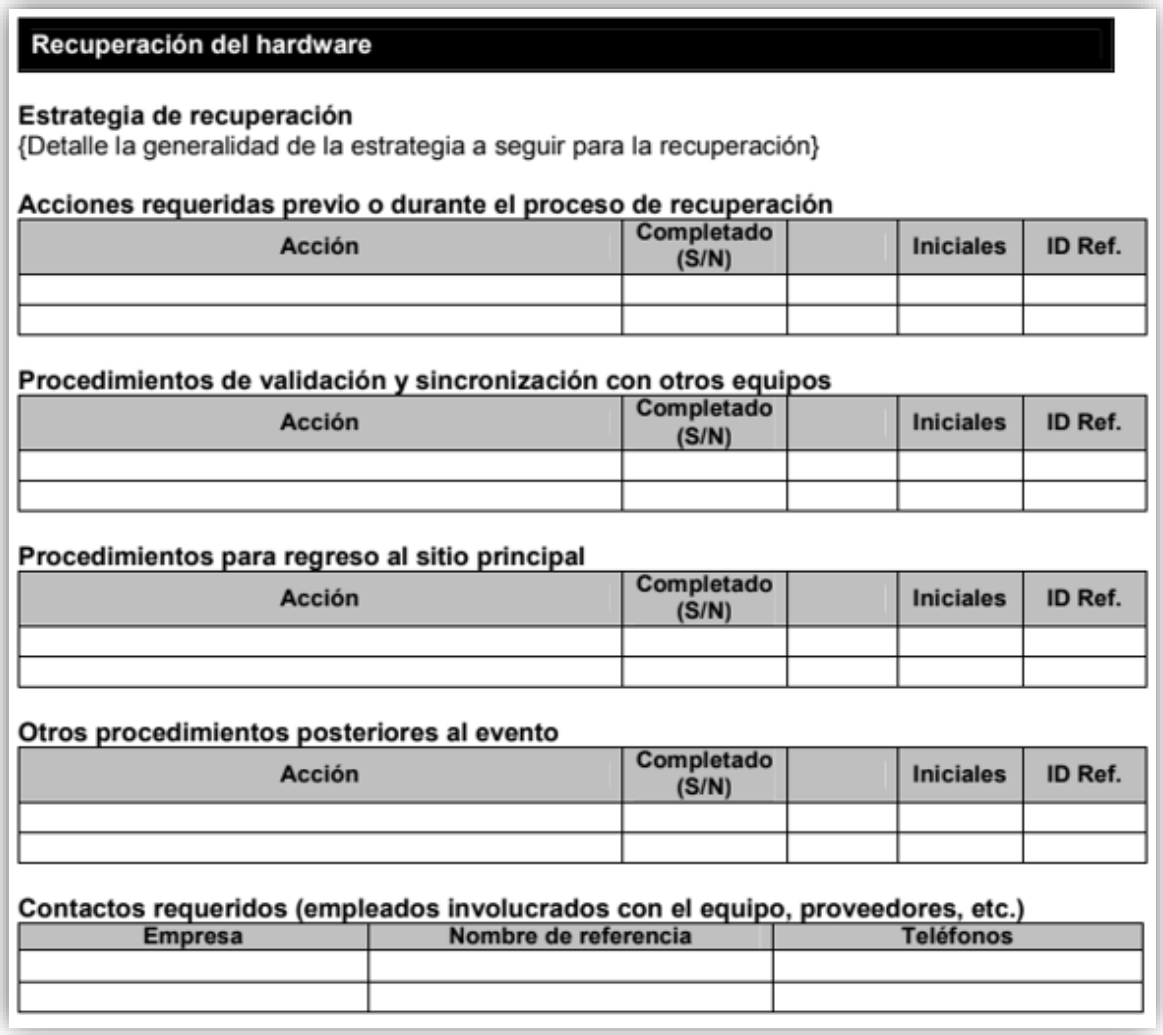
2.4.5.3. Plantillas para procedimientos de recuperación.

Dentro del manual la CCSS (2007), establece un conjunto de plantillas con el propósito de documentar las acciones aplicadas dentro de los procedimientos de recuperación.

Las plantillas de control se encuentran categorizadas según el tipo de activo de TI referenciado al procedimiento de recuperación.

2.4.5.3.1. Hardware

Plantilla de acciones requeridas antes o durante el proceso de recuperación de un hardware (Véase Ilustración 12).



Recuperación del hardware

Estrategia de recuperación
{Detalle la generalidad de la estrategia a seguir para la recuperación}

Acciones requeridas previo o durante el proceso de recuperación

Acción	Completado (S/N)		Iniciales	ID Ref.

Procedimientos de validación y sincronización con otros equipos

Acción	Completado (S/N)		Iniciales	ID Ref.

Procedimientos para regreso al sitio principal

Acción	Completado (S/N)		Iniciales	ID Ref.

Otros procedimientos posteriores al evento

Acción	Completado (S/N)		Iniciales	ID Ref.

Contactos requeridos (empleados involucrados con el equipo, proveedores, etc.)

Empresa	Nombre de referencia	Teléfonos

Ilustración 12 - Plantilla recuperación del hardware.

Fuente: CCSS (2007).

2.4.5.3.2. Aplicaciones.

Plantilla de acciones requeridas antes o durante el proceso de recuperación de una aplicación (Véase Ilustración 13).

Recuperación de la aplicación

Estrategia de Recuperación
{Detalle la generalidad de la estrategia a seguir para la recuperación}

Recursos requeridos previo o durante el proceso de recuperación

ID	Recurso	Ubicación	Responsable

Instalación de la aplicación

Acción	Completado (S/N)	Iniciales	ID Ref.

Procedimientos de validación en la instalación de la aplicación

Acción	Completado (S/N)	Iniciales	ID Ref.

Procedimientos y parámetros para configurar la aplicación

Acción	Completado (S/N)	Iniciales	ID Ref.

Otros procedimientos posteriores al evento

Acción	Completado (S/N)	Iniciales	ID Ref.

Contactos requeridos (empleados involucrados con el equipo, proveedores, etc.)

Empresa	Nombre de referencia	Teléfonos

Notas:

Ilustración 13 - Plantilla de recuperación de la aplicación.
Fuente: CCSS (2007).

2.4.5.3.3. Equipo

Plantilla de acciones requeridas antes o durante el proceso de recuperación de equipo (Véase Ilustración 14).

Recuperación del equipo

Estrategia de recuperación
{Detalle la generalidad de la estrategia a seguir para la recuperación}

Recursos requeridos previo o durante el proceso de recuperación

ID	Recurso	Ubicación	Responsable

Procedimientos para instalar y configurar el equipo de comunicación. Cuando aplique, incluya versiones de sistema operativo y parches

Acción	Completado (S/N)	Iniciales	ID Ref.

Procedimientos requeridos para validar la instalación y configuración

Acción	Completado (S/N)	Iniciales	ID Ref.

Procedimientos de validación y sincronización con otros equipos

Acción	Completado (S/N)	Iniciales	ID Ref.

Otros procedimientos posteriores al evento

Acción	Completado (S/N)	Iniciales	ID Ref.

Contactos requeridos (empleados involucrados con el equipo, proveedores, etc.)

Empresa	Nombre de referencia	Teléfonos

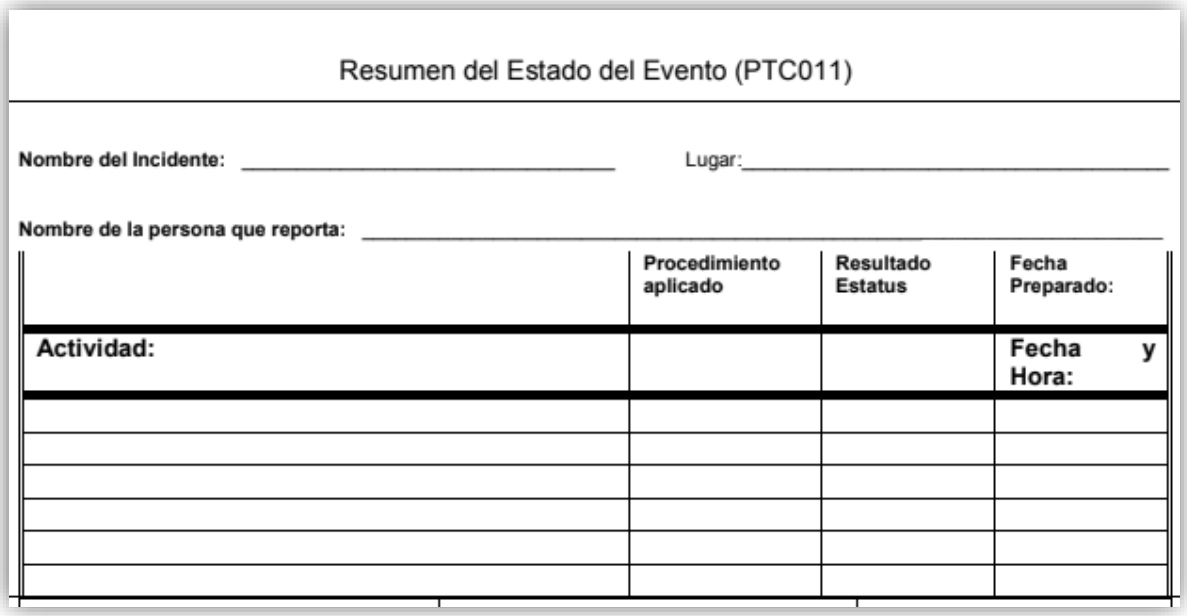
Notas:

Ilustración 14 - Plantilla de recuperación de equipo.

Fuente CCSS (2007)

2.4.5.4. Plantilla resumen del evento.

La CCSS (2007) dentro de su manual para la creación del plan de continuidad, establece una plantilla como bitácora con el objetivo de documentar las actividades realizadas (Véase Ilustración 15).



Resumen del Estado del Evento (PTC011)

Nombre del Incidente: _____ Lugar:_____

Nombre de la persona que reporta: _____

	Procedimiento aplicado	**Resultado Estatus**	**Fecha Preparado:**
Actividad:			**Fecha y Hora:**

Ilustración 15 - Plantilla de recuperación de resumen del estado del evento.

Fuente: CCSS (2007).

2.4.6. ITIL – Diseño del servicio.

IT Infraestructure Library (En adelante ITIL) es un conjunto de publicaciones de mejores prácticas dirigidas a la gestión de servicios de TI que proporciona orientación a los proveedores de servicios sobre la prestación de servicios de TI de calidad, abarcando procesos, funciones y capacidades necesarias para respaldar dicho servicio (Steinberg, Rudd, Lacy, & Hanna, 2011).

Como parte de ITIL en su versión 2011, se encuentra cinco publicaciones basadas en las fases del ciclo de vida del servicio (Véase Ilustración 16), considerando específicamente el diseño del servicio, este se enfoca en garantizar que los servicios proporcionen valor al negocio, tomando como referencia los objetivos del negocio para su correcto diseño.

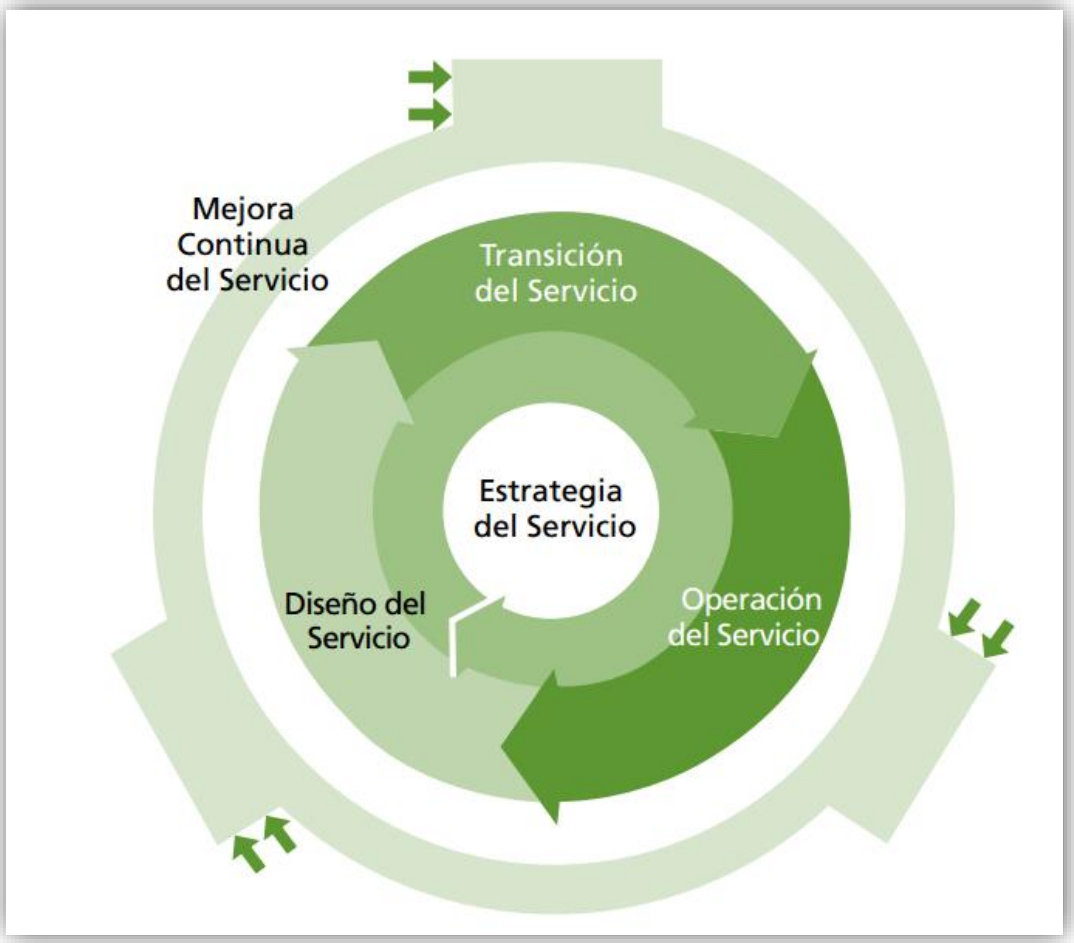


Ilustración 16 - Ciclo de vida de ITIL.
Fuente: Emaze (2017)

La publicación basada en el diseño del servicio proporciona orientación para el correcto diseño y desarrollo de servicios y prácticas para su gestión. Abarca principios y métodos de diseño para convertir los objetivos estratégicos en

portafolios de servicios y activos de servicios. Esta publicación abarca más que el diseño del servicio, además incluye cambios y mejoras para elevar el valor de los servicios para los clientes, continuidad del servicio y acuerdos de nivel de servicio. (Steinberg, Rudd, Lacy, & Hanna, 2011).

Dentro de la publicación del diseño del servicio, detalla el proceso de la gestión de la continuidad de los servicios de TI, que tiene como propósito respaldar el proceso de gestión de la continuidad del negocio, minimizando los riesgos que podrían afectar los servicios de TI.

El proceso de la gestión de continuidad de servicios de TI se encuentra segmentado en cuatro fases.

2.4.6.1. Iniciación.

La etapa de iniciación dentro del proceso de gestión de la continuidad de TI consta de las tres actividades (Véase Tabla 11).

Tabla 11 - Actividades, etapa iniciación.

Actividad	Detalle
Configuración de políticas.	El proceso de gestión de la continuidad de TI debe ser comunicado a los colaboradores involucrados de la organización.
Definir alcance y términos de referencia.	Define el alcance y responsabilidades de todo el *staff* en la organización.
Inicio del proyecto.	Se gestiona lo siguiente: • Distribución de los recursos.

Actividad	Detalle
	• Definición de la organización del proyecto y la estructura de control. • Acuerdos y planes de calidad.

Fuente: Steinberg, Rudd, Lacy, & Hanna (2011).

2.4.6.2. Requerimientos y estrategias.

En esta etapa se define los requerimientos (Véase Tabla 12) del negocio respecto a la continuidad de los servicios de TI, determinando cuánto podría sobrevivir la organización durante una interrupción y los costos que incurre. Además, define las estrategias a considerar para mitigar una interrupción (Steinberg, Rudd, Lacy, & Hanna, 2011).

Tabla 12 – Requerimientos para la continuidad de los servicios de TI

Requerimiento	Descripción.
Análisis de impacto de negocio.	Cuantifica el impacto que tendría la organización en caso de la pérdida de un servicio de TI.
Evaluación de riesgos.	Evalúa el nivel de una amenaza y la medida de vulnerabilidad que mantiene la organización.

Fuente: Steinberg, Rudd, Lacy, & Hanna, (2011).

2.4.6.3. Implementación.

Una vez aprobada la estrategia, los planes de continuidad de los servicios de TI deben producirse de acuerdo con los planes de continuidad del negocio. Las

estrategias deben cubrir acuerdos para reducir los riesgos, opciones de recuperación y las pruebas que garanticen lo planificado (Steinberg, Rudd, Lacy, & Hanna, 2011).

Los planes de continuidad de los servicios de TI necesitan ser desarrollados para permitir que la información que requieren los sistemas y sistemas críticos sea proporcionada o reincorporada dentro de un plazo aceptable para el negocio.

Dentro de un proceso de recuperación, la estructura organizacional sufre un comportamiento distinto a lo normal dentro de las operaciones normales dentro de una organización (Véase Tabla 13).

Tabla 13 - Estructura organizacional - ITCM.

Nivel	Descripción.
Ejecutivo.	Se comprende por los gerentes o comité ejecutivo con la autoridad de control sobre la organización y responsables de la gestión de crisis.
Coordinación.	Normalmente se comprende por colaboradores que se encuentran bajo el nivel ejecutivo. Es responsable de coordinar el esfuerzo de recuperación.
Recuperación.	Equipos de recuperación del negocio y servicios, encargados de funciones vitales del negocio que necesitan ser restablecidas.

Fuente: Steinberg, Rudd, Lacy, & Hanna (2011).

2.4.6.4. Operación.

Se comprende de las actividades aplicadas para establecer el sistema de gestión de continuidad de TI dentro de la organización (Véase Tabla 14). Se debe tener en cuenta que para mantener la relevancia del plan de continuidad de TI requiere el recurrente análisis de impacto de negocio y evaluación de riesgos relacionados con TI con el objetivo de aplicar los cambios necesarios que garanticen la efectividad del plan (Steinberg, Rudd, Lacy, & Hanna, 2011).

Tabla 14 - Actividades - Etapa Operación.

Actividad	Descripción.
Educación, conciencia y entrenamiento.	Garantiza la concienciación de los colaboradores respecto a la continuidad del negocio y de los servicios de TI, por medio de capacitación, concienciación y educación. Permite implantar dentro del trabajo normal, la gestión de las estrategias detalladas dentro del plan de continuidad.
Revisión y auditoria.	Revisión periódica de todos los procesos que conforman el plan de continuidad, para garantizar que se encuentren actualizados según los recursos existentes.
Pruebas.	Garantiza que los componentes críticos de la estrategia que conforma el plan de continuidad sean probados al menos una vez al año.
Gestión del cambio.	Proceso clave para garantizar que los cambios aplicados dentro de las estrategias del plan de continuidad sean evaluados a nivel de impacto. Si los cambios invalidan alguna estrategia del plan de continuidad de TI, este debe ser actualizado y probado antes de su implementación.

Fuente: Steinberg, Rudd, Lacy, & Hanna (2011).

3. Capítulo III: Marco metodológico.

En este capítulo se hace énfasis en el tipo de investigación y la metodología utilizada para el desarrollo de este trabajo final de graduación. Igualmente, se detalla las técnicas e instrumentos requeridos para la recolección de datos, los procedimientos de análisis y las herramientas que respaldan el desarrollo este proyecto.

3.1. Alcance de la investigación.

Una investigación puede contar con tres tipos de alcances (Hernández, Fernández, & Baptista, 2014), los cuales fueron considerados dentro del desarrollo de esta investigación.

El primer alcance abordado es el exploratorio, pues dentro del desarrollo de la investigación es necesario investigar sobre la continuidad del negocio y la continuidad de TI, además de su relación con los análisis BIA y análisis de riesgo, acciones necesarias para conjuntar una base teórica que brinda respaldo a los resultados de esta investigación.

Se aborda también un alcance descriptivo, desarrollado con el objetivo de generar una descripción del problema presentado y el estado actual de la gestión de la continuidad de TI dentro de la organización. Igualmente, es necesario para la descripción de los resultados obtenidos mediante instrumentos y técnicas de investigación.

Es importante resaltar que el alcance final de los estudios cualitativos muchas veces consiste en comprender un fenómeno complejo, por ello el objetivo que mantienen los estudios cualitativos no está en medir las variables del fenómeno, sino en entenderlo (Hernández, et al., 2014).

3.2. Enfoque de la investigación.

Una investigación se compone de un conjunto de procesos sistemáticos, empíricos y críticos aplicados al estudio de un problema. Una investigación se puede desarrollar siguiendo tres enfoques, el cualitativo, el cuantitativo y el mixto, que conlleva una combinación de los dos primeros enfoques (Hernández, et al., 2014).

Tomando en consideración los tres enfoques anteriormente mencionados, este trabajo final de graduación fue desarrollado mediante una investigación con un enfoque cualitativo. Según Hernández, et al., en un enfoque cualitativo el proceso de investigación se desarrolla dinámicamente entre los hechos y su interpretación.

Una investigación con un enfoque cualitativo se enfoca en comprender, profundizar y explorar fenómenos desde la vista de los participantes dentro de su ambiente natural y su relación con el contexto.

Con respecto al enfoque cualitativo, este cuenta con diferentes características (Hernández, et al., 2014), que fueron utilizadas dentro del desarrollo de esta investigación. Se detallan a continuación:

- Revisión de literatura y construcción del marco teórico sobre la continuidad de TI, el análisis de riesgos y el BIA.
- Planteo de un problema relacionado a la continuidad de TI dentro de JASEC, el cual no sigue una secuencia especifica de procesos para su resolución, sino conforme avanza la investigación, se ajusta los criterios de análisis.
- Uso de métodos de recolección de datos y análisis de información, ya que existen recursos documentales desactualizados.
- Se estudia de forma participativa dentro del área de TIC de JASEC, con el objetivo de realizar un análisis de los procesos y las actividades que desempeñan.

Un enfoque cualitativo mantiene ciertas características (Hernández, et al., 2014), las cuales se describe a continuación:

- Durante el desarrollo del proceso de investigación (Véase Ilustración 17), es necesario regresar a distintas etapas.
- La recolección de datos y el correspondiente análisis se realiza como etapas prácticamente simultaneas.
- Se realiza la exploración, descripción y generación de teorías.
- La recolección de datos no sigue un modelo estandarizado.

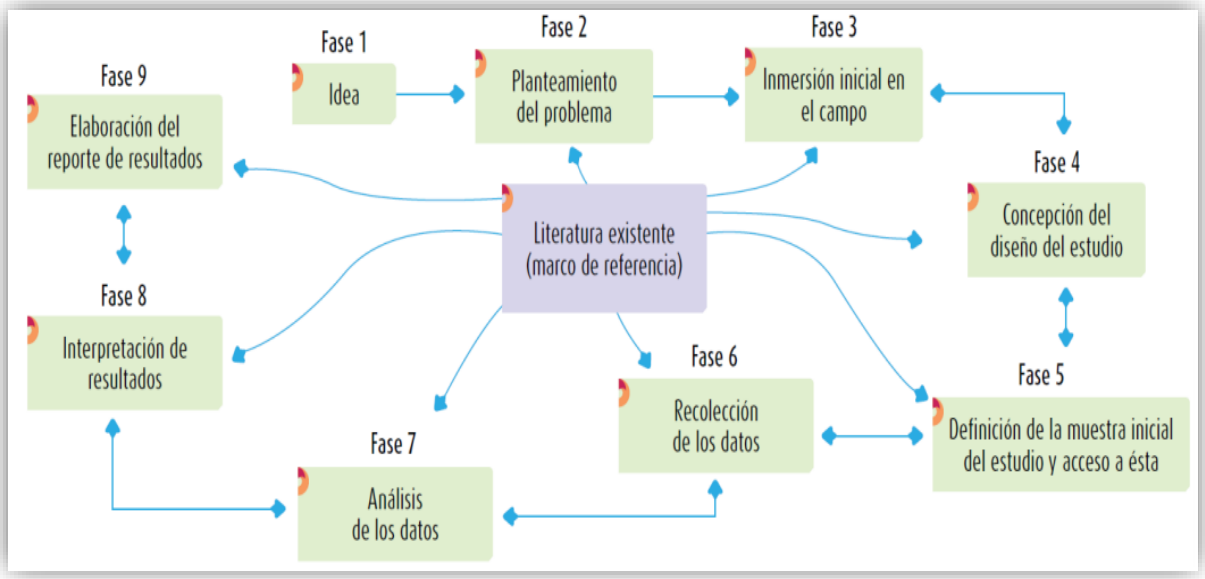


Ilustración 17 - Proceso de investigación cualitativa.

Fuente: Hernández, Fernández, & Baptista (2014).

Además, algunas características que cumple el enfoque cualitativo (Abarca, Alpízar, Rojas, & Sibaja, 2012), son las siguientes:

- Valida información de forma completa.
- La captura de información es realizada de forma flexible y no estructurada.

- Utiliza un diseño de investigación flexible.
- Utiliza una perspectiva holística para el análisis del escenario de investigación.

3.2.1. Diseño de la investigación.

El diseño de esta investigación está basado en el diseño investigación-acción, el cual Hernández, et al. (2014), señalan que su función es resolver problemas cotidianos e inmediatos y brindar mejores prácticas concretas.

Igualmente, Hernández, et al. (2014) mencionan que el diseño investigación-acción contiene las siguientes características:

- Construye el conocimiento por medio de práctica.
- Conlleva un involucramiento de los colaboradores para la identificación de necesidades y en la implementación de soluciones.
- Da inicio de problemas prácticos vinculados con el entorno.
- Genera conciencia sobre el rol que tienen las personas dentro de la transformación.

Desarrollar la investigación utilizando un diseño investigación-acción, permite contar con insumos necesarios para la toma de decisiones, las cuales fomentan el cambio social, la transformación de la realidad y la generación de conciencia en las personas respecto a su papel en la transformación a realizar con los resultados obtenidos de la investigación.

Además, el diseño investigación-acción tiene distintas modalidades y la que mejor se adapta a este trabajo final de graduación es la investigación-acción cooperativa. En la investigación-acción cooperativa los involucrados se relacionan durante todo el proceso y se consideran coinvestigadores (Hernández, et al., 2014).

Los principios que sigue una investigación con un diseño investigación-acción cooperativa son los siguientes:

- Los resultados obtenidos deben generar un impacto positivo.
- Confianza y cooperación entre los involucrados.
- Debe existir empoderamiento de los involucrados.
- El contexto de la investigación es fundamental.

Este método de investigación tiene como característica que los sujetos investigados se convierten en coinvestigadores, dado que los resultados que se obtienen de la investigación son de su interés y por ello, se mantienen activos durante el desarrollo de esta (Abarca, et al., 2008).

3.3. Población.

La población es el objeto de estudio dentro de una investigación, además, según Hernández, et al. (2014), la población se compone de participantes, objetos o colectivos de estudio de los que depende una investigación.

Para el desarrollo de la investigación que soporta este trabajo final de graduación, se define como población objetivo los procesos de negocio que gestiona cada área operativa dentro de JASEC.

La importancia de definir a los procesos de negocio como población objetivo de la investigación se basa en la importancia que mantiene tanto dentro de la organización, como con el área de TIC y los análisis que se realiza dentro de esta investigación.

A esta población, se aplica distintas técnicas y herramientas de investigación cualitativa para conocer su estado actual y delimitarla, con el objetivo de crear la unidad de muestreo a estudiar.

3.4. Unidad de muestreo.

Según Hernández, et al. (2014), la unidad de muestreo son aquellos casos que se alinean a un conjunto de características y especificaciones consideradas dentro de una investigación.

Para el desarrollo de la investigación que apoya este trabajo final de graduación, la unidad de muestreo es el conjunto de procesos críticos del negocio que son soportados por el área de TIC de JASEC.

Importante aclarar que, para esta investigación al ser del tipo cualitativa, no resulta necesario definir una población ni muestra de análisis, dicho detalle tiene como objetivo comprender la gestión de los procesos críticos del negocio y determinar la dependencia existente con respecto al área de TIC de JASEC, actividades necesarias para desarrollar un plan que logre brindar continuidad a dichos procesos.

3.5. Fuente de información.

El desarrollo investigativo de este trabajo final de graduación se respalda con distintas fuentes de información, necesarias para el estudio de la problemática existente y para el desarrollo del plan de continuidad de los procesos críticos de negocio soportados por el área de TIC de JASEC.

Esta investigación se basa en consultas realizadas a fuentes de información, las cuales presentan la siguiente clasificación.

3.5.1. Fuentes de información primaria.

Las fuentes primarias de información se comprenden de información original, sin ningún tipo de filtro, interpretación o evaluación por ningún otro estudio (Silvestrini y Vargas, 2017).

Las fuentes de información primaria usadas son las siguientes:

- Colaboradores de JASEC.
- Normativas y estándares de referencia.
- Documentación relacionada con continuidad de TI desarrollada dentro de JASEC.
- Publicaciones académicas relacionadas con la gestión de continuidad de TI.
- Libros sobre metodología de investigación.
- Plantillas y estándares del área de TIC.

3.5.2. Fuentes de información segundaria.

Con respecto a las fuentes de información secundaria, estas se derivan de una fuente primeria que ha sido reorganizada o evaluada mediante alguna técnica (Silvestrini y Vargas, 2017). Estas permiten tener acceso a contenidos y fuentes primarias.

Las fuentes de información secundaria usadas son las siguientes:

- Trabajos de graduación de universidades públicas o privadas de educación superior.
- Plantillas y estándares del área de TIC sometidos a revisiones.

3.5.3. Fuentes de información terciaria.

Las fuentes de información terciaria corresponden a datos o información obtenida tomadas de guías de obras y que corresponde sobre fuentes secundarias de información (Silvestrini y Vargas, 2017).

Las fuentes de información terciaria usadas son las siguientes:

- Sistema de Bibliotecas del Tecnológico de Costa Rica y su respectivo catalogo en línea.
- Repositorios en línea de bibliotecas de instituciones públicas y privadas de educación superior.

3.6. Sujetos de información.

Para el desarrollo de la investigación, es necesario la participación de distintos colaboradores de JASEC, los cuales son de importancia tanto para la recolección de datos como para el análisis de información y la generación de la propuesta del plan de continuidad.

Los sujetos de información son divididos en tres roles que permiten segmentar la información que brindan como insumo (Véase Tabla 15).

Tabla 15 - Sujetos de información.

Rol	Información.
Jefe del área de TIC.	• Información sobre las razones de desarrollar el proyecto. • Contexto de la organización. • Beneficios de desarrollar un plan de continuidad de TI dentro de la organización.

Rol	Información.
	• Validar las herramientas utilizadas en el desarrollo del proyecto. • Brindar retroalimentación sobre el desarrollo del proyecto.
Colaboradores del área de TIC.	• Conforman una base sólida de información del área y sus procesos. • Conocen la necesidad existente de un plan de continuidad de TI, pues son quienes dan soporte al negocio. • Cuentan con información detallada sobre procesos, buenas prácticas implementadas y procedimientos relevantes para el proyecto. • Conocen las condiciones actuales de la organización respecto a TIC.
Colaboradores encargados de procesos críticos de JASEC.	• Brindan insumos importantes para la identificación de los procesos críticos del negocio y por consiguiente, el desarrollo del plan de continuidad de TI.

Fuente: Elaboración propia.

3.7. Métodos y técnicas de investigación.

Los métodos y técnicas utilizadas dentro de este trabajo final de graduación son especificados por Hernández, et al. (2014) para el desarrollo de investigaciones que tienen relación la teoría con la práctica. Son definidos a continuación.

3.7.1. Método por índices.

El marco teórico que soporta esta investigación se desarrolla por medio del método por índices. El método por índices se desarrolla inicialmente generando un índice con la base teórica básica necesaria para la investigación; conforme se avanza con la investigación, dicho índice se detalla con temas más específicos que ayudan a complementar la investigación.

3.7.2. Observación documental.

Mediante una observación documental implica profundizar dentro de las situaciones propias del área. Según Hernández, et al. (2014), es necesario prestar atención a detalles con el objetivo de explorar ambientes, entender procesos e identificar problemas.

Asimismo, durante el desarrollo de este trabajo final de graduación, se realiza una lectura de documentos, informes y reportes relacionados con la problemática de la investigación.

3.7.3. Entrevistas.

Realizada la observación documental, fue necesario la aplicación de entrevistas con personas relacionadas al área, con el propósito de obtener información adicional que aporte valor a la investigación.

Una entrevista se define como una reunión entre varias partes, donde existe intercambio de información entre el entrevistador y el/los entrevistados (Hernández, et al., 2014).

Además, una entrevista permite la recopilación de información detallada en vista de que la persona que informa comparte oralmente con el investigador aquello concerniente a un tema específico (Vargas, 2012).

Entre los tipos de entrevistas existente, la entrevista semiestructurada es definida por Hernández, et al. (2014), como una entrevista con preguntas predefinidas, pero con la apertura hacia el entrevistador de agregar preguntas adicionales, según como se desarrolle el contexto de la entrevista.

Este tipo de entrevista es utilizada durante el desarrollo de la investigación, por la facilitad de ajuste al momento de ser aplicada.

3.7.4. Grupo focal.

Un grupo focal es comprendido por una reunión entre varias personas con el afán de conversar sobre uno o varios temas a profundidad, dicha reunión es guiada por un experto que define el tiempo disponible, el propósito de la reunión y gestiona la línea a seguir durante el desarrollo de esta (Hernández, et al., 2014).

Mediante un grupo focal se crea un espacio de opinión para captar el pensamiento y experiencia de los participantes, mediante la apertura a explicaciones que permite obtener datos cualitativos (Hamui, Varela., 2012).

Con el uso de esta técnica, pretende que el desarrollo del plan de continuidad de TI sea realizado junto con los colaboradores del área de TIC, ya que estos indican aspectos que es necesario aplicar; además, validan propuestas y generan observaciones.

3.7.5. Cuestionario.

Según Abarca, et al. (2012), un cuestionario se comprende de preguntas con el fin de interrogar sobre asuntos variados, las preguntas pueden ser abiertas, cerradas o mixtas, según la necesidad de la investigación.

Dentro del desarrollo de este trabajo final de graduación, los cuestionarios permiten conocer aspectos sobre los procesos de negocio, su criticidad y relación con el área de TIC de JASEC.

3.8. Análisis de información.

Posterior a aplicar los métodos y técnicas de investigación, se transcribieron los resultados con la finalidad de analizar e interpretar los datos. Se compararon los resultados obtenidos con el objetivo de determinar patrones que permitan identificar similitudes.

Con esto fue posible crear las estrategias necesarias presentes en el apartado 5.9, apoyadas de normas y conocimiento teórico documentado dentro del Capítulo II: Marco teórico, que permitiera cubrir la necesidad existente dentro del problema identificado.

3.9. Procedimiento metodológico.

El marco metodológico para el desarrollo de la investigación que soporta este trabajo final de graduación, está comprendido por 3 etapas, las cuales responden a los objetivos planeados para resolver la problemática existente.

Dichas etapas son definidas según lo establecido dentro de la normativa ISO 22301, siguiendo el modelo PDCA. Importante señalar que al igual como se detalló dentro del marco teórico, el último componente del modelo PDCA no se considera, dado el alcance de este trabajo final de graduación, por lo cual, dicho componente no es considerado en el procedimiento metodológico de esta investigación.

El procedimiento metodológico aplicado en esta investigación está comprendido por actividades secundarias, implementadas dentro de las etapas del modelo PDCA (Véase Ilustración 18).

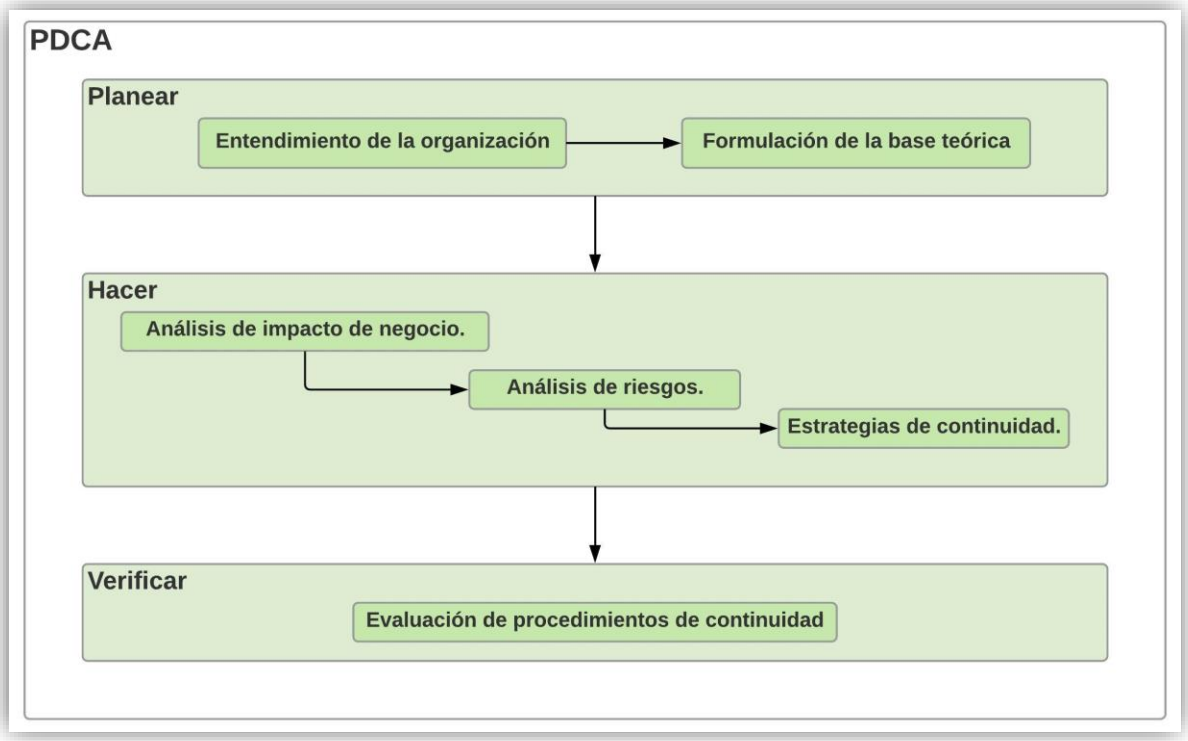


Ilustración 18 - Procedimiento metodológico de la investigación.

Fuente: Elaboración propia.

A continuación, se detalla a profundidad las actividades realizadas dentro de cada etapa que comprende el procedimiento metodológico desarrollado en esta investigación.

3.9.1. Etapa I: Planear.

Iniciando con la metodología PDCA, la investigación da inicio con la etapa de planear; dentro de dicha planeación es necesario considerar un conjunto de actividades establecidas que ayudan a definir las bases necesarias para la investigación.

Se presentan con más detalle las actividades consideradas.

3.9.1.1. Entendimiento de la organización.

Se realiza un entendimiento de la organización y en específico del área de TIC, es necesario identificar los procesos que gestiona el área, servicios que brinda a la organización como área clave del negocio, políticas relacionadas con TIC que mantienen para su cumplimiento dentro de la organización e información sobre los puestos que conforman el área de TIC.

Con el fin de alcanzar el éxito dentro de esta actividad, se ejecutan las siguientes actividades.

- Análisis documental.

Revisión y análisis de documentación existente dentro del área de TIC con el objetivo de identificar consideraciones claves dentro de la gestión de los recursos tecnológicos y que deben ser revisados y abordados dentro de la generación del plan de continuidad de TI.

Además, al entendimiento de la organización se procede a realizar una actualización y unificación de documentación propia del área de TIC de JASEC, que permanecía dispersa y desactualizada; esto se realiza dado que contar con documentación precisa y real del área de TIC era necesario para alcanzar el objetivo principal de este trabajo final de graduación.

- Entrevista.

Recolección y análisis de la información suministrada por colaboradores del área de TIC de JASEC. La información recolectada es necesaria para desarrollar los pasos que comprenden el procedimiento metodológico a implementar dentro de la investigación que soporta este trabajo final de graduación.

El objetivo de aplicar una entrevista a colaboradores del área de TIC es conocer sobre la existencia de análisis de impacto de negocio o análisis de riesgos realizados a TIC.

3.9.1.2. Formulación de la base teórica.

Se recopila la base teórica relacionada con la continuidad de TI, identificando normas, manuales y guías que permiten generar los insumos necesarios para generar un plan de cantidad de TI.

Además, considerando la información detallada dentro del marco teórico (Véase Capítulo II: Marco teórico); se estructura por medio del método de índices los aspectos necesarios a aplicar dentro de la metodología de esta investigación.

3.9.2. Etapa II: Hacer

Conformada la base teórica que sustenta esta investigación, se continúa con el desarrollo de la segunda etapa que comprende la metodología PDCA, la cual corresponde a hacer o desarrollar, palabra que entra más en contexto con la investigación.

Como parte de esta etapa, son consideradas un conjunto de actividades que conllevan a la generación de los insumos necesarios para el desarrollo del plan de continuidad de TI.

Se presenta con detalle cada una de las actividades realizadas dentro procedimiento metodológico.

3.9.2.1. Análisis de impacto de negocio.

El procedimiento metodológico desarrollado específicamente para el BIA, toma como referencia lo recomendado dentro de la guía para realizar el análisis de impacto de negocio desarrollada por MINTIC (2015).

Dicho procedimiento contempla las actividades recomendadas por la guía mencionada anteriormente para identificar los activos críticos dentro del área de TIC (Véase Ilustración 19).

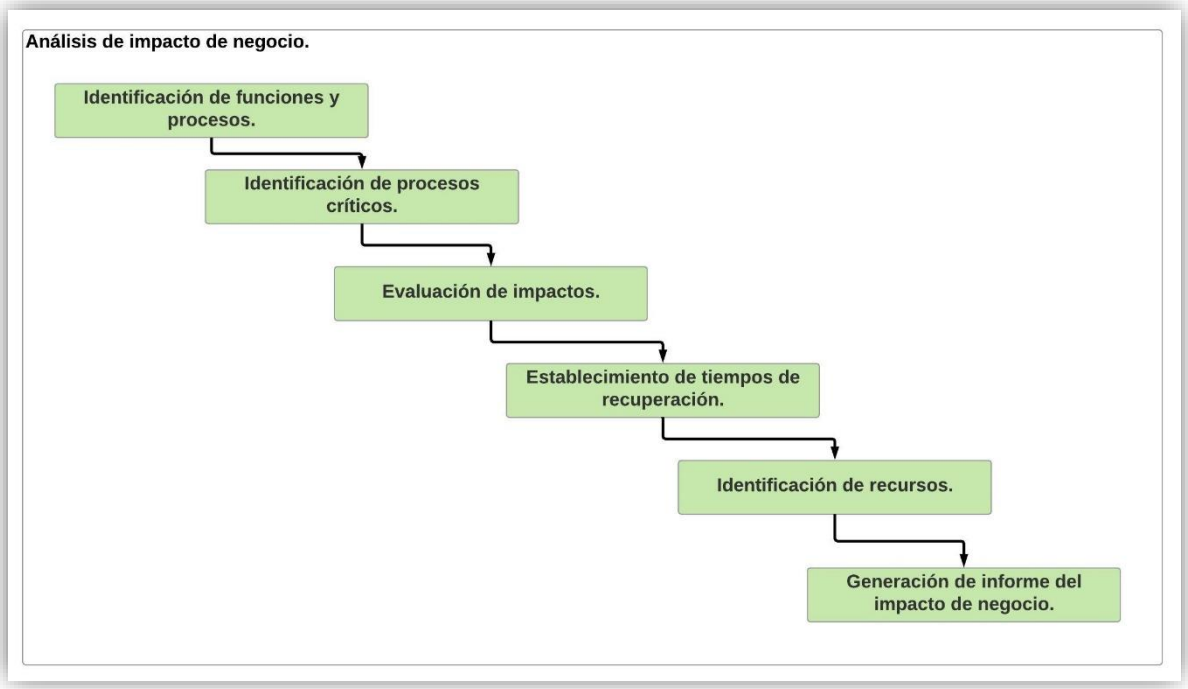


Ilustración 19 - Procedimiento metodológico para el BIA.

Fuente: Elaboración propia.

Cada una de las actividades que contempla el procedimiento metodológico para desarrollar el BIA, se especifica a continuación.

3.9.2.1.1. Identificación de funciones y procesos.

La identificación de las funciones y procesos de cada área dentro de JASEC se realiza con el objetivo de contextualizar las áreas donde se planeó desarrollar el BIA.

Dicha identificación es realizada mediante una observación documental, donde se agrupan en común todos los procesos y sus respectivas actividades, con el objetivo de contar con los insumos necesarios para desarrollar el BIA.

Una vez identificados los procesos y actividades, se agrupan según corresponda con respecto a los departamentos que conforman cada área, con el propósito de facilitar el trabajo que prosigue a esta actividad dentro del procedimiento metodológico.

3.9.2.1.2. Identificación de procesos críticos.

La identificación de los procesos críticos permite conocer aquellos procesos que son clave dentro de las operaciones de cada área en específico.

La criticidad de los procesos es determinada por el grado de dependencia que existe en cada área a nivel interno y por el nivel de soporte que recibe el proceso por parte del área de TIC.

Para dicha identificación se aplican cuestionarios que permiten recolectar y analizar los datos suministrados por los jefes de áreas operativas de JASEC, los datos recolectados son necesarios para determinar los procesos críticos de cada área operativa y los sistemas informáticos que los soportan.

3.9.2.1.3. Evaluación de impactos.

Con esta evaluación se logra identificar el impacto que genera a la organización, una posible interrupción en la operación de los procesos.

La evaluación de impactos se realiza considerando las categorías de impactos (Véase Tabla 16), definidas por la CCSS (2007) dentro de su manual para elaborar un plan de continuidad.

Para conocer el impacto que genera la inactividad de un proceso crítico soportado por TI, se consulta por medio de un formulario aplicado a cada uno de los jefes de las áreas operativas de JASEC.

Tabla 16 - Categorías de impacto.

Categoría	Descripción.
Operacional.	Afectación operativa dentro de la organización.
Legal o regulatorio.	Afectación por medio de una sanción de carácter legal o regulatorio.
Financiero.	Afectación en las finanzas de la organización.
Reputación.	Afectación a nivel de imagen de la organización.

Fuente: CCSS (2007).

3.9.2.1.4. Establecimientos de tiempos de recuperación.

Con el objetivo de establecer los tiempos de recuperación de los procesos críticos de negocio soportados por TI, se consulta el tiempo máximo que podría operar sin los servicios de TI antes de generar una afectación mayor. Dicha consulta se realiza por medio de un formulario aplicado a cada uno de los jefes de las áreas operativas de JASEC.

3.9.2.1.5. Identificación de recursos.

Una vez identificados los procesos críticos, se continúa con la identificación de aquellos recursos del área de TI que les brinda soporte.

La identificación de dichos recursos, permite establecer las estrategias necesarias dentro del plan de continuidad, que garanticen la operación continua de cada uno de los procesos críticos.

Para identificar los recursos críticos se procede a con la generación de una matriz de relación, matriz que permite identificar tanto el *software* como el *hardware* que soporta los procesos críticos identificados dentro del BIA.

3.9.2.1.6. Generación de informe del impacto de negocio.

Como actividad final del procedimiento metodológico para el desarrollo del BIA, se procede a documentar información respecto a los procesos críticos, el impacto que genera una interrupción de dichos procesos y los recursos críticos del área de TIC que los soportan.

Una vez concluido el procedimiento metodológico específico del BIA, se procede a iniciar con el análisis de riesgos.

3.9.2.2. Análisis de riesgos.

Con respecto al análisis de riesgos, el procedimiento metodológico ejecutado para su elaboración sigue como referencia lo establecido dentro de la normativa ISO 31000 (Véase Ilustración 20), la cual especifica un conjunto de actividades para un correcto abordaje de los riesgos.

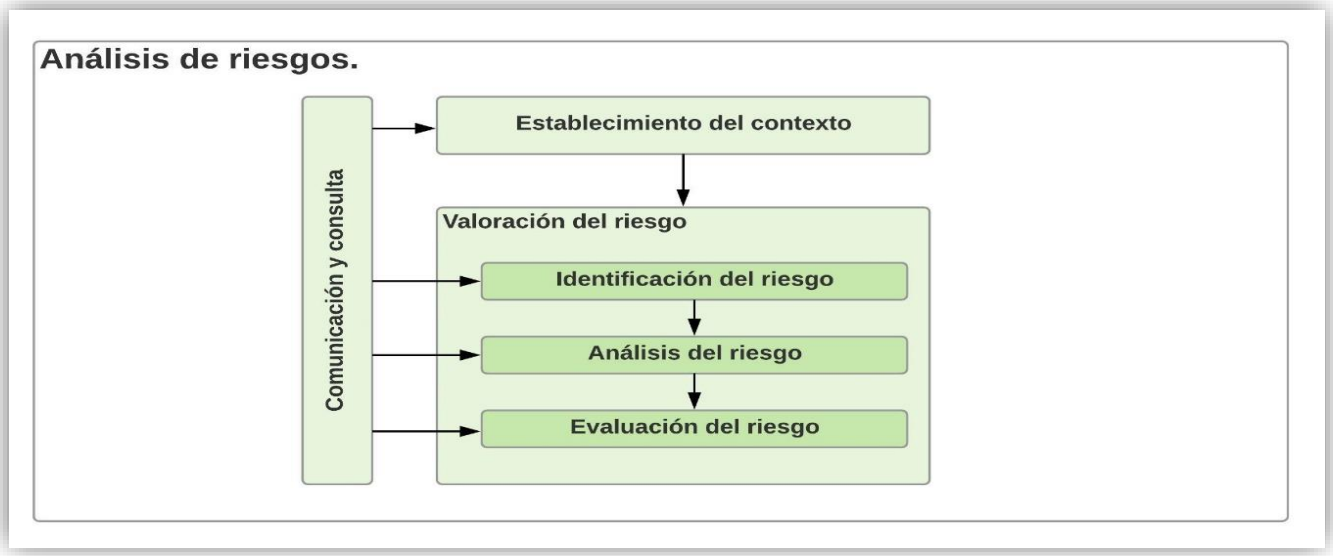


Ilustración 20 - Procedimiento metodológico para el análisis de riesgos.

Fuente: ISO 31000.

Se presenta con detalle cada una de las actividades que comprende el análisis de riesgos a desarrollar dentro de esta investigación.

3.9.2.2.1. Comunicación y consulta.

La comunicación y consulta es una actividad vertical dentro del flujo de actividades del análisis de los riesgos establecido dentro en la normativa ISO 31000, la cual permite mantener efectivamente un canal de comunicación para realizar las consultas necesarias a los colaboradores del área de TIC, independientemente de la actividad que se estuviese ejecutando dentro del flujo.

3.9.2.2.2. Establecimiento del contexto

Importante resaltar que, para una correcta identificación y análisis de los riesgos, se establece el contexto en el cual se desarrolla el análisis de riesgos, tomando como referencia la información obtenida dentro del análisis de impacto de negocio, la cual está relacionada con los activos de TI que soportan los procesos críticos de negocio de JASEC.

3.9.2.2.3. Valoración de riesgos.

Dentro de esta actividad, se realiza la identificación de los riesgos, su correspondiente análisis y la valoración respecto a su nivel de probabilidad de impacto y el nivel de impacto con el que cuenta dentro de las operaciones del área de TIC.

Se detalla las actividades que comprende la valoración de riesgos.

3.9.2.2.4. Identificación del riesgo.

Se identifica los principales riesgos que puede generar una afectación en las operaciones del área de TIC. Además, una vez identificados los riesgos, se consulta las medidas consideradas para la mitigación de los riesgos dentro de las gestiones propias del área de TIC.

Para la identificación de los riesgos, se utiliza como base las categorías de riesgos recomendados por la CCSS (2007), (Véase Tabla 17), dado que el contexto de ambas organizaciones cuenta con similitudes.

Tabla 17 - Categoría de riesgos.

Categoría de riesgo.
Interrupción eléctrica.
Fallos en hardware.
Fallos en software.
Fallos en comunicaciones.
Desastres naturales.
Incendio
Fallos en respaldos.
Virus
Violaciones a la seguridad física.
Intrusión.
Recurso humano.

Fuente: CCSS (2007).

Con el objetivo de alcanzar el éxito dentro de esta actividad, se realiza un grupo focal con colaboradores del área de TIC, específicamente con el jefe del área y colaboradores del departamento de arquitectura y comunicaciones, donde se considera las categorías de riesgos detalladas anteriormente y se valida que cada categoría aplique al contexto de JASEC.

3.9.2.2.5. Análisis del riesgo.

Una vez identificados los riesgos, se procede a realizar un análisis de los riesgos, que permita contar con la información necesaria para tomar las decisiones correspondientes al abordaje que requieren los riesgos dentro del plan de continuidad de TI.

Dentro del análisis de los riesgos, se busca verificar las medidas que toma el área de TIC para la mitigación de los riesgos, según las categorías planteadas en los puntos anteriores, (Véase Tabla 4).

Con el fin de alcanzar el éxito dentro de esta actividad, es necesario desarrollar un grupo focal con colaboradores del área de TIC con el objetivo de verificar mediante consenso de los colaboradores, cuáles medidas son consideradas dentro de las gestiones del área de TIC para la mitigación de los riesgos. (Véase Tabla 18)

Además, para verificar las medidas consideradas para mitigar riesgos que puede afectar a TI, se utiliza una lista de verificación para comprobar las medidas de mitigación de riesgos consideradas por el área de TIC.

Tabla 18 - Lista verificación sobre consideraciones para mitigar riesgos.

Categoría de riesgo	Aspectos mínimos por considerar.	Aplicado
Interrupción eléctrica.	Fuentes alternas de generación eléctrica: UPS y plantas eléctricas.	
	Mantenimiento de las fuentes alternas de generación eléctrica.	
	Estado de la instalación y capacidad eléctricas instalada.	
	Lámparas de emergencia.	
	Señalamiento iluminado de salidas y puertas de emergencia.	
Fallos en Hardware.	Equipo de cómputo utilizado y obsolescencia.	
	Capacidad de redundancia entre servidores.	
	Monitoreo de problemas en los servidores.	
	Contratos de mantenimiento preventivo y correctivo.	
	Condiciones físicas y ambientales (limpieza, humedad, temperatura).	
	Desarrollo local de aplicaciones (metodologías/ estándares).	

Categoría de riesgo	Aspectos mínimos por considerar.	Aplicado
Fallos en Software.	Cambios y configuración en aplicaciones.	
Fallos en comunicaciones	Soporte técnico de los equipos utilizados.	
	Mantenimiento preventivo y correctivo de los equipos de comunicación.	
Desastres naturales.	Pólizas de seguro vigentes.	
	Brigadas de atención ante situaciones de emergencia.	
	Capacitación al personal	
	Rutas de evacuación.	
	Iluminación de pasillos y puertas y salidas de emergencia.	
Incendio.	Pólizas vigentes de seguro.	
	Sistemas automáticos y manuales contra incendio (gabinetes, extintores, aspersores).	
	Uso de materiales retardantes del fuego.	
	No almacenamiento de material combustible.	
	Detectores de humo revisados regularmente.	
Fallos en respaldos.	Procedimientos para respaldo y recuperación de información, fuentes, objetos, documentación y configuración de los sistemas.	
	Periodicidad de los respaldos.	
	Facilidades y protección para el almacenamiento dentro y fuera de sitio.	
	Configuración de los discos duros de los servidores.	
	Documentación actualizada sobre procedimientos de respaldo y recuperación.	
Virus.	Programa antivirus instalado en computadoras y servidores.	
	Configuración y actualización del software antivirus.	
	Consultas regulares de fuentes de información para actualizaciones sobre virus.	

Categoría de riesgo	Aspectos mínimos por considerar.	Aplicado
	Capacitación al personal para identificar potenciales fuentes de ataque de virus.	
	Políticas para el ataque de virus.	
Violaciones a la seguridad física.	Seguridad física para el ingreso al edificio, oficinas y cuartos de servidores y equipos de comunicación.	
	Capacitación al personal para detectar situaciones que puedan representar riesgo o cuestionar la presencia de personas desconocidas o sin identificación.	
	Sistemas de seguridad: circuitos cerrados de televisión, sensores de movimiento, alarmas.	
	Revisión y control de salida e ingreso de equipo de cómputo.	
	Utilización de bitácoras para el registro de ingresos.	
Intrusión.	Procedimientos para otorgamiento de acceso a las aplicaciones y políticas de acceso lógico.	
	Procedimientos para el acceso a los recursos tecnológicos (redes y aplicaciones).	
	Administración y configuración de “firewalls”.	
	Monitoreo de los accesos tanto legítimos como ilegítimos.	
	Disponibilidad de herramientas para el monitoreo de la seguridad.	
Personal	Capacitación.	
	Documentación de las funciones del personal.	

Fuente: Elaboración propia.

3.9.2.2.6. Evaluación del riesgo.

La evaluación de los riesgos brinda la información necesaria para determinar cuáles riesgos requieren una atención más específica dentro del plan de continuidad.

Se evalúa el nivel de probabilidad y el nivel de impacto que alcanzan los riesgos dentro de las operaciones del área de TIC, tomando en consideración la opinión de los colaboradores de cada área considerada desde al BIA.

Con respecto a la evaluación de la probabilidad (Véase Tabla 19), se considera la clasificación especificada por la CCSS (2007) para el análisis del nivel de probabilidad.

Tabla 19 - Nivel de probabilidad usado en análisis de riesgo.

Nivel de probabilidad		Ocurrencia
Muy probable.	10	Es muy probable que ocurra un evento en un periodo de 3 meses.
Probable	7	Es poco probable que ocurra un evento en un periodo de 3 a 6 meses.
Moderada	5	El evento ocurrirá en algún momento en un periodo de 6 meses a 1 año.
Poco probable	3	Es poco probable que el evento suceda, pero podría suceder en un periodo de 1 año a 2 años.
Muy poco probable.	1	Es muy poco probable que el evento se presente en un periodo de 2 años.

Fuente: Elaboración propia.

En el caso de la evaluación del impacto, igualmente se considera la clasificación especificada por la CCSS (2007) para el análisis del nivel de impacto (Véase Tabla 20).

Tabla 20 - Nivel de impacto usado en análisis de riesgo.

Nivel de impacto		Descripción.
Crítico.	10	El evento provoca una interrupción completa dentro de las operaciones del área de TIC de JASEC.

Nivel de impacto		Descripción.
		Provoca una afectación total de los procesos críticos del negocio.
Significativo.	7	El evento provoca una interrupción entre completa y parcial dentro de las operaciones del área de TIC de JASEC. Provoca una afectación parcial de los procesos críticos del negocio.
Moderado.	5	El evento provoca una interrupción en las operaciones del área de TIC de JASEC. Las actividades críticas de negocio no se ven afectadas.
Menor.	3	El evento provoca un impacto leve en las operaciones del área de TIC de JASEC sin generar interrupciones dentro de las operaciones.
Insignificante.	1	El evento no provoca un impacto dentro de las operaciones del área de TIC de JASEC.

Fuente: Elaboración propia.

Con el fin de alcanzar el éxito dentro de esta actividad, se realiza un análisis de cuestionarios, donde se recolecta y analiza los datos recolectados de los colaboradores del área de TIC, datos necesarios para determinar el nivel de probabilidad de ocurrencia e impacto.

De igual modo, se desarrolla una matriz de calor para graficar la criticidad de los riesgos según la probabilidad de ocurrencia e impacto (Véase Tabla 21), tomando en consideración rangos de clasificación (Véase Tabla 22).

Tabla 21 - Mapa de calor para criticidad de los riesgos.

Probabilidad.	Impacto.				
	10	30	50	70	100
	7	21	35	49	70
	5	15	25	35	50
	3	9	15	21	30
	1	3	5	7	10

Fuente: Elaboración propia.

Tabla 22 - Rangos de clasificación de riesgos

Riesgo.	Rango Inferior.	Rango Superior.
Muy alto.	71	100
Alto.	36	70
Medio.	16	35
Bajo.	6	15
Muy Bajo.	1	5

Fuente: Elaboración propia.

3.9.2.3. Estrategias de continuidad.

Una vez desarrollado el BIA y el análisis de riesgos, se continúa con establecer las estrategias de continuidad, tomando como referencia lo establecido dentro de la normativa ISO 22301 como procedimiento metodológico (Véase Ilustración 21).

Ilustración 21 - Procedimiento metodológico para establecer las estrategias de continuidad. Fuente: ISO 22301.

El conjunto de actividades a realizar dentro esta actividad en la investigación son las siguientes.

3.9.2.3.1. Determinación y selección.

Dado que las actividades desarrolladas anteriormente permiten determinar el nivel de criticidad de los activos de TI y el nivel tanto del impacto como de probabilidad de ocurrencia que mantienen los riesgos en esta actividad, se procede a determinar los tipos de estrategias a considerar dentro del plan de continuidad.

Para determinar los tipos de estrategias, se desarrollan grupos focales con colaboradores del área de TIC, tomando como base la información recolectada hasta ese momento.

3.9.2.3.2. Establecer los recursos.

Para la ejecución del plan de continuidad para los activos de TI, es necesario establecer los recursos necesarios para garantizar su operación, por ello, se establece un comité dentro del área de TIC que asegure la correcta ejecución de las estrategias.

Se establecen los roles y responsabilidades asignadas para los colaboradores dentro del plan de continuidad, durante y después de la materialización de un incidente.

Durante el desarrollo de esta actividad, se realiza un grupo focal con el objetivo de analizar y definir los roles para la conformación del comité encargado del plan de continuidad.

3.9.2.3.3. Establecimiento de procedimientos.

Se establecen los procedimientos que garanticen la continuidad de operación de los activos críticos de TI, acorde a los requerimientos alcanzados con los análisis anteriormente realizados.

Con el fin de alcanzar el éxito dentro de esta actividad, se realizan grupos focales con colaboradores del área de TIC de JASEC, con el objetivo de definir las estrategias a considerar dentro del plan de continuidad.

3.9.3. Etapa III: Verificar.

Una vez desarrollado el plan de continuidad de TI, es necesario verificar el desempeño que alcanzan las estrategias definidas. Por tal motivo, se procede a verificar el plan de continuidad mediante una prueba.

El procedimiento metodológico de esta etapa se compone de una única actividad.

3.9.3.1. Evaluación de procedimientos de continuidad.

Dentro de esta actividad, se genera un escenario de prueba que permita evaluar las estrategias de continuidad generadas dentro del plan de continuidad.

La prueba es realizada con un proceso crítico, además es calendarizada y se genera reportes post incidentes y evaluaciones de desempeño que permita validar la eficiencia alcanzada.

4. Capítulo IV: Análisis de resultados.

Este capítulo presenta los resultados obtenidos en la ejecución del procedimiento metodológico planteado en el capítulo anterior.

Los resultados obtenidos corresponden a datos e información recopilada por medio de la aplicación de diferentes instrumentos y analizada con el objetivo de conformar una base sólida de información para alcanzar los objetivos planteados dentro del desarrollo de este trabajo final de graduación.

Como se detalla dentro del procedimiento metodológico (Véase Ilustración 22), la investigación se desarrolla tomando como base la metodología PDCA, por lo tanto, los resultados obtenidos son descritos siguiendo el orden establecido.

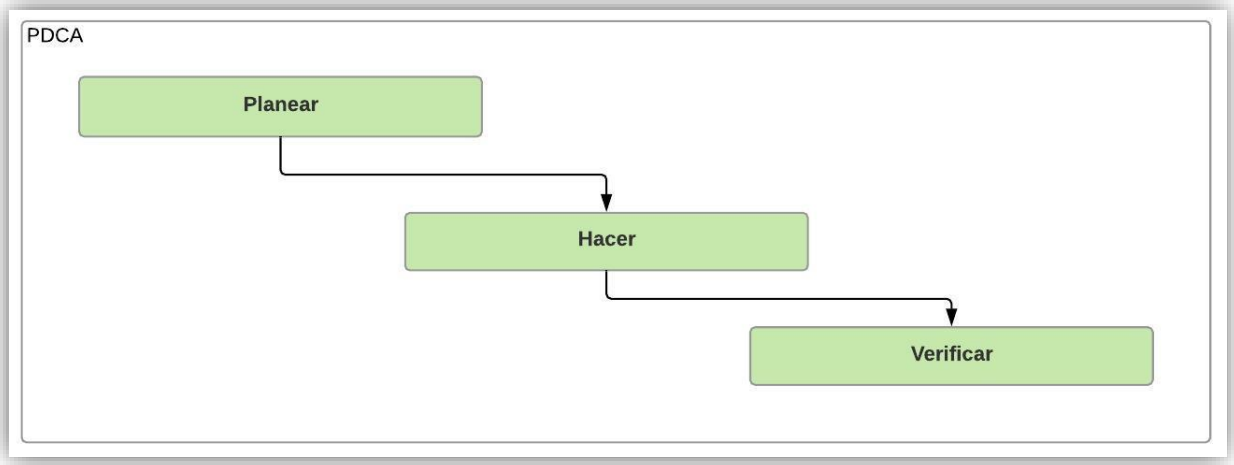


Ilustración 22 - Procedimiento metodológico - vista global.

Fuente: Elaboración propia.

4.1. Etapa I: Planear

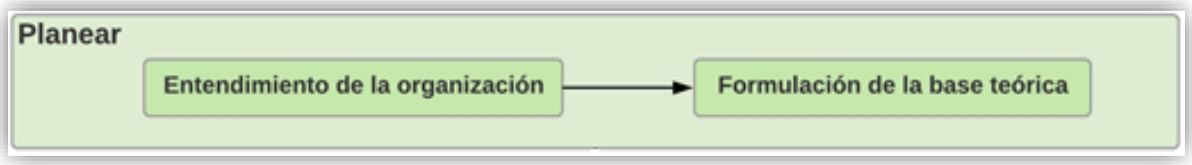
Para el desarrollo de la primera etapa del procedimiento metodológico, se emplearon tres instrumentos que permitieron alcanzar los resultados esperados dentro de cada actividad que comprende esta etapa.

Inicialmente, se realiza una revisión documental que permite conocer el estado actual de la organización. Para cada documento identificado, se recopila datos básicos considerados para el desarrollo de este trabajo final de graduación. La identificación y revisión de estos documentos permite conocer distintos lineamientos gestionados por el área de TIC a nivel interno.

Adicionalmente, para consolidar la base teórica que respalda esta investigación, se realiza una estructura de índices que permite organizar normas, metodologías, mejores prácticas vinculadas tanto a la continuidad de TI como al análisis de riesgos y el BIA necesarios para crear un plan de continuidad de TI.

Por último, una entrevista con colaboradores del área de TIC de la organización; tiene como objetivo ampliar el conocimiento existente de la organización y del área de TI y, además se implementa un grupo focal desarrollado que tiene como objetivo validar la propuesta de teórica a aplicar y adicionalmente, de forma conjunta con los colaboradores del área de TIC, se presenta la propuesta metodológica a utilizar dentro de la investigación, igualmente se toma en consideración recomendaciones y la experiencia de los colaboradores participantes.

Ilustración 23 - Etapa planear - Actividades.



Fuente: Elaboración propia.

4.1.1. Entendimiento de la organización.

Como parte del entendimiento de la organización, se recolecta y documenta información que mantiene relación con el objetivo principal de esta investigación.

Lo abordado dentro del entendimiento de la organización se encuentra en la información sobre documentación, activos de TI, monitoreo de TI y colaboradores del área de TIC; a continuación, se detallan.

4.1.1.1. Documentación.

La documentación existente en la organización y que mantiene relación con el plan de continuidad a desarrollar dentro de este trabajo final de graduación, tiene la siguiente clasificación: formularios, instructivos, normativas.

Se detalla los documentos correspondientes de cada clasificación, el detalle de cada documento se encuentra en Apéndice 9.2

- Formularios.
    - Control de cambios en sistemas de producción.
    - Plan anual de mantenimiento preventivo.
    - Solicitud de cuentas y acceso a sistemas.
    - Solicitud de cambios en la intranet.
    - Reporte de fallas de sistemas.
- Instructivos.
    - Incidencias en los equipos y sistemas informáticos.
    - Mantenimiento de servidores físicos y virtuales.
    - Monitoreo de los servicios de red informática.
    - Seguimiento y medición de los procesos del área de TIC.

  - Mantenimiento de los sistemas de seguridad de la red informática.
  - Respaldo y recuperación de información de bases de datos Informix. y Oracle.
- Normativas.
  - Marco normativo de la política de seguridad de información.
  - Política de uso de correo electrónico.
  - Política de seguridad de información.
  - Política de instalación y acreditación de soluciones y cambios.
  - Política de administración de cambios.
  - Procedimiento para administración de cambios.
  - Política de contratación de terceros.

4.1.1.2. Activos de TI.

Dentro de los activos de TI más importantes que gestiona el área de TIC de JASEC se encuentra sistemas informáticos, servidores y equipos de comunicación. (Véase Apéndice 9.1)

Como parte del entendimiento de la organización y dada la necesidad de contar con información real de los activos de TI que gestiona el área de TIC, se realiza una actualización del inventario de activos de TI.

4.1.1.2.1. Sistemas.

Dentro de JASEC se gestiona 28 sistemas informáticos que soportan las operaciones diarias de las distintas áreas de negocio que conforman la organización, aunque existen sistemas de uso muy específicos para algunas áreas, en cambio otros sistemas son utilizados por varias áreas de negocio, aumentando así el alcance que mantienen dentro de las operaciones.

4.1.1.2.2. Servidores.

Como parte de los servidores que son gestionados dentro de JASEC, se encuentran 109 servidores, de los cuales 10 son servidores físicos y los restantes 99 servidores son virtuales.

Los servidores son utilizados para operar por ejemplo los aplicativos de los sistemas informativos, la central telefónica y las bases de datos que almacenan los datos que producen y gestiona cada uno de los sistemas informáticos.

4.1.1.2.3. Equipo de comunicación.

El equipo de comunicación encargado de permitir el tráfico de datos dentro de sedes de JASEC, se encuentra conformado por 28 *switches*, cuatro *routers* y cuatro *wireless.*

El equipo se encuentra distribuido en las sedes que cuenta JASEC según la necesidad demandada.

4.1.1.3. Monitoreo de TI.

Dentro del área de TIC, se gestiona un ambiente de monitoreo del ancho de banda, sistemas, centro de datos y los ambientes virtualizados; se detalla a continuación.

4.1.1.3.1. Ancho de banda.

El monitoreo del ancho de banda se realiza por medio de un portal web, el cual permite detectar variaciones en el consumo del ancho de banda e identificar posibles problemas que puedan suceder.

Igualmente se gestiona el de acceso a los sitios de Internet por medio de una herramienta (*web filter*, su nombre en inglés), esta herramienta facilita filtrar los sitios que los colaboradores tienen acceso, con el objetivo de que aquellas páginas web que no son seguras, no puedan ser accedidas.

Además, otra función del *web filter* es controlar el ancho de banda destinado al uso para ciertos servicios, como por ejemplo la visualización de videos en *Youtube* o escuchar música en *Spotify*; esta medida tiene como objetivo no comprometer el ancho de banda existente dentro de las instalaciones.

4.1.1.3.2. Sistemas informáticos.

El área de TIC es responsable de brindar soporte tanto físico como virtual a cada uno de ellos, por esto mantienen constante monitoreo de los sistemas informáticos por medio de un software de monitoreo que permite conocer de forma automática y precisa el estado actual de cada uno.

4.1.1.3.3. Centro de datos.

En el centro de datos (*datacenter,* su nombre en inglés) se ubica los equipos de gestión de los sistemas y las comunicaciones de JASEC, por ello, es considerado como el activo más crítico y, su constante monitoreo se justifica como prioridad para el área de TIC.

El centro de datos utiliza controles de temperatura que, por medio de aire acondicionado, mantiene dentro de los intervalos recomendados la temperatura dentro del centro de datos; función vital para garantizar el correcto funcionamiento de los equipos.

Además, dentro del centro de datos se mantiene un sistema cerrado de cámaras, las cuales permiten tener control de las personas que ingresan y las acciones que realizan dentro. Igualmente, el acceso al centro de datos se encuentra restringido únicamente a personal autorizado.

4.1.1.3.4. Ambientes virtualizados.

Por medio de ambientes virtualizados, se gestiona algunos de los sistemas con los que cuenta la organización; además, se mantiene ambientes virtualizados dedicados para el desarrollo y pruebas.

Dado lo anterior, se mantiene un monitoreo constante de todos los ambientes virtualizados, dado la importancia que tiene dentro de las operaciones de diferentes áreas operativas.

4.1.1.4. Colaboradores.

Con respecto al personal que cuenta el área de TIC de JASEC, esta se encuentra conformada por 12 colaboradores, cuyas funciones se encuentran divididas según el departamento al que pertenezcan (Véase Anexo 2).

El área de TIC se encuentra dividido en tres departamentos, los cuales se encargan de la gestión de la arquitectura y comunicaciones, gestión de calidad y riesgos, gestión de sistemas, mantenimiento y desarrollo respectivamente.

4.1.2. Formulación de la base teórica.

Con el objetivo de generar la base teórica que respalda esta investigación, se diseña una estructura de índices (Véase Ilustración 24), la cual facilita la organización de

estándares, normas y metodologías necesarias para el desarrollo de la metodología utilizada dentro de esta investigación.

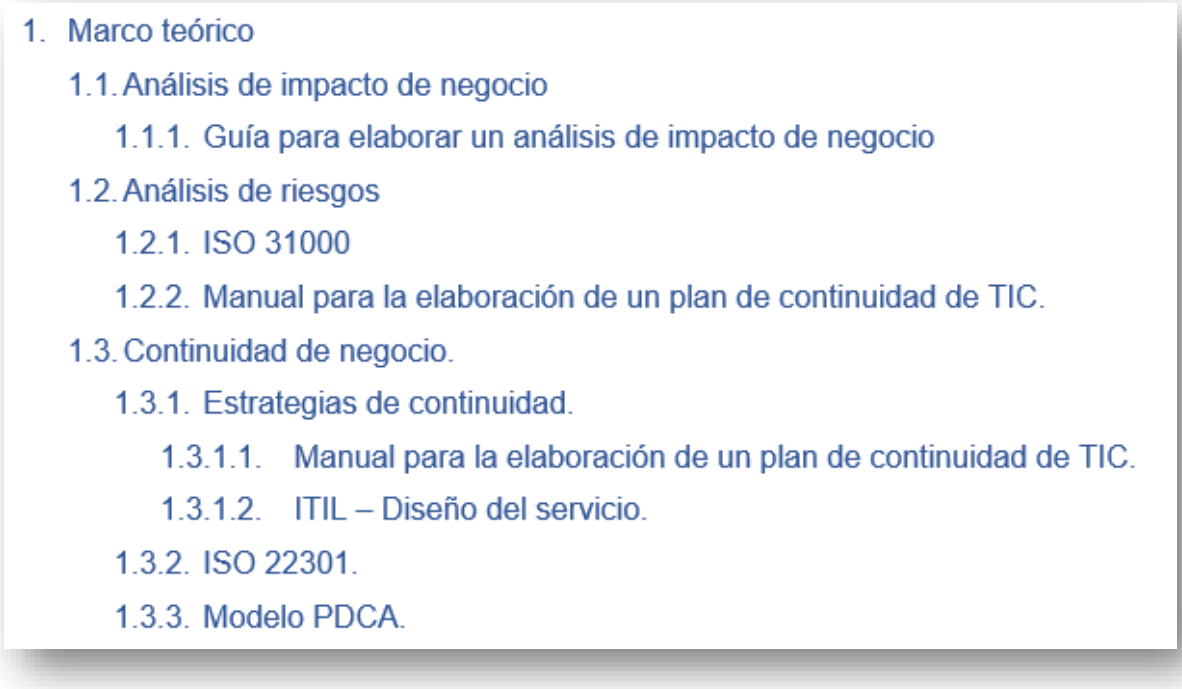


Ilustración 24 - Estructura de Índices.

Fuente: Elaboración propia.

4.2. Etapa II: Hacer

Dentro de la segunda etapa de la metodología PDCA, se desarrolla una serie de actividades principales que permiten recopilar y analizar información proveniente de los colaboradores de las áreas de negocio de la organización, información clave para el desarrollo del plan de continuidad de TI (Véase Ilustración 25).

Ilustración 25 - Etapa hacer – Actividades
Fuente: Elaboración propia.

4.2.1. Análisis de impacto de negocio.

Para el desarrollo de la primera actividad que comprende esta etapa, se emplean cuatro instrumentos que permiten alcanzar los resultados esperados dentro de cada subactividad que la comprenden.

Inicialmente, se realiza una revisión documental con el fin de identificar todos los procesos de negocio que realiza las áreas operativas de JASEC. Dicha información sirve como insumo para la elaboración de los demás instrumentos utilizados.

Continuando con la investigación, se crea y aplica dos cuestionarios a cada uno de los jefes de las áreas operativas de JASEC; el primer cuestionario tiene como objetivo identificar los procesos críticos de negocio de cada correspondiente área; el segundo cuestionario tiene tres propósitos principales, identificar los sistemas informáticos críticos que soportan las operaciones de cada área de negocio, evaluar el impacto que generaría una posible interrupción de dichos sistemas y los tiempos máximos que cada área podría operar sin impactar el negocio.

Por último, se diseña un cuadro de relaciones que permite mapear los sistemas informáticos con el *hardware* que lo soporta y con esto, identificar los activos críticos del área de TI.

Los resultados obtenidos con la aplicación de dichas herramientas, se detalla en cada una de las subactividades que comprende el BIA.

4.2.1.1. Identificación de funciones y procesos.

Con respecto a esta actividad, se realiza una identificación de procesos y procedimientos de las áreas operativas de JASEC, como resultado de la revisión documental realizada, se identificaron los procesos y procedimientos que comprenden cada área operativa de la organización.

A modo de resumen, se detalla la cantidad de procesos de negocio existentes con sus respectivas actividades por área operativa (Véase Tabla 23).

Tabla 23 - Detalle de identificación de funciones y procesos de negocio.

Procesos de negocio.		
Área	**Cantidad de procesos**	**Cantidad de procedimientos.**
Distribución.	20	305
Servicios administrativos.	43	90
Nuevos desarrollos.	3	9
Operación comercial	11	45
Producción.	2	18
Facturación	4	10
Secretaría	4	12

Fuente: Elaboración propia.

4.2.1.2. Identificación de procesos críticos.

Los procesos críticos con sus respectivas actividades identificadas por medio del cuestionario (Véase Apéndice 9.4) aplicado a los jefes de las áreas operativas de JASEC son los siguientes (Véase Tabla 24).

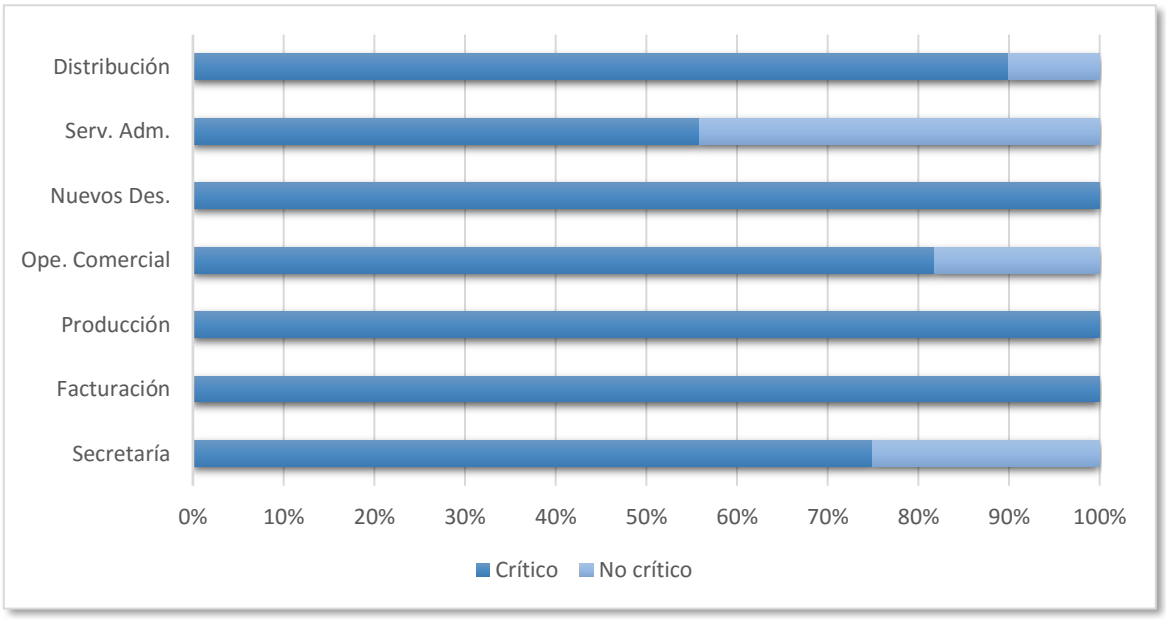
Tabla 24 - Detalle de identificación proceso crítico.

Procesos críticos.		
Área	**Cantidad de procesos críticos.**	**Cantidad de procedimientos críticos.**
Distribución.	18	84
Servicios administrativos.	24	34
Nuevos desarrollos.	3	6
Operación comercial	9	32
Producción.	2	13
Facturación	4	4
Secretaría	3	4

Fuente: Elaboración propia

Analizando los datos obtenidos, se determina que el porcentaje de procesos críticos identificados alcanza el 100% de la totalidad en tres áreas operativas y, en tres de las cuatro áreas operativas faltantes, el porcentaje de procesos críticos se encuentra desde el 75% hasta un 90% (Véase Gráfico 1).

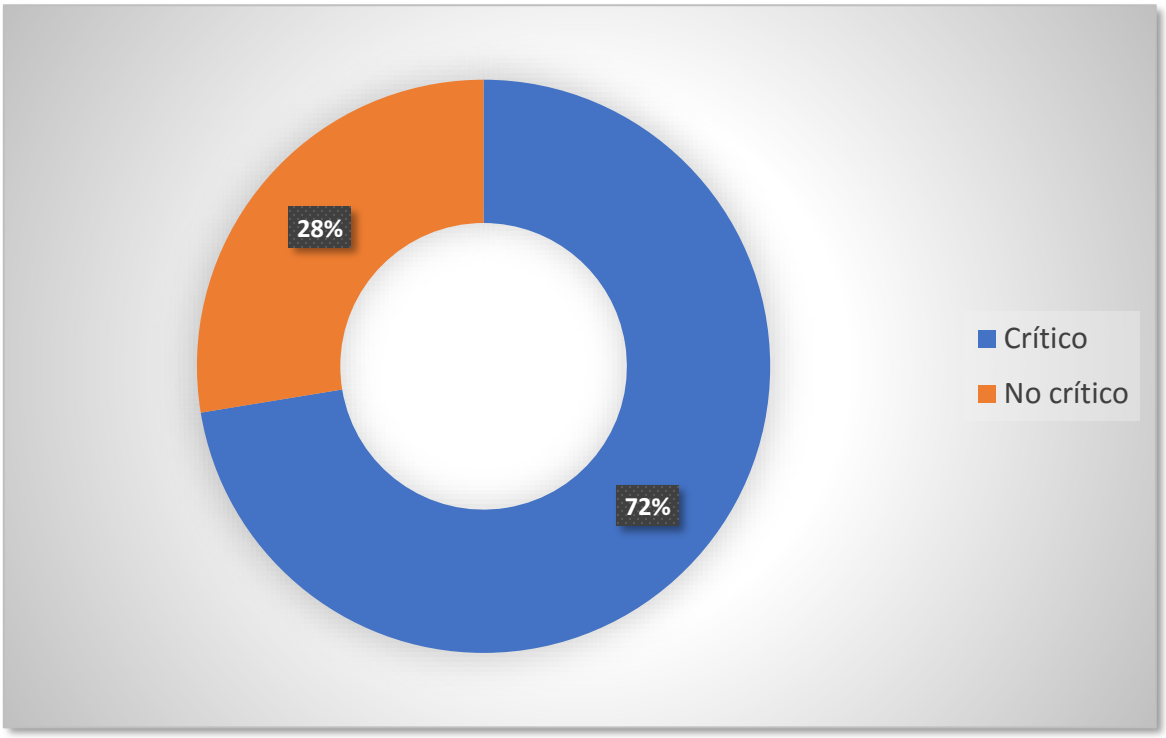
Gráfico 1 - Porcentaje de procesos críticos de negocio.



Fuente: Elaboración propia.

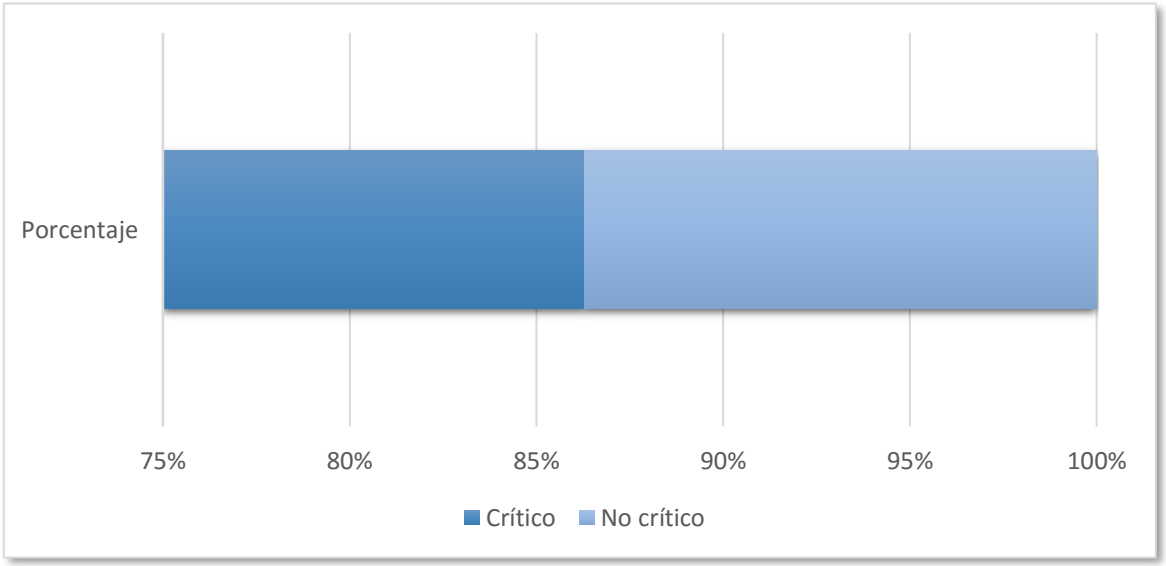
En cuanto al nivel cuantitativo, la cantidad de procesos críticos alcanza un 72% del total de procesos existentes dentro de la organización (Véase Gráfico 2); en cambio, el nivel porcentual, tomando como referencia el Gráfico 1 y, considerando que un factor primordial para determinar la criticidad de un proceso es su dependencia de TIC para su correcta gestión, a nivel porcentual se identifica que las TIC tienen una influencia en el 86% de las operaciones de la organización (Véase Gráfico 3).

Gráfico 2 - Criticidad de los procesos.



Fuente: Elaboración propia.

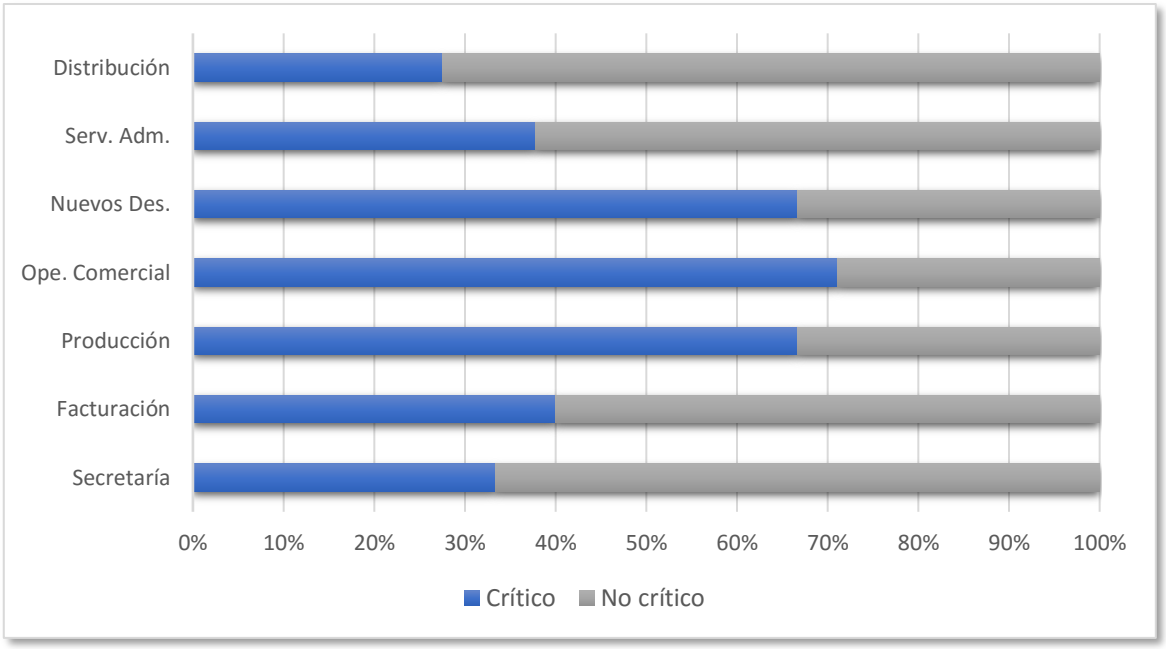
Gráfico 3 - Influencia de los procesos críticos dentro de las operaciones.



Fuente: Elaboración propia.

Además, el porcentaje de actividades críticas identificadas no sobrepasa el 40% en cuatro de las áreas operativas, en cambio en las restantes tres, los procesos críticos alcanzan un nivel superior al 75% (Véase Gráfico 4).

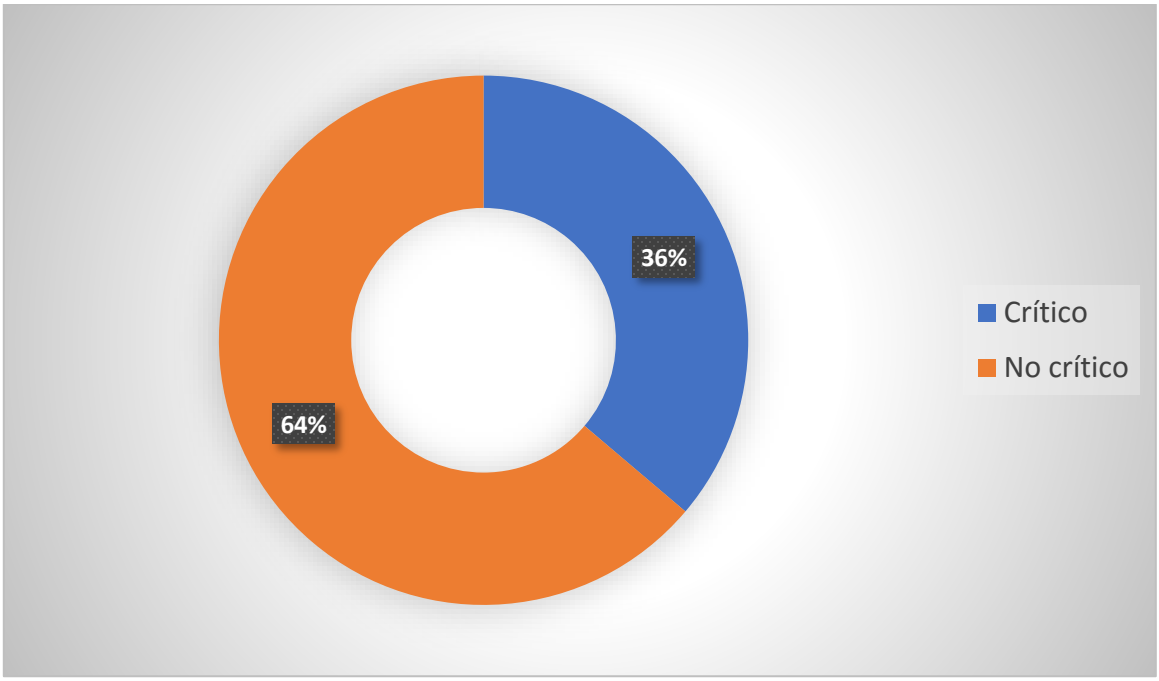
Gráfico 4 - Porcentaje de actividades críticas - Individual.



Fuente: Elaboración propia.

A nivel global, las actividades críticas representan un 36% de la totalidad de procedimientos que se desarrollan dentro de las áreas operativas de la organización (Véase Gráfico 5).

Gráfico 5 - Porcentaje de actividades críticas - Global.



Fuente: Elaboración propia.

Es importante aclarar que los criterios enunciados a los jefes de las áreas operativas para seleccionar los procesos críticos fueron los siguientes:

- El proceso es clave dentro de las gestiones del área.
- El proceso se realiza de forma automática.
- El proceso mantiene dependencia de los servicios que ofrece el área de TIC.

Es importante aclarar que un criterio considerado para determinar los procesos de negocio fue definido como la dependencia existente de los procesos a desarrollarse por medio de la infraestructura y tecnología que gestiona el área de TIC.

Igualmente, dentro de los procesos de negocio que cada área gestiona, existen otros procesos críticos, pero no son considerados al no existir una dependencia de la infraestructura y tecnología que gestiona el área de TIC.

4.2.1.3. Evaluación de impactos.

Respecto a la evaluación de impactos, como resultado de la aplicación del cuestionario a cada jefe de las áreas operativas de JASEC, se logra evidenciar los siguientes resultados (Véase Tabla 1).

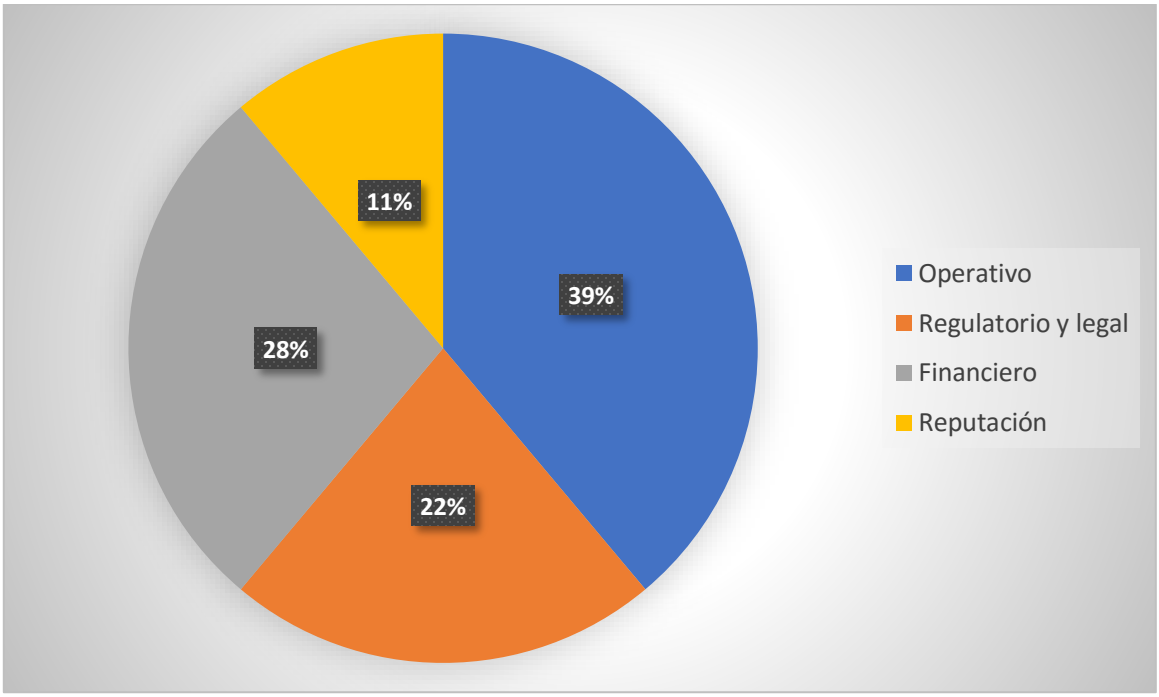
Tabla 25 - Evaluación de impactos.

Impacto	Áreas operativas						
	Servicios Adm.	Operación comercial	Nuevos desarrollos	Distribución	Produccion	Facturación	Secretaría
Operativo	X	X	X	X	X	X	X
Regulatorio y legal	X	X	X	X			
Financiero	X	X	X		X	X	
Reputacion		X				X	

Fuente: Elaboración propia.

En contraste con los resultados obtenidos, no contar con el apoyo que brinda el área de TIC a las demás áreas operativas de JASEC, genera un mayor impacto en el ámbito operativo y financiero.

Gráfico 6 - Porcentaje de alcance de impacto.



Fuente: Elaboración propia.

4.2.1.4. Establecimiento de tiempos de recuperación.

Respecto al establecimiento de tiempos de recuperación, como resultado de la aplicación del cuestionario a los jefes de las áreas operativas de JASEC, se define los tiempos estimados que cada área operativa podría operar sin el apoyo del área de TIC (Véase Tabla 26).

Tabla 26 - Tiempos máximos sin apoyo de TI.

Procesos críticos.	
Área	**Tiempo máximo**
Distribución.	2 horas
Servicios administrativos.	2 horas
Nuevos desarrollos.	4 horas
Operación comercial	1 hora

Procesos críticos.	
Área	**Tiempo máximo**
Producción.	4 horas
Facturación	1 hora
Secretaría	8 horas

Fuente: Elaboración propia.

4.2.1.5. Identificación de recursos.

La identificación de los recursos de TI que necesitan las áreas operativas para el correcto funcionamiento de sus procesos críticos, inicialmente se realiza por medio del cuestionario y permitiendo a los jefes de cada área identificar cuáles sistemas informáticos soportan sus gestiones. (Véase Apéndice 9.5)

Identificados los sistemas informáticos, se relacionan por medio de un cuadro de relación con las áreas operativas de la organización, facilitando mapear cuáles sistemas informáticos son usados por cada área (Véase Tabla 27).

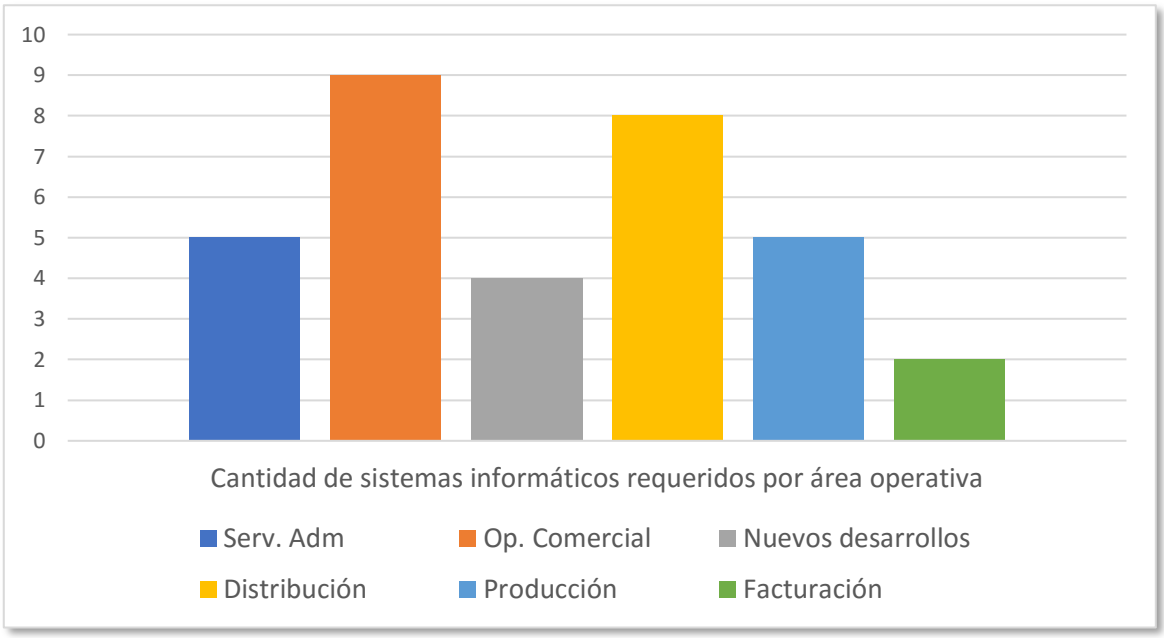
Tabla 27 - Identificación de sistemas informáticos críticos.

		Áreas					
		Servicios Adm.	Operación comercial	Nuevos desarrollos	Distribución	Produccion	Facturación
Soportan procesos críticos	SICURA		X		X		
	Recursos Humanos	X			X	X	
	SLAM		X		X		
	OMS						
	DMS						
	APRIPRO						
	SAC		X				
	SIFAJ	X		X	X	X	
	SIPAC		X				
	SIF						
	SISHISTREC						X
	SIDEGA		X				
	RECAF	X		X	X	X	
	SEVRI						
	GEOMEDIA						
	SGE Suite						
	SISEVA	X		X	X	X	
	SISINFO		X				
	SISRED						
	SCADA						
	SWF						
	SWQ						
	SMI		X				
	SICE		X		X		
	Migrador						
	DELPHOS	X		X	X	X	
	SIJ		X				X
	Office (Excel, Word, ...)						
	HELP DESK						

Fuente: Elaboración propia.

Tomando como referencia los datos del cuadro X, se logra determinar que dentro de Operación comercial y Distribución son las áreas operativas que tienen una mayor dependencia hacia sistemas informáticos.

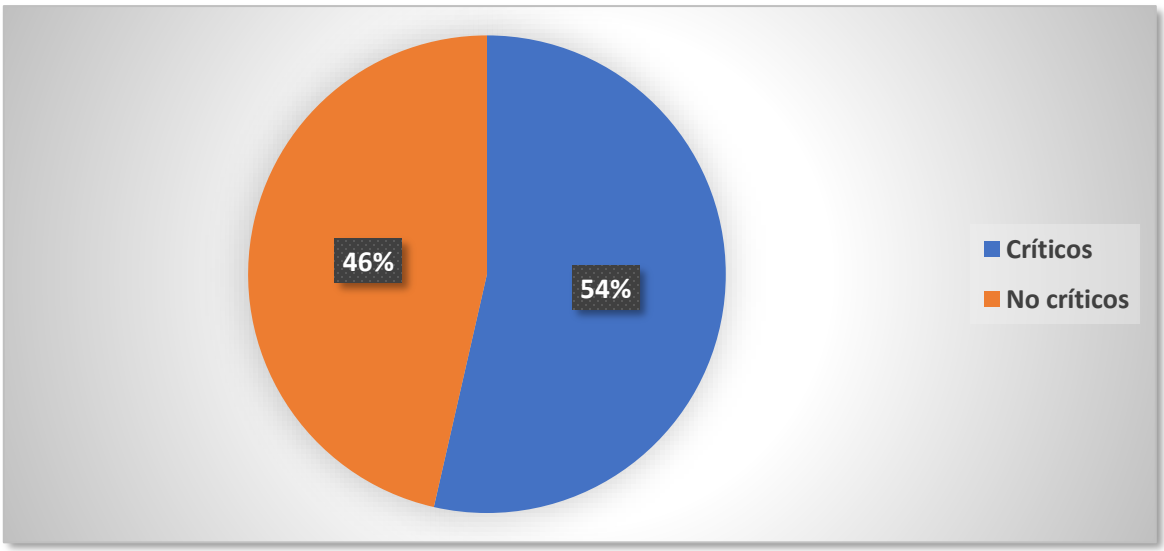
Gráfico 7 - Cantidad de procesos críticos por área operativa.



Fuente: Elaboración propia.

Además, considerando los datos brindados por los jefes de las áreas operativas, el 54% de los sistemas informáticos son requeridos para soportar los procesos críticos de cada área (Véase Gráfico 8).

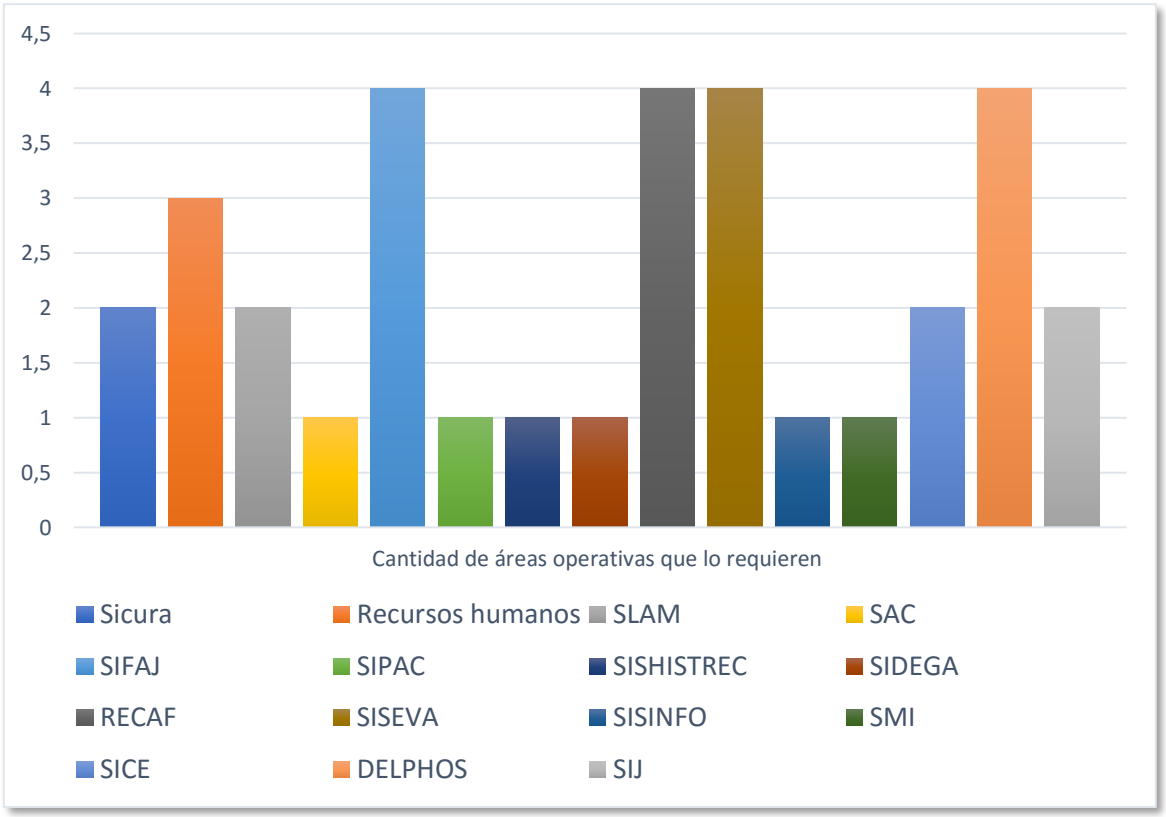
Gráfico 8 - Porcentaje de procesos críticos.



Fuente: Elaboración propia.

Igualmente, se logra determinar que SIFAJ, RECAF, SISEVA y DELPHOS (Véase Gráfico 9) son los sistemas informáticos más requeridos por las áreas operativas de la organización.

Gráfico 9 - Dependencia de sistemas informáticos.



Fuente: Elaboración propia.

Una vez identificados los sistemas informáticos que soportan los procesos críticos de negocio, por medio de un cuadro de relación, se identifica los servidores que soportan cada uno de los sistemas informáticos (Véase Tabla 28).

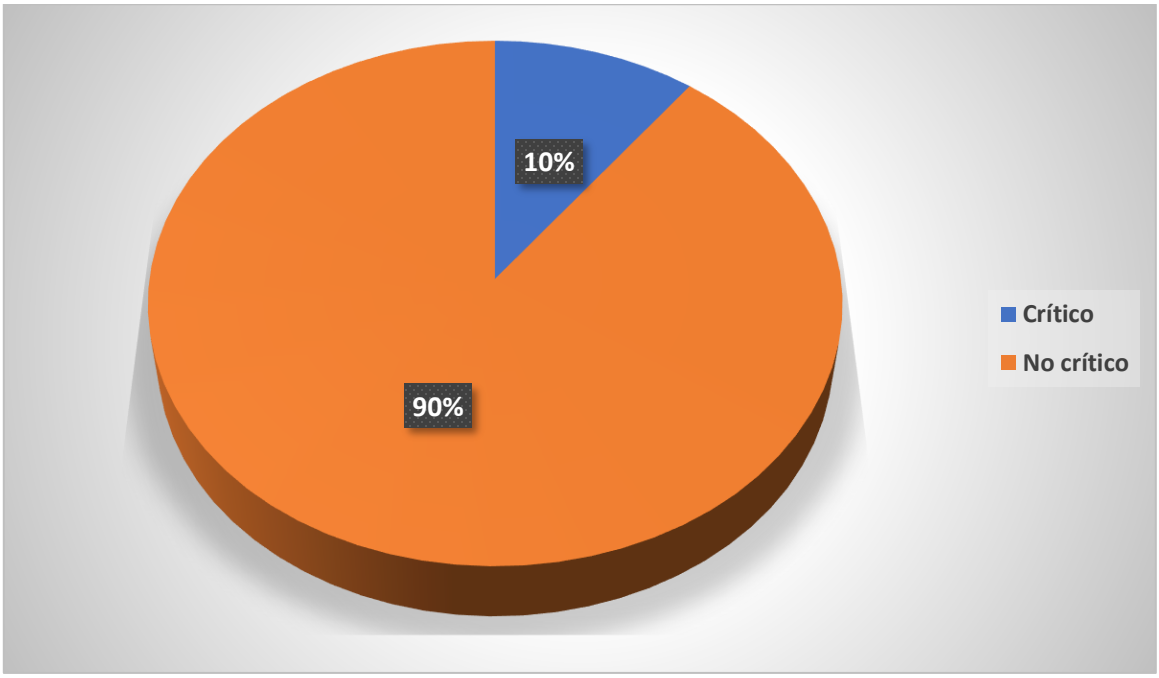
Tabla 28 - Uso de servidores.

		Servidores										
		Virtual					Fisico					
		Aplicativo					Aplicativo	Base datos				
		SRV-APPSORACLE	SIFAJ_SERVER	SRV-SIFAJ	SRV-RH	JASECSIDEGA	Humanos	Financiero	Srvprd11	Srvdes11	Srvsty11	Sun E-250
Sistemas de Información y aplicaciones	SICURA			X	X			X				
	Recursos Humanos						X		X	X		
	SLAM							X				
	SAC							X				
	SIFAJ		X	X					X	X		
	SIPAC					X		X		X		
	SIF					X		X		X		
	SISHISTREC		X					X				
	SIDEGA							X				
	RECAF		X									
	SISEVA		X									
	SISINFO		X						X	X		
	SWF								X	X		
	SWQ		X						X	X		
	SMI			X					X	X		
	SICE								X	X		
	DELPHOS	X										
	SIJ											X

Fuente: Elaboración propia.

Con el mapeo de los activos de TI realizado, se logra conocer con exactitud el nivel de proporción de dependencia que existe a cada uno de los servidores con respecto a los sistemas informáticos que soportan (Véase Gráfico 10).

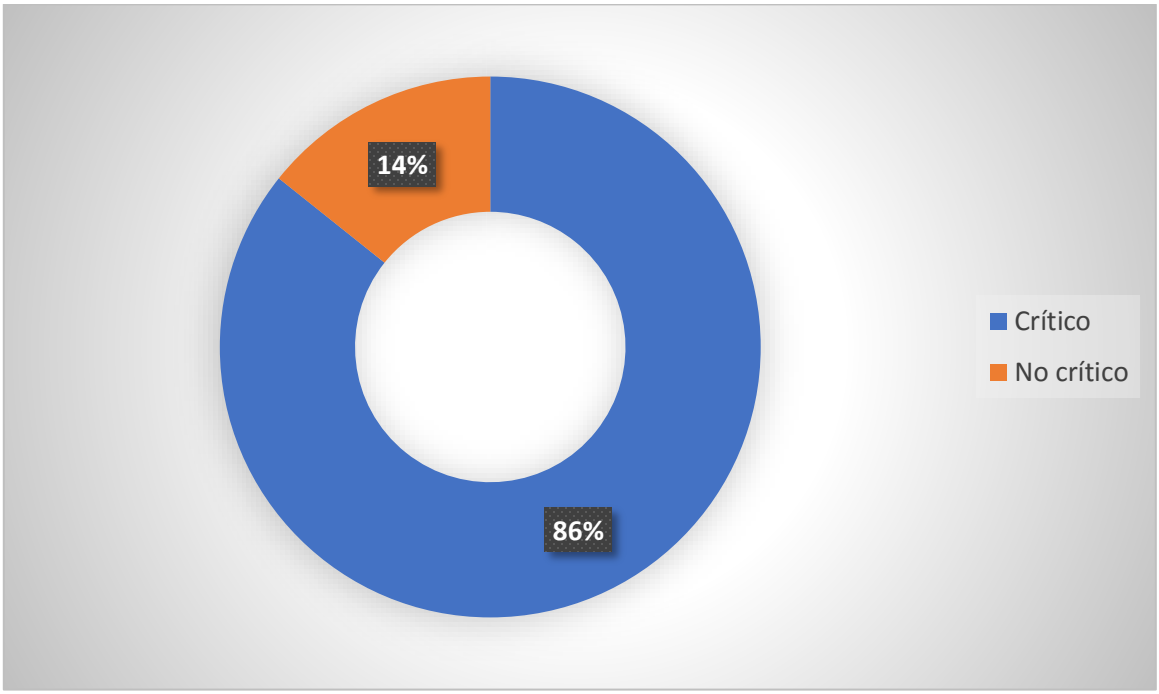
Gráfico 10 - Porcentaje de servidores críticas.



Fuente: Elaboración propia.

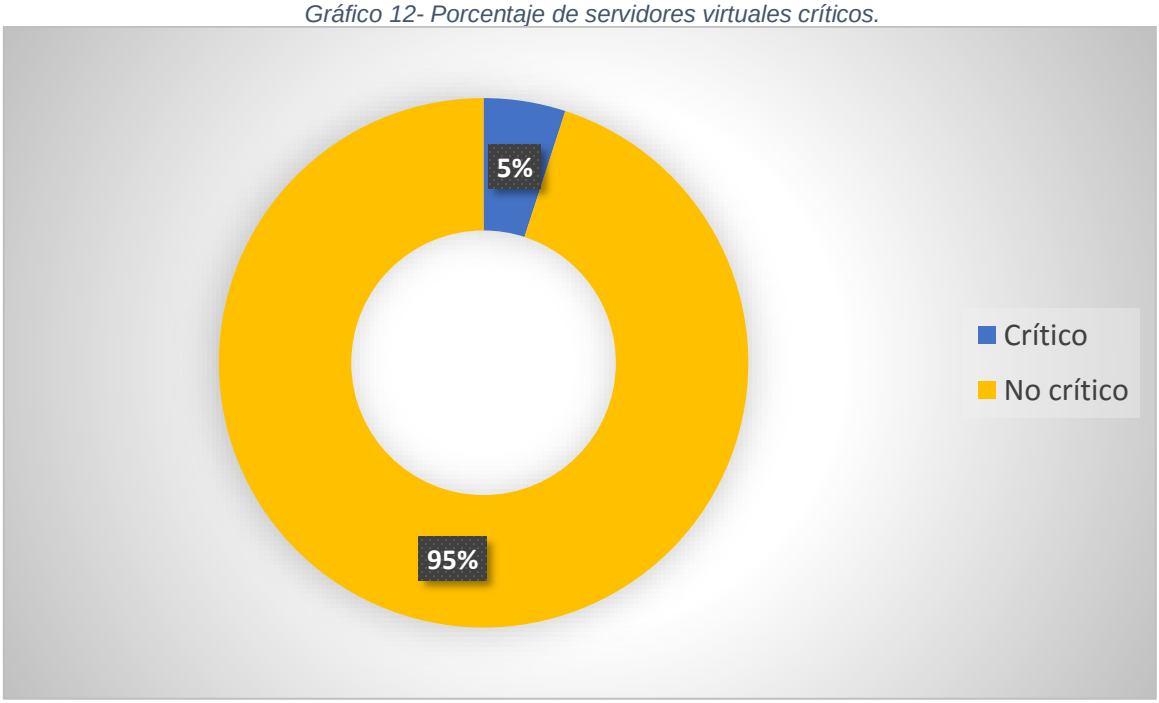
Con respecto a los servidores físicos, los sistemas informáticos críticos se encuentran alojados en un 86% de los servidores existentes (Véase Gráfico 11). En cambio, la dependencia existente hacia los servidores virtuales es notablemente más baja, ya que un cinco por ciento del total, aloja sistemas informáticos críticos (Véase Gráfico 12).

Gráfico 11 – Porcentaje de servidores físicos críticos.



Fuente: Elaboración propia.

Gráfico 12- Porcentaje de servidores virtuales críticos.



Fuente: Elaboración propia.

4.2.2. Análisis de riesgos.

Para el desarrollo de la segunda actividad que comprende esta etapa, se emplea cuatro instrumentos que permiten alcanzar los resultados esperados dentro de cada subactividad que la comprende.

Inicialmente, se realiza un grupo focal con colaboradores del área de TIC que permite discutir las categorías de riesgos con las cuales se pretende trabajar. El objetivo de dicha discusión es validar que las categorías propuestas aplican al contexto de la organización.

Posteriormente, se aplica un cuestionario a los colaboradores del departamento de gestión de sistemas, mantenimiento y desarrollo, y del departamento de gestión de arquitectura y comunicaciones, con el objetivo de verificar cuales medidas mínimas son aplicadas para la reducción de riesgos.

Con el fin de evaluar los niveles de probabilidad de ocurrencia y de impacto que mantienen los riesgos, se aplica un cuestionario que facilita emitir dicho criterio según la experiencia de los colaboradores del área de TIC.

Por último, una vez obtenidos los datos referentes a los niveles de probabilidad de ocurrencia y de impacto que pueden alcanzar los riesgos relacionados a TI, se realiza una matriz de calor que permita identificar los riesgos con mayor nivel de impacto.

Los resultados obtenidos con la aplicación de dichas herramientas, se detallan en cada una de las subactividades que comprende el análisis de riesgos.

4.2.2.1. Establecimiento del contexto.

El contexto donde se desarrolló el análisis de riesgos, se establece que el análisis de riesgos se enfoca en una posible afectación a los activos de TI, específicamente sistemas de información, servidores y equipos de comunicación que gestiona el área de TIC de JASEC.

La decisión de enfocar el análisis de riesgos hacia dichos activos de TI, se basa en los resultados obtenidos dentro del BIA.

4.2.2.2. Valoración de riesgos.

La valoración de riesgos se efectuó desarrollando las tres actividades que la conforman. Los resultados obtenidos en cada una de las actividades, se detallan a continuación.

4.2.2.2.1. Identificación del riesgo.

Tomando como referencia las categorías de riesgos descritas en el marco teórico, se efectuó un grupo focal con el jefe del área y colaboradores del departamento de arquitectura y comunicaciones, y se valida que cada categoría cumpliera según el contexto de JASEC y del área de TIC.

Las categorías de riesgos definidas para dar continuidad a las demás subactividades que comprenden la valoración de riesgos fueron las siguientes (Véase Tabla 29).

Tabla 29 - Categorías de riesgo.

Categoría de riesgo.
Interrupción eléctrica.
Fallos en hardware.
Fallos en software.
Fallos en comunicaciones.
Desastres naturales.
Incendio
Fallos en respaldos.
Virus
Violaciones a la seguridad física.
Intrusión.
Recurso humano.

Fuente: CCSS (2017).

4.2.2.2.2. Análisis del riesgo.

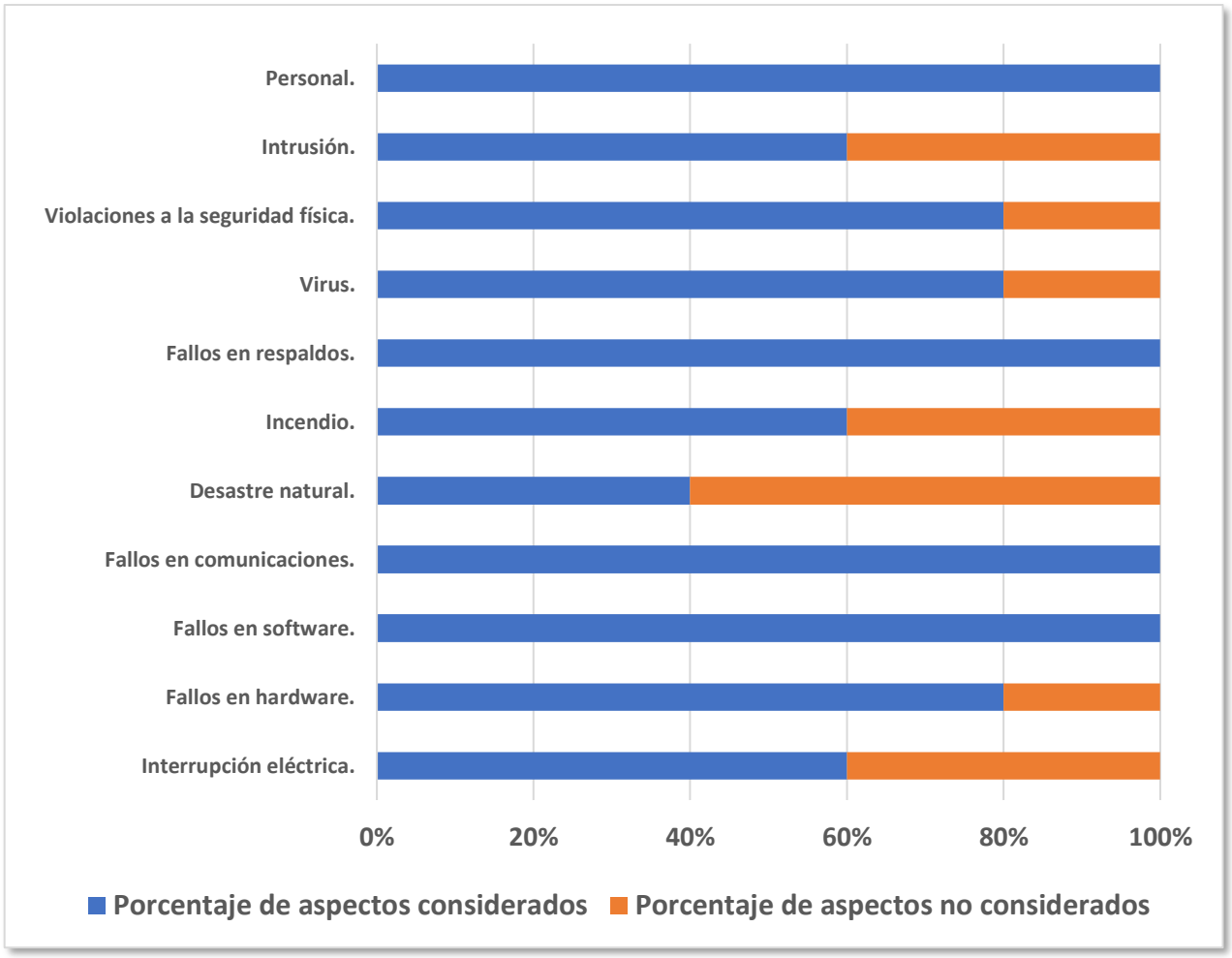
Por medio de un cuestionario aplicado a los colaboradores del departamento de gestión de sistemas, mantenimiento y desarrollo, y del departamento de arquitectura y comunicación, se analiza los aspectos mínimos aplicados dentro de las gestiones realizadas por el área de TIC para mitigar los riesgos de TI.

El cuestionario aplicado toma como referencia los aspectos mínimos a considerar para la mitigación de riesgos de TI recomendado dentro del manual para la elaboración de un plan de continuidad de TI (CCSS, 2007) en cada una de las categorías de riesgos definidas en la subactividad anterior.

Aplicar el instrumento, tiene también como objetivo ampliar el conocimiento sobre el nivel de compromiso existente alrededor de atender y mitigar los efectos que puede generar la materialización de un riesgo.

Según los resultados obtenidos del cuestionario aplicado (Véase Apéndice 9.6), el porcentaje de aspectos que son considerados para la mitigación de los riesgos por cada categoría de riesgo son los siguientes (Véase Gráfico 13).

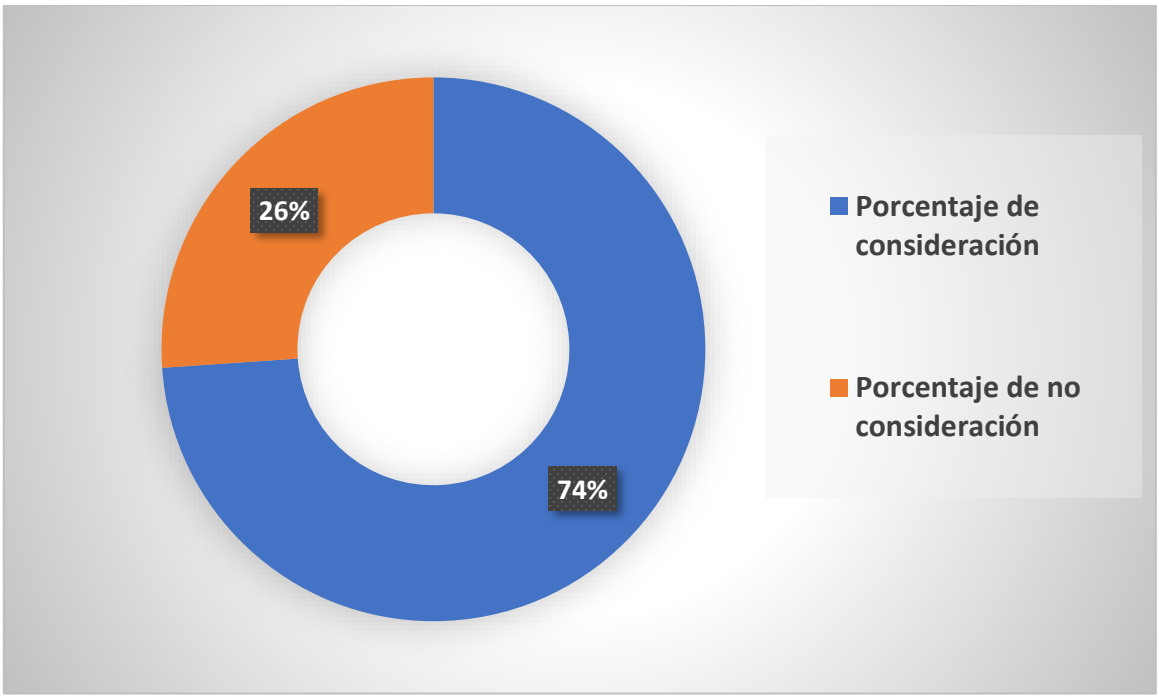
Gráfico 13 - Porcentaje de aspectos mitigadores de riesgos considerados.



Fuente: Elaboración propia.

Asimismo, se logra determinar que, dentro del área de TIC existe anuencia a mitigar la materialización de los riesgos relacionados a TI, dado que el 74% de los aspectos recomendados son aplicados dentro de las gestiones del área (Véase Gráfico 14).

Gráfico 14 - Porcentaje general de aspectos mitigadores de riesgos.



Fuente: Elaboración propia.

4.2.2.2.3. Evaluación del riesgo.

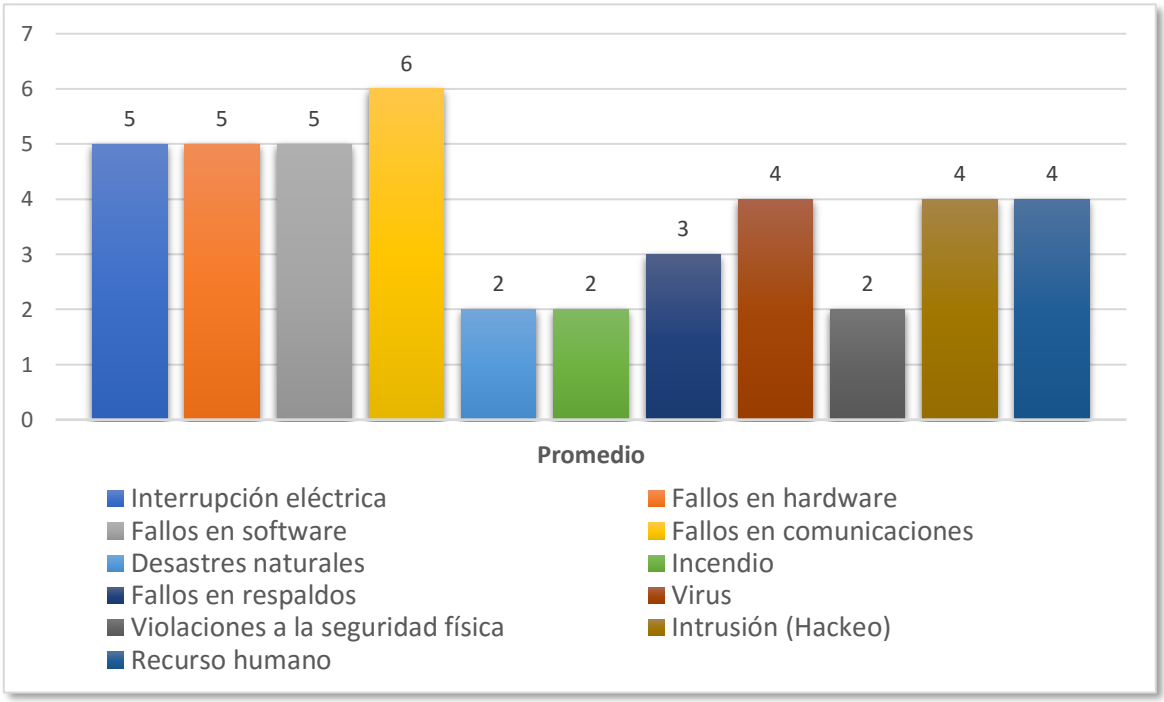
La evaluación de los riesgos relacionados a TI se realiza por medio de un cuestionario elaborado en *Google Forms* y enviado a todos los colaboradores del área de TIC de la organización, quienes basados en la experiencia que cuentan, brindaron una valoración objetiva (Véase Apéndice 9.7).

En el cuestionario se evalúa el nivel de probabilidad de ocurrencia y el nivel de impacto que alcanza cada categoría de riesgo, tomando como referencia una escala (Véase Tabla 19 y Tabla 20) que facilita realizar dicha evaluación.

El cuestionario enviado a 12 colaboradores y contestado por ocho de ellos, considerando las respuestas (Véase Apéndice 9.8) brindadas en cada categoría de riesgo, se aplica un promedio que facilita hacer el cálculo del nivel del riesgo.

Con respecto al nivel de probabilidad de ocurrencia, según las valoraciones realizadas por los colaboradores del área de TIC, se logra promediar los valores obtenidos por categoría de riesgo (Véase Gráfico 15).

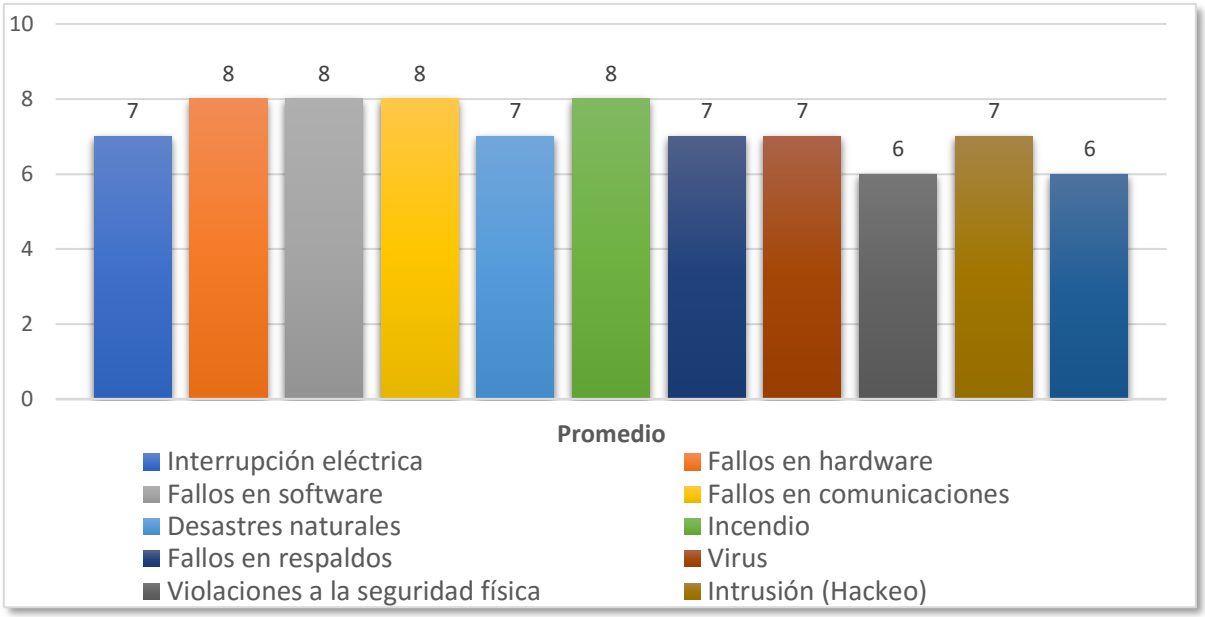
Gráfico 15 - Niveles de probabilidad de ocurrencia.



Fuente: Elaboración propia.

En el caso del nivel de impacto, considerando las valoraciones emitidas por los colaboradores del área de TIC, se promedia los valores obtenidos por categoría de riesgo (Véase Gráfico 16).

Gráfico 16 - Niveles de impacto.



Fuente: Elaboración propia.

Considerando los valores presentados anteriormente, se realiza un cuadro donde se multiplica el promedio del nivel de probabilidad de ocurrencia con el promedio del nivel de impacto (Véase Tabla 30), con el fin de determinar el nivel de riesgo que alcanza cada categoría de riesgo dentro del área de TIC.

Tabla 30 - Matriz probabilidad e impacto.

	Categoría de riesgo	Probabilidad	Impacto	Nivel
1	Interrupción eléctrica.	5	7	35
2	Fallos en Hardware.	5	8	40
3	Fallos en Software.	5	8	40
4	Fallos en comunicaciones	6	8	48
5	Desastres naturales.	2	7	14
6	Incendio.	2	8	16
7	Fallos en respaldos.	3	7	21
8	Virus.	4	7	28
9	Violaciones a la seguridad física.	2	6	12
10	Intrusión.	4	7	28
11	Recurso humano.	4	6	24

Fuente: Elaboración propia.

Para una mejor representación gráfica, se coloca cada nivel de riesgo alcanzado por cada categoría dentro de una matriz de calor (Véase Tabla 31) y con esto, determinar el grado de criticidad, tomando como referencia los intervalos establecidos en el marco metodológico (Véase Tabla 22).

Tabla 31 - Matriz de calor.

Probabilidad	Impacto				
				4	
				2,3	
				6,7,11	1,11
				5,9	

Fuente: Elaboración propia.

Se logra evidenciar por medio del cuestionario aplicado a los colaboradores del área de TI, que los riesgos relacionados con fallos de *hardware*, fallos de *software y* fallos en comunicaciones son los que alcanzan un mayor nivel de riesgo. Tomando como referencia esta evidencia, las estrategias de continuidad se enfocan en contrarrestar estas categorías de riesgos, dado el nivel de riesgo que alcanzan.

4.2.3. Estrategias de continuidad.

Para el desarrollo de la última actividad que comprende esta etapa, se emplea un instrumento que permite alcanzar los resultados esperados dentro de cada subactividad que la comprende.

Desarrollando grupos focales, se logra conseguir los objetivos que pertenecen a cada una de las subactividades. Dentro de lo alcanzado se encuentra lo siguiente:

- Creación de estrategias proactivas.
- Creación de estrategias reactivas.
- Procedimiento de activación del plan.
- Organización encargada del plan de continuidad.
- Consideraciones a tomar en cuenta para cerrar un plan de continuidad.

4.2.3.1. Establecer los recursos.

Una correcta gestión de un plan de continuidad de TI, necesita contar con personal que sea responsable de ejecutar diferentes estrategias según la necesidad existente al momento de su activación.

Como parte del esfuerzo realizado por medio de un grupo focal con los colaboradores del área de TIC, se define los roles y sus respectivas responsabilidades dentro de la gestión del plan de continuidad; además, se asigna

los colaboradores, tomando como referencia las responsabilidades que mantiene dentro de su departamento y las responsabilidades asignadas como parte del rol a cubrir dentro del plan de continuidad.

4.2.3.2. Establecimiento de procedimientos.

Basado en la criticidad de los activos del área de TIC, los procedimientos de continuidad fueron creados de acuerdo con el impacto que genera una interrupción de los activos críticos dentro de las operaciones de negocio de JASEC.

Para el desarrollo de los procedimientos se realiza varios grupos focales, donde en conjunto con los colaboradores del área de TIC se establece los alcances y pasos a seguir (Véase Tabla 32).

Tabla 32 - Descripción de grupos focales.

Grupo focal #1	
Participantes	**Objetivo**
Colaboradores del departamento de gestión de la arquitectura y comunicaciones.	Definición de estrategias proactivas.
Grupo focal #2	
Participantes	**Objetivo**
Colaboradores del departamento de gestión, arquitectura y comunicación y jefe del departamento de sistemas, mantenimiento y desarrollo.	Definición de estrategias reactivos.
Grupo focal #3	
Participantes	**Objetivo**
Colaboradores del departamento de gestión de la arquitectura y comunicaciones.	Proceso de activación e inspecciones de cierre del plan de continuidad.

Fuente: Elaboración propia.

5. Capítulo V: Propuesta solución.

A continuación se presenta la propuesta solución generada a partir de la investigación realizada en este trabajo final de graduación.

5.1. Introducción del plan de continuidad de TI.

Un plan de continuidad de TI para el área de tecnologías de información y comunicación consiste en un plan de acción donde se especifican las acciones a seguir para recuperar las funciones operativas de forma parcial o total y, restaurarlas a su ambiente de trabajo normal en un tiempo determinado, ante una eventualidad o interrupción no deseada que impacte aquellos procesos críticos. Este plan lleva consigo un análisis de impacto a negocio y un análisis de riesgos que respalda las estrategias tanto proactivas como reactivas, planteadas dentro del plan de continuidad de TI.

Las estrategias planteadas permiten a la institución identificar cuáles opciones tiene para brindar continuidad a las operaciones que son altamente dependientes de la tecnología de información; además, dichas estrategias están enfocadas en mejorar la capacidad de la empresa para regresar a su estado estable, o a la condición anterior a la ocurrencia de un incidente que afectó sus operaciones normales.

5.2. Alcance del plan de continuidad de TI

El alcance de este plan de continuidad de TI limita el ámbito de acción con estrategias que responden a los activos críticos y los riesgos de TI identificados en el BIA y el análisis de riesgos respectivamente.

5.3. Organización.

Los colaboradores que compone el equipo responsable de gestionar y ejecutar el plan de continuidad de TI dentro de las operaciones propias del área de TIC de la organización. Dicho equipo se encuentra debidamente organizado, permitiendo la asignación de responsabilidades (Véase Ilustración 26).

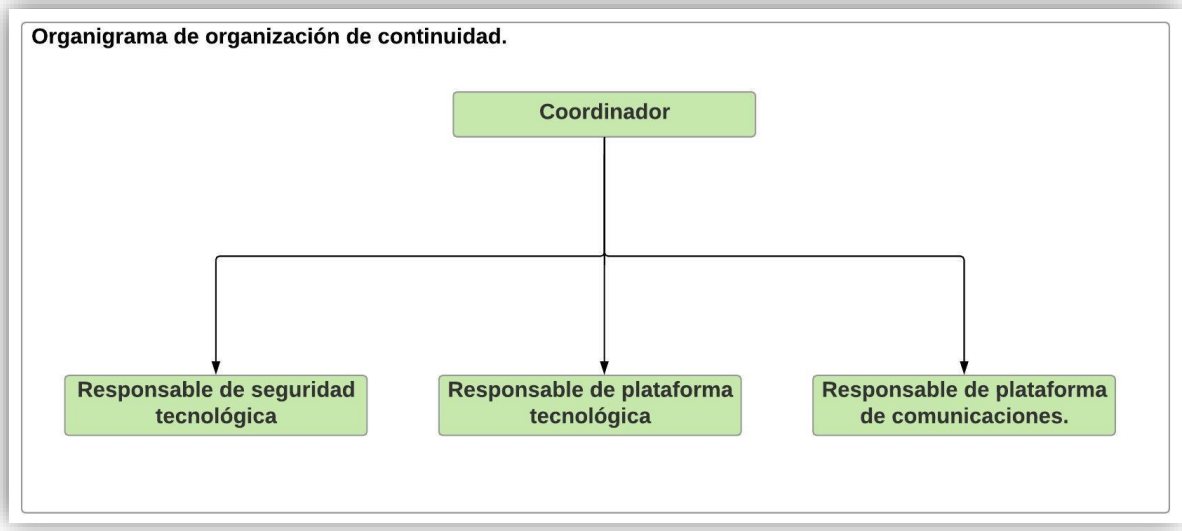


Ilustración 26 - Organigrama de organización de continuidad.

Fuente: Elaboración propia

5.3.1. Coordinador del plan de continuidad de TI.

Es la persona responsable de la correcta ejecución del plan de continuidad de TI, debe confirmar la orden de inicio en la ejecución del plan de continuidad, coordinar

las actividades de contingencia con los diferentes integrantes del equipo responsable del plan de continuidad de TI, seguir el estado de las estrategias aplicadas, y confirmar el cierre del plan y retorno a la normalidad.

Entre sus responsabilidades se encuentran:

- Ejecutar el plan de continuidad, previa confirmación de activación.
- Reunir al equipo responsable del plan en el punto de encuentro, en caso de ser necesario.
- Realizar un análisis conjunto de la situación.
- Coordinar los lugares y personas donde se ejecutará el plan.
- Mantener contacto con todas las personas responsables internas y externas involucradas.
- Supervisar la correcta implementación de las actividades requeridas del plan de continuidad de TI.
- Supervisar con el personal de seguridad que las personas acaten las indicaciones de emergencia que se les indique y atender a los usuarios internos y externos afectados.
- Hacer seguimiento del estado de la operación de los servicios y actividades en contingencia.
- Supervisar el retorno a la normalidad de la operación de las áreas afectadas, documentar acciones y lecciones aprendidas, y confirmar el cierre del plan.

5.3.2. Responsable de seguridad tecnológica

Es la persona responsable del cumplimiento normativo y operativo de los procesos, sistemas y activos tecnológicos relacionados con la seguridad de la información.

Entre sus responsabilidades está:

- Realizar una inspección conjunta de los activos de tecnología que soportan la seguridad de la información.
- Coordinar el uso y restauración de respaldos de información.
- Hacer seguimiento del uso y control de acceso de la plataforma tecnológica.
- Coordinar la restauración de perfiles de usuario, permisos de uso y gestión de información.
- Hacer seguimiento de la configuración de activos que se requiera instalar.
- Sí aplica preparar perfiles temporales para el personal que requiera trabajar.
- Supervisar el traslado de activos tecnológicos, físicos y de información a sitios alternos, y certificar el retorno de dichos activos.
- Certificar las condiciones de seguridad, disponibilidad, confidencialidad e integridad de la información y la plataforma tecnológica antes del cierre del plan de continuidad de TI.

5.3.3. Responsable de la plataforma tecnológica.

Es la persona responsable de validar la integridad y disponibilidad de los activos que componen la plataforma tecnológica, estos son: servidores físicos y virtuales, unidades de almacenamiento, repositorios, servicios de tecnología e información digital y unidades de creación de respaldo.

Entre sus responsabilidades está:

- Inspeccionar los activos que componen la plataforma tecnológica, principalmente centro de datos y sitios alternos de procesamiento de información.
- Evaluar la integridad de los activos de tecnología.
- Coordinar las actividades relacionadas con la recuperación de servidores físicos, virtuales y repositorios.

- Coordinar las actividades relacionadas con la recuperación funcional de los servicios de tecnología de la institución.
- Coordinar la configuración de activos de procesamiento de información que se requieran como activos para contingencias.
- Certificar el funcionamiento correcto de los activos de tecnología previo al cierre del plan de continuidad.

5.3.4. Responsable de la plataforma de comunicaciones.

Es la persona responsable de validar la integridad y disponibilidad de los activos que componen la plataforma de comunicaciones, estos son: switches, routers, central y unidades de telefonía, enlaces de comunicación, cableado de datos y voz, VPN.

Entre sus responsabilidades está:

- Inspeccionar los activos que componen la plataforma de comunicaciones, principalmente centro de datos y sitios alternos de procesamiento de información.
- Evaluar la integridad de los activos de comunicación.
- Coordinar las actividades relacionadas con la recuperación de *routers, switches*, enlaces y VPN.
- Coordinar las actividades de revisión y reemplazo de cableado estructural.
- Coordinar la configuración de activos de comunicación que se requieran como activos para contingencias.
- Certificar el funcionamiento correcto de los activos de comunicación previo al cierre del plan de continuidad.

Igualmente, existen otros colaboradores claves dentro de la gestión del plan de continuidad de TI que deben ser considerados, dependiendo de la estrategia de continuidad a ejecutar.

5.3.5. Responsable del área funcional.

Es la persona encargada de coordinar al personal y las actividades en cada área funcional de la institución. Entra en función cuando existe alguna afectación dentro de su área.

Entre sus responsabilidades está:

- Actualizar la información relacionada con el flujo de procesos de su área funcional.
- Actualizar el directorio del personal a su cargo.
- Actualizar el inventario de servicios, equipo tecnológico e información que requieren para sus funciones críticas.
- Coordinar el programa de capacitación y entendimiento de temas relacionados con los planes de continuidad de TI.
- Efectuar evaluaciones y análisis de riesgos para detectar incumplimientos normativos.
- Participar en las investigaciones de incidentes.
- Coordinar las actividades que estén a su cargo y de su personal, relacionadas con la ejecución del plan de continuidad de TI.
- Atender al personal bajo su responsabilidad ante cualquier eventualidad.
- Mantener la comunicación con el personal involucrado en la ejecución técnica y operativa del plan de continuidad de TI, y brindar apoyo de ser necesario.
- Coordinar pruebas y certificar las actividades del plan de continuidad TI relacionadas con su área funcional.

5.3.6. Responsable de seguridad en instalaciones.

Es la persona líder responsable de la integridad de las instalaciones físicas donde se realiza las actividades de misión crítica, administrativas y de soporte de la institución. Para fines del plan de continuidad de TI, brinda apoyo en caso de requerir inspecciones y validaciones de espacios físicos.

Entre sus responsabilidades está:

- Inspeccionar la integridad física de las instalaciones.
- Notificar si se requiere de activar sitios alternos de trabajo.
- Hacer seguimiento del estado de la operación de los servicios y actividades en contingencia.
- Supervisar la integridad de los servicios básicos que se requieren para realizar las actividades de la institución.
- Coordinar los trabajos necesarios para recuperar los espacios de trabajo para la operación normal de las diferentes áreas.
- Certificar las instalaciones y espacios de trabajo para permitir el retorno del personal, supervisar el retorno a la normalidad de la operación de las áreas afectadas, documentar acciones y lecciones aprendidas, y confirmar el cierre del plan.

5.3.7. Directorio del equipo responsable.

En función de las responsabilidades a cada rol, se documenta el directorio del personal que conforma el equipo responsable del plan de continuidad de TI (Véase Tabla 33).

Tabla 33 - Directorio del equipo responsable.

Rol	Nombre	Teléfono	Extensión	Área.
Coordinador del Plan de Continuidad:	-	-	-	Área de TIC.
Responsable de seguridad en instalaciones físicas:	-	-	-	Salud ocupacional.
Responsable de seguridad tecnológica:	-	-	-	Área de TIC
Responsable de la plataforma tecnológica:	-	-	-	Área de TIC
Responsable de la plataforma de comunicaciones:	-	-	-	Área de TIC.
Responsable del departamento funcional:				
Proyectos Sustantivos	-	-	-	Área de TIC.
Proyectos de apoyo	-	-	-	Área de TIC.

Fuente: Elaboración propia

5.4. Ejecución y conclusión del plan de continuidad de TI.

Dentro de la gestión del plan de continuidad de TI, un segmento clave a definir son los responsables tanto de iniciar el plan de continuidad de TI como de cerrarlo.

5.4.1. Responsables de iniciar el plan de continuidad de TI.

El plan de continuidad debe iniciarse cada vez que exista una eventualidad que impacte en la operación y el ambiente normal para realizar las operaciones de JASEC.

El plan de Continuidad puede ser iniciado por:

- La Junta Directiva
- Gerencia
- El responsable del área de Tecnologías de Información y comunicación.
- El responsable del área funcional impactada
- El responsable del servicio o los activos de tecnología que se vean impactados o interrumpidos ante un evento.

5.4.2. Responsables de cerrar el plan de continuidad de TI.

El plan de continuidad de TI puede ser cerrado una vez que se cumpla con las actividades de retorno a la operación normal (ver sección 5).

El plan de Continuidad debe ser cerrado en conjunto por:

- El responsable de la UEN de Tecnologías de Información
- El responsable del área funcional impactada
- El coordinador del Plan de Continuidad

5.5. Activación de plan de continuidad de TI.

La activación del plan de continuidad de TI conlleva una serie de actividades secuenciales que son necesarias para aplicar las estrategias necesarias según el incidente presentado.

5.5.1. Notificación inicial.

Al momento de ocurrir un incidente, el colaborador que lo identifica debe notificar al personal señalado en la sección responsables de iniciar el plan de continuidad de TI (Véase Plantilla de notificación inicial.).

En caso de ser varias personas quienes detecten un incidente, la persona con el nivel jerárquico más alto debe notificar a los responsables de iniciar el plan.

5.5.2. Evaluación de incidente.

Una vez que se reciba la notificación inicial, y que el responsable notifique la autorización de la aplicación del plan de continuidad, el coordinador del plan notifica y reúne en el punto de encuentro a todo el personal requerido para su ejecución en caso de ser necesario.

El equipo del plan de continuidad revisa las observaciones hechas por el personal que detecta el incidente y, realiza una inspección del incidente que se materializa y el impacto a las operaciones de la institución.

5.5.3. Activación del plan de continuidad.

Una vez que se identifica plenamente el incidente y sus consecuencias en la operación, se confirma con el responsable de iniciar el plan que se ejecuta, las actividades necesarias para mantener las operaciones críticas y recuperar el ambiente normal de la institución.

Cuando se defina a los integrantes del equipo necesarios en la resolución del incidente y la aplicación de la estrategia, así como las tareas a realizar por cada

miembro, se procede a la ejecución de estrategias reactivas para la continuidad de TI en función de los procesos operativos que hayan sido impactados y de su criticidad para la institución.

5.6. Ejecución de estrategias reactivas para la continuidad de TI.

Una vez gestionada la ejecución de estrategias reactivas para la continuidad de TI con el objetivo de restablecer la operación de procesos críticos de negocio, es necesario primeramente considerar lo siguiente:

- Se verifica la seguridad e integridad del personal de la JASEC y personas externas, además de que los procesos de evacuación y acciones ante emergencias se hayan cumplido y la situación esté controlada, en caso de ser necesario.
- El coordinador del plan de continuidad crea una bitácora de ejecución del plan para dar seguimiento a las actividades a realizar del plan (Véase 5.9.4.3).
- El Coordinador del Plan de Continuidad notifica al responsable de las áreas funcionales impactadas por el incidente sobre la ejecución del plan y los requerimientos necesarios por parte del personal para la correcta recuperación de funciones.
- El responsable respectivo de las áreas funcionales impactadas debe comunicar y coordinar las actividades pertinentes con el personal bajo su cargo, además de dar seguimiento a la ejecución del plan de continuidad.

Una vez considerado lo anterior, se procede a aplicar las estrategias correspondientes según el activo de TI impactado (Véase Plantillas para estrategias reactivas.)

5.7. Estrategias de continuidad.

Dentro del plan de continuidad se detalla un conjunto de estrategias dirigidas a anticipar y/o responder a incidentes que afecten los procesos críticos de las áreas operativas de la organización.

5.7.1. Estrategias proactivas.

Las estrategias planteadas buscan impedir la materialización de un riesgo y/o reducir las consecuencias de una interrupción por medio de inspecciones preventivas aplicadas por colaboradores de la organización (Véase Tabla 34).

Tabla 34 - Estrategias proactivas

	Código plantilla	**Responsable**	**Plantilla**
Inspecciones diarias generales.	PO-01	• Responsable de la seguridad en instalaciones.	Véase Ilustración 27.
Inspecciones diarias específicas.	PO-02	• Responsable de plataforma tecnológica.	Véase Ilustración 28.
Inspecciones semanales generales.	PO-03	• Responsable de la seguridad en instalaciones.	Véase Ilustración 29.
Inspecciones semanales específicas.	PO-04	• Responsable de plataforma tecnológica.	Véase Ilustración 30.

	Código plantilla	Responsable	Plantilla
Inspecciones mensuales.	PO-05	• Responsable de plataforma tecnológica. • Responsable de plataforma de comunicaciones.	Véase Ilustración 31.
Inspecciones ante evidencia de anomalías.	PO-06	• Responsable de plataforma tecnológica. • Responsable de plataforma de comunicaciones	Véase Ilustración 32.

Fuente: Elaboración propia

5.7.2. Estrategias reactivas.

Las estrategias planteadas tienen como objetivo reanudar el servicio u operación de los activos lo más pronto posible, luego de sufrir una interrupción generada por la materialización de un riesgo.

Las estrategias reactivas (Véase Tabla 35) están dirigidos a los activos que soportan los procesos críticos de negocio de JASEC.

Tabla 35 - Estrategias reactivas.

Activo	Código plantilla	Responsable	Plantilla
Comunicación avanzada en edificio central.	PR-01	• Responsable de plataforma de comunicaciones	Véase Ilustración 33, Ilustración 34 e Ilustración 35.
Comunicación avanzada en planteles.	PR-02	• Responsable de plataforma de comunicaciones	Véase Ilustración 36, Ilustración 37 e Ilustración 38.
Servidores físicos.	PR-03	• Responsable de plataforma tecnológica.	Véase Ilustración 39, Ilustración 40 e Ilustración 41.
Servidores virtuales.	PR-04	• Responsable de plataforma tecnológica.	Véase Ilustración 42, Ilustración 43 e Ilustración 44.
Base de datos: Informix.	PR-05	• Responsable de plataforma tecnológica.	Véase Ilustración 45,Ilustración 46.
Base de datos: Oracle 9i, 10g.	PR-06	• Responsable de plataforma tecnológica.	Véase Ilustración 47, Ilustración 48, Ilustración 49 e Ilustración 50.
Aplicativos: Oracle 10g.	PR-07	• Responsable de plataforma tecnológica.	Véase Ilustración 51, Ilustración 52 e Ilustración 53.
Aplicativos: Oracle 9i.	PR-08	• Responsable de plataforma tecnológica.	Véase Ilustración 54 e Ilustración 55.

Fuente: Elaboración propia

5.8. Cierre de plan de continuidad.

En esta sección se muestra los elementos que deben verificarse dentro de la organización (Véase Tabla 36).

Dependiendo del incidente que se haya presentado, puede requerirse una inspección minuciosa por parte de los colaboradores encargados. De igual forma, dependiendo de la contingencia, no todos los puntos que se presentan a continuación se deben llevar a cabo.

Tabla 36 - Estrategias de cierre.

Elemento a verificar	Código plantilla	Responsable	Plantilla
Infraestructura física.	PC-01	• Responsable de la seguridad en instalaciones.	Véase Ilustración 56.
Áreas de trabajo.	PC-02	• Responsable de la seguridad en instalaciones.	Véase Ilustración 57.
Instalaciones eléctricas.	PC-03	• Responsable de la seguridad en instalaciones.	Véase Ilustración 58.
Comunicaciones.	PC-04	• Responsable de plataforma de comunicaciones.	Véase Ilustración 59.
Activos de información.	PC-05	• Responsable de plataforma tecnológica.	Véase Ilustración 60.

Elemento a verificar	Código plantilla	Responsable	Plantilla
Software y acceso a información.	PC-06	• Responsable de plataforma tecnológica.	Véase Ilustración 61.
Datos e información almacenada.	PC-07	• Responsable de plataforma tecnológica.	Véase Ilustración 62.

Fuente: Elaboración propia

5.9. Plantillas.

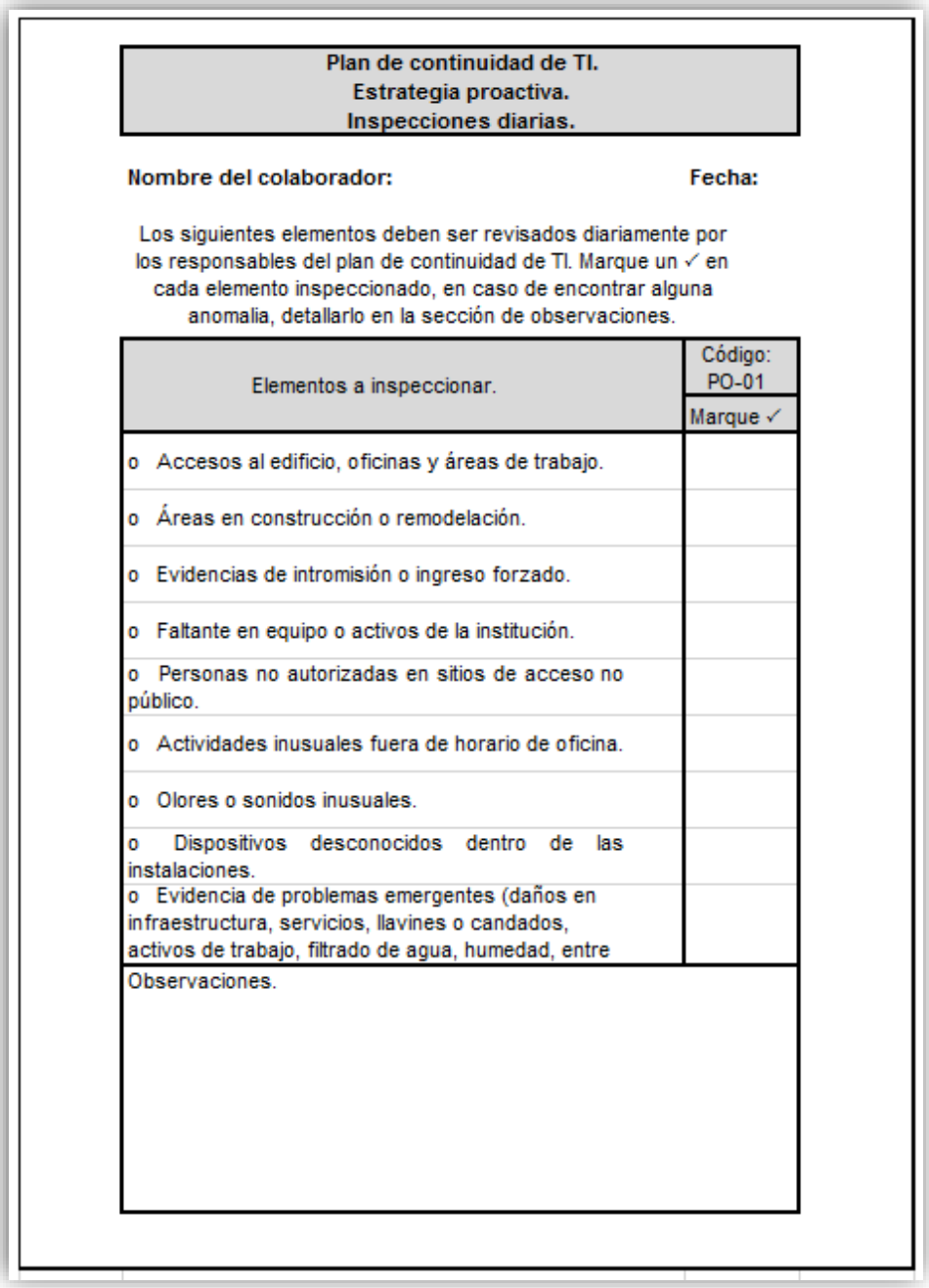
A continuación, se presentan las plantillas a utilizar en la gestión del plan de continuidad de TI. Las plantillas contemplan las estrategias proactivas, reactivas y de cierre del plan de continuidad, igualmente se presenta plantillas para las bitácoras, notificaciones.

5.9.1. Plantillas para estrategias proactivas.

Se presentan las plantillas con las estrategias proactivas que conforman el plan de continuidad de TI.

5.9.1.1. Inspecciones diarias generales.

Los siguientes elementos deben ser revisados diariamente por los responsables del área funcional o encargados de seguridad.



Plan de continuidad de TI.
Estrategia proactiva.
Inspecciones diarias.

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados diariamente por los responsables del plan de continuidad de TI. Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PO-01 Marque ✓
o Accesos al edificio, oficinas y áreas de trabajo.	
o Áreas en construcción o remodelación.	
o Evidencias de intromisión o ingreso forzado.	
o Faltante en equipo o activos de la institución.	
o Personas no autorizadas en sitios de acceso no público.	
o Actividades inusuales fuera de horario de oficina.	
o Olores o sonidos inusuales.	
o Dispositivos desconocidos dentro de las instalaciones.	
o Evidencia de problemas emergentes (daños en infraestructura, servicios, llavines o candados, activos de trabajo, filtrado de agua, humedad, entre	
Observaciones.	

Ilustración 27 – Plantilla de inspecciones diarias generales.
Fuente: Elaboración propia

5.9.1.2. Inspecciones diarias específicas.

Los siguientes elementos deben ser revisados diariamente por los responsables del área de TIC.

Plan de continuidad de TI.
Estrategia proactiva.
Inspecciones diarias.

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados diariamente por los responsables del plan de continuidad de TI. Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PO-02 Marque ✓
o Funcionalidad del equipo de comunicación (teléfonos, fax, intercomunicadores, timbres).	
o Funcionalidad del equipo de trabajo (computadoras personales, impresoras, periféricos utilizados, entre otros).	
o Integridad física de los activos en Centro de Datos.	

Observaciones.

Ilustración 28 - Plantilla de inspecciones diarias específicas.
Fuente: Elaboración propia

5.9.1.3. Inspecciones semanales generales.

Los siguientes elementos deben ser revisados semanalmente por los responsables del área funcional o encargados de seguridad.

Plan de continuidad de TI
Estrategia proactiva
Inspecciones semanal.

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados diariamente por los responsables del plan de continuidad de TI. Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PO-03 Marque ✓
o Integridad de equipo de emergencia (extintores, alarmas, luces de emergencia, cámaras, entre otros).	
o Paneles de control de seguridad.	
o Números de emergencia.	
o Integridad de la infraestructura física de la institución.	
o Integridad de la infraestructura de servicios (luz, teléfono).	
Observaciones.	

Ilustración 29 - Plantilla de inspecciones semanales generales.
Fuente: Elaboración propia

5.9.1.4. Inspecciones semanales específicas.

Los siguientes elementos deben ser revisados semanalmente por los responsables del área de TIC.

Plan de continuidad de TI
Estrategia proactiva
Inspecciones semanal.

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados diariamente por los responsables del plan de continuidad de TI. Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PO-04 Marque ✓
o Sistemas de respaldo de servicio.	
o Revisión y reportes diarios de inspecciones.	
Observaciones.	

Ilustración 30 - Plantilla de inspecciones semanales específicas.
Fuente: Elaboración propia

5.9.1.5. Inspecciones mensuales.

Los siguientes elementos deben ser revisados mensualmente por los responsables del plan de continuidad.

Plan de continuidad de TI
Estrategia proactiva
Inspecciones mensual.

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados diariamente por los responsables del plan de continuidad de TI. Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PO-05 Marque ✓
o Inspección de funcionalidad de equipo de emergencia (alarmas, sirenas, y grabación de cámaras de seguridad, entre otros).	
o Infraestructura de comunicaciones (cableado, activos, switches, router).	
o Conteo de activos de la institución para el plan de continuidad.	
o Inspección de funcionalidad de la infraestructura tecnológica de JASEC.	
o Revisión de reportes semanales.	
Observaciones.	

Ilustración 31 - Plantilla de inspecciones mensuales.
Fuente: Elaboración propia

5.9.1.6. Inspecciones ante evidencia de anomalías.

En caso de encontrar evidencias de intrusiones, daños físicos a activos de tecnología o equipos, se debe realizar una inspección minuciosa de la infraestructura tecnológica. Estas inspecciones consisten en, pero no se limitan a:

Plan de continuidad de TI
Estrategia proactiva
Inspecciones ante anomalias.

Nombre del colaborador: **Fecha:**

En caso de encontrar evidencias de intrusiones, daños físicos a activos de tecnología o equipos con funcionalidad anormal, se debe realizar una inspección minuciosa de la infraestructura tecnológica, para identificar riesgos latentesl. Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PO-06
	Marque ✓
o Accesos físicos a centros de procesamientos de información y centro de datos.	
o Accesos lógicos a los sistemas de información.	
o Acceso a sistemas operativos en servidores físicos y gestores de servidores virtuales.	
o Acceso a configuración y administración de equipo de comunicaciones.	
o Acceso y uso de equipos de almacenamiento de información.	
o Integridad física de los activos de tecnología.	
o Integridad física del cableado de comunicaciones.	
o Instalación y configuración de cableado de comunicaciones y red.	
o Acceso físico a centros de almacenamiento de unidades de respaldo.	
o Acceso físico y lógico de equipos de trabajo.	
o Acceso a activos de información.	
Observaciones.	

Ilustración 32 - Plantilla de inspecciones ante evidencia de anomalías.
Fuente: Elaboración propia

5.9.2. Plantillas para estrategias reactivas.

Se presentan las plantillas con las estrategias reactivas que conforman el plan de continuidad de TI.

5.9.2.1. Comunicación avanzada en edificio central.

Estrategia reactiva para habilitar la comunicación avanzada del edificio central en caso de sufrir una interrupción.

Plan de continuidad de TI
Estrategia reactiva
Comunicación avanzada en edificio central

Nombre del colaborador: **Fecha:**

Estrategia reactiva para restaurar la comunicación avanzada del edificio central en caso de sufrir una interrupción.

Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Protocolo de restauración	Código: PR-01 Marque ✓
1) Analizar el reporte generado.	
2) Probar disponibilidad del equipo en la red.	
a) Ping al equipo	
b) ARP al equipo	
i) ¿No hay respuesta?	
(1) Efectuar una inspección visual del equipo	
(a) Equipo encendido	
(b) Puertos encendidos	
(c) Led de alerta no encendido	
(d) Cableado de comunicaciones	
(e) Instalaciones eléctricas	
(f) Revisar integridad física del equipo	
(i) ¿Fallo físico?	
1. Revisar disponibilidad de la red	
a. Ping a un equipo externo	
2. Desmontar equipo del rack en CD	
3. Revisar parte electrónica del equipo	
a. ¿Confirmación de daño en equipo?	

Ilustración 33 - Parte I - Estrategia PR-01
Fuente: Elaboración propia

Protocolo de restauración	Código: PR-01 Marque ✓
i. Contactar Cisco	
ii. Supervisar reemplazo e instalación de equipo nuevo	
(2) Conectarse directamente al equipo	
3) Ingresar vía SSH al equipo o consola.	
a) Analizar los tipos de errores generado por el equipo.	
i) ¿Resolución en menos de una hora?	
(1) Aplicar plan correctivo en el equipo	
4) Revisar la configuración del equipo y verificar que está en su totalidad	
a) Estado de interfaz	
b) Configuración de interfaces	
c) Enrutamientos	
d) Estado de cada interfaz	
e) ¿No está del todo?	
i) Ingresar a repositorio de soporte técnico	
ii) Copiar respaldo de configuración del equipo	
iii) Pegar respaldo por medio de consola al equipo	
5) Revisión de Log.	
a) Revisar alertas	
b) Revisar errores	
c) Revisar notificaciones del equipo	
i) ¿Resolución en menos de una hora?	
(1) Aplicar plan correctivo en el equipo	

Ilustración 34 - Parte II - Estrategia PR-01

Fuente: Elaboración propia

Protocolo de restauración	Código: PR-01 Marque ✓
ii) ¿Resolución en más de una hora?	
(1) Revisar disponibilidad de la red	
(a) Ping a un equipo externo	
(2) Verificar VLAN	
(3) Verificar DHCP	
(4) Verificar enrutamiento estático y dinámico	
(5) Definir configuraciones	
(a) Realizar plan correctivo	
(b) ¿Error requiere soluciones específicas avanzadas?	
1. Ejecutar soporte de mantenimiento con proveedor	
Observaciones.	

Ilustración 35 - Parte III - Estrategia PR-01

Fuente: Elaboración propia

5.9.2.2. Comunicación avanzada en los planteles.

Estrategia reactiva para habilitar la comunicación avanzada en los planteles en caso de sufrir una interrupción.

Plan de continuidad de TI
Estrategia reactiva.
Comunicación avanzada en los planteles

Nombre del colaborador: **Fecha:**

Estrategia reactiva para restaurar la comunicación avanzada en los planteles en caso de sufrir una interrupción.

Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Protocolo de restauración	Código: PR-02
	Marque ✓
1) Analizar el reporte generado por el NOC.	
2) Probar disponibilidad del equipo en la red.	
a) Ping al equipo	
b) ARP al equipo	
i) ¿No hay respuesta?	
(1) Efectuar una inspección visual del equipo	
(a) Equipo encendido	
(b) Puertos encendidos	
(c) Led de alerta no encendido	
(d) Cableado de comunicaciones	
(e) Instalaciones eléctricas	
(f) Revisar integridad física del equipo	
(i) ¿Fallo físico?	
1. Revisar disponibilidad de la red	
a. Ping a un equipo externo	
2. Desmontar equipo del rack en CD	
3. Revisar parte electrónica del equipo	
a. ¿Confirmación de daño en equipo?	

Ilustración 36 - Parte I - Estrategia PR-02

Fuente: Elaboración propia

Protocolo de restauración	Código: PR-02 Marque ✓
ii. Supervisar reemplazo e instalación de equipo nuevo	
(2) Conectarse directamente al equipo	
3) Ingresar vía SSH al equipo o consola.	
a) Analizar los tipos de errores generado por el equipo.	
i) ¿Resolución en menos de una hora?	
(1) Aplicar plan correctivo en el equipo	
4) Revisar la configuración del equipo y verificar que está en su totalidad	
a) Estado de interfaz	
b) Configuración de interfaces	
c) Enrutamientos	
d) Estado de cada interfaz	
e) ¿No está del todo?	
i) Ingresar a repositorio de soporte técnico	
ii) Copiar respaldo de configuración del equipo	
iii) Pegar respaldo por medio de consola al equipo	
5) Revisión de Log.	
a) Revisar alertas	
b) Revisar errores	
c) Revisar notificaciones del equipo	
i) ¿Resolución en menos de una hora?	
(1) Aplicar plan correctivo en el equipo	
ii) ¿Resolución en más de una hora?	
(1) Revisar disponibilidad de la red	
(a) Ping a un equipo externo	
(2) Verificar VLAN	

Ilustración 37 - Parte II - Estrategia PR-02.

Fuente: Elaboración propia.

Protocolo de restauración	Código: PR-02 Marque ✓
(3) Verificar DHCP	
(4) Verificar enrutamiento estático y dinámico	
(5) Definir configuraciones	
(a) Realizar plan correctivo	
(b) ¿Error requiere soluciones específicas avanzadas?	
1. Ejecutar soporte de mantenimiento con proveedor	
Observaciones.	

Ilustración 38 - Parte III - Estrategia PR-02.

Fuente: Elaboración propia.

5.9.2.3. Servidores físicos.

Estrategia reactiva para habilitar los servidores físicos en caso de sufrir una interrupción.

Plan de continuidad de TI
Estrategia reactiva
Servidores físicos

Nombre del colaborador: **Fecha:**

Estrategia reactiva para habilitar los servidores fisicos en caso de sufrir una interrupción.

Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Protocolo de restauración	Código: PR-03 Marque ✓
1) Efectuar un ping a la dirección IP del servidor y debe haber una respuesta.	
2) Si existe una respuesta se debe tratar de conectarse a través de acceso remoto si lo tiene habilitado.	
3) Si existe conexión se revisa el causante del problema. (Inicia con Dep Soporte)	
a) Asegurar que el active directory se está ejecutando (dominio).	
i) En caso de que no estar ejecutándose se debe se debe revisar y levantar el servicio.	
ii) De existir problemas con el active directory, semanalmente se efectúa un respaldo del sistema operativo, el cual se encuentra en \\10.1.4.40\bck_ad por lo tanto se debe restablecer el servidor con dicho respaldo.	
iii) En caso de que el problema no se resuelva se debe crear e implementar un servidor virtual y efectuar la instalación del nuevo servidor de Active directory.	

Ilustración 39 - Parte I - Estrategia PR-03

Fuente: Elaboración propia.

Protocolo de restauración	Código: PR-03 Marque ✓
b) Asegurar que el servicio de IIS se está ejecutando (web).	
i) Si el servicio de IIS no se está ejecutando se debe reiniciar el servicio.	
ii) Si el servicio no levanta se debe desinstalar y reinstalar el IIS.	
iii) Se debe importar el paquete del servidor para restablecer el servicio.	
iv) Si el problema es el Joomla, se debe reinstalar y luego ejecutar el último respaldo efectuado.	
4) En caso de que no se pueda conectar al servidor web, revisar la configuración del firewall perimetral, ya que dicho servidor se encuentra en la DMZ y se requieren permisos para accederlo.	
5) Si el servidor de dominio no responde al ping se debe trasladar al Centro de Datos a revisar el servidor, el mismo se encuentra en el rack APC que se encuentra al lado del rack SUN. Se debe revisar que el servidor se encuentre encendido.	
6) Se debe revisar el estado actual del servidor, para ello se debe conectar un monitor y observar el estado actual del servidor.	
7) Se debe revisar el hardware para encontrar fallas físicas y en caso de requerirse se debe brindar mantenimiento al servidor.	

Ilustración 40 - Parte II - Estrategia PR-02

Fuente: Elaboración propia.

Protocolo de restauración	Código: PR-03 Marque ✓
a) Se debe desconectar el servidor y efectuar una revisión del hardware, incluyendo fuentes de poder, memoria RAM, procesador, tarjeta madre, alimentación eléctrica, entre otros para identificar el problema. De estar alguna parte dañada se debe efectuar todo el trámite de contratación en proveeduría para poder sustituirla.	
8) Una vez instalado el servidor, si fue necesario la reinstalación se debe restaurar usando el respaldo que se había efectuado con anterioridad. Dicho respaldo se encuentra en \\10.1.4.40\bck_ad.	
9) En caso de que no necesite la reinstalación, se debe conectar de nuevo el equipo y restablecer el servicio.	
Observaciones.	

Ilustración 41 - Parte III - Estrategia PR-02

Fuente: Elaboración propia.

5.9.2.4. Servidores virtuales.

Estrategia reactiva para habilitar los servidores virtuales en caso de sufrir una interrupción.

Plan de continuidad de TI
Estrategia reactiva
Servidores virtuales.

Nombre del colaborador: **Fecha:**

Estrategia reactiva para restaurar los servidores virtuales en caso de sufrir una interrupción.

Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Protocolo de restauración	Código: PR-04 Marque ✓
1) Acceder a la consola del VMware VSphere Client por medio del servidor 10.1.4.199 a través de escritorio remoto (RDP).	
2) Una vez dentro, ejecutar la aplicación que se encuentra en el escritorio VMware VSphere Client.	
3) Si la aplicación VMware VSphere Client no se ejecuta se debe reinstalar.	
4) Si el servidor de vCenter no se encuentra encendido se debe hacer:	
a) Se debe ejecutar la aplicación VMware VSphere Client y se debe cambiar la dirección IP a 10.1.4.112.	
b) Una vez dentro debe efectuar click derecho sobre el servidor vCenter_Win2k8 →Power→Power On.	
5) Si aun así el servidor de vCenter no levanta se debe hacer lo que indica los puntos 8 y 9.	
6) Se busca el servidor virtual que está presentando problemas.	
a) Se debe revisar que se encuentre encendido.	

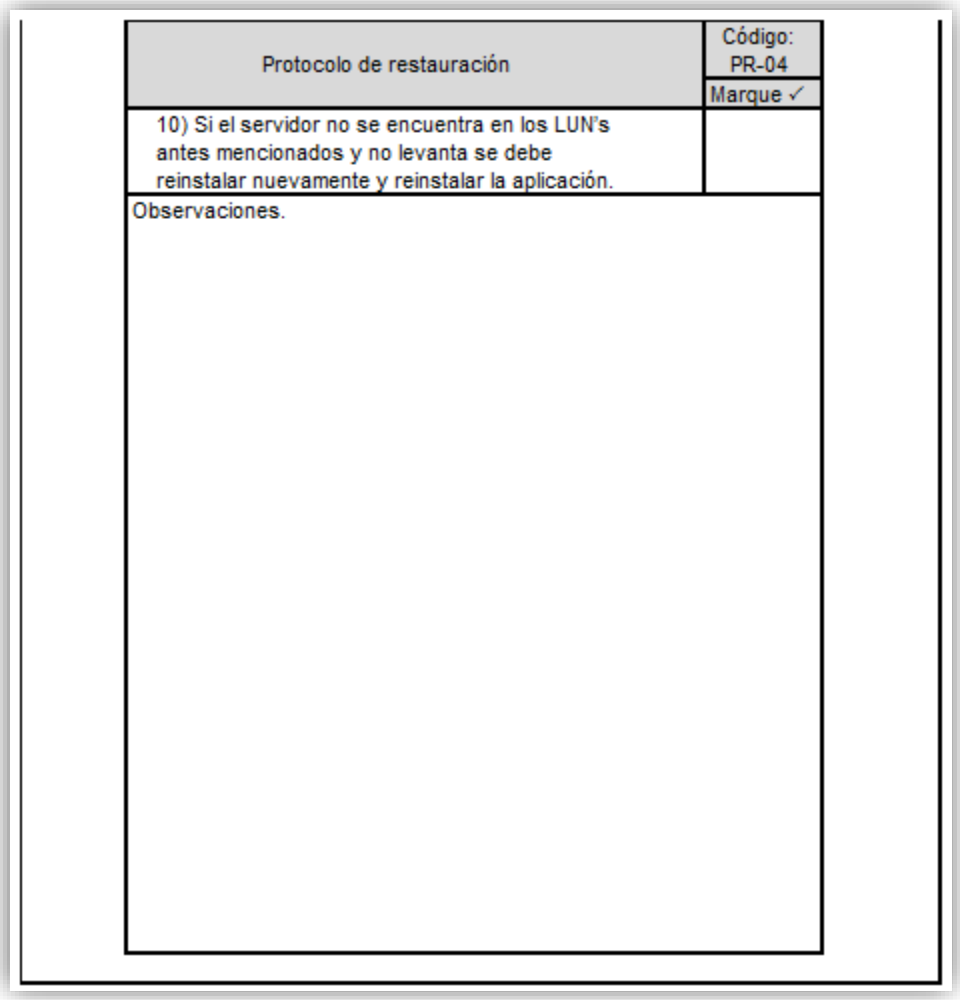
Ilustración 42 - Parte I - Estrategia PR-04

Fuente: Elaboración propia.

Protocolo de restauración	Código: PR-04 Marque ✓
b) Si no se encuentra encendido se debe seguir el procedimiento 6I111 Encendido y apagado de servidores físicos y virtuales.	
7) Si el servidor no enciende se habilita el modo de consola. Click derecho → Open Console. Esto para observar si está presentando algún mensaje de error que impide que el servidor levante.	
8) Si no se encuentra solución para que el servidor virtual levante se debe revisar el LUN de la SAN donde se encuentra la máquina virtual. Esto debido a que se encuentra configurado para que las máquinas virtuales que se encuentran en NetApp1_LUN1 y NetApp2_LUN2 hagan respaldos 2 veces a la semana de dichas configuraciones.	
9) Si el servidor virtual se encuentra en alguno de los 2 LUN's mencionados se debe hacer:	
a) Se debe ingresar a Home → NetApp →Backup and Recovery →Restore y elegir la fecha en que se desea efectuar la restauración.	
b) Luego se escoge el servidor en la lista, se da click derecho en la opción Restore.	
c) Se debe de esperar un tiempo prudencial mientras se realiza la restauración.	
d) Luego de esto se revisa que el servidor haya levantado.	
e) En caso de que el servidor aun no levante se debe seguir restaurando en una fecha anterior a la efectuada (seguir paso a, b y c).	
f) Si definitivamente el servidor virtual no levanta, se debe reinstalar nuevamente y reinstalar la aplicación.	

Ilustración 43 - Parte II - Estrategia PR-04.

Fuente: Elaboración propia.



Protocolo de restauración	Código: PR-04
	Marque ✓
10) Si el servidor no se encuentra en los LUN's antes mencionados y no levanta se debe reinstalar nuevamente y reinstalar la aplicación.	
Observaciones.	

Ilustración 44 - Parte III - Estrategia PR-04

Fuente: Elaboración propia.

5.9.2.5. Base de datos: Informix.

Estrategia reactiva para habilitar la base de datos Informix en caso de sufrir una interrupción.

Plan de continuidad de TI
Estrategia reactiva
Base de datos: Informix

Nombre del colaborador: **Fecha:**

Estrategia reactiva para habilitar la base de datos Informix en caso de sufrir una interrupción.

Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Protocolo de restauración	Código: PR-05 Marque ✓
1) Levantar respaldo de la Base de dato en el servidor alterno	
a) Verificar que el servidor está ocioso (sin uso por otros usuarios)	
b) Borrar BD en servidor de respaldo	
c) Trasladar documentos de respaldo del Disco duro externo de respaldos al servidor	
d) Ejecutar actualización (levantar BD, estructura de tablas e información) en servidor de respaldo por medio de comando	
2) Recopilar información de las actividades realizadas entre el momento del último respaldo y la ocurrencia de la falla	
a) Coordinar con jefe del área de facturación para autorización	
b) Coordinar con personal para actualizar información:	
i) Coordinar con el encargado de Atención al Cliente para la actualización de la anulación de recibos y servicios al cliente	
ii) Coordinar con personal de apoyo del asistente técnico facturar y cobrar sobre la información obtenida previa a su procesamiento	
iii) El Asistente técnico coordina, recopila y valida la información procesada	

Ilustración 45 - Parte I - Plantilla estrategia PR-05.

Fuente: Elaboración propia.

Protocolo de restauración	Código: PR-05 Marque ✓
3) Aplicar el procedimiento de respaldo y recuperación/actualización de bases de datos y aplicaciones.	
a) El asistente técnico facturar y cobrar procesa la información otorgada	
b) Validan que la información haya sido levantada exitosamente por parte del personal de apoyo	
c) Notificar actualización exitosa de la información	
d) Depurar base de datos para establecerlo como transaccional	
4) Efectuar las pruebas necesarias para corroborar que se restableció el servicio.	
a) Validar que Informix se encuentra en línea (online)	
b) Validar espacio en disco	
c) Validar desempeño del servidor (procesador y memoria RAM)	
d) Validar respuesta de la base de datos en sistema de consulta general (consultas aleatorias)	
e) Validar con los usuarios el restablecimiento de operación productiva	
5) Ejecutar comando para copiar Log a cinta manualmente (Desde consola)	
Observaciones.	

Ilustración 46 - Parte II - Plantilla estrategia PR-05.

Fuente: Elaboración propia.

5.9.2.6. Base de datos: Oracle 9i, 10g.

Estrategia reactiva para habilitar la base de datos Oracle 9i o 10g, en caso de sufrir una interrupción.

Plan de continuidad de TI
Estrategia reactiva
Base de datos: Oracle 9i, 10g.

Nombre del colaborador: **Fecha:**

Estrategia reactiva para habilitar la base de datos Oracle 9i o 10g, en caso de sufrir una interrupción.

Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Protocolo de restauración	Código: PR-06 Marque ✓
1) Revisar si hay servicios colapsando la BD	
2) ¿Si hay?	
a) Terminar el servicio que genera bloqueo b) Terminar la sesión del usuario c) ¿No responde? i) Desconectar al usuario d) Verificar que la BD responde (después de máximo 10 minutos)	
3) ¿Base de datos no responde?	
Realizar el procedimiento de reinicio de la base de datos, según la base de datos que corresponda	
a) BASE DE DATOS JASEC	
i) Digitar: telnet SIPAC/SICURA o Digitar: telnet SIFAJ/SISRH ii) Usuario: xxxx, clave: xxx iii) Digitar: sqlplus /nolog iv) Digitar: conn /as sysdba v) Digitar shutdown immediate vi) Si después de un tiempo a no baja, se debe de abrir otro telnet y digitar shutdown abort vii) Una vez que la BD esta abajo se digita startup viii)Digitar Exit para salir del command prompt.	
b) BASE DE DATOS JASEC SICURA	

Ilustración 47 - Parte I - Plantilla estrategia PR-06.

Fuente: Elaboración propia.

Protocolo de restauración	Código: PR-06 Marque ✓
i) Digitar: telnet ii) Usuario: xxxx, clave: xxxx iii) Digitar: cd admin iv) Digitar: cd sicura v) Digita cd scripts vi) Digitar: ./abajo_sicura.sh vii) Digitar: cat abajo_sicura.sh	
viii)¿Script no funciona?	
(1) Se copia export ORACLE_SID=sicura y se hace el shutdown de forma manual (2) Digita sqlplus /nolog (3) Digitar: conn /as sysdba (4) Digitar: shutdown immediate (5) Si después de un tiempo a determinar no baja, se debe de abrir otro telnet y digitar shutdown abort ix) Digitar: ./arriba_sicura.sh x) Digitar Exit para salir del command prompt	
c) REVISAR TNSNAMES DE BASE DE DATOS (Prueba de conexión de base de datos)	
i) telnet ii) Usuario: xxxx, clave: xxxx iii) Digitar: cd product iv) Digitar: cd 9.2 v) Digitar: cd network vi) Digitar: cd admin	

Ilustración 48 - Parte II - Plantilla estrategia PR-06.

Fuente: Elaboración propia.

Protocolo de restauración	Código: PR-06 Marque ✓
vii) Digitar: cat open tnsnames.ora viii)Digitar: tnsping xxxxx <-- nombre del dblink que se desea probar.	
d) Verificar el listener de base de datos (Prueba de conexión)	
i) telnet ii) Usuario: xxxx, clave: xxxx iii) Digitar: sqlplus /nolog iv) Digitar: conn /as sysdba v) Digitar: lsnrctl status vi) Si da el siguiente error:	
(1) TNS-12541: TNS:no listener (2) TNS-12560: TNS:protocol adapter error (3) TNS-00511: No listener (4) Solaris Error: 146: Connection refused	
vii) Digitar: lsnrctl start (1) El siguiente mensaje indica que el listener está bien:	
i. The command completed succesfully	
viii)Digitar: lsnrctl status (1) El siguiente mensaje indica que el listener está bien:	
i. The command completed succesfully.	
4) Pasos a seguir para reiniciar los servidores Bases de Datos, desde el command prompt (cmd):	
a) SERVIDORES (V440 -> SIPAC/SICURA)	
i) Digitar: telnet (V440 -> SIPAC/SICURA) ii) Digitar: Usuario: xxx, clave: xxx iii) Digitar: init 5 (apagado)	

Ilustración 49 - Parte III - Plantilla estrategia PR-06.

Fuente: Elaboración propia.

Protocolo de restauración	Código: PR-06 Marque ✓
iv) Digitar: init 6 (reiniciar) 5) En caso de apagarse el equipo se procede a reiniciarlo manualmente	
6) ¿Base de datos no responde?	
a) Realizar procedimiento de restablecimiento de la base de datos con el respaldo i) Revisar manual de procedimiento de restablecimiento de BD	
7) ¿Base de datos no responde?	
a) Respaldar equipo en contingencia (servidor de pruebas) b) Restaurar con respaldo de BD en equipo de contingencia c) Renombrar IP en servidor de contingencia.	
Observaciones.	

Ilustración 50 - Parte IV - Plantilla estrategia PR-06.

Fuente: Elaboración propia.

5.9.2.7. Aplicativos: Oracle 10g.

Estrategia reactiva para habilitar algún aplicativo de Oracle 10g. en caso de sufrir una interrupción.

Plan de continuidad de TI
Estrategia reactiva
Aplicativos: Oracle 10g.

Nombre del colaborador: **Fecha:**

Estrategia reactiva para habilitar algún aplicativo de Oracle 10g en caso de sufrir una interrupción.

Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Protocolo de restauración	Código: PR-07 Marque ✓
1) Ingresar a servidor de aplicativos.	
2) Ingresar Interfaz Gráfica de Servidor de Aplicaciones (OAS).	
3) ¿Interfaz no responde?	
a) Acceder por medio de acceso remoto al servidor de aplicaciones.	
b) Reiniciar la interfaz gráfica.	
c) ¿Interfaz no responde?	
i) Revisar servicios del servidor que utiliza la interfaz	
ii) ¿Servicios no responden?	
(1) Reiniciar los servicios.	
(2) ¿Servicios no pueden reiniciarse?	
(a) Reiniciar el servidor.	
4) Revisar estado del uso del servidor.	
5) ¿Fallan todos los servicios?	
a) Reiniciar el servicio de aplicaciones (gráfica).	
b) ¿Servicios no funcionan?	
i) Revisar conectividad de BD.	
ii) ¿Problemas con BD?	
(1) Realizar pasos anteriores.	
6) Revisar estado de cada aplicativo.	

Ilustración 51 - Parte I - Plantilla estrategia PR-07.

Fuente: Elaboración propia.

Protocolo de restauración	Código: PR-07 Marque ✓
7) ¿Falla en un aplicativo?	
a) Reiniciar el aplicativo.	
b) ¿No funciona?	
i) Revisar conectividad de BD.	
ii) ¿Problemas con BD?	
(1) Revisar prioridad de servicios con otros aplicativos.	
(2) Terminar tareas del aplicativo que genera conflicto.	
(3) ¿No hay tareas con conflictos?	
(a) Realizar pasos anteriores.	
iii) Crear un nuevo archivo de ambiente para aplicativo.	
iv) ¿No funciona?	
(1) Respaldar carpeta del aplicativo en servidor de producción.	
(2) Respaldar carpeta Oracle\forms\server en servidor de producción.	
(3) Renombrar carpetas del aplicativo en servidor de contingencia.	
(a) Formas.	
(b) Reportes.	
(c) Recursos.	
(4) Redireccionar el aplicativo al servidor de contingencia.	
8) Realizar pruebas de conectividad y acceso.	
9) ¿Servidor de aplicaciones no responde?	
a) Respaldar carpeta de sistemas en servidor de producción.	

Ilustración 52 - Parte II - Plantilla estrategia PR-07.

Fuente: Elaboración propia.

Protocolo de restauración	Código: PR-07 Marque ✓
b) Respaldar carpeta Oracle\forms\server en servidor de producción.	
c) Renombrar carpeta de sistemas en servidor de contingencia.	
d) Copiar carpetas de servidor de producción en servidor de contingencia.	
e) Redireccionar enlaces a equipo de contingencia (habilitar servicios).	
Observaciones.	

Ilustración 53 - Parte III - Plantilla estrategia PR-07.

Fuente: Elaboración propia.

5.9.2.8. Aplicativos: Oracle 9i.

Estrategia reactiva para habilitar algún aplicativo de Oracle 9i, en caso de sufrir una interrupción.

Plan de continuidad de TI
Estrategia reactiva
Aplicativos: Oracle 9i.

Nombre del colaborador: **Fecha:**

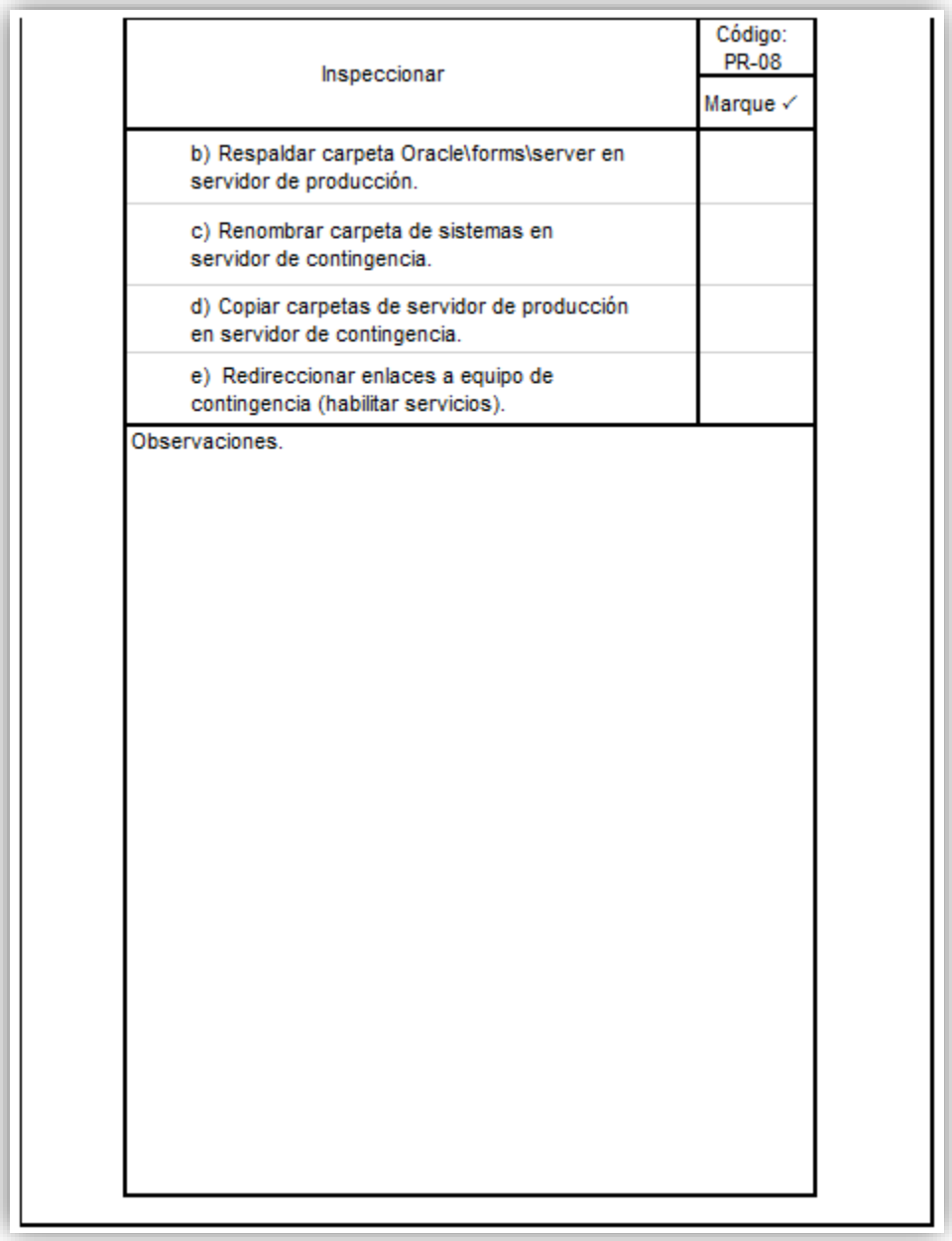
Estrategia reactiva para habilitar algún aplicativo de Oracle 9i en caso de sufrir una interrupción.

Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Protocolo de restauración	Código: PR-08 Marque ✓
1) Ingresar a servidor de aplicativos.	
2) Revisar alertas del OC4J.	
3) ¿Pérdida de comunicación?	
a) Reiniciar OC4J.	
b) ¿No responde?	
i) Verificar los servicios de Oracle del servidor.	
ii) ¿Servicios caídos?	
(1) Reiniciar servicios.	
(2) ¿No responden?	
(a) Reiniciar el equipo.	
4) Revisar BD.	
a) Revisar conectividad en BD.	
b) ¿Problemas con BD?	
i) Revisar prioridad de servicios con otros aplicativos.	
ii) Terminar tareas del aplicativo que genera conflicto.	
(1) ¿No hay tareas con conflictos?	
(a) Revisar prioridad de servicios en BD 10g (cuando aplica).	
(b) Realizar pasos anteriores.	
5) ¿Servidor o aplicaciones no responde?	
a) Respaldar carpeta de sistemas en servidor de producción.	

Ilustración 54 - Parte I - Plantilla estrategia PR-08.

Fuente: Elaboración propia.



Inspeccionar	Código: PR-08 Marque ✓
b) Respaldar carpeta Oracle\forms\server en servidor de producción.	
c) Renombrar carpeta de sistemas en servidor de contingencia.	
d) Copiar carpetas de servidor de producción en servidor de contingencia.	
e) Redireccionar enlaces a equipo de contingencia (habilitar servicios).	
Observaciones.	

Ilustración 55 - Parte II - Plantilla estrategia PR-08.

Fuente: Elaboración propia.

5.9.3. Plantillas de uso para cierre de plan de continuidad.

5.9.3.1. Infraestructura física.

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI, con la intención de cerrar el plan de continuidad de TI. Se debe marcar una X en cada elemento inspeccionado, en caso de encontrar alguna anomalía, detallarlo en la sección de observaciones.

Plan de continuidad de TI
Cierre de plan de continuidad de TI
Infraestructura física

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intension de cerrar el plan de continuidad de TI.
Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PC-01 Marque ✓
a) Daños estructurales en paredes (grietas, cuarteaduras, pedazos sueltos, falseados, entre otros).	
b) Daños estructurales en techos (grietas, pedazos sueltos, partes caídas, estructura de soporte suelto, entre otros).	
c) Daños en puertas y ventanas / control de acceso permitido.	
d) Daños en cielorraso.	
e) Escombros, polvo u obstáculos presentes.	
f) Espacios de trabajo (escritorios, silla, cajones, archiveros, mueblería general).	
g) Integridad en pasillos, corredores y escaleras.	
h) Integridad física en áreas de descanso / públicas.	
i) Señas de humo, fuego, cortos circuitos, fugas de agua, entre otros, presentes dentro y fuera de las instalaciones.	
j) Integridad de salidas de emergencia y sitios de reunión.	
k) Infraestructura eléctrica.	
l) Equipo de detección de humo / extintores en funcionamiento.	
m) Cámaras de seguridad.	
n) Iluminación de emergencia.	
Observaciones.	

Ilustración 56 - Plantilla de inspecciones de cierre - Infraestructura física.

Fuente: Elaboración propia.

5.9.3.2. Áreas de trabajo.

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI, con la intención de cerrar el plan de continuidad de TI. Se debe marcar una X en cada elemento inspeccionado, en caso de encontrar alguna anomalía, detallarlo en la sección de observaciones.

Plan de continuidad de TI
Cierre de plan de continuidad de TI
Áreas de trabajo

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intension de cerrar el plan de continuidad de TI.
Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PC-02
	Marque ✓
1) Espacios disponibles y libres de polvo o suciedad.	
2) Mobiliario disponible para realizar funciones.	
3) Servicios eléctricos y de agua disponibles.	
4) Salidas de emergencia habilitadas.	
5) Control de acceso para permitir sólo personal autorizado.	
6) Sistemas y/o equipo de emergencia revisado y disponible.	
7) Para centros de datos se debe revisar, además:	
a) Espacios para racks y cableado de comunicaciones en condiciones óptimas.	
b) Aire acondicionado.	
c) Equipo de control ambiental (humedad, temperatura, entre otros).	
d) Espacios de control de temperatura e infraestructura especial.	

Observaciones.

Ilustración 57 - Plantilla de inspecciones de cierre - Áreas de trabajo.

Fuente: Elaboración propia.

5.9.3.3. Instalaciones eléctricas.

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI, con la intención de cerrar el plan de continuidad de TI. Se debe marcar una X en cada elemento inspeccionado, en caso de encontrar alguna anomalía, detallarlo en la sección de observaciones.

Plan de continuidad de TI
Cierre de plan de continuidad de TI
Instalaciones électricas

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intension de cerrar el plan de continuidad de TI.
Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PC-03
	Marque ✓
1) Acometida de servicios eléctricos regulada y asegurada.	
2) Verificación de todo el cableado eléctrico en las instalaciones.	
3) Contactos eléctricos en condiciones óptimas (no expuestos o dañados, sin humo, sin ruidos extraños, con cortos), con el voltaje adecuado según el equipo a utilizar.	
4) Planta de respaldo de energía eléctrica habilitada.	
5) UPS íntegros y en funcionamiento óptimo.	
6) Supresores de picos de voltaje donde se requieran.	
Observaciones.	

Ilustración 58 - Plantilla de inspecciones de cierre - Instalaciones eléctricas.

Fuente: Elaboración propia.

5.9.3.4. Comunicaciones.

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intención de cerrar el plan de continuidad de TI. Se debe marcar una X en cada elemento inspeccionado, en caso de encontrar alguna anomalía, detallarlo en la sección de observaciones.

Plan de continuidad de TI
Cierre de plan de continuidad de TI
Comunicaciones

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intension de cerrar el plan de continuidad de TI.
Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PC-04
	Marque ✓
1) Cableado de comunicaciones y tendido de cables en condiciones óptimas y seguras.	
2) Instalación de cableado de datos y telefónico en las áreas de trabajo.	
3) Instalaciones de comunicaciones al exterior en condiciones óptimas.	
4) Aparatos de comunicación en condiciones de trabajo.	
5) Equipo de datos en condiciones óptimas (switches, routers, puntos de acceso).	
6) Equipo de comunicación y enrutamiento en condiciones óptimas.	
7) Equipo telefónico y de fax (donde aplique).	
8) Servicios de control de tráfico de datos, comunicaciones, seguridad y control de acceso habilitados y en funcionamiento normal.	
Observaciones.	

Ilustración 59 - Plantilla de inspecciones de cierre - Comunicaciones.

Fuente: Elaboración propia.

5.9.3.5. Activos de información.

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intención de cerrar el plan de continuidad de TI. Se debe marcar una X en cada elemento inspeccionado, en caso de encontrar alguna anomalía, detallarlo en la sección de observaciones.

Plan de continuidad de TI
Cierre de plan de continuidad de TI
Activos de información

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intension de cerrar el plan de continuidad de TI.
Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PC-05 Marque ✓
1) Servidores en centro de datos disponible.	
2) Sistemas de almacenamiento de información y respaldos.	
3) Servicios de control de acceso y herramientas de seguridad de información.	
4) Dominio de la institución.	
5) Impresoras y centros de copiado.	
6) Activos de tecnología del personal operativo y administrativo.	
Observaciones.	

Ilustración 60 - Plantilla de inspecciones de cierre - Activos de información.

Fuente: Elaboración propia.

5.9.3.6. Software y acceso a información.

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intención de cerrar el plan de continuidad de TI. Se debe marcar X en cada elemento inspeccionado, en caso de encontrar alguna anomalía, detallarlo en la sección de observaciones.

Plan de continuidad de TI
Cierre de plan de continuidad de TI
Software y acceso a información

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intension de cerrar el plan de continuidad de TI.
Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PC-06
	Marque ✓
1) Aplicaciones y servicios de la institución habilitados.	
2) Comunicación entre áreas operativas y centro de datos a nivel lógico (aplicaciones y bases de datos).	
3) Acceso controlado a los usuarios y nivel de acceso.	
4) Capacidad de procesamiento, desempeño e integridad.	
5) Seguridad de información.	
Observaciones.	

Ilustración 61 - Plantilla de inspecciones de cierre - Sistemas informáticos y acceso a información.

Fuente: Elaboración propia.

5.9.3.7. Datos e información almacenada.

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI, con la intención de cerrar el plan de continuidad de TI. Se debe marcar una X en cada elemento inspeccionado, en caso de encontrar alguna anomalía, detallarlo en la sección de observaciones.

Plan de continuidad de TI
Cierre de plan de continuidad de TI
Datos e información almacenada

Nombre del colaborador: **Fecha:**

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intension de cerrar el plan de continuidad de TI.
Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PC-07
	Marque ✓
1) Cuentas de usuario.	
2) Permisos de acceso.	
3) Información de contribuyentes.	
4) Información de operaciones de servicios y atención a clientes.	
5) Correo electrónico.	
6) Respaldos.	
7) Inventarios de activos de tecnología.	
Observaciones.	

Ilustración 62 - Plantilla de inspecciones de cierre - Datos e información almacenada.

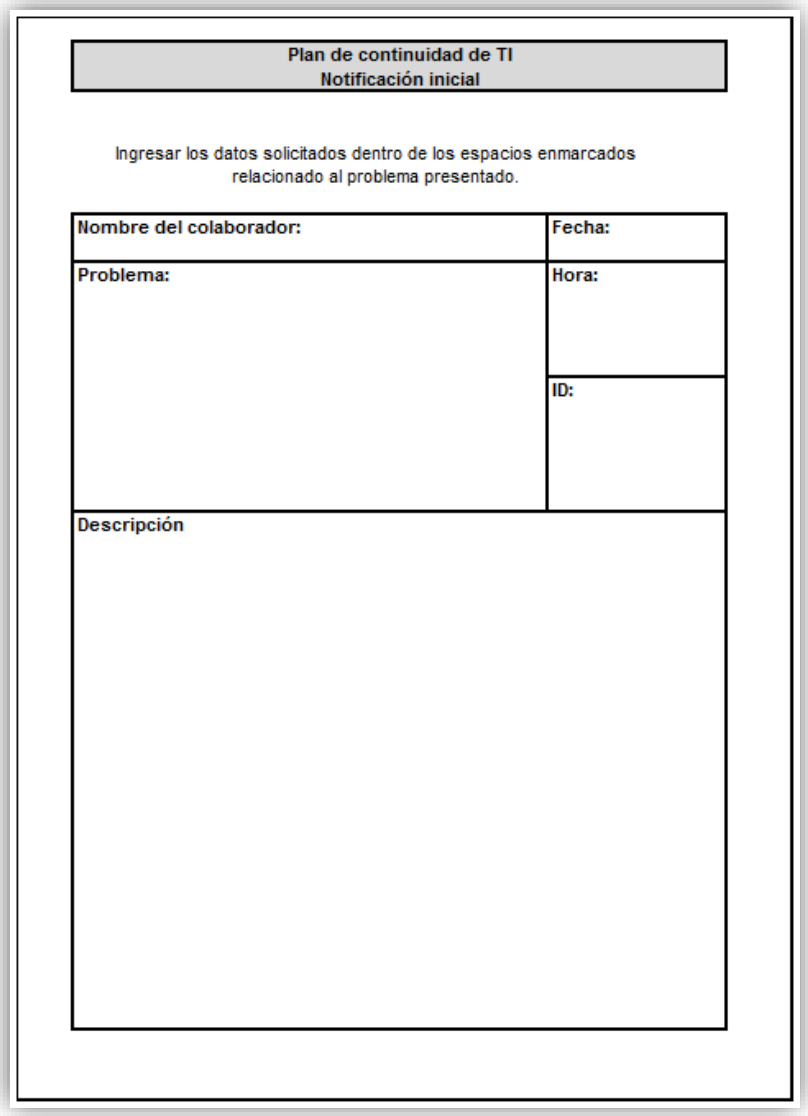
Fuente: Elaboración propia.

5.9.4. Plantillas de gestión.

A continuación se presenta las plantillas de gestión que permiten documentar información respecto a la notificación inicial, bitácoras de estrategias y cierre.

5.9.4.1. Plantilla de notificación inicial.

Requiere el ingreso los datos solicitados dentro de los espacios enmarcados relacionado al problema presentado.



Plan de continuidad de TI
Notificación inicial

Ingresar los datos solicitados dentro de los espacios enmarcados relacionado al problema presentado.

Nombre del colaborador:	**Fecha:**
Problema:	**Hora:**
	ID:
Descripción	

Ilustración 63 - Plantilla de notificación inicial.
Fuente: Elaboración propia.

5.9.4.2. Plantilla de bitácora para procedimientos proactivos.

Permite registrar los datos del colaborador a cargo y detallar las estrategias proactivas implementadas.

Plan de continuidad de TI
Bitácora de estrategias proactivos.

Registrar los datos solicitados y detallar las estrategias proactivas implementadas.

Bitácora de estrategias proactivos.		
Responsable:		**Fecha**
Código de estrategia proactiva.	**Detalle**	**Completado (Sí/No)**

Ilustración 64 - Plantilla de bitácora de estrategias proactivas.
Fuente: Elaboración propia.

5.9.4.3. Plantilla de bitácora para procedimientos reactivos.

Permite registrar los datos del colaborador a cargo y detallar las estrategias reactivas implementadas.

Plan de continuidad de TI
Bitácora de estrategias reactivas.

Registrar los datos solicitados y detallar las estrategias reactivas implementadas.

Bitácora de estrategias reactivas.		ID problema
Responsable:		Fecha
Código de estrategia reactiva.	Detalle	Completado (Sí/No)

Ilustración 65 - Bitácora de estrategias reactivas.
Fuente: Elaboración propia.

5.9.4.4. Plantilla de control para inspecciones de cierre de plan de continuidad.

Permite registrar los datos del colaborador a cargo y detallar las inspecciones de cierre implementadas.

Plan de continuidad de TI
Bitácora de inspecciones de cierre.

Registrar los datos solicitados y detallar las inspecciones de cierre implementadas.

Bitácora de inspecciones de cierre.		ID problema
Responsable:		Fecha
Código de inspección.	Detalle	Completado (Sí/No)

Ilustración 66 - Plantilla de bitácora de inspecciones de cierre.
Fuente: Elaboración propia.

5.10. Actualización del plan de continuidad.

La actualización del plan de continuidad de TI debe responder ante la necesidad de agregar, modificar o eliminar información que impacte directamente las estrategias proactivas, reactivas o de cierre contempladas dentro de este plan.

Es necesario gestionar una actualización del plan de continuidad cuando:

- Se cambie el alcance del plan de continuidad de TI.
- Se agreguen o modifiquen procedimientos de control documental.
- Sean establecidas nuevas responsabilidades a los equipos y personal ejecutor del plan de continuidad de TI.
- Se realice incorporaciones y/o restructuración de la infraestructura tecnológica de la institución.
- Se haga incorporaciones y/o cambios en los procesos críticos.
- Se incorpore o actualice tanto el análisis de impacto de negocio o el análisis de riesgo.
- Cualquier cambio que la institución considere pertinente dentro del plan, en conjunto con los colaboradores del área de TIC.

Toda revisión del documento debe hacerse anualmente para verificar su conocimiento y cumplimiento, así como definir cambios que puedan ser requeridos para el plan.

Todo cambio en este documento debe ser resumido en el control de versiones del plan de continuidad de TI y aprobado por el responsable del área de TIC y cualquier otra área que pueda ser impactada con los cambios.

5.11. Capacitación.

Los colaboradores de la organización en general deben conocer el contenido de este plan de continuidad de TI para entender los pasos y tareas que se realiza en caso de una contingencia.

La capacitación formal de las estrategias proactivas, reactivas y de cierre, así como los pasos a seguir dentro de cada uno, deben ser otorgados al personal encargado de ejecutar el plan de continuidad de TI. El alcance de dicha capacitación dependerá de las actividades formales que debe ejecutar cada miembro del equipo.

La capacitación referente a la activación y cierre del plan de continuidad de TI debe realizarse anualmente para todo el personal de la institución, y con respecto al personal encargado de las estrategias proactivas, reactivas y de cierre, debe capacitarse cada vez que se realice un cambio mayor en el plan de continuidad o cada seis meses para validar su conocimiento y cumplimiento.

5.12. Verificación del plan de continuidad.

Se realiza una verificación del plan de continuidad, esto para alcanzar lo establecido en el último objetivo específico.

Por medio de una lista de verificación (Véase Tabla 37), se especifica si cada uno de los pasos que comprende el plan de continuidad es aplicado al momento de presentarse una interrupción en la operación normal de un activo.

Tabla 37 - Verificación del plan de continuidad

Actividad	Completado (Si/No)	Referencia
Notificación inicial.	Sí	Véase 9.9.1
Ejecución de estrategia reactiva.	Sí	Véase 9.9.2
Documentación de bitácora.	Sí	Véase 9.9.3
Cierre de plan de continuidad	Sí	Véase 9.9.4

Fuente: Elaboración propia.

6. Capítulo VI: Conclusiones.

A continuación, se detalla las conclusiones que surgen a través de los resultados obtenidos durante las etapas del procedimiento metodológico que comprende esta investigación. Además, se realiza una recapitulación de los objetivos planteados dentro de este trabajo final de graduación, detallando la metodología y técnicas o instrumentos implementados

6.1. Conclusiones.

A continuación, se abordan las conclusiones del trabajo final de graduación.

- La investigación permite identificar que el 72% de los procesos de negocio que gestionan las áreas operativas son críticos.
- Con respecto a los procedimientos que comprende cada proceso de negocio, el 36% de la totalidad corresponde a actividades que dependen de TIC para su correcta gestión.
- Considerando que un factor clave para determinar la criticidad de un proceso es su dependencia hacia procesos y servicios que brinda el área de TIC, se determina que las TIC tienen una influencia en el 86% de las operaciones de la organización.
- Los procesos críticos de negocio son soportados por el 54% de los sistemas informáticos que gestiona el área de TIC.
- A nivel global, únicamente el 10% de los servidores soportan los sistemas informáticos críticos.
- Los colaboradores de las áreas operativas señalan que el impacto que genera una posible interrupción de la operación de un proceso crítico genera un impacto operativo y financiero dentro de la organización.

- Dentro de los aspectos mínimos para mitigar los riesgos relacionados con TI estimados dentro de la investigación, el área de TIC dentro de sus gestiones cumple el 74% de la totalidad.
- Según la experiencia de los colaboradores del área de TIC, los riesgos que cuentan con mayor nivel de probabilidad de ocurrencia e impacto están relacionados con fallos de *hardware, software* y las comunicaciones.
- Como parte de las estrategias de continuidad de TI, se crearon estrategias proactivas que buscan minimizar una posible interrupción relacionada a las categorías de riesgos de TI contempladas dentro de la investigación.
- Dada la relación existente entre los activos críticos de TI identificados y los riesgos con mayor nivel, permite crear estrategias reactivas enfocadas a restablecer su operación en caso de tener afectación por la materialización de un riesgo.
- Se considera inspecciones puntuales para dar cierre al plan de continuidad de TI, contempla elementos tanto a nivel organizacional como específicos del área de TI, con el objetivo de garantizar el restablecimiento y la continuidad de las operaciones.
- Dentro del plan continuidad de TI se asigna roles y responsabilidades a colaboradores, que permite canalizar equitativamente los esfuerzos.
- El plan de continuidad de TI permite ser gestionado por colaboradores que conocen su rol y se encuentran familiarizados con las responsabilidades interpuestas.
- Dentro del área de TIC existe una alta dependencia hacia colaboradores específicos, esto debido a que cuentan con amplio conocimiento sobre procesos internos del área de TIC y, al no estar documentado, el abandono por parte de alguno de estos colaboradores provocaría una fuga de información importante.

- Debido a que el área de TIC no cuenta con un sitio alterno, imposibilita la creación de estrategias que facilitan mayores alternativas para garantizar la continuidad a los procesos críticos identificados.

6.1.1. Recapitulación de objetivos.

Se muestra un mapeo de los objetivos establecidos para el trabajo final de graduación, se detalla la metodología, técnicas e instrumentos utilizados para lograr los objetivos, y al final se indica si se cumplen los objetivos.

Tabla 38 - Recapitulación de objetivos.

Objetivo	Metodología	Técnica e instrumento	¿Se cumple?
Identificar los procesos críticos de negocio en JASEC y la relación existente con los activos de TI gestionados por el área de TIC.	Análisis de impacto de negocio.	Revisión documental. Cuestionarios. Cuadro de relación. Guía para realizar el análisis de impacto de negocio.	Sí
Determinar los riesgos asociados a los activos de TI de JASEC, considerando su respectivo nivel probabilidad de ocurrencia e impacto.	Análisis de riesgos.	Grupo focal. Cuestionario. Matriz de calor. ISO 31000.	Sí
Preparar las estrategias de respuesta y recuperación necesarias dentro el plan de continuidad para los activos de TI que soportan procesos	Estrategias de continuidad.	Grupo focal. ISO 22301. Manual para el elaborar un plan de continuidad de	Sí

Objetivo	Metodología	Técnica e instrumento	¿Se cumple?
críticos de negocio de JASEC.		la gestión de información y comunicación.	
Validar mediante de la ejecución de una prueba, la efectividad del plan de continuidad para los activos de TI.	Evaluación de las estrategias de continuidad.	Prueba tipo lista de verificación.	Sí

Fuente: Elaboración propia.

7. Capítulo VII: Recomendaciones

Como resultado de realizar este trabajo final de graduación, este capítulo presenta un conjunto de recomendaciones que se brindan a la organización.

- Gestionar revisiones al plan de continuidad de TI con el propósito de validar su cumplimiento con respecto a la situación actual del área de TI.
- Establecer un sitio alterno que permita trasladar las operaciones en caso de que un riesgo mayor se materialice.
- Analizar la implementación de soluciones en la nube que facilite contar con una infraestructura que permita mayor disponibilidad y por consiguiente elevar el valor empresarial de la organización.
- Compartir el plan de continuidad de TI y educar a los colaboradores de las distintas sedes para estandarizar los procesos y la comunicación.
- Crear y gestionar un plan de actualización de activos de TI con el objetivo de disminuir tanto la obsolescencia de los activos como una posible materialización de un riesgo relacionado a hardware o software obsoleto.
- Actualizar la documentación existente, ya que debido al cambio de la estructura organizacional, la nomenclatura usada en muchos documentos no corresponde.
- Incentivar un ambiente organizacional que acerque a las demás áreas operativas a establecer un plan de continuidad de negocio integral.
- Establecer como meta dentro del área de TIC, la creación de un plan de recuperación de desastres.

8. Capítulo VIII: Referencias bibliográficas.

A continuación, se presentan las referencias bibliográficas de los recursos utilizados dentro del trabajo final de graduación.

Abarca, A., Alpízar, F., Rojas, C., & Sibaja, G. (2012). *Técnicas cualitativas de investigación*. San José, Costa Rica: Editorial Universidad de Costa Rica.

Alvarado, D. F., & Zumba, L. A. (2015). *Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para Riesgos aplicado a la Universidad de Cuenca*. Recuperado de http://dspace.ucuenca.edu.ec/handle/123456789/22342 el 12 de Agosto de 2018.

Cienfuegos, I. (2013). Risk Management theory: the integrated perspective and its application in the public sector [*Teoría de la gestión de riesgos: una perspectiva integrada y su aplicación en el sector público*]. Estado, Gobierno, Gestión Pública (21), 89-126.

CCSS (2007). *Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones*. Recuperado de https://www.academia.edu/9225021/Caja_Costarricense_de_Seguro_Social_Tabla_de_Contenidos el 17 de abril de 2015.

Bravo, J. (2008). *Gestión de procesos*. Santiago, Chile: Editorial Evolución S.A.

Hamui, A., Varela, M., (20121). *La técnica de grupos focales*. Recuperado de http://biblioteca.icap.ac.cr/BLIVI/COLECCION_UNPAN/BOL_DICIEMBRE_2013_69/UNED/2012/investigacion_cualitativa.pdf el 6 de agosto del 2018

Hernández, R., Fernández, C. & Baptista, M. (2014). *Metodología de la investigación*. (6a ed.). México: McGraw-Hill.

Huércano (s.f). *ITIL v3 Manual integro*. Extraído de http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf el 6 de setiembre del 2018.

International Organization for Standardization. (2012). 22301: *Sistemas de continuidad del negocio.*

International Organization for Standardization (2011). 31000: *Gestión del riesgo. Principios y directrices*. Colombia: ICONTEC Internacional.

Kirvan P. (2013). *Guía de evaluación de riesgos de TI*. Extraído de https://searchdatacenter.techtarget.com/es/tutoriales/Guia-de-evaluacion-de-riesgos-de-TI el 16 de octubre del 2018.

Kumsuprom, S. (2010). *Structured approach to organisational ICT risk management: An empirical study in Thai businesses*. Recuperado de http://researchbank.rmit.edu.au/view/rmit:7515 el 11 de agosto de 2018.

Livingstone, G (2010). *Business Impact Analysis: The all-important foundation*. Recuperado de http://email.mir3.com/X6b0ncW0N001Gk5Xf000NK0 el 22 de agosto del 2018.

Ministerio Secretaría General de la Presidencia (2016). *Conceptos generales sobre enfoque de procesos de negocios.* Recuperado de https://goo.gl/8Zqx1s el 17 de octubre del 2018.

MINTIC (2015). *Guía para realizar el Análisis de Impacto de Negocios BIA.* Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf el 20 de agosto del 2018.

Rouse, M (2018). *Mapa de riesgos (mapa de calor de riesgos)*. Recuperado de https://searchdatacenter.techtarget.com/es/definicion/Mapa-de-riesgos-mapa-de-calor-de-riesgos

Silvestrini, M. y Vargas, J. (2017). *Fuentes de información primaria, secundaria y terciaria.* Recuperado de http://ponce.inter.edu/cai/manuales/FUENTESPRIMARIA.pdf el 20 de setiembre del 2018.

Steinberg, R. A., Rudd, C., Lacy, S. & Hanna, A. (2011). *ITIL Service Desing,TSO.*

Vargas, I. (2012). *La entrevista en la investigación cualitativa: Nuevas tendencias y retos.* Extraído el 9 de agosto del 2018 de http://biblioteca.icap.ac.cr/BLIVI/COLECCION_UNPAN/BOL_DICIEMBRE_2013_69/UNED/2012/investigacion_cualitativa.pdf

9. Capítulo X: Apéndices.

En este capítulo, se presenta los apéndices que contienen información complementaria.

9.1. Apéndice A: Inventario de TI.

En este apéndice se presenta el inventario de TI actualizado y gestionado por el área de TIC de la organización. Se contempla únicamente los activos involucrados directamente con el plan de continuidad de TI.

9.1.1. Inventario de comunicaciones.

Se detalla el inventario de equipo de comunicaciones existente dentro de la organización.

Inventario de comunicaciones			
Equipo	Cantidad	Tipo de equipo	Ubicación
CISCO- XXXX	1	Switch	Bosque.
CISCO- XXXX	2	Switch	Bosque.
CISCO- XXXX	1	Switch	Oficina Central.
CISCO- XXXX	1	Switch	Oficina Central.
CISCO- XXXX	3	Wireless	Oficina Central.
CISCO- XXXX	3	Switch	Oficina Central.
CISCO- XXXX	1	Switch	Oficina Central.
CISCO- XXXX	1	Switch	Oficina Central.
CISCO- XXXX	1	Switch	Fátima
CISCO- XXXX	1	Switch	Fátima
CISCO- XXXX	10	Switch	Fátima
CISCO- XXXX	1	Wireless	Fátima
CISCO- XXXX	1	Switch	Cerrillos
CISCO- XXXX	1	Router	Unidad ejecutora
CISCO- XXXX	2	Switch	Unidad ejecutora
CISCO- XXXX	1	Router	Birris
CISCO- XXXX	1	Switch	Birris
CISCO- XXXX	1	Router	Birris
CISCO- XXXX	1	Router	Tuis
CISCO- XXXX	1	Switch	Tuis
CISCO-XXXX	2	Switch	Sub-Tejar

9.1.2. Inventario de servidores físicos.

Se detalla el inventario de servidores físicos existentes dentro de la organización.

Inventario de Servidores Físicos.						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
Humanos	Windows 2000 Service Pack 4	Intel® Pentium® 4 CPU 3.20GHz	37.3 GB	2 GB	Aplicativo: • SISRH (Sistema de Recursos Humanos)	Fátima
Financiero	SunOS 5.9 Solaris 9 9/04 s9s_u7wos_09 SPARC	2 procesadores UltraSPARC-IIIi sparcv9 floating point processor 1062 MHz	4 DiscosDuros de 73.40 GB	4 GB	Bases de Datos: • SICURA • SLAM • SIPAC • SISHISTREC • SIF • SAC • SIDEGA	Edificio Central
srvprd11	Oracle Linux Server 7.1	Intel® Xeon® CPU E5-2620 v3 @ 2.40GHz	1 TB	16 GB	Bases de Datos: • SIFAJ • SISRH • SICE • SMI • SWF • SWQ • SISINFO	Edificio Central
srvdes11	Oracle Linux Server 7.1	Intel® Xeon® CPU E5-2620 v3 @ 2.40GHz	1 TB	16 GB	Bases de Datos: • SIFAJ • SISRH • SICE • SMI • SWF • SWQ	Edificio Central

Inventario de Servidores Físicos.						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
					• SISINFO • SIF • SIPAC	
srvsty11	Oracle Linux Server 7.1	Intel® Xeon ® CPU E5-2620 v3 @ 2.40GHz	1 TB	16 GB	Respaldo de la Base de Datos de producción	Cerrillos
DC1JASEC	Windows Server Standard 2008	Intel Xeon 2.00 GHz	146 GB	3 GB	• Active Directory	

9.1.3. Inventario de servidores virtuales.

Se detalla el inventario de servidores virtuales existente dentro de la organización.

Inventario de Servidores Virtuales						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
SRV-APPSORACLE	Windows Server 2008 R2 Service Pack 1	Intel® Xeon ® CPU E5-2665 0 @ 2.40GHz	99.8 GB	4 GB	Aplicativo: • Migrador de Facturas Infocomunicaciones	Edificio Central
SIFAJ_SERVER	Windows Server 2003 R2 Service Pack 2	Intel® Xeon ® CPU E5-2665 0 @ 2.40GHz	145 GB	13 GB	Aplicativos: • SISINFO (Sistema de Infocomunicaciones) • RCAF (Sistema de Reasignación de Costos) • SWQ (Sistema de Quejas) • SIFWEB (Sistema de Consulta del FAG)	Edificio Central

Inventario de Servidores Virtuales						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
					• SISHISTREC (SISTEMA HISTORICO DE RECIBOS) • SISEVA (Sistema Evaluación del desempeño) • SIFAJ_PRUEBAS (Sistema Financiero Administrativo de JASEC de Pruebas) • DCC_PRUEBAS (Sistema de Documentos por Cobrar de Pruebas)	
SRV-SIFAJ	Windows Server 2003 R2 Service Pack 2	Intel® Xeon ® CPU E5-2665 0 @ 2.40GHz	99.9 GB	4 GB	Aplicativos: • SICURA (Sistema de Cumplimiento de la Reglamentación de ARESEP) • SIFAJ (Sistema Financiero Administrativo de JASEC) • SMI (SISTEMA HISTORICO DE RECIBOS)	Edificio Central
SRV-RH	Windows Server 2003 R2 Service Pack 2	Intel® Xeon ® CPU E5-2665 0 @ 2.40GHz	99.9 GB	4 GB	Aplicativo: • SISRH (Sistema de Recursos Humanos)	Edificio Central
JASECSIDEGA	Windows Server 2003 R2 Service Pack 2	Intel® Xeon ® CPU E5-2665 0 @ 2.40GHz	400 GB	4 GB	Aplicativo: • SIPAC (Sistema de Plataforma de Atención al Cliente) • SIF (Fondo de Ahorro, Retiro y Garantías) • SIDEGA • UTILFACT	Edificio Central

Inventario de Servidores Virtuales						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
srv_tarificacion	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• Tarificacion Internet	Edificio central
srv_webinfo	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• Sitio web Infocomunicaciones	Edificio central
srv_webservice	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• Webservice Internet	Edificio central
Cisco WLAN Controller	Linux	Intel Xeon 2.40 GHz	8 GB	2 GB	• Controlador LAN	Edificio central
DC2JASEC	Microsoft Windows 2008 Server Standard	Intel Xeon 2.40 GHz	137 GB	4 GB	• Active Directory	Edificio central
Management	Microsoft Windows 2008 Server Standard	Intel Xeon 2.40 GHz	100 GB	3 GB	• Administración virtualización	Edificio central
nemesis2	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	280 GB	6 GB	• Sitio web Joomla	Edificio central
Nexus VNMC	Linux Red Hat Enterprise 5	Intel Xeon 2.40 GHz	20 GB	2 GB	• Virtual Network Management Center	Edificio central
Nexus VSG	Linux	Intel Xeon 2.40 GHz	3 GB	2 GB	• Virtual Security Gateway	Edificio central
Nexus VSM	Linux	Intel Xeon 2.40 GHz	3 GB	2 GB	• Virtual Supervisor Module	Edificio central
SACDESARROLLO	Microsoft Windows XP Professional	Intel Xeon 2.40 GHz	150 GB	3 GB	• SAC Desarrollo	Edificio central

Inventario de Servidores Virtuales						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
Serv_Sistemas	Microsoft Windows 2008 Server Enterprise	Intel Xeon 2.40 GHz	300 GB	8 GB	• QlikView	Edificio central
SERVER_FACT	Microsoft Windows 2008 Server Standard	Intel Xeon 2.40 GHz	137 GB	4 GB	• SLAM, UtilFact	Edificio central
SEVERSAC	Microsoft Windows 2003 Server Standard	Intel Xeon 2.40 GHz	68 GB	4 GB	• SAC Monitor	Edificio central
siebelserver	Microsoft Windows 2003 Server Enterprise	Intel Xeon 2.40 GHz	230 GB	4 GB	• SIEBEL	Edificio central
srv_apps	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	3 GB	• Apps OMS, UTILFACT	Edificio central
srv_qwizard	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• Sistema de tiquetes	Edificio central
srv_delphos	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	200 GB	4 GB	• Delphos	Edificio central
srv_sacdesarrollo	Microsoft Windows 2008 Server Standard	Intel Xeon 2.40 GHz	100 GB	3 GB	• SAC Desarrollo	Edificio central
srv_energyaxis	Microsoft Windows 2008 Server R2 Enterprise	Intel Xeon 2.40 GHz	1 TB	32 GB	• Energy Axis	Edificio central
srv_energyaxis_db	Microsoft Windows	Intel Xeon 2.40 GHz	1 TB	16 GB	• Oracle Energy Axis	Edificio central

Inventario de Servidores Virtuales						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
	2008 Server R2 Enterprise					
srv_epower	Microsoft Windows 2008 Server Standard	Intel Xeon 2.40 GHz	500 GB	6 GB	• Epower	Edificio central
ftp_inside	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	150 GB	2 GB	• FTP	Edificio central
srv_gis	Linux Ubuntu 12.10	Intel Xeon 2.40 GHz	100 GB	3 GB	• GIS	Edificio central
srv_gisdb	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• SQL Server BD GIS	Edificio central
srv_intranet	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	150 GB	4 GB	• Intranet	Edificio central
srv_kaspersky	Microsoft Windows 2008 Server R2 Enterprise	Intel Xeon 2.40 GHz	100 GB	4 GB	• Kaspersky	Edificio central
srv_kerio_debian	Linux Debian 6	Intel Xeon 2.40 GHz	100 GB	6 GB	• Kerio	Edificio central
srv_ntp	Linux Debian 8	Intel Xeon 2.40 GHz	50 GB	2 GB	• NTP	Edificio central
srv_prime	Microsoft Windows 2008 Server R2 Enterprise	Intel Xeon 2.40 GHz	150 GB	8 GB	• Prime	Edificio central
srv_sacproduccion2	Microsoft Windows 2008 Server Standard	Intel Xeon 2.40 GHz	50 GB	4 GB	• SAC Monitor	Edificio central
srv_prtg	Microsoft Windows	Intel Xeon 2.40 GHz	100 GB	4 GB	• Sistema Monitoreo PRTG	Edificio central

Inventario de Servidores Virtuales						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
	2008 Server R2					
srv_radius	Microsoft Windows 2008 Server Standard	Intel Xeon 2.40 GHz	120 GB	4 GB	• Radius	Edificio central
srv_recovery	Microsoft Windows 2008 Server R2 Standard	Intel Xeon 2.40 GHz	250 GB	4 GB	• Recovery	Edificio central
srv_sacmonitor	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• Desarrollo de SAC Monitor	Edificio central
srv_socket2	Microsoft Windows 2003 Server Standard	Intel Xeon 2.40 GHz	50 GB	4 GB	• Socket SAC	Edificio central
VCS-Vmware	Microsoft Windows 2008 Server R2 Enterprise	Intel Xeon 2.40 GHz	100 GB	4 GB	• VDI	Edificio central
srv_appsoracle	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• Aplicaciones Oracle	Edificio central
srv_ipam	Linux Ubuntu16.04	Intel Xeon 2.40 GHz	50 GB	2 GB	• IPAM Infocomunicaciones	Edificio central
srv_ion	Microsoft Windows XP Professional	Intel Xeon 2.40 GHz	50 GB	3 GB	• ION Despacho	Edificio central
monitoreo_enlaces	Microsoft Windows 7 Profesional	Intel Xeon 2.40 GHz	60 GB	4 GB	• Monitoreo enlaces Canopy	Edificio central
srv_historiador	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• Historiador Despacho	Edificio central

Inventario de Servidores Virtuales						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
srv_sesuite	Microsoft Windows 2012 Server	Intel Xeon 2.40 GHz	100 GB	8 GB	• SE Suite Riesgos	Edificio central
srv_gstarcad	Microsoft Windows 2012 Server	Intel Xeon 2.40 GHz	50 GB	2 GB	• GStarCAD	Edificio central
kiwisyslog	Microsoft Windows 7 Profesional	Intel Xeon 2.40 GHz	50 GB	2 GB	• Syslog Kiwi	Edificio central
srv_apex	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• Apex	Edificio central
srv_apipro	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	100 GB	8 GB	• ApiPro Birris	Edificio central
srv_socketmetropoli	Microsoft Windows 2008 Server Standard	Intel Xeon 2.40 GHz	50 GB	4 GB	• Socket SAC	Edificio central
srv_wsus	Microsoft Windows 2012 Server R2	Intel Xeon 2.40 GHz	400 GB	6 GB	• WSUS	Edificio central
vCenter_appliance	Linux SUSE Enterprise 11	Intel Xeon 2.40 GHz	125 GB	8 GB	• vCenter	Edificio central
vCenter_vsc	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	50 GB	4 GB	• Virtual Storage Console	Edificio central
srv_acm	Linux	Intel Xeon 2.40 GHz	20 GB	4 GB	• Central Telefonica	Edificio central
srv_altus	Microsoft Windows 7 Profesional	Intel Xeon 2.40 GHz	100 GB	4 GB	• Central Telefonica	Edificio central
srv_aqm	Linux	Intel Xeon 2.40 GHz	20 GB	4 GB	• Central Telefonica	Edificio central

Inventario de Servidores Virtuales						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
srv_cucm-p1	Linux Red Hat Enterprise 6	Intel Xeon 2.40 GHz	80 GB	6 GB	• Central Telefonica	Edificio central
srv_cucm-s1	Linux Red Hat Enterprise 6	Intel Xeon 2.40 GHz	80 GB	6 GB	• Central Telefonica	Edificio central
srv_ewc	Linux	Intel Xeon 2.40 GHz	132 GB	6 GB	• Central Telefonica	Edificio central
srv_ewe	Linux	Intel Xeon 2.40 GHz	132 GB	6 GB	• Central Telefonica	Edificio central
srv_imp1	Linux Red Hat Enterprise 6	Intel Xeon 2.40 GHz	80 GB	4 GB	• Central Telefonica	Edificio central
srv_imp2	Linux Red Hat Enterprise 6	Intel Xeon 2.40 GHz	80 GB	4 GB	• Central Telefonica	Edificio central
srv_management	Microsoft Windows 7 Profesional	Intel Xeon 2.40 GHz	100 GB	4 GB	• Central Telefonica	Edificio central
srv_motorgrabacion	Linux CentOS 6	Intel Xeon 2.40 GHz	120 GB	4 GB	• Central Telefonica	Edificio central
srv_socialminer	Linux Red Hat Enterprise 6	Intel Xeon 2.40 GHz	160 GB	8 GB	• Central Telefonica	Edificio central
srv_uccx1	Linux Red Hat Enterprise 6	Intel Xeon 2.40 GHz	292 GB	10 GB	• Central Telefonica	Edificio central
srv_uccx2	Linux Red Hat Enterprise 6	Intel Xeon 2.40 GHz	146 GB	10 GB	• Central Telefonica	Edificio central
srv_unity1	Linux Red Hat Enterprise 6	Intel Xeon 2.40 GHz	160 GB	4 GB	• Central Telefonica	Edificio central
srv_unity-ha	Linux Red Hat Enterprise 6	Intel Xeon 2.40 GHz	160 GB	4 GB	• Central Telefonica	Edificio central
srv_socketjasec	Microsoft Windows 2008 Server R2	Intel Xeon 2.40 GHz	50 GB	4 GB	• Socket SAC	Edificio central
srv_app-public	Microsoft Windows 2012 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• App Externo	Edificio central
srv_factelectronica	Microsoft Windows	Intel Xeon 2.40 GHz	100 GB	4 GB	• Factura Electronica	Edificio central

Inventario de Servidores Virtuales						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
	2012 Server R2					
srv_horizon-secure	Microsoft Windows 2012 Server R2	Intel Xeon 2.40 GHz	100 GB	6 GB	• Horizon Secure	Edificio central
srv_web	Microsoft Windows 2012 Server R2	Intel Xeon 2.40 GHz	150 GB	8 GB	• Web Wordpress	Edificio central
EMS-Aurora	Microsoft Windows 7 Profesional	Intel Xeon 2.40 GHz	465 GB	3 GB	• Aurora Infocomunicaciones	Edificio central
srv_app-jasec	Microsoft Windows 2012 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• App interno	Edificio central
srv_areva	Microsoft Windows XP Professional	Intel Xeon 2.40 GHz	50 GB	3 GB	• AREVA Despacho	Edificio central
srv_argos	Microsoft Windows 2012 Server R2	Intel Xeon 2.40 GHz	150 GB	6 GB	• Argos Auditoria	Edificio central
srv_argosdb	Microsoft Windows 2012 Server R2	Intel Xeon 2.40 GHz	250 GB	6 GB	• BD Argos Auditoria	Edificio central
srv_cert	Microsoft Windows 2008 Server Standard	Intel Xeon 2.40 GHz	100 GB	4 GB	• Certificado Cisco Jabber	Edificio central
srv_gestiondoc	Microsoft Windows 2012 Server R2	Intel Xeon 2.40 GHz	100 GB	4 GB	• Gestión Documental	Edificio central
srv_horizon	Microsoft Windows	Intel Xeon 2.40 GHz	100 GB	16 GB	• Horizon View	Edificio central

Inventario de Servidores Virtuales						
Equipo	Sistema Operativo	Procesador	Disco Duro	RAM	Funcionalidad	Ubicación
	2012 Server R2					
srv_intelli	Microsoft Windows 10	Intel Xeon 2.40 GHz	50 GB	4 GB	• Intelli Despacho	Edificio central
srv_powerscape	Microsoft Windows 7 Profesional	Intel Xeon 2.40 GHz	100 GB	4 GB	• PowerScape	Edificio central
srv_terminal	Microsoft Windows 2012 Server R2	Intel Xeon 2.40 GHz	100 GB	8 GB	• Terminal Services	Edificio central
vCenter_App_VDI	Linux SUSE Enterprise 11	Intel Xeon 2.40 GHz	300 GB	24 GB	• vCenter VDI	Edificio central

9.1.4. Inventario de aplicativos.

Se detalla el inventario de sistemas informáticos o aplicativos existentes dentro de la organización.

Inventario de sistemas informáticos.					
Sistema	**Módulos**	**Herramienta de desarrollo**	**Servidor de base de datos**	**Ubicación**	**Dueño**
SICURA	-	-	FINANCIERO (Instancia SICURA) Equipo marca SUN V440 ORACLE 9i	Centro de Datos Edificio Central	Depto GSMD
Recursos Humanos	-	-	srvprd11 Equipo marca Dell Power Edge R430 ORACLE 10g	Centro de Datos Edificio Central	Depto GSMD
SLAM	-	-	FINANCIERO (Instancia SICURA) Equipo marca SUN V440 ORACLE 9i	Centro de Datos Edificio Central	Depto GSMD BD

Inventario de sistemas informáticos.					
Sistema	**Módulos**	**Herramienta de desarrollo**	**Servidor de base de datos**	**Ubicación**	**Dueño**
SAC	-	-	FINANCIERO (Instancia JASEC) Equipo marca SUN V440 ORACLE 9i	Centro de Datos Edificio Central	Depto GSMD BD
SIFAJ	-	-	srvprd11 Equipo marca Dell Power Edge R430 ORACLE 10g	Centro de Datos Edificio Central	Depto GSMD
SIPAC	-	-	FINANCIERO (Instancia JASEC) Equipo marca SUN V440 ORACLE 9i	Centro de Datos Edificio Central	Depto GSMD
SIF	-	-	FINANCIERO (Instancia JASEC) Equipo marca SUN V440 ORACLE 9i	Centro de Datos Edificio Central	Depto GSMD
SISHISTREC	-	-	FINANCIERO (Instancia JASEC) Equipo marca SUN V440 ORACLE 9i	Centro de Datos Edificio Central	Depto GSMD
SIDEGA	-	-	FINANCIERO (Instancia JASEC) Equipo marca SUN V440 ORACLE 9i	Centro de Datos Edificio Central	Depto GSMD BD
RECAF	-	-	srvprd11 Equipo marca Dell Power Edge R430 ORACLE 10g	Centro de Datos Edificio Central	Depto GSMD
SISEVA	-	-	srvprd11 Equipo marca Dell Power Edge R430 ORACLE 10g	Centro de Datos Edificio Central	Depto GSMD
SISINFO	-	-	srvprd11 Equipo marca Dell Power Edge R430 ORACLE 10g	Centro de Datos Edificio Central	Depto GSMD

Inventario de sistemas informáticos.					
Sistema	**Módulos**	**Herramienta de desarrollo**	**Servidor de base de datos**	**Ubicación**	**Dueño**
SWF	-	-	srvprd11 Equipo marca Dell Power Edge R430 ORACLE 10g	Centro de Datos Edificio Central	Depto GSMD BD
SWQ	-	-	srvprd11 Equipo marca Dell Power Edge R430 ORACLE 10g	Centro de Datos Edificio Central	Depto GSMD
SMI	-	-	srvprd11 Equipo marca Dell Power Edge R430 ORACLE 10g	Centro de Datos Edificio Central	Depto GSMD
SICE	-	-	FINANCIERO (Instancia JASEC) Equipo marca SUN V440 ORACLE 9i	Centro de Datos Edificio Central	Depto GSMD BD
Migrador	-	-	Virtual BD MySQL	Centro de Datos Edificio Central	Depto GSMD
DELPHOS	-	-	Virtual	Centro de Datos Edificio Central	Depto Planificación Institucional
SIJ	-	-	Equipo marca SUN modelo E250	Centro de Datos	Depto GCR

9.2. Apéndice B: Procesos y procedimientos del área de TIC.

En este apéndice se detallan los procesos y procedimientos por departamentos funcionales del área de tecnologías de información y comunicación de JASEC.

9.2.1. Gestión de la arquitectura y comunicaciones.

A continuación, se detalla cada uno de los procesos del departamento funcional con sus respectivos procedimientos.

Procesos por Departamento.	
Departamento	Gestión de la arquitectura y comunicaciones.
Proceso	**Procedimiento.**

Comunicaciones	• Dar asistencia a:
	  ○ Central Telefónica.
	  ○ Equipo Activo.
	  ○ Enlaces (con Birrís y Bancos).

	• Mantener la operación continua, de la red de comunicaciones (intranet, extranet) de JASEC, así como de las estaciones de trabajo, servidores, sistemas de comunicación, sitios Web.

Mantenimiento	• Se da mantenimiento, tanto en hardware como en software a los siguientes componentes:
	  ○ Computadoras personales.
	  ○ Servidores.
	  ○ Cableado.

	• El mantenimiento abarca antivirus, sistema operativo, software de sistemas, correo electrónico, internet, entre otros.
	• Mantener y optimizar los diferentes ambientes computacionales con que cuente JASEC.
	• Monitorear y efectuar los ajustes pertinentes a los diferentes sistemas operativos y evaluar su eficiencia operativa.
	• Ejecutar los procedimientos de respaldo, recuperación y restauración de las diferentes bases de datos de los sistemas de información en producción que utilicen esta tecnología.

Procesos por Departamento.	
Departamento	Gestión de la arquitectura y comunicaciones.
Proceso	**Procedimiento.**
	• Dar el seguimiento adecuado a la red para evitar saturación y caídas por falta de recursos en los servidores respectivos.
Aplicaciones	• Dar soporte de primera línea a las siguientes aplicaciones: o Sistemas (recaudadores en línea y desconectadas). o Intranet. o Internet.
Administración	• Llevar a cabo el control de las actividades administrativas que conllevan el soporte técnico.
Seguridad	• Administrar permisos, control de accesos y evitar ataques maliciosos a la red.

9.2.2. Gestión de calidad y riesgos.

A continuación, se detalla cada uno de los procesos del departamento funcional con sus respectivos procedimientos.

Procesos por Departamento.	
Departamento	Gestión de calidad y riesgos.
Proceso	**Procedimiento.**
Proyectos de apoyo	• Realizar investigaciones para determinar la factibilidad de un proyecto y para el diseño, desarrollo, implantación y mantenimiento de sistemas de información y desarrollo de programas o de aplicaciones específicas.
	• Recopilar y analizar la información del sistema o aplicación que se desarrollará para la respectiva unidad organizacional.

Procesos por Departamento.	
Departamento	Gestión de calidad y riesgos.
Proceso	**Procedimiento.**
	• Determinar la estructura lógica y física de sistemas de información o aplicación y determinar el tipo de organización, métodos de acceso y otros elementos conexos.
	• Describir los diversos programas que constituyen un sistema de información, según las normas y otros estándares vigentes en el área de Tecnologías de Información
	• Hacer reportes de control.
	• Preparar la documentación del sistema de información tanto en el nivel técnico como en el de usuario, según las normas y estándares vigentes en el área de Tecnologías de Información.
	• Capacitar al usuario en el uso del sistema de información.
	• Brindar mantenimiento a sistemas de información y efectuar los ajustes necesarios durante su periodo de vigencia.
	• Crear procedimientos de definición de archivos y depurar catálogos.
	• Analizar respaldos y la recuperación de los diccionarios y prever situaciones anómalas.
	• Identificar, resolver y documentar terminaciones anormales del sistema en producción.

9.2.3. Gestión de sistemas, mantenimiento y desarrollo.

A continuación, se detalla cada uno de los procesos del departamento funcional con sus respectivos procedimientos.

Procesos por Departamento.	
Departamento	Gestión de la sistemas, mantenimiento y desarrollo.
Proceso	**Procedimiento.**
Proyectos sustantivos**.**	• Brindar recomendaciones acerca del desarrollo de sistemas de información en el área de Servicios Sustantivos.
	• Desarrollo en la contratación de los sistemas de información aplicables para las distintas dependencias de la Institución (encargado de los proyectos sustantivos de JASEC). Actualmente en el software de distribución eléctrica, en el de producción y área de servicio al cliente.
	• Elaborar estándares y procedimientos para el desarrollo de sistemas de información. Generalmente los procedimientos son elaborados por personal que no es de JASEC, es decir, personal contratado y no propio de la institución.
	• Administrar los sistemas que se utilizan en JASEC.
	• Contratar consultoría para la implementación de sistemas en el área de distribución eléctrica.
	• Asesorar a las dependencias de JASEC en el tema de los sistemas de información para el área de proyectos sustantivos.
	• Adquisición de licencias de desarrollo ORACLE, con el fin de dar el mantenimiento adecuado a los diferentes sistemas desarrollados y para el desarrollo de nuevos sistemas.

9.3. Apéndice C: Revisión documental - Estado actual.

En este apéndice se a modo resumen los documentos encontrados como parte de la revisión documental realizada dentro de la organización.

9.3.1. Formularios

Un formulario corresponde a un documento ya sea físico o digital que permite a un usuario introducir datos de forma estructurada, facilitando ser procesado y almacenado.

Nombre	Detalle
Control de cambios de sistemas en producción.	Corresponde a un formulario que documenta todas las actividades necesarias para aplicar un cambio en los sistemas que se encuentran en producción, dicho formulario contempla aspectos que deben ser detallados, como, por ejemplo, la solicitantes y responsables de la aprobación del cambio, análisis de los riesgos que implica y los planes de retorno, aprobación, implementación y post implementación.
Plan anual de mantenimiento preventivo.	Formulario que permite documentar información de control sobre los mantenimientos preventivos realizados a lo largo de un año, especificando los responsables de efectuarlo y las fechas agendadas para su aplicación.
Solicitud de cuentas y acceso a sistemas.	Facilita la documentación de información sobre las personas que realizan solicitudes de acceso a sistemas, detallando datos personales del solicitante y los sistemas que desea tener acceso.
Solicitud de cambios en la intranet.	Permite documentar información sobre las personas que realizan solicitudes de cambios en la intranet, detallando datos personales del solicitante, tipo de cambio y quienes autorizan dicho cambio.

Nombre	Detalle
Reporte de falla de sistema.	Formulario que facilita documentar información sobre las personas que realizan el reporte y la descripción de este. Además, permite documentar los datos del colaborador que recibe y atiende el reporte.

9.3.2. Instructivo.

Un instructivo corresponde a un documento que especifica una seria de instrucciones que permite a un usuario, actuar de acuerdo como es requerido según la una determinada situación.

Nombre	Detalle
Incidencias en los equipos y sistemas informáticos.	Establecer las actividades a seguir para realizar la solicitud y resolución de incidencias en los sistemas y equipos informativos.
Mantenimiento de servidores físicos y virtuales.	Establece las acciones a seguir para llevar a cabo el mantenimiento de los servidores tanto físicos como virtuales que gestiona el área de TIC.
Monitoreo de los servicios de la red informática.	Constituye las actividades a seguir para realizar el monitorio de los servicios de la red informativa e infraestructura de TI.
Seguimiento y medición de los procesos del área de TIC.	Establece los indicadores de gestión que permiten evaluar el grado de cumplimiento de los objetivos y metas del área de TIC.

Nombre	Detalle
Mantenimiento de los sistemas de seguridad de la red informática.	Detalla las acciones a seguir para realizar el mantenimiento de los sistemas de seguridad de la informática.
Respaldo y recuperación de información de base de datos Informix y Oracle.	Constituye las actividades necesarias para realizar un respaldo y recuperación de las bases de datos Informix y Oracle.

9.3.3. Normativas.

Corresponde a una forma documentada de lineamientos que deben ser seguidos y aplicados dentro de las gestiones que desarrollan los colaboradores.

Nombre	Detalle
Marco Normativo de la Política de Seguridad de la Información.	Presenta los lineamientos de seguridad de la información para que sea aplicada por el personal interno y externo de la JASEC, y por los actuales y potenciales clientes y proveedores.
Política de Uso del Correo Electrónico.	Norma lo relacionado a la gestión los correos electrónicos que son emitidos desde JASEC o alguno de sus funcionarios o colaboradores en general a nombre de JASEC y destinados al público en general.
Política de instalación y acreditación de soluciones y cambios.	Establece los lineamientos para administrar, planificar y controlar la instalación y acreditación de soluciones y cambios, con el fin de garantizar la integridad y seguridad del ambiente de Producción y su plataforma tecnológica física y lógica.

Nombre	Detalle
Política de administración de cambios.	Establece los lineamientos para asegurar y administrar la solicitud, análisis, diseño, revisión y aprobación de los cambios al software y sistemas de información de JASEC.
Política de contratación de terceros.	Constituye los lineamientos y compromisos compartidos en la JASEC referente a la contratación de terceros, la cual le permitirá actuar proactivamente ante situaciones que podrían comprometer su integridad.

9.4. Apéndice D: Cuestionario para identificar procesos críticos.

En este apéndice se incluyen los cuestionarios aplicados dentro del análisis BIA a los jefes de las áreas operativas de JASEC con el objetivo de identificar los procesos críticos.

9.4.1. Cuestionario aplicado al área de Distribución.

Cuestionario aplicado al jefe del área de distribución con el objetivo de identificar los procesos críticos.

Cuestionario

El objetivo de este cuestionario es determinar los procesos y actividades criticas gestionadas dentro de su área operativa.

Marque con una X el procedimiento que considere critica dentro de las operaciones del área que lidera.

Nota: Considere como un factor de criticidad se determina por la dependencia del procedimiento hacia ejecutarse de forma automática por medio de un sistema informático.

Proceso	Procedimiento	Critico
Mejoras a la Red Distribución Eléctrica	• Reporte de Cliente, registrado en Reporte de mantenimiento de Red.	X
	• Se programa la inspección	
	• Se ejecuta la inspección y se realiza croquis de situación actual.	
	• Se analiza croquis de situación actual y se elabora croquis de situación propuesta de mejora.	
	• Se analiza y se realizan correcciones sobre el croquis de la situación propuesta.	
	• Con el croquis aprobado se abre el expediente para la mejora.	
	• Se programa y ejecuta la mejora.	
	Se supervisa y ejecutan las correcciones necesarias sobre la mejora.	
	• Terminada la obra se registra reporte de obras realizadas en la OTC.	
	• Se inspecciona y ejecutan las correcciones necesarias sobre la obra terminada.	
	• Satisfecha la obra, se registra el formulario de levantamiento de montajes y/o materiales instalados, desmantelados o reubicados en la red de distribución eléctrica.	
	• Se devuelven materiales.	X
	• Se ejecuta trámite de pago si el trabajo lo realizó un contratista.	X
	• Se liquidan materiales, si hay diferencias se analizan y se realizan las gestiones necesarias para corregirlas.	X
	• Se entrega copia del levantamiento para que se registre, previa inspección, la información en el Sistema de Información Geográfica (GIS).	X
	• Se almacenan los documentos relacionados	

Proceso	Procedimiento	Critico
Daños a la Red de Distribución Eléctrica.	• Se produce y reporta un daño en la red de distribución eléctrica.	X
	• Si daño es producido por un tercero se recolecta su información.	
	• Se abre expediente y se asigna cuadrilla para reparar daño.	
	• Se analiza magnitud del daño y materiales para solucionarlo.	
	• Si el daño afectó alumbrado público, se ejecutan acciones para analizar el estado y proceso de atención.	
	• Se analiza la existencia de materiales para solucionar el problema, si no hay suficientes se solicita requisición.	
	• Se asigna el tipo cuenta por cobrar, según corresponda.	
	• Se establece y realiza la conexión de los puntos donde se puede reestablecer el servicio eléctrico.	
	• Se ejecuta reparación del daño en la red de distribución eléctrica.	
	• Se supervisa y ejecutan las correcciones necesarias sobre el daño.	
	• Se concluye reparación, Terminada la obra se registra reporte de obras realizadas en la OTC.	
	• Se inspecciona y ejecutan las correcciones necesarias sobre la obra terminada.	
	• Satisfecha la obra, se ejecutan las acciones para reestablecer el servicio en el resto de la zona.	
	• Se verifica el restablecimiento del servicio eléctrico, corrigiendo cualquier problema.	
	• Se registra el formulario de levantamiento de montajes y/o materiales instalados, desmantelados o reubicados en la red de distribución eléctrica.	
	• Se devuelven materiales, analizando y ajustando cualquier diferencia.	X
	• Si el daño fue causado por tercero se ejecutan las acciones administrativas y legales para el cobro correspondiente.	
	• Se realiza la liquidación del material analizando y ajustando cualquier diferencia.	X
	• Se entrega copia del levantamiento para que se registre, previa inspección, la información en el Sistema de Información Geográfica (GIS).	X
	• Se almacenan los documentos relacionados.	
Atender Averías	• Cliente reporta la avería en las líneas de distribución.	X
	• Se registra reporte de averías y determina la prioridad de atención.	X

Proceso	Procedimiento	Critico
	• Se programa reparación y asigna la Cuadrilla de Averías.	
	• Se realiza diagnóstico, que determina si la cuadrilla de averías puede reparar el daño o no, según magnitud de la avería.	
	• Si la cuadrilla no puede repararlo, se pasa el caso a las cuadrillas de mantenimiento.	
	• Si la cuadrilla de averías puede solucionar la avería, realiza el trabajo, determinando previamente si cuenta con los materiales o necesitarán elaborar la requisición.	
	• Se reporta solución del problema, registrándola en el reporte de averías.	X
	• Se realiza inspección, y se realizan las correcciones necesarias, registrando las observaciones en el reporte de averías.	
	• Cuando el trabajo está conforme a las especificaciones técnicas, se verifica la cantidad de material utilizado contra la cantidad de material reportado, si a diferencias se realizan las gestiones del caso para corregirlas.	
	• Si no es fin de mes se almacenan los documentos relacionados. Si es fin de semana se elabora liquidación de materiales, corrigiendo cualquier diferencia.	X
	• Se realiza la liquidación de material analizando y ajustando cualquier diferencia.	X
	• Se entrega copia del levantamiento para que se registre, previa inspección, la información en el Sistema de Información Geográfica (GIS).	X
	• Se almacenan los documentos relacionados.	
Limpieza de Líneas	• Se reporta la presencia de escombros en las líneas de distribución eléctrica.	X
	• Se registra reporte.	
	• Se realiza inspección si se considera necesario.	
	• Se solicita los permisos necesarios en los casos que la limpieza se deba realizar en zonas protegidas o privadas.	X
	• Se programa el trabajo, planificando si es necesario realizar suspensión del servicio, si esto es necesario se ejecuta según procedimiento.	
	• Se realiza la limpieza de líneas.	
	• Se registra reporte de mano de obra de trabajos realizados OTC.	
	• Se realiza inspección, y se realizan las correcciones necesarias registrando las observaciones en el reporte de mano de obra de trabajos realizados OTC.	

Proceso	Procedimiento	Critico
	• Se almacenan los documentos relacionados.	
Control de inventarios	• Se programa la Cuadrilla del Proceso POMS para el levantamiento físico del inventario.	
	• Se realiza el levantamiento de los materiales en el camión y en la bodega de mantenimiento.	
	• Si existen materiales del inventario que no se han requisado se solicita la elaboración de la requisición (es) para reponer los materiales.	X
	• Se revisa el estado del inventario inicial, el material gastado, el material requisado y el inventario final.	X
	• Se registra el formulario de inventario de materiales a cuadrilla de mantenimiento y se determina si faltan o sobran materiales y se envía copia.	
	• Se realizan las gestiones para corregir los sobrantes o faltantes encontrados.	X
	• Se corrigen las diferencias en el inventario.	
	• Se notifica la justificación del faltante o sobrante de materiales.	
	• Se decide si se aumenta o disminuye la cantidad de materiales del inventario.	X
	• Se elabora el informe del estado del inventario.	
	• Se almacenan los documentos relacionados.	X
Reparaciones en Propiedad Privada	• Cliente solicita reparación.	
	• Se recibe y firma solicitud presentada por el cliente.	
	• Se analiza la solicitud, si la misma no cumple con los aspectos de forma, se notifica al cliente, para que éste los corrija.	
	• Las solicitudes correctas son estudiadas para analizar si se aprueba o no la solicitud; si no es aprobada se le notifica al cliente dándole las razones del caso y se archiva la solicitud; si es aprobada se abre expediente por la reparación.	
	• Se realiza inspección.	
	• Se solicita elaboración de requisiciones.	
	• Se solicita por escrito el presupuesto por la reparación.	
	• Se le informa al cliente el costo de la reparación. Si el cliente decide no realizar reparación se almacena la información en el expediente de reparaciones no realizadas.	X

Proceso	Procedimiento	Critico
	• Si el cliente decide hacer reparación, puede cancelar de contado, para ello cancela el monto en la UEN SCL, la cual realiza un recibo que entrega al cliente con una copia para al Proceso POMS; o puede cancelar el monto cargándolo al recibo, para ello se entrega copia del expediente a la UEN SCL, la cual inicia con los cargos por la reparación al recibo del Cliente y notifica al Proceso POMS.	
	• Se programa reparación.	
	• Se realiza la reparación y se llena el reporte de mano de obra de trabajos realizados OTC.	
	• Se inspecciona y ejecutan las correcciones necesarias sobre la obra terminada.	
	• Satisfecha la obra, se registra el formulario de levantamiento de montajes y/o materiales instalados, desmantelados o reubicados.	
	• Se devuelven materiales.	X
	• Si se superó o se utilizó menos de lo presupuestado, se le notifica al cliente, si es necesario se solicita por escrito presupuesto. Si el cliente cancela por medio recibo se le notifica a la UEN SCL para que ésta ejecute los trámites del caso, en el recibo. Si el cliente cancela de contado la UEN SCL realiza recibo con el cobro o devolución del dinero, enviando una copia al Proceso POMS.	X
	• Se realiza la liquidación de material analizando y ajustando cualquier diferencia.	
	• Se almacenan los documentos relacionados.	
Cambio de Aceite	• Se toman las muestras de aceite en los equipos de la Subestación y se elabora el informe de análisis de aceite.	
	• Se analiza el informe del estado del aceite de los equipos de la Subestación y se determinan si el aceite se encuentra dentro de los parámetros aceptados.	
	• Si las muestras de aceite no se encuentran dentro de los parámetros aceptados se programa y asigna la Cuadrilla del Proceso POMS para realizar el cambio de aceite.	
	• Se solicita la elaboración de la requisición.	X
	• Si es necesario, se planifica y ejecuta, según el procedimiento, la suspensión del servicio eléctrico.	
	• Se realiza el cambio de aceite.	
	• Se inspecciona y ejecutan las correcciones necesarias.	X
	• Satisfecha la obra, se registra el reporte de mano de obra de trabajos realizados OTC.	

Proceso	Procedimiento	Critico
	• Se coloca el aceite en mal estado en estañones y lo entrega al Centro de Control El Bosque.	
	• Se elabora el reporte del estado del aceite en la Subestación, entregando copias a la UEN de Distribución y Coordinador del Proceso POMS.	
	• Se almacenan los documentos relacionados.	
Mantenimiento de Subestaciones y Patio de Interruptores	• Se programa la inspección de campo a la Subestación Reductora o al Patio de Interruptores.	
	• Se realiza la inspección de campo, revisa el estado de la Subestación Reductora o del Patio de Interruptores y realiza la termografía.	
	• Se registra el reporte de inspección visual en subestaciones y determina si se encuentra en buenas condiciones, si las hay se elabora el informe del estado de la Subestación reductora o del Patio de interruptores. Si no hay buenas condiciones se asigna a la Cuadrilla del Proceso POMS o al Contratista para realizar los trabajos.	X
	• Se solicita la elaboración de la requisición.	X
	• Si es necesario, se planifica y ejecuta, según el procedimiento, la suspensión del servicio eléctrico.	
	• Se inicia el trabajo.	
	• Se supervisa y ejecutan las correcciones necesarias sobre la mejora.	X
	• Terminada la obra se registra reporte de obras realizadas en la OTC.	
	• Se inspecciona y ejecutan las correcciones necesarias sobre la obra terminada.	
	• Satisfecha la obra, se registra el formulario de levantamiento de montajes y/o materiales instalados, desmantelados o reubicados en la red de distribución eléctrica.	X
	• Se devuelven materiales.	X
	• Se ejecuta el trámite de pago si el trabajo lo realizó un contratista.	X
	• Se liquidan materiales, si hay diferencias se analizan y se realizan las gestiones necesarias para corregirlas.	
	• Si se instalaron, reubicaron o desmantelaron activos, se entrega copia del levantamiento para que se registre, previa inspección, la información en el Sistema de Información Geográfica (GIS).	
	• Se elabora el informe del estado de la Subestación Reductora o del Patio de Interruptores, entregando copia del informe al Subgerente, al Líder de la UEN de Distribución y al Coordinador del Proceso POMS.	

Proceso	Procedimiento	Critico
	• Se almacenan los documentos relacionados.	X
Mejoras de Voltaje	• El Cliente reporta las fluctuaciones de corriente.	
	• Se registra reporte de mantenimiento de la red.	
	• Se programa equipo analizador de redes y la inspección de campo.	
	• Se realiza la inspección de campo e instala el equipo analizador de redes, se elabora el croquis de la situación actual.	
	• Se retira el equipo analizador de redes eléctricas.	
	• Se analiza el croquis de la situación actual y el resultado del equipo analizador de redes.	
	• Si no existe ningún problema se le notifica al cliente, explicando las causas, se almacena la documentación relacionada en el archivo de mejoras de voltaje no aprobadas.	
	• Si no existen problemas de voltaje, pero existe otro tipo de problemas se debe proceder conforme con el procedimiento de Daños a la red de distribución eléctrica.	
	• Si existen problemas de voltaje se elabora el croquis de la propuesta de mejora y define los materiales a utilizar.	
	• Se analiza la propuesta de la mejora de voltaje. Si no es aprobada se corrige.	
	• Una vez aprobada la propuesta se abre un expediente exclusivo para la mejora de voltaje.	
	• Se programa mejora y asigna cuadrilla.	
	• Se solicita la elaboración de la requisición.	X
	• Si es necesario, se planifica y ejecuta, según el procedimiento, la suspensión del servicio eléctrico.	
	• Se inicia el trabajo	
	• Se supervisa y ejecutan las correcciones necesarias sobre la mejora.	
	• Si el trabajo no cumple las especificaciones se registra por medio de un reporte de mano de obra de trabajos realizados OTC, se instala y posteriormente se retira el equipo analizador de redes, se analizan sus resultados, si éstos se encuentran fuera de rango se inicia el proceso de mejora.	
	• Si los rangos están según especificaciones se realiza inspección final, corrigiendo cualquier anomalía.	
	• Satisfecha la obra, se registra el formulario de levantamiento de montajes y/o materiales instalados, desmantelados o reubicados en la red de distribución eléctrica.	

Proceso	Procedimiento	Critico
	• Se devuelven materiales.	X
	• Se ejecuta trámite de pago si el trabajo lo realizó un contratista.	X
	• Se liquidan materiales, si hay diferencias se analizan y se realizan las gestiones necesarias para corregirlas.	
	• Se entrega copia del levantamiento para que se registre, previa inspección, la información en el Sistema de Información Geográfica (GIS).	
	• Se almacenan los documentos relacionados.	X
Reclamo por Daños en Propiedad Privada	• Se recibe la notificación del reclamo por el daño de la UEN SCL.	
	• Se programa la inspección de campo y se asigna al personal.	
	• Se solicita información del evento (daño), y se realiza inspección.	
	• Se realiza el estudio técnico y se llena el formulario del estudio técnico de reclamos por daños.	
	• Se envía el estudio a UEN SCL, quién lo comunica al cliente. Si el cliente no está de acuerdo presenta apelación por escrito en la UEN SCL, quién la envía al Proceso POMS.	
	• En el proceso POMS vuelve a revisar expediente. Si no se acepta apelación se justifica recomendación anterior, si se acepta apelación se corrige el estudio técnico y la recomendación brindada y se envía la respuesta de la apelación presentada por el Cliente a la UEN SCL.	
	• Se almacenan los documentos relacionados.	
Suspensiones Programadas del Servicio Eléctrico	• Si la suspensión es solicitada por Proceso POMS, el Profesional y el Técnico del Proceso POMS detectan la necesidad la solicitan informando a los involucrados. Se realiza la inspección de campo y se determina las maniobras a realizar. Se elabora la nota de maniobras y se asigna al personal	
	• Si la suspensión es solicitada por un cliente (interno), solicita por escrito la solicitud de suspensión y realización de maniobras, y realiza aviso a los abonados afectados. Se realiza la inspección de campo y se determina las maniobras a realizar. Se elabora la nota de maniobras y se asigna al personal	
	• Se recibe la nota de maniobras y se programa al personal para realizarlas	
	• Se entrega la nota de maniobras a todos los involucrados y protocolo a los Encargados de Cuadrilla, se verifica esta entrega, si la misma no se ha dado se facilita la documentación respectiva al personal técnico involucrado	X

Proceso	Procedimiento	Critico
	• Si no se encuentran los sitios de maniobra si decide si se continúa o no con el proceso, si no se continúa se comunica al personal y esperan a que se encuentre en los puntos indicados.	X
	• Si se está en los puntos indicados se realiza la coordinación de las maniobras para la suspensión del servicio eléctrico	
	• Si la suspensión del servicio eléctrico es solicitada por el Proceso POMS, la Cuadrilla del Proceso POMS ejecuta el trabajo e informa al Operador del Centro Control El Bosque (CCB) la conclusión del mismo	
	• Si la suspensión del servicio eléctrico es solicitada por el Cliente Interno, éste ejecuta el trabajo e informa al Operador del CCB la conclusión del mismo	X
	• Se reestablece el servicio eléctrico ubicándose en los puntos indicados	
	• Se verifica el restablecimiento del servicio, ejecutando las acciones correctivas necesarias	
	• Se registra y entrega el protocolo	
	• Se verifica que todos los protocolos se hayan entregado, estén llenos y analiza la información registrada, si existe alguna inconsistencia se corrige	
	• Se almacenan los documentos relacionados	
Desconexiones del Servicio Eléctrico Solicitadas por Empresas	• Cliente externo solicita que le realicen la desconexión del servicio eléctrico	
	• Se revisa solicitud, si no cumple con aspectos necesarios es devuelta para su corrección, si la solicitud cumple con requisitos se le da el VBº	
	• Se verifica si la desconexión del servicio eléctrico se requiere para días hábiles o no hábiles.	
	• Si la solicitud es para días no hábiles se debe: o Enviar por fax la solicitud presentada por el Cliente al CCB o Verificar que la solicitud cuente con el VBº del Coordinador del Proceso POMS, si no lo tiene se hace las gestiones del caso para su registro o Programar la desconexión y asignar la Cuadrilla de Averías o Realizar la desconexión del servicio eléctrico o Informar de la desconexión del servicio eléctrico antes de iniciar al CCB o Anotar en la bitácora la desconexión del servicio eléctrico o Realizar el trabajo e informar la finalización del mismo al CCB	

Proceso	Procedimiento	Critico
	○ Realizar e informar sobre la reconexión del servicio eléctrico ○ Registro en bitácora la reconexión del servicio eléctrico	
	• Si la solicitud es para días hábiles se debe: ○ Programar la desconexión y asignar la Cuadrilla de Mantenimiento ○ Informar de la desconexión del servicio eléctrico en el momento de iniciar al CCB ○ Anotar en la bitácora la desconexión del servicio eléctrico ○ Realizar la desconexión del servicio eléctrico ○ Realizar el trabajo y una vez que lo concluye informar al CCB ○ Realizar la reconexión del servicio eléctrico ○ Una vez que concluye la reconexión del servicio eléctrico, informar al CCB ○ Anotar en la bitácora la reconexión del servicio eléctrico	
Trámites de Estudio	• Cliente solicita el estudio para obtener el servicio eléctrico	
	• Se llena la solicitud, se realiza la confección de recibo por la cancelación del estudio y se entrega copia al Cliente y se llena el formulario de control en la base de datos, en el cual indica que el estado del recibo se encuentra en el estado "pendiente de pago"	
	• El cliente cancela el recibo de estudio de ingeniería en la UEN SCL	
	• UEN SCL elabora el recibo especial y envía la copia del mismo al Proceso PDR	
	• Se recibe el recibo especial, se abre el expediente del estudio y se informa al Coordinador del Proceso PDR	
	• Se coordina con los Profesionales y los Técnicos la inspección de campo	
	• Se cambia en la base de datos el estado del registro a "pendiente de estudio"	
	• Se realiza inspección de campo y se elabora el diseño de la obra	
	• Se elabora el presupuesto de la obra	

Proceso	Procedimiento	Critico
	• Se llevan a cabo las revisiones necesarias sobre el estudio de campo y el presupuesto. Si el estudio de campo presenta disconformidades técnicas o de cálculo, el Profesional del Proceso PDR corrige el estudio de campo y el diseño de la obra. Si el presupuesto presenta disconformidades técnicas o de cálculo, el Técnico del Proceso PDR corrige el presupuesto	
	• Se coloca el visto bueno (VBº) en el estudio de campo y en el presupuesto	
	• El Asistente Administrativo del Proceso PDR cambia el estado del registro en la base de datos a "estudio ejecutado"	
	• Se le informa al Cliente el costo de obra, las opciones que tiene para realizar la construcción de la obra y las opciones para cancelar la obra	
	• El Cliente informa al Asistente Administrativo que va a construir la obra con JASEC	
	• Se llena la solicitud confección de recibo por el costo de la obra e informa al Coordinador del Proceso PDR	
	• Si el Cliente decide cancelar con financiamiento se debe proceder conforme con el procedimiento de Cuentas por Cobrar	
	• Si el Cliente decide cancelar de contado, cancela el costo total de la obra en la UEN SCL; la cual elabora el recibo especial por el costo de la obra, entrega copia al Cliente y envía copia del mismo al Proceso PDR. recibe el recibo especial o nota del plan de financiamiento y pagaré cancelado	
	• Si el Cliente decide construir la obra con un particular se debe proceder conforme con el procedimiento sobre Recepción de obras realizadas por particulares	
	• Se almacenan los documentos relacionados	X
Construcción de Obras Ejecutadas por JASEC y Contratistas	• Se programa la construcción de la obra y asigna al responsable	X
	• Se solicita el No. de cuenta contable OTC	X
	• Se crea en la base de datos la Orden de Trabajo Interna, colocándola en estado "pendiente"	
	• Se realiza estaqueo si la obra lo necesita, el cual se revisa y de ser necesario se corrige	
	• Se solicita la elaboración de la requisición	X
	• Se inicia la construcción de la obra	
	• Si la construcción de la obra requiere la suspensión del servicio eléctrico, se debe proceder conforme con el procedimiento de suspensiones programadas del servicio eléctrico	X
	• Se realiza la inspección de campo durante la ejecución de la obra, realizando las modificaciones del caso	X

Proceso	Procedimiento	Critico
	• Se concluye la construcción de la obra	
	• Se registra el reporte de mano de obra de trabajos realizados OTC	X
	• Se realiza la inspección de campo final, y se corrige cualquier problema encontrado	
	• Se registra el formulario de levantamiento de montajes y/o materiales instalados, desmantelados o reubicados en la obra	
	• Se realiza la devolución de materiales nuevos y desmantelados	X
	• Si la construcción de la obra la realizó un Contratista, se debe proceder conforme con el procedimiento de Trámite de pago en la UEN Distribución	
	• Se elabora la liquidación de materiales, corrigiendo cualquier diferencia	X
	• Se entrega copia del levantamiento para que se registre, previa inspección, la información en el Sistema de Información Geográfica (GIS)	X
	• Se realiza la estimación de materiales y de mano de obra empleados en la obra	
	• Se coloca en la base de datos el estado de liquidada a la Orden de Trabajo	
	• Se almacenan los documentos relacionados	X
	• Si el mes finalizó, se elabora el informe de obras finalizadas y se envía copia del informe de obras finalizadas al Proceso PC	X
Recepción de Obras Ejecutadas por Particulares	• Cliente solicita requisitos técnicos para construir la obra por medios privados. Se le informa sobre el procedimiento a seguir y entrega requisitos técnicos	
	• Si el Cliente realiza el diseño de la obra con un particular, entrega el mismo en el Proceso PDR para su revisión y aprobación, corrigiendo cualquier problema	
	• Si el Cliente realiza el diseño de la obra con JASEC, se realiza inspección de campo y se elabora el diseño de la obra	
	• Se elabora el presupuesto de la obra	
	• Se llevan a cabo las revisiones necesarias sobre el estudio de campo y el presupuesto. Si el estudio de campo presenta disconformidades técnicas o de cálculo, el Profesional del Proceso PDR corrige el estudio de campo y el diseño de la obra. Si el presupuesto presenta disconformidades técnicas o de cálculo, el Técnico del Proceso PDR corrige el presupuesto	
	• Se coloca el visto bueno (VBº) en el estudio de campo y en el presupuesto	
	• Se registra la base de datos de control en el sistema	

Proceso	Procedimiento	Critico
	• Se registra la solicitud de recibo por el 3% de inspección, energización y por la instalación de las luminarias. Si es necesario se incluye el 7% por el diseño de la obra	
	• El Cliente cancela la solicitud de recibo en la UEN SCL	
	• UEN SCL elabora el recibo especial y envía copia del mismo al Proceso PDR	
	• Se le solicita al Cliente una nota que indique quien será el responsable por la construcción de la obra	X
	• Cliente notifica al Proceso PDR el inicio de la obra y el responsable por la construcción de la misma	X
	• Se realiza la inspección de campo durante la ejecución de la obra, el cliente realiza las modificaciones del caso	
	• El Cliente entrega el transformador (es) y la luminaria (s) así como la factura y la garantía de los mismos en el Proceso AME	
	• Se solicita inspección y aprobación del transformador (es) y de la luminaria (s). Si transformadores o luminarias no cumplen con especificaciones, el cliente debe sustituirlos	X
	• Se notifican de la aprobación del equipo	
	• Se asigna el número consecutivo al transformador (es) y lo entrega al responsable de la ejecución de la obra	
	• Se ingresa la luminaria (s) en el inventario y se almacena	
	• El Cliente notifica la conclusión de la obra y solicita la inspección y energización	
	• Se realiza la inspección de campo final, y el cliente corrige cualquier problema encontrado	
	• Se coordina y realiza la energización de la obra	X
	• Se realiza la inspección de campo, y el cliente corrige cualquier problema encontrado	X
	• Se registra el formulario de levantamiento de montajes y/o materiales instalados, desmantelados o reubicados, entregando una copia al Sistema de Información Geográfico (GIS), quien, previa inspección registra la información en el Sistema de Información Geográfica (GIS)	
	• Se notifica al Cliente la aceptación de la obra	X
	• Se cambia el estado de la base de datos de control a obra recibida y se entrega la nota de aceptación de la obra al Cliente	
	• El Cliente recibe la nota de aceptación de la obra y entrega un informe ejecutivo	X
	• Se recibe y firma el informe presentado por el Cliente y envía copia al Proceso PC	X
	• Se almacenan los documentos relacionados	

Proceso	Procedimiento	Critico
Servicios Temporales	• Cliente solicita un servicio temporal o provisional	
	• Se registra solicitud de servicio y solicitud confección de recibo para ejecutar el estudio	
	• Cliente cancela el costo de estudio por el servicio provisional en la UEN SCL, la cual elabora el recibo especial y envía copia del mismo al Proceso PDR	
	• Se realiza la inspección de campo y se verifica si es posible brindar el servicio.	
	• Si no se puede brindar el servicio eléctrico se le informa al Cliente las causas y se archiva información relacionada	
	• Si se puede brindar el servicio eléctrico, se registra la autorización para servicios temporales	
	• Se envía por fax la autorización para servicios temporales a la UEN SCL	X
	• Se informa al Cliente el resultado del estudio técnico	
	• Se almacena la información relacionada	
	• Si se va a brindar el servicio temporal, se procede con el procedimiento sobre Instalación de Medidores	
Visado de Planos	• El Cliente solicita una constancia en la que JASEC le garantice que en esa propiedad se le puede brindar el servicio eléctrico	
	• Se registra la solicitud y la confección de recibo para ejecutar el estudio, y le solicita dos copias del plano catastro	
	• El Cliente entrega las copias del plano catastro en el Proceso PDR y cancela el costo por el estudio en la UEN SCL, la cual elabora el recibo especial y envía copia del mismo al Proceso PDR	
	• Se coordina y elabora inspección para verificar si el sitio cuenta con las condiciones necesarias para prestar el servicio eléctrico	X
	• Se elabora la certificación, indicando si el sitio cuenta o no con las condiciones necesarias para prestar el servicio eléctrico	
	• Se revisa la certificación, corrigiendo cualquier error	
	• Si la certificación está correcta, se autoriza firmando la misma	
	• Se entrega la certificación (original y copia) al Cliente	
	• Se almacenan los documentos relacionados	X

Proceso	Procedimiento	Critico
Alquiler de Transformadores	• Cliente solicita el estudio por el alquiler del transformador	X
	• Se registra la solicitud y la confección de recibo por el estudio solicitado y se informa al Cliente los requisitos que debe cumplir para concretar el alquiler	
	• El Cliente cancela el recibo en la UEN SCL, la cual elabora el recibo especial y envía la copia de recibo al Proceso PDR	
	• Se recibe la copia de recibo y abre expediente por el alquiler del transformador	X
	• Se realiza la inspección de campo y se verifica que el sitio cuente con las condiciones necesarias. Si el sitio no cuenta con las condiciones se le informa al Cliente las causas por las cuales no se le puede brindar el servicio eléctrico	
	• Si el sitio cuenta con las condiciones necesarias se elabora el presupuesto por la instalación y el alquiler del transformador(es)	
	• Se revisa el estudio técnico y el presupuesto, corrigiendo cualquier inconsistencia	
	• Se autoriza el estudio técnico y el presupuesto	X
	• Se le informa al Cliente el costo por la instalación y el alquiler del transformador (es)	
	• Si el Cliente no decide alquilar el transformador se archiva el expediente	X
	• Si el alquiler del transformador es inferior a un mes, se le solicita al Cliente una nota que indique el responsable por el alquiler, así como el No. de medidor al cual se le debe cargar algún costo por daños al equipo. El Cliente entrega la nota	X
	• Se solicita el No. de cuenta contable OTC. Se asigna el No. de cuenta contable OTC	
	• Se llena la solicitud de confección de recibo por la instalación, desmantelamiento, alquiler del transformador y depósito de garantía (si es necesario)	
	• Si el alquiler del transformador es superior a un mes, se envía detalle de los costos de instalación, desmantelamiento y alquiler a la UEN SCL, con base en el presupuesto autorizado. El Cliente presenta los requisitos necesarios y cancela el recibo en la UEN SCL, la cual elabora el recibo especial y remite la copia y notifica al Proceso PDR que el Cliente cumplió con todos los requisitos y firmó el contrato	
	• Se coordina la instalación del equipo	
	• Se solicita la elaboración de la requisición (es), se realiza la requisición y se entrega el equipo	
	• Se realiza la instalación del equipo	

Proceso	Procedimiento	Critico
	• Cliente notifica al Proceso PDR a UEN SCL que pueden desmantelar el transformador (es)	
	• Si el alquiler es superior a un mes, la UEN SCL solicita el desmantelamiento del transformador al Proceso PDR	X
	• Se coordina y realiza la desinstalación del transformador y se verifica que el transformador esté en buen estado	X
	• Si el transformador no se encuentra en buen estado y el alquiler es inferior a un mes, se le informa por escrito a la UEN SCL el No. de medidor al cual se le debe cargar el costo por el daño al transformador	
	• Si el transformador no se encuentra en buen estado y el alquiler es superior a un mes, se le informa por escrito a la UEN SCL para que retenga la garantía por el equipo	
	• Si el transformador se encuentra en buen estado y el alquiler es superior a un mes, se le notifica a la UEN SCL para que devuelva el depósito de garantía al Cliente	X
	• Se realiza la devolución del equipo	X
	• Se recibe el equipo y entrega el control devolución de materiales	
	• Se elabora la liquidación por la instalación y desmantelamiento del transformador (es)	
	• Se revisa la liquidación por la instalación y el desmantelamiento del transformador, si hay errores se corrige	
	• Se almacenan los documentos relacionados	
Instalación de Luminarias	• Cliente solicita la instalación de la luminaria	
	• Se llena la solicitud instalación alumbrado público	X
	• Se programa y realiza la inspección de campo. Si el sitio no cuenta con las condiciones necesarias, se debe proceder de acuerdo con el procedimiento de construcción de obras ejecutadas por JASEC o Contratistas	X
	• Si el sitio cuenta con las condiciones necesarias, se archiva temporalmente la solicitud instalación alumbrado público y se programa la instalación de la luminaria	
	• Se asigna el trabajo por ruta a la Cuadrilla de AP o al Contratista	
	• Se solicita la elaboración de la requisición (es)	
	• Se instala la luminaria (s)	
	• Se realiza el levantamiento de montajes y/o materiales, al llenar el reporte de repuestos utilizados para el alumbrado público	

Proceso	Procedimiento	Critico
	• Se llena el reporte de mano de obra de trabajos realizados OTC	
	• Se verifica que la luminaria (s) esté funcionando	X
	• Si la luminaria (s) no está funcionando, se debe proceder de acuerdo con el procedimiento de reparación de luminarias	
	• Si la luminaria (s) está funcionando, el Técnico de AP elabora la liquidación de materiales, si hay diferencias se corrigen	X
	• Si la liquidación de materiales no presenta anomalías, se coloca el Visto bueno (VB9) en la liquidación de materiales.	
	• Se entrega copia del reporte de repuestos utilizados alumbrado público para que se registre, previa inspección, la información en el Sistema de Información Geográfica (GIS).	
	• Se almacenan los documentos relacionados	X
Reparación de Luminarias	• El Cliente solicita por escrito, teléfono o en forma personal la reparación de la luminaria.	X
	• Se registra el reporte de alumbrado público.	
	• Se archiva temporalmente el reporte de alumbrado público y programa la reparación de la luminaria.	
	• Se asigna el trabajo por ruta a la Cuadrilla de AP o al Contratista	
	• Se determina si la Cuadrilla de AP o el Contratista cuenta con los repuestos necesarios. Si no se cuenta con los repuestos necesarios, él se solicita la elaboración de la requisición (es)	
	• Cuadrilla de AP o el Contratista repara la luminaria	
	• Se llena el reporte de alumbrado público y el reporte de repuestos utilizados para el alumbrado público, se devuelven los repuestos y cabezotes en mal estado	
	• Se guarda los cabezotes en buen estado	
	• Se verifica, en trabajo de campo, que las luminarias estén funcionando, si hay problemas se corrigen	
	• Si las luminarias de la muestra están funcionando y el trabajo lo realizó un Contratista, se debe proceder de acuerdo con el procedimiento de Trámite de pagos en la UEN de Distribución	
	• Se elabora la liquidación de materiales, corrigiendo cualquier diferencia	
	• Se entrega copia del reporte de repuestos utilizados alumbrado público para que se registre, previa inspección, la información en el Sistema de Información Geográfica (GIS)	
	• Se almacenan los documentos relacionados.	

9.4.2. Cuestionario aplicado al área de Apoyo.

Cuestionario aplicado al jefe del área de apoyo con el objetivo de identificar los procesos críticos.

Cuestionario

El objetivo de este cuestionario es determinar los procesos y actividades criticas gestionadas dentro de su área operativa.

Marque con una X el procedimiento que considere critica dentro de las operaciones del área que lidera.

Nota: Considere como un factor de criticidad la dependencia del procedimiento hacia ejecutarse de forma automática por medio de un sistema informático.

Proceso	Procedimiento	Critico
Empleo	• Análisis Ocupacional Análisis y actualización del manual de puestos.	X
	• Clasificación y Valoración de Puestos Definición de requisitos mínimos a cumplir, definición de habilidades, destrezas, conocimiento, formación académica, naturaleza del puesto, funciones a realizar, etc.	X
	• Reclutamiento y Selección. Generación de concursos primero a lo interno y externo de la institución.	
	• Recepción de ofertas y análisis.	
	• Planificación de Recursos humanos. Determinar la demanda de recursos en el futuro y determinar la oferta interna. Si la oferta interna es mayor que la demanda se realiza un proceso de reestructuración en la organización. Si la demanda es mayor que la oferta se realiza el proceso de reclutamiento.	
Desarrollo de Recursos Humanos	• Inducción de nuevos empleados y reinducción de empleados internos por cambio de puesto. Se proporciona al empleado información general de la empresa: normas, procedimientos, marco legal, normas de higiene, seguridad, servicios que brinda la empresa, beneficios, presentación del personal, entre otros. Además, una inducción de seis meses en el área específica de trabajo.	
	• Capacitación. Detección de necesidades de capacitación a través de formularios que se envían a nivel de jefatura para conocer cuántas personas	

Proceso	Procedimiento	Critico
	requieren capacitación y qué necesidades de capacitación solicitan. Esto con el fin de priorizar necesidades y realizar el plan de capacitación institucional.	
	• Desarrollo Orientar al personal acerca de las áreas en que puede capacitarse con el fin promover la superación y la escala de puestos dentro de la institución.	
Compensación y prestaciones	• Planilla. Realización de diversos trámites con el fin de pagar a los funcionarios el salario respectivo. El pago de salarios se efectúa por concepto de: horas laborales, horas extra, beneficios, dedicación exclusiva, cargas sociales, deducciones por préstamos, deducciones de otras instituciones por compromisos que adquieren los funcionarios como: Bancos y entidades financieras, INS, Colegios Profesionales, Juzgados (Embargos y Pensiones Alimenticias), entre otros. También, facturación envía el recibo eléctrico de cada funcionario para realizar la respectiva deducción. Además, se realizan pagos extraordinarios por: salario escolar y aguinaldo. Se registran pagos por: indemnizaciones, prestaciones y vacaciones.	X
	• Registros operativos Actualización del expediente de cada funcionario, registro de vacaciones y acciones de personal.	X
Seguridad social y salud	• Coordinación de Capacitaciones	
Relaciones laborales	• Manejo de conflictos laborales	

Proceso	Procedimiento	Critico
Investigación de recursos humanos	• Realización de investigaciones para obtener la percepción del usuario en cuanto a: comunicación, trato, horario, capacitaciones, servicios médicos, condiciones de infraestructura, entre otros.	
Liderar plan de compras	• Producir en conjunto con la gerencia y usuarios el plan anual de adquisiciones para agrupar e integrar las necesidades comunes de los departamentos. El proceso de agrupar lo realiza un Gestor coordinador de toda la licitación, el cual debe de coordinar con los diferentes departamentos para realizar una sola compra de productos en común (paquetes de gestión) para presentarlo ante la proveeduría y así iniciar el plan de compras.	X
Iniciar el plan de compras	• Iniciar la gestión de compras conduciendo todos los procedimientos de contratación necesarios (licitaciones, contrataciones) y cualquier otro que la administración determine.	
	• Velar por la legalidad de los procedimientos (de acuerdo con la Ley de Contratación Administrativa)	
	• Revisión del paquete de gestión de compras conformado por el cartel, la reserva presupuestaria y acta de decisión inicial para solicitar la gestión de la licitación.	
	• Verificación de requisitos (revisión de los rubros aprobados, que este contablemente correcto, que el cartel esté bien definido, revisión del acta de licitación y otros documentos)	X
	• Publicación del cartel	
	• Análisis de oferentes	
	• Adjudicación del oferente.	

Proceso	Procedimiento	Critico
Creación del expediente licitatorio	• Creación del expediente licitatorio, el cual está conformado por: o Orden de compra, la cual se produce a través del SIFAJ. o Cartel. o Reserva presupuestaria (consultas a presupuesto por medio del SIFAJ) o Carta de presupuesto, indica la disponibilidad de la reserva presupuestaria o Plan de compras o Ofertas de participantes en la licitación. o Informes técnicos y legales. o Aclaraciones o Certificación de la CCSS o Recomendaciones de proveeduría o Actas de adjudicación. o Otros documentos	X
Registro de Proveedores	• Administración y mantenimiento del registro de proveedores.	
Custodia de Expedientes	• Administración y custodia de expedientes administrativos	
Garantías	• Administración y custodia de garantías.	
Solicitudes	• Atención de aclaraciones, subsanaciones, peticiones de proveedores, clientes y usuarios.	

Proceso	Procedimiento	Critico
Recibo	• Recibo de material por concepto de: compras (locales o importaciones), préstamo o donación. Para recibir el material, el solicitante (usuario de cualquier departamento) debe generar un documento de aprobación con respecto a, que lo recibido es lo que se solicitó y adjuntar una copia de la orden de compra, cartel o factura correspondiente.	
	• Revisión de lo que se recibe corresponde efectivamente a lo solicitado. En caso de alguna inconformidad el almacén y solicitante hacen el reclamo a la institución que provee el material a través de un oficio.	
Solicitud de requisición	• El usuario realiza una solicitud de requisición por escrito.	
	• Se consulta y registra en el sistema.	X
Préstamo de activos	• Solicitudes por medio de vales, para el préstamo de herramientas por instituciones externas o subestaciones.	
Almacenamiento	• Verificación de documentación para aprobar el almacenamiento del material.	X
	• Se identifica y registra en inventario el material.	X
Control	• Revisión periódica de las existencias contra saldos.	X
	• Revisión constante del estado físico de los materiales en custodia.	

Proceso	Procedimiento	Critico
Despacho de bienes materiales y equipo	• Revisión de existencia de material asignado al solicitante contra salida del mismo.	X
	• Aprobación de solicitud de requisición para el despacho de activo.	X
	• Actualización en el sistema con respecto a la cantidad disponible de activos.	X
	• Registro en Excel del responsable de recibir el activo.	X
Control de Caja Chica	• La Junta Directiva autoriza el monto de caja chica a utilizar por cada departamento, por lo que el proceso de administrar los recursos financieros debe controlar, revisar y aprobar la liquidación de dichos fondos.	X
Cuentas por Cobrar	• Control de cuentas por cobrar.	X
	• Conciliar los montos generados por los recaudadores y el proceso de Facturar y Cobrar. Del proceso Facturar y Cobrar se envían Reportes los cuales se ingresan manualmente en SIFAJ para verificar los montos a cobrar para luego verificar que coincida con lo registrado.	
Cuentas por pagar	• Control de cuentas por pagar.	X
	• Controlar que los pagos que se realizan se hagan de acuerdo a la orden de compra.	X
	• Solicitudes de pagos de todos los departamentos, procesos a través del SIFAJ	X
Inversiones	• Realizar depósitos en cuenta bancaria para ganar intereses.	X
Control Bancario	• Revisar los movimientos en las cuentas originados por transacciones.	X
	• Controlar el proceso desde que está el dinero en el Banco hasta que se utiliza.	X
Custodia de Gara	• Custodia de garantías de los activos que se adquieren.	
	• Custodia de cheques y transacciones.	

Proceso	Procedimiento	Critico
	• Revisar y archivar todas las custodias de garantía que están por vencerse para todos los departamentos	
Recepción de Información	• Recopilar diariamente todas las transacciones que se realizan en la institución para analizar la información, aplicarla y registrarla.	X
Registros contables	• Llevar registros contables de las partes no integradas al SIFAJ (como inventarios, registro y control de la flotilla de vehículos, control de activos fijos, ingresos, registros manuales de la facturación comercial (El SIPAC no tiene interfaz con el SIFAJ, por lo que hay que registrar manualmente los asientos), entre otros).	
Flujo de bienes y servicios	• Realizar el control interno a nivel institucional a través de la revisión de las transacciones, para dar su visto bueno o realizar ajustes contables.	X
	• Registro, control y supervisión del flujo de transacciones de caja chica, salarios, gastos de representación, pago de servicios, pago de dieta (Junta Directiva), salarios, entre otros.	X
Estados financieros	• Analizar y supervisar cada una de las transacciones que se llevan a cabo a nivel institucional.	X
	• Girar estados financieros institucionales para ser reconocidos por la Junta Directiva, Gerencia, Líderes, Auditoría Interna, para su aprobación.	X
	• Cierres Mensuales	X
Estudios	• Realizar estudios especiales cuando son requeridos por la administración o instituciones externas.	X
Transporte	• Confección de licitación para la compra de vehículos. Análisis técnico de ofertas y presentación de información ante la Gerencia o Junta Directiva.	
	• Coordinar el mantenimiento preventivo y correctivo de la flota vehicular (unidades grandes, pequeñas y articuladas (ej: grúas, montacargas, retroexcavadoras))	X
	• Adquirir repuestos y accesorios	
	• Préstamos de unidades	

Proceso	Procedimiento	Critico
	• Revisión de flotilla vehicular para el cambio de la misma con la agencia contratada cuando se finaliza el tiempo definido en el contrato para su utilización (por obsolescencia). Utilizan planes quinquenales en donde se entregan las unidades adquiridas en dicha agencia como parte del pago a las mismas.	
Mantenimiento Preventivo y Correctivo de Instalaciones	• Mantenimiento de las instalaciones físicas de JASEC (edificios, garajes, reparaciones por daños eléctricos, zonas verdes, pintura, etc.)	
Aseo y Vigilancia	• Confección de licitación para la contratación de los servicios externos contratados. Análisis técnico de ofertas recibidas y presentación de candidatos ante la Gerencia y Junta Directiva.	
	• Coordinar y supervisar las actividades para el personal de limpieza y vigilancia.	
Seguridad electrónica	• Confección de licitación para la compra de soluciones de seguridad electrónica. Análisis técnico de ofertas y presentación de información ante la Gerencia o Junta Directiva.	
	• Supervisión del buen funcionamiento del circuito cerrado de seguridad o CCTV.	
Administración de Pólizas de incendios	• Administración de pólizas de incendio de todas las instalaciones y la flota vehicular.	
	• Compras de pólizas	
	• Retiro de pólizas	
Trámites	• Solicitud de vacaciones a Recursos Humanos del personal que tiene a cargo.	

Proceso	Procedimiento	Critico
Modelo de tarifas	• Mantener el equilibrio financiero de la institución a través de la planificación económica financiera, de la consecución oportuna de recursos propios y externos y del análisis financiero y económico de los planes, programas y proyectos.	
	• Cumplir con las directrices emanadas de ARESEP, en cuanto a todos los aspectos relacionados con los modelos de tarifas.	
	• Acumular la información financiera necesaria para justificar los aumentos automáticos y los extraordinarios de acuerdo a los criterios que se han establecido por la normativa vigente.	
Atención de requerimientos	• Atender de forma oportuna los requerimientos relacionados con las tarifas que puede solicitar la ARESEP, la Junta Directiva y la Gerencia General.	
Estudios Tarifarios	• Realizar estudios tarifarios integrales un par de veces al año.	
	• Realizar estudios automáticos por consumos del ICE, de forma más frecuente que los estudios tarifarios.	
Históricos	• Extraer la información de: los sistemas Comerciales y de Facturación (JASEC tiene un desfase de un mes en el cierre contable y toda la planeación tarifaria se hace con la última cifra contable oficial) con respecto al modelo tarifario, y de Producción, Distribución o Proyectos con respecto a la información de los indicadores técnicos; para procesar dicha información en hojas de Excel.	X
Ciclo pres	• Coordinar y orientar la toma de decisiones en cuanto a la planificación financiera y operativa a corto plazo, asegurando la	X

Proceso	Procedimiento	Critico
	formulación, ejecución, control y evaluación del Plan Anual Operativo y del Proceso Presupuestario en apego a la normativa legal y técnica vigente.	
	• Formulación, control, validación del ciclo presupuestario a través del SIFAJ.	X
	• Seguimiento del ciclo presupuestario.	X
Planes de evaluación	• Realizar planes de evaluación físico y financiero.	
Análisis de cierre	• Análisis del ciclo presupuestario con respecto de lo planeado contra lo ejecutado.	
Ajustes al presupuesto	• Realizar ajustes al presupuesto ordinario y extraordinario.	
PAO	• Coordinar la elaboración del PAO; actualización de la misión, visión, estrategias, cuadro de mando integral, en coordinación con el Proceso de Planificación Institucional y lineamientos del Plan Nacional y el Plan de energía.	X
Informes	• Informes de ejecución y cierres mensuales.	
	• Informe mensual de los presupuestos de obras.	
	• Informes de avance de los proyectos y el cambio en las finanzas del mismo. •	

9.4.3. Cuestionario aplicado al área de Proyectos.

Cuestionario aplicado al jefe del área de proyectos con el objetivo de identificar los procesos críticos.

Cuestionario

El objetivo de este cuestionario es determinar los procesos y actividades criticas gestionadas dentro de su área operativa.

Marque con una X el procedimiento que considere critica dentro de las operaciones del área que lidera.

Nota: Considere como un factor de criticidad la dependencia del procedimiento hacia ejecutarse de forma automática por medio de un sistema informático.

Proceso	Procedimiento	Critico
Planificar y Desarrollar Proyectos	• Planificar y desarrollar la Institución en generación de proyectos en los procesos sustantivos de la misma (Producción, Distribución y Atender al Cliente) y los procesos de apoyo. Teniendo presencia en proyectos tales como: Sistema Hidroeléctrico Birrís, Convenio ICE Toro III, BOT – energía en bloque, multipropósito en cuanto a los proyectos de infraestructura desarrollando la misma en edificios, instalaciones eléctricas, mobiliario.	X
	• Apoyar y participar en la creación de convenios para el desarrollo de proyectos, alianzas estratégicas y multipropósitos.	X
	• Desarrollar nuevos servicios.	
	• Asesoría en infraestructura a nivel de la institución.	X
Soporte a Proyectos	• Se encarga de la administración de macro procesos.	X
	• Procesar rediseños.	X
	• Dar asesoría a las dependencias de JASEC.	
Proyección y Conservación del Ambiente	• Proteger el ambiente en aspectos tales como el aspecto social.	
	• Coordinación con la SETENA, para los estudios de impacto ambiental, en los procesos y proyectos de JASEC.	X

9.4.4. Cuestionario aplicado al área de Servicio al cliente.

Cuestionario aplicado al jefe del área de servicio al cliente con el objetivo de identificar los procesos críticos.

Cuestionario

El objetivo de este cuestionario es determinar los procesos y actividades criticas gestionadas dentro de su área operativa.

Marque con una X el procedimiento que considere critica dentro de las operaciones del área que lidera.

Nota: Considere como un factor de criticidad la dependencia del procedimiento hacia ejecutarse de forma automática por medio de un sistema informático.

Proceso	Procedimiento	Critico
Plataforma de Servicios	• Atención de consultas de Clientes	X
	• Atención de solicitudes a clientes	X
	• Registro de solicitudes (servicios nuevos, cambios en el servicio actual, entre otros)	X
Cajas	• Recepción dinero por pagos por conceptos de pagos de servicios y arreglos de pago	X
Atención Central Telefónica	• Atención de consultas de clientes	X
	• Registro manual de estadísticas de atención	
Servicios eléctricos	**Pre inspección**	
	• Recepción de órdenes de trabajo de plataforma de servicios •	X
	• Al final del día se toman las órdenes y se realiza el proceso de designación de rutas	X
	• Se ejecuta la pre inspección	
	• Se registran resultados de la pre inspección en el sistema	X
	Instalación Servicios Eléctricos	
	• Outsourcing ejecuta la instalación de servicios aprobados en la pre inspección	
	• Al final del día se registra en el sistema los resultados de la instalación	X
	• Revisión aleatoria de medidores instalados por la empresa externa	

Proceso	Procedimiento	Critico
	Reinstalación y Desinstalación de Servicios Eléctricos	
	• Al inicio de cada día se realizan consultas en el sistema SIJ para determinar los clientes morosos y clientes que se pusieron al día en sus deudas con JASEC	
	• Se programa trabajos de reinstalación y desinstalación dentro de las rutas de trabajo	X
	• Outsourcing ejecuta trabajo	
	• Al final del día se registra en el sistema los resultados	X
	Actualización de Información	
	• Resultados del trabajo, registrado en SICURA, se transfiere de manera automática al SIPAC.	X
Laboratorio de medidores	• Adquisición y mantenimiento de inventario de medidores.	
	• Investigación sobre nuevas tecnologías de medidores.	
Gestión Administrativa	• Apoyo a los procesos de Servicios Eléctricos y Laboratorio de Medidores.	
Lecturas	**Lectura Residencial Automatizada**	
	• Definición de ciclos de lectura, los cuales están distribuidos en pueblos y éstos en rutas.	
	• Re digitación de información de instalación de servicios por medio de informes del SIPAC al SIJ.	X
	• Descarga de rutas del SIJ al Hand Help.	X
	• Se realiza lectura con el Hand Help, registrando y revisando excepciones de consumo, las cuales son alertadas en el sistema.	X
	• Se descarga información de lectura del Hand Help al sistema SIJ.	X
	• Revisión de carga, analizando las excepciones reportadas y lecturas que se encuentran fuera de rangos, sobre las cuales se ejecuta un proceso de inspección para determinar las causas de ello.	X

Proceso	Procedimiento	Critico
	• Si la inspección determina que es necesario realizar trabajos sobre la instalación (cambio de medidor, reparación del mismo, entre otros), se registra orden en el SIPAC.	X
	Lectura Residencial Manual	
	• Definición de ciclos de lectura, los cuales están distribuidos en pueblos y éstos en rutas.	
	• Se realiza lectura manual.	
	• Resultado de la lectura se registra en SIJ.	X
	Lectura Industrial	
	• Se descarga la lectura de manera remota por medio de una portátil.	X
Facturación	• Se realiza facturación, tomando como insumos las lecturas, multas, tarifas y movimientos de facturas.	X
	• No se imprimen recibos, con las siguientes excepciones: o Cliente lo solicita o Clientes que pagan por adelantado recibos o Recibos de funcionarios que van para Recursos Humanos.	X
	• Si no se cuenta con lectura para algún cliente, se factura obteniendo el promedio de los últimos 6 meses más un aumento del 15%.	X
Cobros	**Actualización de Información**	
	• El sistema SIJ actualiza la información del sistema SAC, con los resultados de los ciclos de facturación.	X
	Cobro en Línea – Recaudadores y Caja Interna	
	• Cada vez que un abonado realiza un pago éste se registra en línea en el sistema SAC.	X
	Cobro Manual - Recaudadores	
	• El abonado realiza el pago.	
	• Al final del día se deposita el cobro y se realiza el registro en el sistema SAC.	X
	Cobro por Lotes - Recaudadores	
	• Se cuenta con información local de lo adeudado de cada abonado, esta información es actualizada al final del día.	X

Proceso	Procedimiento	Critico
	• Abonado realiza el pago.	
	• El cobro se registra de manera local y al final del día se envía un archivo encriptado a las oficinas de JASEC, por medio de e-mail o llave maya.	X
	• Se descarga la información del cobro en el sistema SAC.	X
	• Se envían a recaudadores archivos de cobros de los abonados al final del día.	X
	Actualización de Información	
	• La información registrada en SAC es transferida automáticamente al SIJ, para que éste actualice la información de cobros y morosidad.	X

9.4.5. Cuestionario aplicado al área de Producción.

Cuestionario aplicado al jefe del área de producción con el objetivo de identificar los procesos críticos.

Cuestionario

El objetivo de este cuestionario es determinar los procesos y actividades criticas gestionadas dentro de su área operativa.

Marque con una X el procedimiento que considere critica dentro de las operaciones del área que lidera.

Nota: Considere como un factor de criticidad la dependencia del procedimiento hacia ejecutarse de forma automática por medio de un sistema informático.

Proceso	Procedimiento	Critico
Mantener Generación	• Mantenimiento preventivo de caminos para que no haya obstáculos.	
	• Plantear acciones para mejorar, buscar alternativas.	
	• Almacenamiento menor de las tuberías, herrajes y otros accesorios para facilitar el desempeño adecuado y oportuno de eventuales fallas.	X
	• Ejecución del plan de mantenimiento preventivo, así como la atención de actividades de mantenimiento correctivo.	X
	• Disminución de tiempos muertos en la reparación de daños por medio de un adecuado stock de repuestos, herramientas, equipos y planeamiento.	X
	• Limpieza de tomas y funcionamiento adecuado de protecciones en equipos de regulación.	
	• Minimizar el riesgo de deslizamientos por medio de obras de estabilización.	
	• Sistema de regulación en canales de conducción.	X
	• Captación de materia prima asegurando que no existan obstáculos en las parrillas de entrada.	X
	• Estar pendientes de poder abastecer el embalse, en coordinación constante con los niveles de entrada al embalse asegurando el máximo abastecimiento del mismo.	X
	• Comunicar irregularidades mayores que afectan la infraestructura del sistema.	X
Operar Generación	• Mantener las plantas en operación el mayor tiempo posible; tenerlas a disposición, que no se salgan de línea	X
	• Revisión de los equipos.	X
	• Control de niveles óptimos del embalse.	X
	• Mantener el control sobre el funcionamiento de las plantas	X
	• Mantener el control sobre el funcionamiento del agua en los embalses.	X
	• Monitorear cuánta agua hay, mediante el sistema SCADA.	X
	• Controlar la labor de los oficiales de seguridad.	

9.4.6. Cuestionario aplicado al área de secretaria de junta directiva.

Cuestionario aplicado al jefe del área de secretaria de actas de junta directiva con el objetivo de identificar los procesos críticos.

Cuestionario

El objetivo de este cuestionario es determinar los procesos y actividades criticas gestionadas dentro de su área operativa.

Marque con una X el procedimiento que considere critica dentro de las operaciones del área que lidera.

Nota: Considere como un factor de criticidad la dependencia del procedimiento hacia ejecutarse de forma automática por medio de un sistema informático.

Proceso	Procedimiento	Critico
Agenda	• Programar la agenda.	
	• Preparar el material a utilizarse en la Sesiones de Junta Directiva.	
	• Control de Agenda.	
Actas	• Grabar actas.	
	• Elaborar las actas.	
	• Llevar a cabo el resguardo de actas.	
	• Publicar las actas o transmitir los acuerdos de la Junta a toda la institución.	X
	• Llevar el control de todos acuerdos de la Junta Directiva.	X
Caja Chica	• Administrar la caja chica.	
	• Confección y pago de planilla para los miembros de la Junta Directiva.	X
	• Control de presupuesto de la Junta Directiva.	
Informes	• Generar informes para la Junta Directiva, departamentos de Jasec y otras instituciones como la Contraloría, ARESEP y MINAET.	X

9.5. Apéndice E: Cuestionario para identificar sistemas críticos y valorar impactos y tiempos máximos de operación sin apoyo del área de TIC.

En este apéndice se incluyen los cuestionarios aplicados dentro del análisis BIA a los jefes de las áreas operativas de JASEC con el objetivo de identificar los sistemas informáticos críticos, valorar el impacto de una interrupción y los tiempos máximos de operación sin el apoyo del área de TIC que cada área operativa puede alcanzar.

9.5.1. Cuestionario área de apoyo.

Cuestionario aplicado al jefe del área de apoyo.

9.5.1.1. Sistemas críticos soportados por el área de TIC.

Sección del cuestionario dirigida a identificar los sistemas críticos.

Sistemas críticos soportados por el área de TIC.

¿Cuales sistemas soportados por el área de TIC, apoyan procesos críticos de su área?

Se detallan los departamentos gestionados por el área de Servicios Administrativos y los sistemas que soporta por el área de TIC.

	Proveeduría	Almacén	Adm de activos, mant. de vehículos y edificios
SICURA	☐	☐	☐
Recursos Humanos	☑	☑	☑
SLAM	☐	☐	☐
SAC	☐	☐	☐
SIFAJ	☑	☑	☑
SIPAC	☐	☐	☐
SIF	☐	☐	☐
SISHISTREC	☐	☐	☐
SIDEGA	☐	☐	☐
RECAF	☑	☑	☑
SISEVA	☑	☑	☑
SISINFO	☐	☐	☐
SWF	☐	☐	☐
SWQ	☐	☐	☐
SMI	☐	☐	☐
SICE	☐	☐	☐
Migrador	☐	☐	☐
DELPHOS	☑	☑	☑
SLI	☐	☐	☐
Office (Excel, Word, ...)	☐	☐	☐

9.5.1.2. Impacto de la interrupción de un proceso dentro de la organización.

Sección del cuestionario dirigida a identificar el impacto de una interrupción.

Impacto

El impacto de la interrupción de un proceso dentro de la organización puede representar una afectación según la siguiente clasificación.

Categoría	Descripción.
Operacional.	Afectación operativa dentro de la organización.
Legal o regulatorio.	Afectación por medio de una sanción de carácter legal o regulatorio.
Financiero.	Afectación en las finanzas de la organización.
Reputación.	Afectación a nivel de imagen de la organización.

La interrupción de un proceso crítico soportado por el área de TIC, ¿Qué tipo de impacto generaría dentro del negocio?

Impacto

- [x] Operativo.
- [x] Regulatorio y legal.
- [x] Finaciero.
- [ ] Reputación.

9.5.1.3. Tiempo máximo que podría operar sin el apoyo del área de TIC.

Sección del cuestionario dirigida a identificar el tiempo máximo de operación sin apoyo del área de TIC.

¿Cuál es el tiempo máximo que podría operar sin el apoyo del área de TIC?

2 horas

9.5.2. Cuestionario área de Distribución.

Cuestionario aplicado al jefe del área de distribución.

9.5.2.1. Sistemas críticos soportados por el área de TIC.

Sección del cuestionario dirigida a identificar los sistemas críticos.

Sistemas críticos soportados por el área de TIC.

¿Cuales sistemas soportados por el área de TIC, apoyan procesos críticos de su área?

	Planificación y desarrollo la red.	Operación del sistema.	Mantenimiento del sistema.	Alumbrado publico.	Servicios tecnicos.
SICURA	☐	☐	☐	☐	☑
Recursos Humanos	☑	☑	☑	☑	☑
SLAM	☐	☐	☐	☐	☑
SAC	☐	☐	☐	☐	☐
SIFAJ	☑	☑	☑	☑	☑
SIPAC	☐	☐	☐	☐	☐
SIF	☐	☐	☐	☐	☐
SISHISTREC	☐	☐	☐	☐	☐
SIDEGA	☐	☐	☐	☐	☐
RECAF	☑	☑	☑	☑	☑
SISEVA	☑	☑	☑	☑	☑
SISINFO	☐	☐	☐	☐	☐
SWF	☐	☐	☐	☐	☐
SWQ	☐	☐	☐	☐	☐
SMI	☐	☐	☐	☐	☐
SICE	☐	☐	☐	☐	☑
Migrador	☐	☐	☐	☐	☐
DELPHOS	☑	☑	☑	☑	☑
SLI	☐	☐	☐	☐	☐
Office (Excel, Word, ...)	☐	☐	☐	☐	☐

9.5.2.2. Impacto de la interrupción de un proceso dentro de la organización.

Sección del cuestionario dirigida a identificar el impacto de una interrupción

9.5.2.3. Tiempo máximo que podría operar sin el apoyo del área de TIC.

Impacto

El impacto de la interrupción de un proceso dentro de la organización puede representar una afectación según la siguiente clasificación.

Categoría	Descripción.
Operacional.	Afectación operativa dentro de la organización.
Legal o regulatorio.	Afectación por medio de una sanción de carácter legal o regulatorio.
Financiero.	Afectación en las finanzas de la organización.
Reputación.	Afectación a nivel de imagen de la organización.

La interrupción de un proceso crítico soportado por el área de TIC, ¿Qué tipo de impacto generaría dentro del negocio?

Impacto

- [x] Operativo.
- [x] Regulatorio y legal.
- [ ] Finaciero.
- [ ] Reputación.

Sección del cuestionario dirigida a identificar el tiempo máximo de operación sin apoyo del área de TIC

¿Cuál es el tiempo máximo que podría operar sin el apoyo del área de TIC?

2 horas

9.5.3. Cuestionario área de Producción.

Cuestionario aplicado al jefe del área de producción.

9.5.3.1. Sistemas críticos soportados por el área de TIC.

Sistemas críticos soportados por el área de TIC.

¿Cuales sistemas soportados por el área de TIC, apoyan procesos críticos de su área?

	Mantener generacion.	Operar generacion.
SICURA	☐	☐
Recursos Humanos	☑	☑
SLAM	☐	☐
SAC	☐	☐
SIFAJ	☑	☑
SIPAC	☐	☐
SIF	☐	☐
SISHISTREC	☐	☐
SIDEGA	☐	☐
RECAF	☑	☑
SISEVA	☑	☑
SISINFO	☐	☐
SWF	☐	☐
SWQ	☐	☐
SMI	☐	☐
SICE	☐	☐
Migrador	☐	☐
DELPHOS	☑	☑
SLI	☐	☐
Office (Excel, Word, ...)	☐	☐

Sección del cuestionario dirigida a identificar los sistemas críticos.

9.5.3.2. Impacto de la interrupción de un proceso dentro de la organización.

Sección del cuestionario dirigida a identificar el impacto de una interrupción.

Impacto

El impacto de la interrupción de un proceso dentro de la organización puede representar una afectación según la siguiente clasificación.

Categoría	Descripción.
Operacional.	Afectación operativa dentro de la organización.
Legal o regulatorio.	Afectación por medio de una sanción de carácter legal o regulatorio.
Financiero.	Afectación en las finanzas de la organización.
Reputación.	Afectación a nivel de imagen de la organización.

La interrupción de un proceso crítico soportado por el área de TIC, ¿Qué tipo de impacto generaría dentro del negocio?

Impacto

- [x] Operativo.
- [ ] Regulatorio y legal.
- [x] Finaciero.
- [ ] Reputación.

9.5.3.3. Tiempo máximo que podría operar sin el apoyo del área de TIC

Sección del cuestionario dirigida a identificar el tiempo máximo de operación sin apoyo del área de TIC.

¿Cuál es el tiempo máximo que podría operar sin el apoyo del área de TIC?

4 horas

9.5.4. Cuestionario área de Proyectos.

Cuestionario aplicado al jefe del área de producción.

9.5.4.1. Sistemas críticos soportados por el área de TIC.

Sección del cuestionario dirigida a identificar los sistemas críticos.

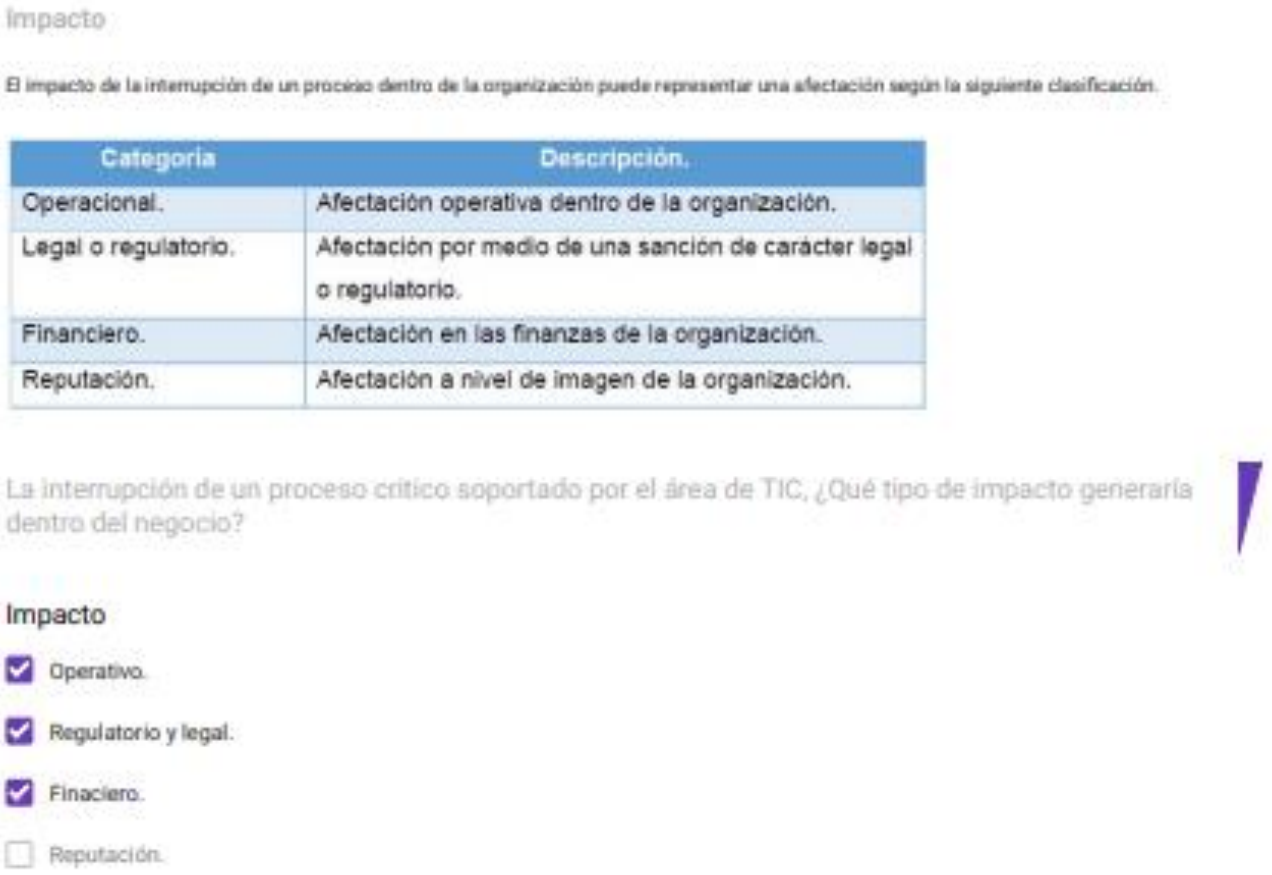
Sistemas críticos soportados por el área de TIC.

¿Cuales sistemas soportados por el área de TIC, apoyan procesos críticos de su área?

	Planificar y desarrollar proyectos	Soporte a proyectos	Proyección y conservación del ambiente
SICURA	☐	☐	☐
Recursos Humanos	☐	☐	☐
SLAM	☐	☐	☐
SAC	☐	☐	☐
SIFAJ	☑	☑	☐
SIPAC	☐	☐	☐
SIF	☐	☐	☐
SISHISTREC	☐	☐	☐
SIDEGA	☐	☐	☐
RECAF	☑	☑	☐
SISEVA	☑	☑	☐
SISINFO	☐	☐	☐
SWF	☐	☐	☐
SWQ	☐	☐	☐
SMI	☐	☐	☐
SICE	☐	☐	☐
Migrador	☐	☐	☐
DELPHOS	☑	☑	☐
SIJ	☐	☐	☐
Office (Excel, Word, ...)	☐	☐	☐

9.5.4.2. Impacto de la interrupción de un proceso dentro de la organización.

Sección del cuestionario dirigida a identificar el impacto de una interrupción



Impacto

El impacto de la interrupción de un proceso dentro de la organización puede representar una afectación según la siguiente clasificación.

Categoría	Descripción.
Operacional.	Afectación operativa dentro de la organización.
Legal o regulatorio.	Afectación por medio de una sanción de carácter legal o regulatorio.
Financiero.	Afectación en las finanzas de la organización.
Reputación.	Afectación a nivel de imagen de la organización.

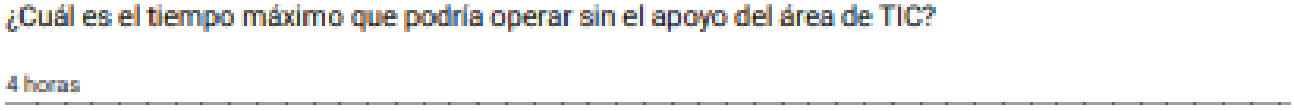
La interrupción de un proceso crítico soportado por el área de TIC, ¿Qué tipo de impacto generaría dentro del negocio?

Impacto

- [x] Operativo.
- [x] Regulatorio y legal.
- [x] Finaciero.
- [ ] Reputación.

9.5.4.3. Tiempo máximo que podría operar sin el apoyo del área de TIC.

Sección del cuestionario dirigida a identificar el tiempo máximo de operación sin apoyo del área de TIC



¿Cuál es el tiempo máximo que podría operar sin el apoyo del área de TIC?

4 horas

9.5.5. Cuestionario área de Secretaria de Juntas Directiva.

Cuestionario aplicado a la secretaria de la junta directiva.

9.5.5.1. Sistemas críticos soportados por el área de TIC.

Sección del cuestionario dirigida a identificar los sistemas críticos.

Sistemas críticos soportados por el área de TIC.

¿Cuales sistemas soportados por el área de TIC, apoyan procesos críticos de su área?

	Agenda	Actas	Caja chica	Informes
SICURA	☐	☐	☐	☐
Recursos Humanos	☐	☐	☐	☐
SLAM	☐	☐	☐	☐
SAC	☐	☐	☐	☐
SIFAJ	☐	☐	☑	☐
SIPAC	☐	☐	☐	☐
SIF	☐	☐	☐	☐
SISHISTREC	☐	☐	☐	☐
SIDEGA	☐	☐	☐	☐
RECAF	☐	☐	☐	☐
SISEVA	☐	☐	☐	☐
SISINFO	☐	☐	☐	☐
SWF	☐	☐	☐	☐
SWQ	☐	☐	☐	☐
SMI	☐	☐	☐	☐
SICE	☐	☐	☐	☐
Migrador	☐	☐	☐	☐
DELPHOS	☐	☐	☐	☐
SLI	☐	☐	☐	☐
Office (Excel, Word, ...)	☐	☐	☐	☐

9.5.5.2. Impacto de la interrupción de un proceso dentro de la organización.

Sección del cuestionario dirigida a identificar el impacto de una interrupción.

Impacto

El impacto de la interrupción de un proceso dentro de la organización puede representar una afectación según la siguiente clasificación.

Categoría	Descripción.
Operacional.	Afectación operativa dentro de la organización.
Legal o regulatorio.	Afectación por medio de una sanción de carácter legal o regulatorio.
Financiero.	Afectación en las finanzas de la organización.
Reputación.	Afectación a nivel de imagen de la organización.

La interrupción de un proceso crítico soportado por el área de TIC, ¿Qué tipo de impacto generaría dentro del negocio?

Impacto

- [x] Operativo.
- [ ] Regulatorio y legal.
- [ ] Finaciero.
- [ ] Reputación.

9.5.5.3. Tiempo máximo que podría operar sin el apoyo del área de TIC.

Sección del cuestionario dirigida a identificar el tiempo máximo de operación sin apoyo del área de TIC.

¿Cuál es el tiempo máximo que podría operar sin el apoyo del área de TIC?

8 horas

9.5.6. Cuestionario área de Servicio al Cliente.

Cuestionario aplicado a la secretaria de la junta directiva.

9.5.6.1. Sistemas críticos soportados por el área de TIC

Sección del cuestionario dirigida a identificar los sistemas críticos.

Sistemas críticos soportados por el área de TIC.

¿Cuales sistemas soportados por el área de TIC, apoyan procesos críticos de su área?

	Atender a clientes	Servicios tecnicos	Facturar y cobrar
SICURA	☐	☑	☐
Recursos Humanos	☐	☐	☐
SLAM	☐	☐	☑
SAC	☐	☐	☑
SIFAJ	☐	☐	☐
SIPAC	☑	☐	☐
SIF	☐	☐	☐
SISHISTREC	☐	☐	☐
SIDEGA	☐	☐	☑
RECAF	☐	☐	☐
SISEVA	☐	☐	☐
SISINFO	☐	☐	☑
SWF	☐	☐	☐
SWQ	☐	☐	☐
SMI	☐	☐	☑
SICE	☐	☑	☐
Migrador	☐	☐	☐
DELPHOS	☐	☐	☐
SLJ	☐	☐	☑
Office (Excel, Word, ...)	☐	☐	☐

9.5.6.2. Impacto de la interrupción de un proceso dentro de la organización.

Sección del cuestionario dirigida a identificar el impacto de una interrupción

Impacto

El impacto de la interrupción de un proceso dentro de la organización puede representar una afectación según la siguiente clasificación.

Categoría	Descripción.
Operacional.	Afectación operativa dentro de la organización.
Legal o regulatorio.	Afectación por medio de una sanción de carácter legal o regulatorio.
Financiero.	Afectación en las finanzas de la organización.
Reputación.	Afectación a nivel de imagen de la organización.

La interrupción de un proceso crítico soportado por el área de TIC, ¿Qué tipo de impacto generaría dentro del negocio?

Impacto

- [x] Operativo.
- [x] Regulatorio y legal.
- [x] Finaciero.
- [x] Reputación.

9.5.6.3. Tiempo máximo que podría operar sin el apoyo del área de TIC.

Sección del cuestionario dirigida a identificar el tiempo máximo de operación sin apoyo del área de TIC

¿Cuál es el tiempo máximo que podría operar sin el apoyo del área de TIC?

1 hora.

9.6. Apéndice F: Lista de verificación sobre aspectos mínimos considerados para la mitigación de riesgos.

En este apéndice se incluye la lista de verificación aplicada a los colaboradores del área de TIC de JASEC con el objetivo de verificar los aspectos mínimos considerados para la mitigación de los riesgos relacionados a TI.

9.6.1. Lista de verificación aplicada.

Se presenta la lista de verificación aplicada a los colaboradores del área de TIC.

Categoría de riesgo	Aspectos mínimos por considerar.	Aplicado
Interrupción eléctrica.	Fuentes alternas de generación eléctrica: UPS y plantas eléctricas.	si
	Mantenimiento de las fuentes alternas de generación eléctrica.	si
	Estado de la instalación eléctrica y capacidad eléctrica instalada.	si
	Lámparas de emergencia.	no
	Señalamiento iluminado de salidas y puertas de emergencia.	no
Fallos en Hardware.	Equipo de cómputo utilizado y obsolescencia.	no
	Capacidad de redundancia entre servidores.	si
	Monitoreo de problemas en los servidores.	si
	Contratos de mantenimiento preventivo y correctivo.	si
	Condiciones físicas y ambientales (limpieza, humedad, temperatura).	si
Fallos en Software.	Desarrollo local de aplicaciones (metodologías/ estándares).	si
	Cambios y configuración en aplicaciones.	si
Fallos en comunicaciones	Soporte técnico de los equipos utilizados.	si
	Mantenimiento preventivo y correctivo de los equipos de comunicación.	si
Desastres naturales.	Pólizas de seguro vigentes.	no
	Brigadas de atención ante situaciones de emergencia.	si
	Capacitación al personal	no
	Rutas de evacuación.	si
	Iluminación de pasillos y puertas y salidas de emergencia.	no
Incendio.	Pólizas vigentes de seguro.	no
	Sistemas automáticos y manuales contra incendio (gabinetes, extintores, aspersores).	si
	Uso de materiales retardantes del fuego.	si
	No almacenamiento de material combustible.	si
	Detectores de humo revisados regularmente.	no
Fallos en respaldos.	Procedimientos para respaldo y recuperación de información, fuentes, objetos, documentación y configuración de los sistemas.	si
	Periodicidad de los respaldos.	si
	Facilidades y protección para el almacenamiento dentro y fuera de sitio.	si
	Configuración de los discos duros de los servidores.	si
	Documentación actualizada sobre procedimientos de respaldo y recuperación.	si
Virus.	Programa antivirus instalado en computadoras y servidores.	si
	Configuración y actualización del software antivirus.	si
	Consultas regulares de fuentes de información para actualizaciones sobre virus.	si
	Capacitación al personal para identificar potenciales fuentes de ataque de virus.	no
	Políticas para el ataque de virus.	si
Violaciones a la seguridad física.	Seguridad física para el ingreso al edificio, oficinas y cuartos de servidores y equipos de comunicación.	si
	Capacitación al personal para detectar situaciones que puedan representar riesgo o cuestionar la presencia de personas desconocidas o sin identificación.	no
	Sistemas de seguridad: circuitos cerrados de televisión, sensores de movimiento, alarmas.	si
	Revisión y control de salida e ingreso de equipo de cómputo.	si
	Utilización de bitácoras para el registro de ingresos.	si
Intrusión.	Procedimientos para otorgamiento de acceso a las aplicaciones y políticas de acceso lógico.	si
	Procedimientos para el acceso a los recursos tecnológicos (redes y aplicaciones).	si
	Administración y configuración de "firewalls".	si
	Monitoreo de los accesos tanto legítimos como ilegítimos.	no
	Disponibilidad de herramientas para el monitoreo de la seguridad.	no
Personal	Capacitación.	si
	Documentación de las funciones del personal.	si

9.7. Apéndice G: Cuestionario para el análisis de riesgos.

En este apéndice se incluye el cuestionario aplicado a los colaboradores del área de TIC de JASEC con el objetivo de evaluar el nivel de probabilidad de ocurrencia y nivel de impacto que tienen los riesgos relacionados a TI.

9.7.1. Información general.

Todos los cuestionarios, a modo de introducción contienen la siguiente sección.

Análisis del nivel de riesgo.

El siguiente formulario tiene como objetivo recibir una valoración por parte de los colaboradores del área de TIC con respecto a el nivel que puede alcanzar los riesgos que puedan afectar a TIC. Al momento de emitir el criterio, tomando en consideración únicamente los servidores, sistemas de información y aplicaciones y los equipos de comunicación.

Se toman como referencia la siguiente clasificación de riesgos.

Categoría de riesgo
Interrupción eléctrica.
Fallos en Hardware.
Fallos en Software.
Fallos en comunicaciones
Desastres naturales.
Incendio.
Fallos en respaldos.
Virus.
Violaciones a la seguridad física.
Intrusión.
Recurso humano.

Nivel de riesgo.

¿Qué es el nivel de riesgo?

Es el grado de exposición al riesgo que se determina a partir del análisis de la probabilidad de ocurrencia del evento y de la magnitud de su impacto dentro de las operaciones.

Las valoraciones a continuación presentadas, están relacionadas directamente a TIC.

9.7.2. Cuestionario #1.

Se presenta la primera respuesta recibida del cuestionario.

Análisis del nivel de riesgo.

Probabilidad

¿Qué es Probabilidad?

La probabilidad mide la capacidad de ocurrencia del riesgo en el tiempo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de probabilidad		Ocurrencia
Nivel	Valor	
Muy probable.	10	Es muy probable que ocurra un evento en un periodo de 3 meses.
Probable	7	Es poco probable que ocurra un evento en un periodo de 3 a 6 meses.
Moderada	5	El evento ocurrirá en algún momento en un periodo de 6 meses a 1 año.
Poco probable	3	Es poco probable que el evento suceda, pero podría suceder en un periodo de 1 año a 2 años.
Muy poco probable.	1	Es muy poco probable que el evento se presente en un periodo de 2 años.

Nivel de probabilidad.

La valoración del nivel de probabilidad de ocurrencia de un riesgo asociado a la clasificación presentada a continuación.

Según la clasificación de riesgos presentada, ¿Cuál nivel de probabilidad asigna a cada uno?

*

	1	3	5	7	10
Interrupción eléctrica	○	◉	○	○	○
Fallos en hardware	○	○	◉	○	○
Fallos en software	○	◉	○	○	○
Fallos en comunicaciones	○	○	○	◉	○
Desastres naturales	◉	○	○	○	○
Incendio	◉	○	○	○	○
Fallos en respaldos	○	◉	○	○	○
Virus	○	○	◉	○	○
Violaciones a la seguridad física	○	◉	○	○	○
Intrusión (Hackeo)	○	◉	○	○	○
Recurso humano	○	○	◉	○	○

Impacto

¿Qué es Impacto?

El impacto mide el nivel de daño provocado una vez manifestado el riesgo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de impacto		Descripción.
Nivel	Valor	
Crítico.	10	El evento provoca una interrupción completa dentro de las operaciones del área de TIC de JASEC. Provoca una afectación total de los procesos críticos del negocio.
Significativo.	7	El evento provoca una interrupción entre completa y parcial dentro de las operaciones del área de TIC de JASEC. Provoca una afectación parcial de los procesos críticos del negocio.
Moderado.	5	El evento provoca una interrupción en las operaciones del área de TIC de JASEC. Las actividades críticas de negocio no se ven afectadas.
Menor.	3	El evento provoca un impacto leve en las operaciones del área de TIC de JASEC sin generar interrupciones dentro de las operaciones. La afectación en las actividades de negocio es menor a 30%.
Insignificante.	1	El evento no provoca un impacto dentro de las operaciones del área de TIC de JASEC. La afectación en las actividades de negocio es

Nivel de impacto.

La valoración del nivel de impacto causado por una posible materialización de un riesgo asociado a la clasificación presentada a continuación.

¿Cuál nivel de impacto considera que generaría una posible materialización de un riesgo asociado a la clasificación presentada?

*

	1	3	5	7	10
Interrupción eléctrica	○	○	○	○	◉
Fallos en hardware	○	○	○	○	◉
Fallos en software	○	○	○	○	◉
Fallos en comunicaciones	○	○	○	○	◉
Desastres naturales	○	○	○	○	◉
Incendio	○	○	○	○	◉
Fallos en respaldos	○	○	○	○	◉
Virus	○	○	○	○	◉
Violaciones a la seguridad física	○	○	○	○	◉
Intrusión (Hackeo)	○	○	○	○	◉
Recurso humano	○	○	○	○	◉

9.7.3. Cuestionario # 2.

Se presenta la segunda respuesta recibida del cuestionario.

Análisis del nivel de riesgo.

Probabilidad

¿Qué es Probabilidad?

La probabilidad mide la capacidad de ocurrencia del riesgo en el tiempo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de probabilidad		Ocurrencia
Nivel	Valor	
Muy probable.	10	Es muy probable que ocurra un evento en un periodo de 3 meses.
Probable	7	Es poco probable que ocurra un evento en un periodo de 3 a 6 meses.
Moderada	5	El evento ocurrirá en algún momento en un periodo de 6 meses a 1 año.
Poco probable	3	Es poco probable que el evento suceda, pero podría suceder en un periodo de 1 año a 2 años.
Muy poco probable.	1	Es muy poco probable que el evento se presente en un periodo de 2 años.

Nivel de probabilidad.

La valoración del nivel de probabilidad de ocurrencia de un riesgo asociado a la clasificación presentada a continuación.

Según la clasificación de riesgos presentada, ¿Cuál nivel de probabilidad asigna a cada uno?

*

	1	3	5	7	10
Interrupción eléctrica	○	○	◉	○	○
Fallos en hardware	○	○	◉	○	○
Fallos en software	○	◉	○	○	○
Fallos en comunicaciones	○	◉	○	○	○
Desastres naturales	○	◉	○	○	○
Incendio	◉	○	○	○	○
Fallos en respaldos	○	○	◉	○	○
Virus	○	○	○	◉	○
Violaciones a la seguridad física	○	◉	○	○	○
Intrusión (Hackeo)	○	○	○	◉	○
Recurso humano	○	◉	○	○	○

Impacto

¿Qué es Impacto?

El impacto mide el nivel de daño provocado una vez manifestado el riesgo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de impacto		Descripción.
Nivel	Valor	
Crítico.	10	El evento provoca una interrupción completa dentro de las operaciones del área de TIC de JASEC. Provoca una afectación total de los procesos críticos del negocio.
Significativo.	7	El evento provoca una interrupción entre completa y parcial dentro de las operaciones del área de TIC de JASEC. Provoca una afectación parcial de los procesos críticos del negocio.
Moderado.	5	El evento provoca una interrupción en las operaciones del área de TIC de JASEC. Las actividades críticas de negocio no se ven afectadas.
Menor.	3	El evento provoca un impacto leve en las operaciones del área de TIC de JASEC sin generar interrupciones dentro de las operaciones. La afectación en las actividades de negocio es menor a 30%.
Insignificante.	1	El evento no provoca un impacto dentro de las operaciones del área de TIC de JASEC. La afectación en las actividades de negocio es

Nivel de impacto.

La valoración del nivel de impacto causado por una posible materialización de un riesgo asociado a la clasificación presentada a continuación.

¿Cuál nivel de impacto considera que generaría una posible materialización de un riesgo asociado a la clasificación presentada?

*

	1	3	5	7	10
Interrupción eléctrica	○	○	○	○	◉
Fallos en hardware	○	○	○	○	◉
Fallos en software	○	○	○	○	◉
Fallos en comunicaciones	○	○	○	○	◉
Desastres naturales	○	○	○	○	◉
Incendio	○	○	○	○	◉
Fallos en respaldos	○	○	○	○	◉
Virus	○	○	○	◉	○
Violaciones a la seguridad física	○	○	○	◉	○
Intrusión (Hackeo)	○	○	○	◉	○
Recurso humano	○	○	◉	○	○

9.7.4. Cuestionario # 3.

Se presenta la tercera respuesta recibida del cuestionario.

Análisis del nivel de riesgo.

Probabilidad

¿Qué es Probabilidad?

La probabilidad mide la capacidad de ocurrencia del riesgo en el tiempo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de probabilidad		Ocurrencia
Nivel	Valor	
Muy probable.	10	Es muy probable que ocurra un evento en un periodo de 3 meses.
Probable	7	Es poco probable que ocurra un evento en un periodo de 3 a 6 meses.
Moderada	5	El evento ocurrirá en algún momento en un periodo de 6 meses a 1 año.
Poco probable	3	Es poco probable que el evento suceda, pero podría suceder en un periodo de 1 año a 2 años.
Muy poco probable.	1	Es muy poco probable que el evento se presente en un periodo de 2 años.

Nivel de probabilidad.

La valoración del nivel de probabilidad de ocurrencia de un riesgo asociado a la clasificación presentada a continuación.

Según la clasificación de riesgos presentada, ¿Cuál nivel de probabilidad asigna a cada uno?

*

	1	3	5	7	10
Interrupción eléctrica	○	○	○	○	◉
Fallos en hardware	○	◉	○	○	○
Fallos en software	○	○	○	○	◉
Fallos en comunicaciones	○	○	○	◉	○
Desastres naturales	○	◉	○	○	○
Incendio	◉	○	○	○	○
Fallos en respaldos	◉	○	○	○	○
Virus	○	◉	○	○	○
Violaciones a la seguridad física	○	◉	○	○	○
Intrusión (Hackeo)	○	○	◉	○	○
Recurso humano	○	○	◉	○	○

Impacto

¿Qué es Impacto?

El impacto mide el nivel de daño provocado una vez manifestado el riesgo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de impacto		Descripción.
Nivel	Valor	
Crítico.	10	El evento provoca una interrupción completa dentro de las operaciones del área de TIC de JASEC. Provoca una afectación total de los procesos críticos del negocio.
Significativo.	7	El evento provoca una interrupción entre completa y parcial dentro de las operaciones del área de TIC de JASEC. Provoca una afectación parcial de los procesos críticos del negocio.
Moderado.	5	El evento provoca una interrupción en las operaciones del área de TIC de JASEC. Las actividades críticas de negocio no se ven afectadas.
Menor.	3	El evento provoca un impacto leve en las operaciones del área de TIC de JASEC sin generar interrupciones dentro de las operaciones. La afectación en las actividades de negocio es menor a 30%.
Insignificante.	1	El evento no provoca un impacto dentro de las operaciones del área de TIC de JASEC. La afectación en las actividades de negocio es

Nivel de impacto.

La valoración del nivel de impacto causado por una posible materialización de un riesgo asociado a la clasificación presentada a continuación.

¿Cuál nivel de impacto considera que generaría una posible materialización de un riesgo asociado a la clasificación presentada?

*

	1	3	5	7	10
Interrupción eléctrica	◉	○	○	○	○
Fallos en hardware	○	○	○	◉	○
Fallos en software	○	○	○	◉	○
Fallos en comunicaciones	○	○	○	◉	○
Desastres naturales	○	○	◉	○	○
Incendio	○	○	○	○	◉
Fallos en respaldos	○	○	○	◉	○
Virus	○	○	○	◉	○
Violaciones a la seguridad física	○	○	◉	○	○
Intrusión (Hackeo)	○	○	○	◉	○
Recurso humano	○	○	◉	○	○

9.7.5. Cuestionario # 4.

Se presenta la cuarta respuesta recibida del cuestionario.

Análisis del nivel de riesgo.

Probabilidad

¿Qué es Probabilidad?

La probabilidad mide la capacidad de ocurrencia del riesgo en el tiempo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de probabilidad		Ocurrencia
Nivel	Valor	
Muy probable.	10	Es muy probable que ocurra un evento en un periodo de 3 meses.
Probable	7	Es poco probable que ocurra un evento en un periodo de 3 a 6 meses.
Moderada	5	El evento ocurrirá en algún momento en un periodo de 6 meses a 1 año.
Poco probable	3	Es poco probable que el evento suceda, pero podría suceder en un periodo de 1 año a 2 años.
Muy poco probable.	1	Es muy poco probable que el evento se presente en un periodo de 2 años.

Nivel de probabilidad.

La valoración del nivel de probabilidad de ocurrencia de un riesgo asociado a la clasificación presentada a continuación.

Según la clasificación de riesgos presentada, ¿Cuál nivel de probabilidad asigna a cada uno?

*

	1	3	5	7	10
Interrupción eléctrica	○	○	○	◉	○
Fallos en hardware	○	◉	○	○	○
Fallos en software	○	◉	○	○	○
Fallos en comunicaciones	○	◉	○	○	○
Desastres naturales	◉	○	○	○	○
Incendio	◉	○	○	○	○
Fallos en respaldos	○	○	◉	○	○
Virus	○	◉	○	○	○
Violaciones a la seguridad física	◉	○	○	○	○
Intrusión (Hackeo)	◉	○	○	○	○
Recurso humano	○	◉	○	○	○

Impacto

¿Qué es Impacto?

El impacto mide el nivel de daño provocado una vez manifestado el riesgo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de impacto		Descripción.
Nivel	Valor	
Crítico.	10	El evento provoca una interrupción completa dentro de las operaciones del área de TIC de JASEC. Provoca una afectación total de los procesos críticos del negocio.
Significativo.	7	El evento provoca una interrupción entre completa y parcial dentro de las operaciones del área de TIC de JASEC. Provoca una afectación parcial de los procesos críticos del negocio.
Moderado.	5	El evento provoca una interrupción en las operaciones del área de TIC de JASEC. Las actividades críticas de negocio no se ven afectadas.
Menor.	3	El evento provoca un impacto leve en las operaciones del área de TIC de JASEC sin generar interrupciones dentro de las operaciones. La afectación en las actividades de negocio es menor a 30%
Insignificante.	1	El evento no provoca un impacto dentro de las operaciones del área de TIC de JASEC. La afectación en las actividades de negocio es

Nivel de impacto.

La valoración del nivel de impacto causado por una posible materialización de un riesgo asociado a la clasificación presentada a continuación.

¿Cuál nivel de impacto considera que generaría una posible materialización de un riesgo asociado a la clasificación presentada?

*

	1	3	5	7	10
Interrupción eléctrica	○	○	○	○	◉
Fallos en hardware	○	○	○	○	◉
Fallos en software	○	○	○	○	◉
Fallos en comunicaciones	○	○	○	○	◉
Desastres naturales	○	○	◉	○	○
Incendio	○	○	◉	○	○
Fallos en respaldos	◉	○	○	○	○
Virus	○	◉	○	○	○
Violaciones a la seguridad física	○	◉	○	○	○
Intrusión (Hackeo)	○	◉	○	○	○
Recurso humano	○	○	◉	○	○

9.7.6. Cuestionario # 5.

Se presenta la quinta respuesta recibida del cuestionario.

Análisis del nivel de riesgo.

Probabilidad

¿Qué es Probabilidad?

La probabilidad mide la capacidad de ocurrencia del riesgo en el tiempo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de probabilidad		Ocurrencia
Nivel	Valor	
Muy probable.	10	Es muy probable que ocurra un evento en un periodo de 3 meses.
Probable	7	Es poco probable que ocurra un evento en un periodo de 3 a 6 meses.
Moderada	5	El evento ocurrirá en algún momento en un periodo de 6 meses a 1 año.
Poco probable	3	Es poco probable que el evento suceda, pero podría suceder en un periodo de 1 año a 2 años.
Muy poco probable.	1	Es muy poco probable que el evento se presente en un periodo de 2 años.

Nivel de probabilidad.

La valoración del nivel de probabilidad de ocurrencia de un riesgo asociado a la clasificación presentada a continuación.

Según la clasificación de riesgos presentada, ¿Cuál nivel de probabilidad asigna a cada uno?

*

	1	3	5	7	10
Interrupción eléctrica	◉	○	○	○	○
Fallos en hardware	○	○	◉	○	○
Fallos en software	○	○	◉	○	○
Fallos en comunicaciones	○	○	◉	○	○
Desastres naturales	◉	○	○	○	○
Incendio	◉	○	○	○	○
Fallos en respaldos	○	◉	○	○	○
Virus	○	◉	○	○	○
Violaciones a la seguridad física	○	◉	○	○	○
Intrusión (Hackeo)	○	○	◉	○	○
Recurso humano	○	○	◉	○	○

Impacto

¿Qué es Impacto?

El impacto mide el nivel de daño provocado una vez manifestado el riesgo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de impacto		Descripción.
Nivel	Valor	
Crítico.	10	El evento provoca una interrupción completa dentro de las operaciones del área de TIC de JASEC. Provoca una afectación total de los procesos críticos del negocio.
Significativo.	7	El evento provoca una interrupción entre completa y parcial dentro de las operaciones del área de TIC de JASEC. Provoca una afectación parcial de los procesos críticos del negocio.
Moderado.	5	El evento provoca una interrupción en las operaciones del área de TIC de JASEC. Las actividades críticas de negocio no se ven afectadas.
Menor.	3	El evento provoca un impacto leve en las operaciones del área de TIC de JASEC sin generar interrupciones dentro de las operaciones. La afectación en las actividades de negocio es menor a 30%.
Insignificante.	1	El evento no provoca un impacto dentro de las operaciones del área de TIC de JASEC. La afectación en las actividades de negocio es

Nivel de impacto.

La valoración del nivel de impacto causado por una posible materialización de un riesgo asociado a la clasificación presentada a continuación.

¿Cuál nivel de impacto considera que generaría una posible materialización de un riesgo asociado a la clasificación presentada?

*

	1	3	5	7	10
Interrupción eléctrica	○	○	◉	○	○
Fallos en hardware	○	○	◉	○	○
Fallos en software	○	○	◉	○	○
Fallos en comunicaciones	○	○	◉	○	○
Desastres naturales	○	○	◉	○	○
Incendio	○	○	◉	○	○
Fallos en respaldos	○	○	◉	○	○
Virus	○	○	◉	○	○
Violaciones a la seguridad física	○	○	◉	○	○
Intrusión (Hackeo)	○	○	◉	○	○
Recurso humano	○	○	◉	○	○

9.7.7. Cuestionario # 6.

Se presenta la sexta respuesta recibida del cuestionario.

Análisis del nivel de riesgo.

Probabilidad

¿Qué es Probabilidad?

La probabilidad mide la capacidad de ocurrencia del riesgo en el tiempo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de probabilidad		Ocurrencia
Nivel	Valor	
Muy probable.	10	Es muy probable que ocurra un evento en un periodo de 3 meses.
Probable	7	Es poco probable que ocurra un evento en un periodo de 3 a 6 meses.
Moderada	5	El evento ocurrirá en algún momento en un periodo de 6 meses a 1 año.
Poco probable	3	Es poco probable que el evento suceda, pero podría suceder en un periodo de 1 año a 2 años.
Muy poco probable.	1	Es muy poco probable que el evento se presente en un periodo de 2 años.

Nivel de probabilidad.

La valoración del nivel de probabilidad de ocurrencia de un riesgo asociado a la clasificación presentada a continuación.

Según la clasificación de riesgos presentada, ¿Cuál nivel de probabilidad asigna a cada uno?

*

	1	3	5	7	10
Interrupción eléctrica	○	○	○	○	◉
Fallos en hardware	○	○	○	◉	○
Fallos en software	○	○	◉	○	○
Fallos en comunicaciones	○	○	○	◉	○
Desastres naturales	◉	○	○	○	○
Incendio	○	○	◉	○	○
Fallos en respaldos	○	◉	○	○	○
Virus	○	◉	○	○	○
Violaciones a la seguridad física	○	◉	○	○	○
Intrusión (Hackeo)	○	○	◉	○	○
Recurso humano	○	○	○	◉	○

Impacto

¿Qué es Impacto?

El impacto mide el nivel de daño provocado una vez manifestado el riesgo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Nivel de impacto		Descripción.
Nivel	Valor	
Crítico.	10	El evento provoca una interrupción completa dentro de las operaciones del área de TIC de JASEC. Provoca una afectación total de los procesos críticos del negocio.
Significativo.	7	El evento provoca una interrupción entre completa y parcial dentro de las operaciones del área de TIC de JASEC. Provoca una afectación parcial de los procesos críticos del negocio.
Moderado.	5	El evento provoca una interrupción en las operaciones del área de TIC de JASEC. Las actividades críticas de negocio no se ven afectadas.
Menor.	3	El evento provoca un impacto leve en las operaciones del área de TIC de JASEC sin generar interrupciones dentro de las operaciones. La afectación en las actividades de negocio es menor a 30%.
Insignificante.	1	El evento no provoca un impacto dentro de las operaciones del área de TIC de JASEC. La afectación en las actividades de negocio es

Nivel de impacto.

La valoración del nivel de impacto causado por una posible materialización de un riesgo asociado a la clasificación presentada a continuación.

¿Cuál nivel de impacto considera que generaría una posible materialización de un riesgo asociado a la clasificación presentada?

*

	1	3	5	7	10
Interrupción eléctrica	◉	○	○	○	○
Fallos en hardware	○	◉	○	○	○
Fallos en software	○	○	◉	○	○
Fallos en comunicaciones	○	○	◉	○	○
Desastres naturales	○	○	◉	○	○
Incendio	○	○	○	○	◉
Fallos en respaldos	○	○	◉	○	○
Virus	○	○	○	○	◉
Violaciones a la seguridad física	○	○	○	◉	○
Intrusión (Hackeo)	○	○	○	◉	○
Recurso humano	○	○	○	◉	○

9.8. Apéndice H: Niveles de probabilidad de ocurrencia e impacto.

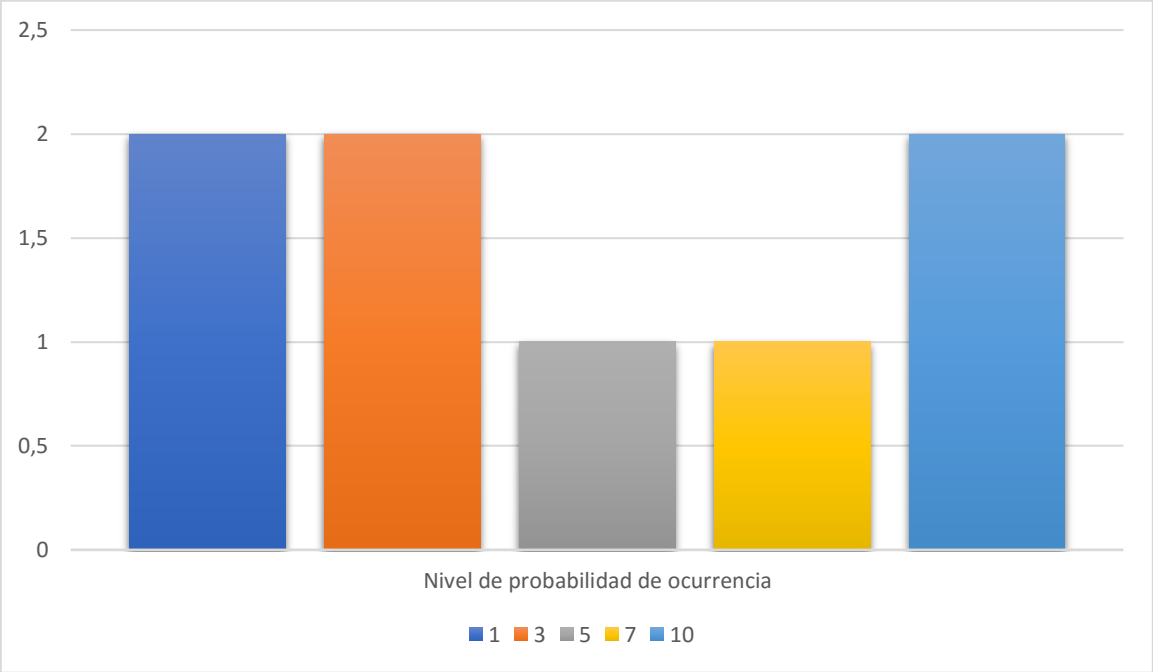
En este apéndice se presentan un conjunto de gráficos que representan a modo de resumen, los resultados obtenidos en los cuestionarios del apéndice G.

9.8.1. Nivel de probabilidad de ocurrencia.

Los siguientes gráficos representan los niveles de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.

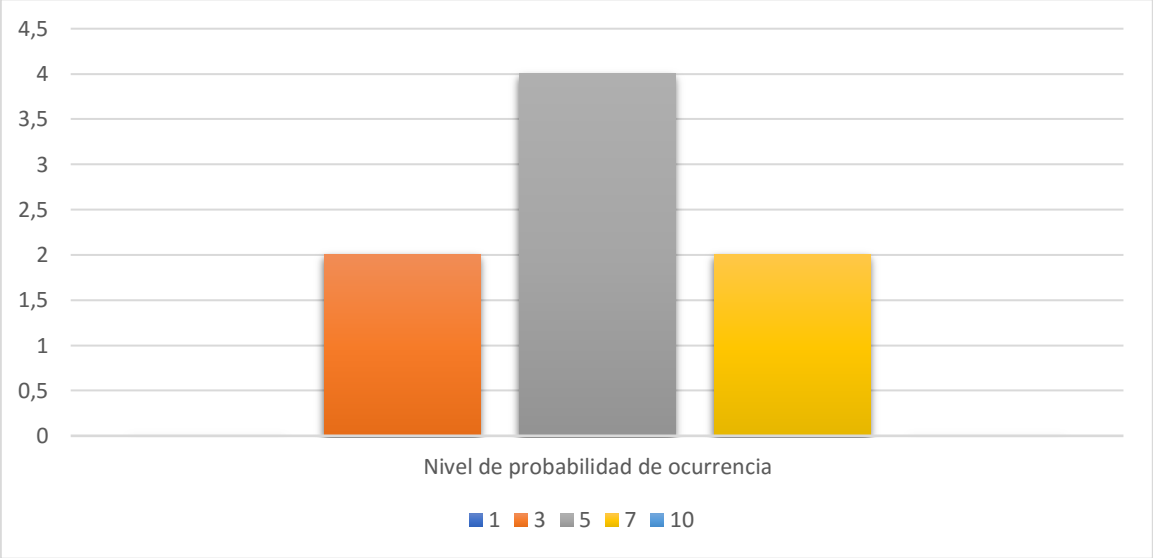
9.8.1.1. Interrupción eléctrica.

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.



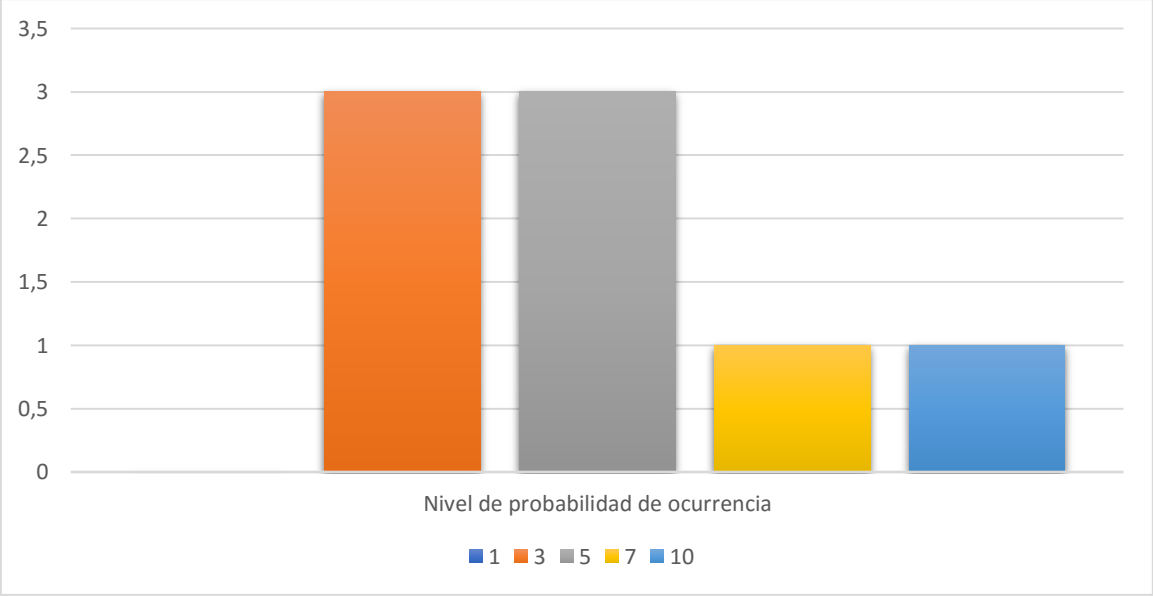
9.8.1.2. Fallos en hardware.

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.



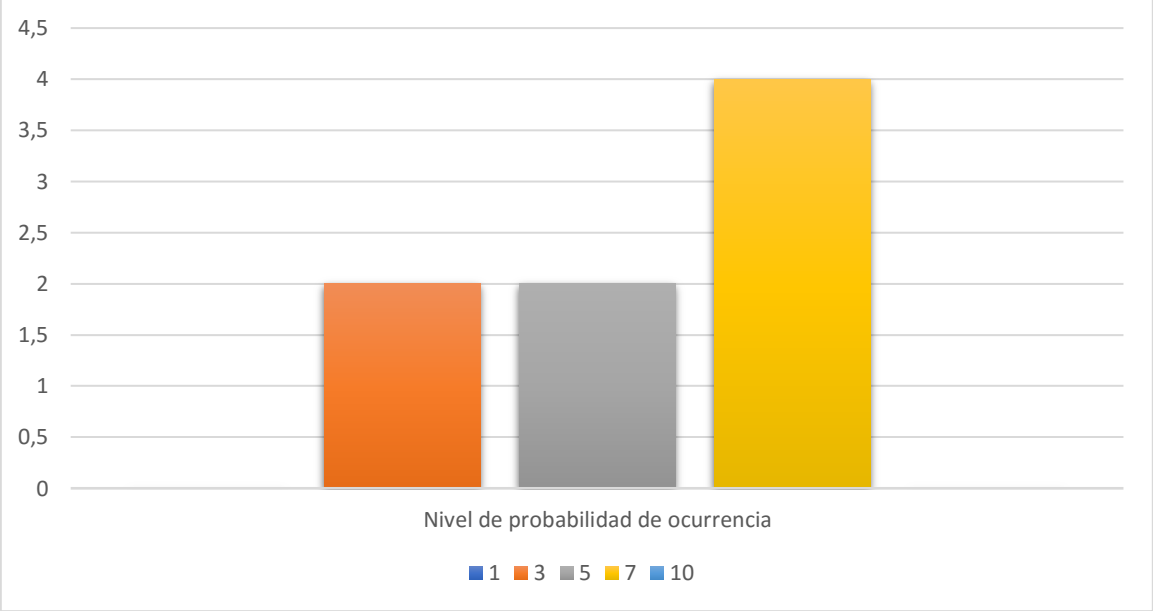
9.8.1.3. Fallos en software.

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.



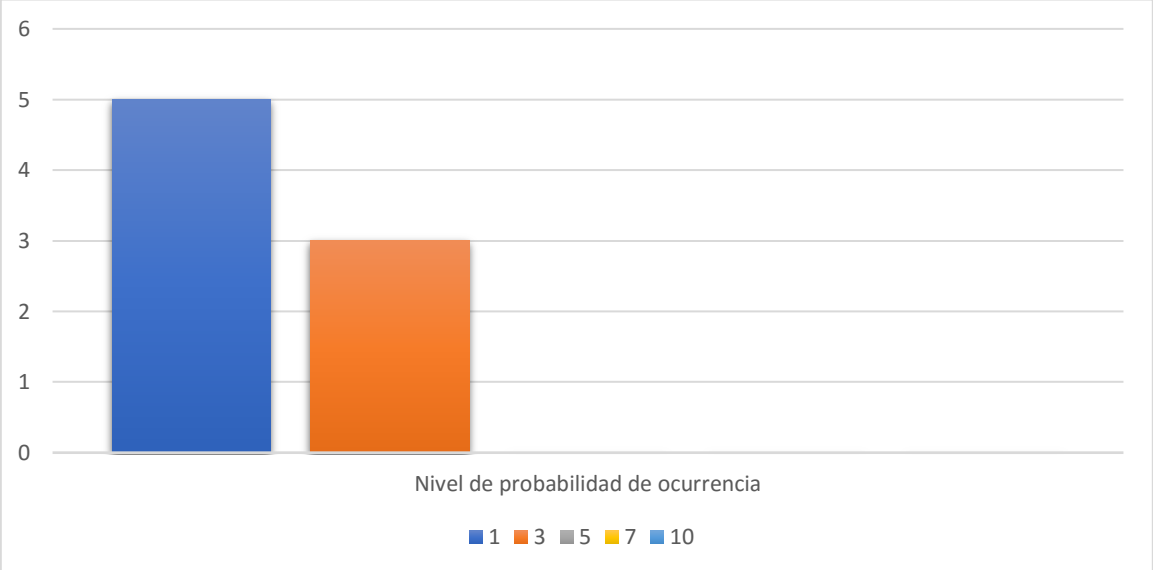
9.8.1.4. Fallos en comunicaciones.

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.



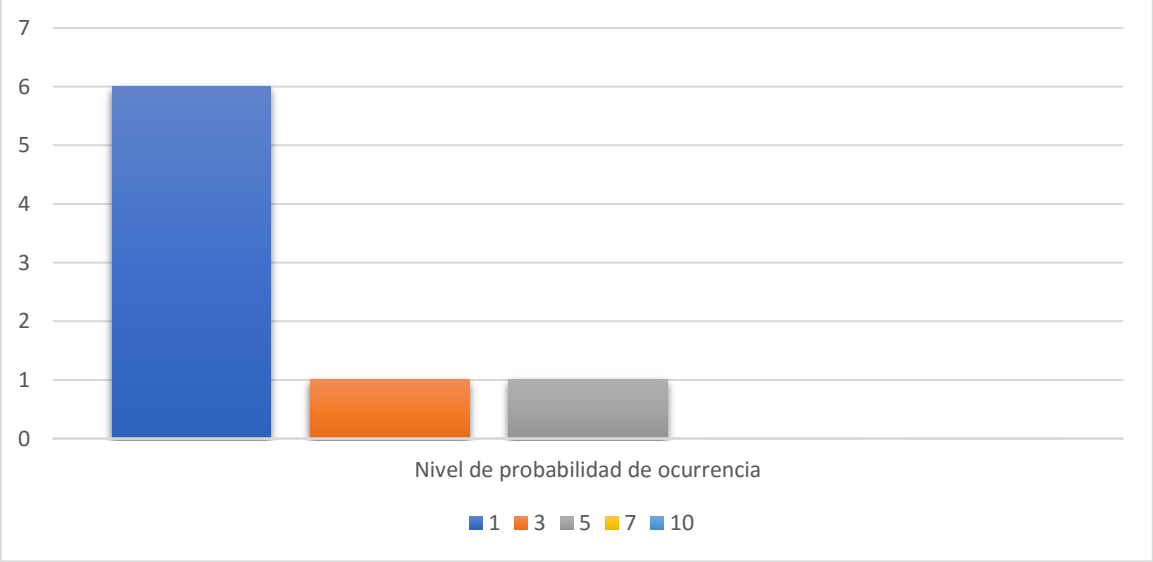
9.8.1.5. Desastres naturales.

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.



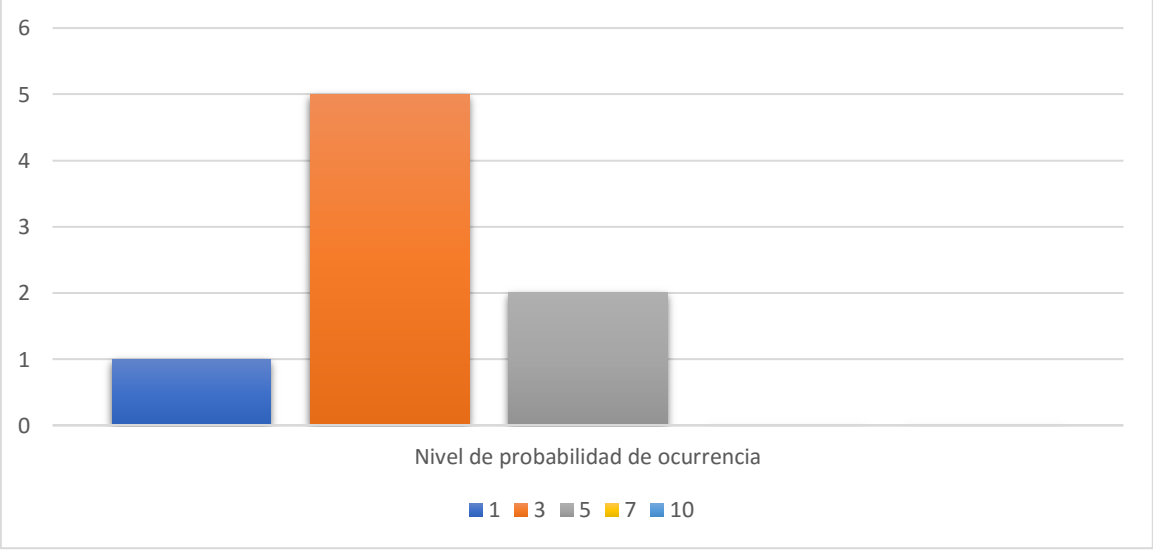
9.8.1.6. Incendio

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.



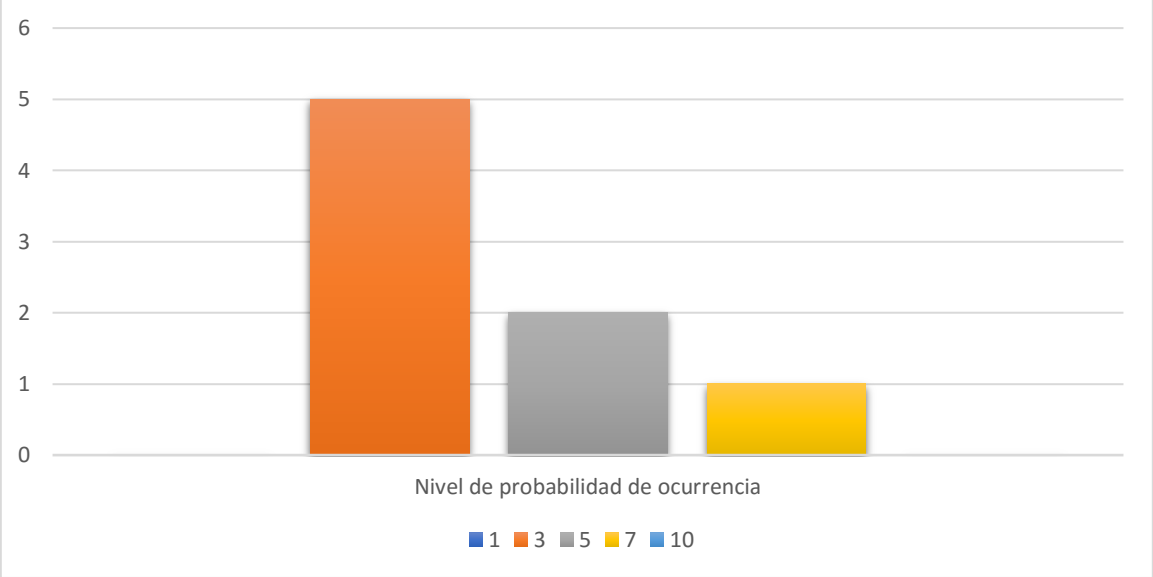
9.8.1.7. Fallos en respaldos.

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.



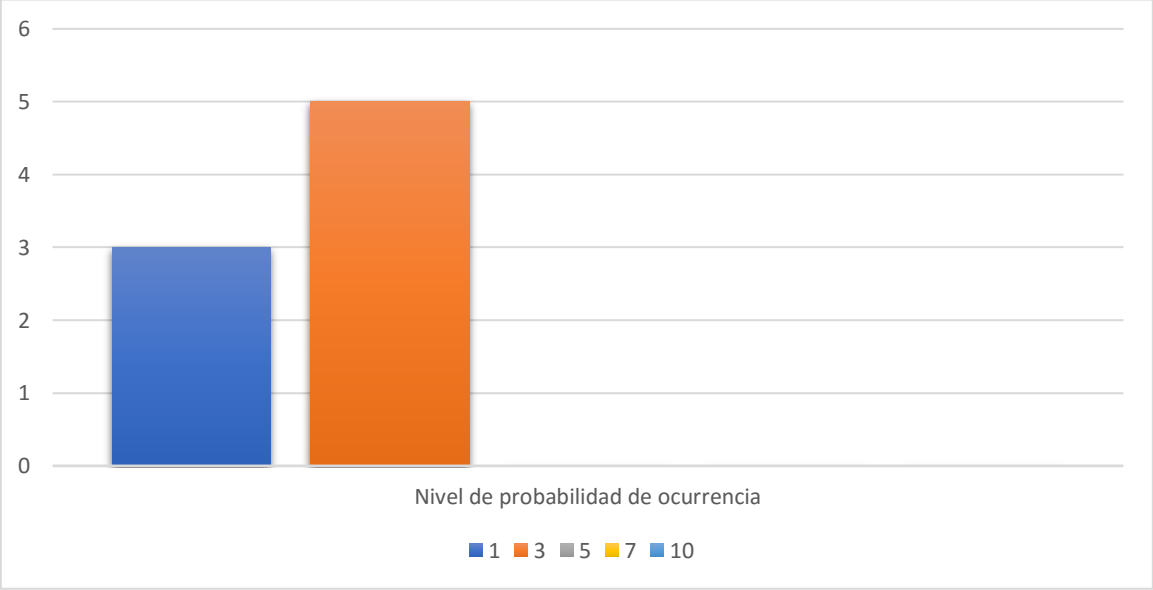
9.8.1.8. Virus

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.



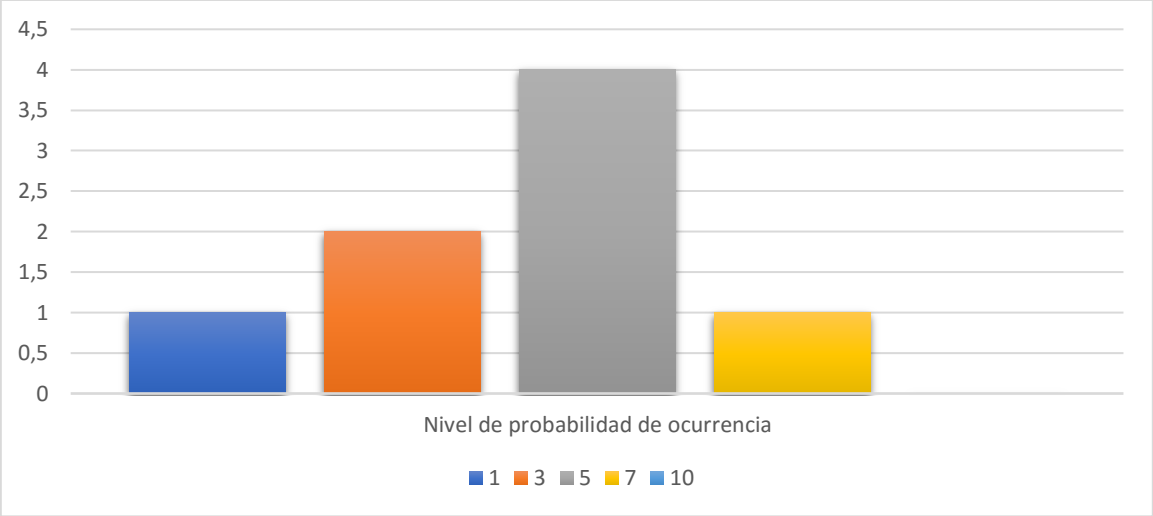
9.8.1.9. Violaciones a la seguridad física.

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.



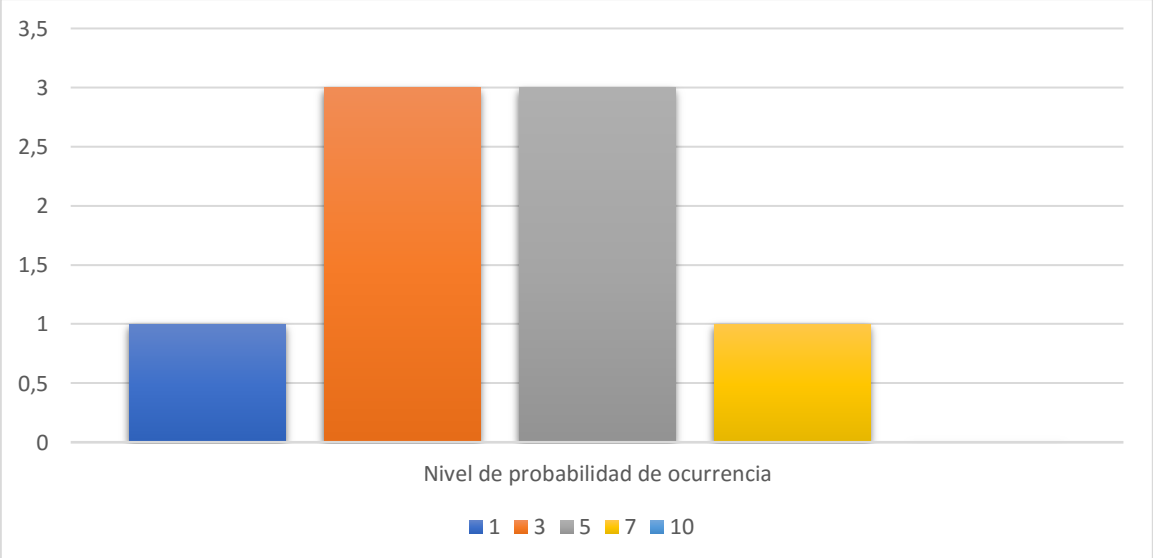
9.8.1.10. Intrusión.

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.



9.8.1.11. Recurso humano

Nivel de probabilidad de ocurrencia de los riesgos de TI, determinado por los colaboradores del área de TIC.

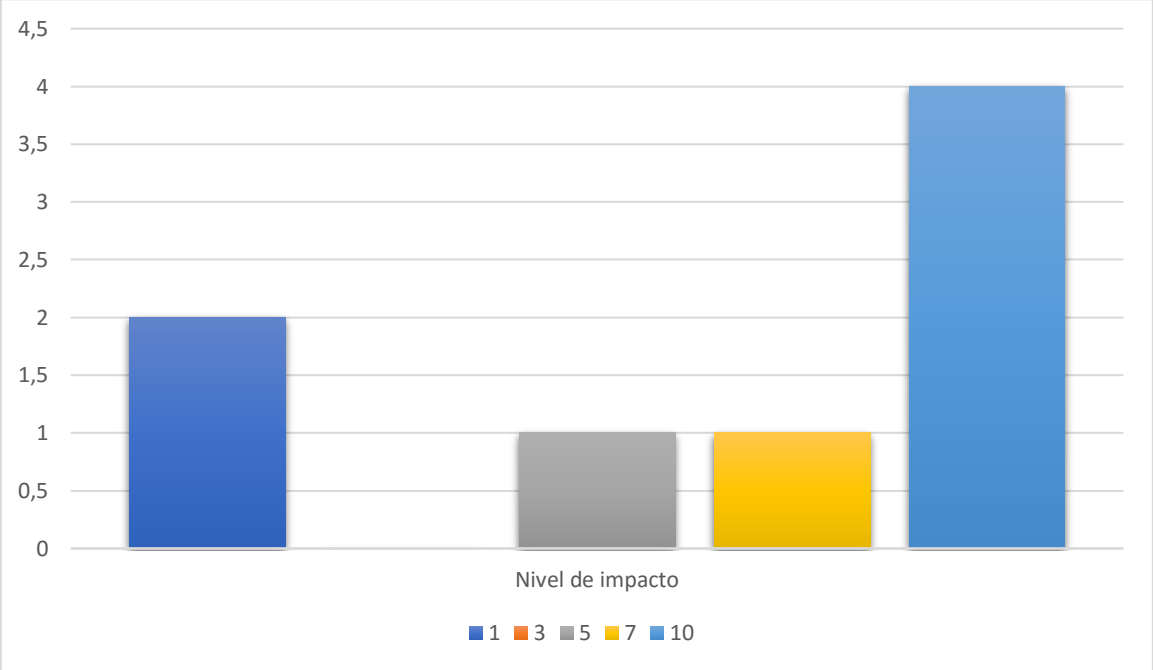


9.8.2. Nivel de impacto.

Los siguientes gráficos representan los niveles de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.

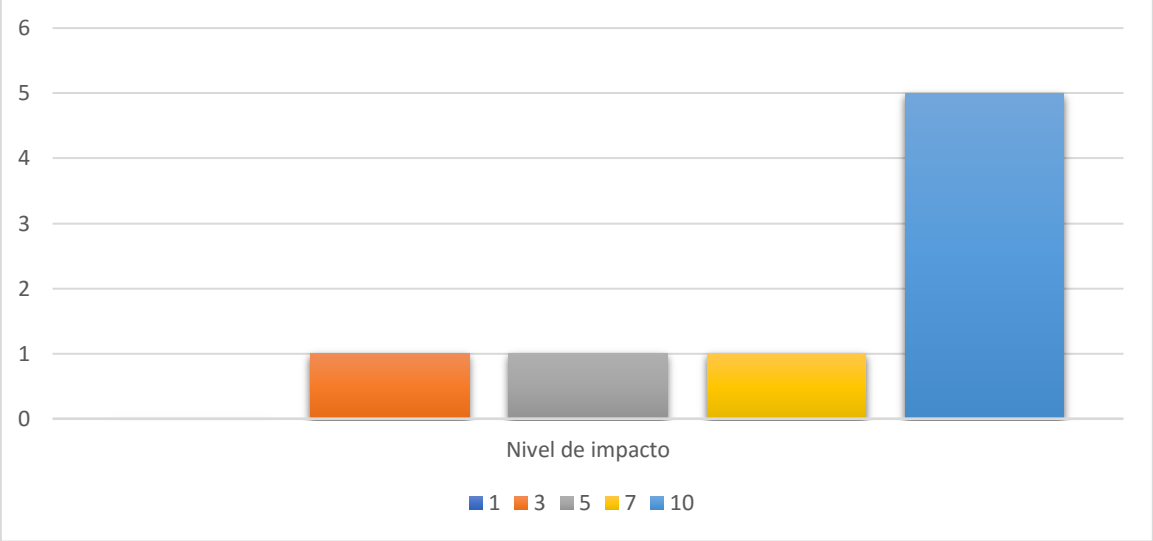
9.8.2.1. Interrupción eléctrica.

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.



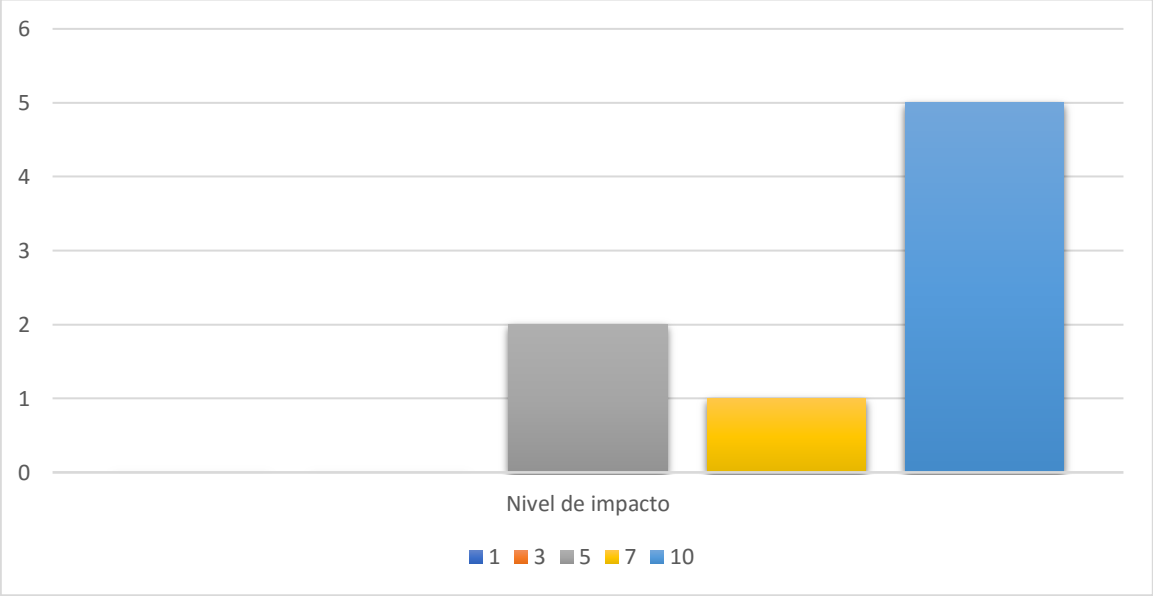
9.8.2.2. Fallos en hardware

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.



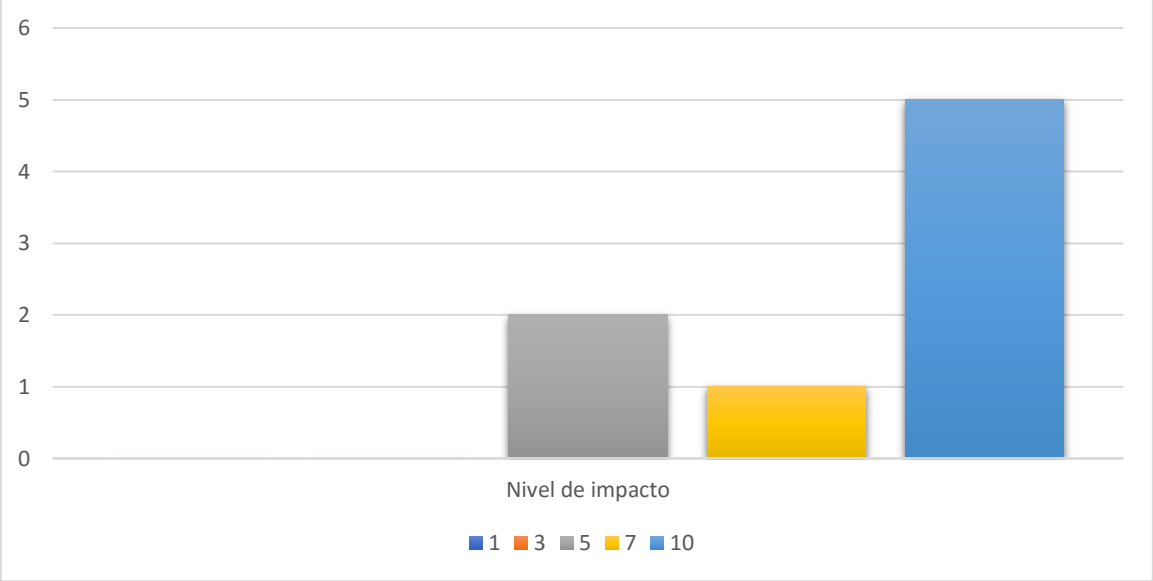
9.8.2.3. Fallos en software.

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.



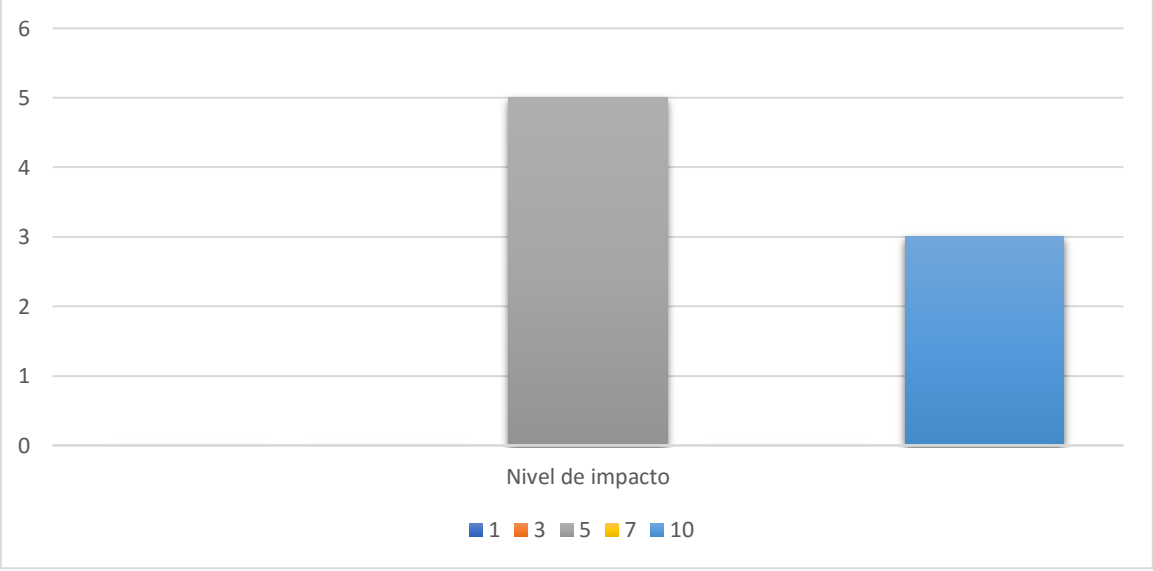
9.8.2.4. Fallos en comunicaciones.

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.



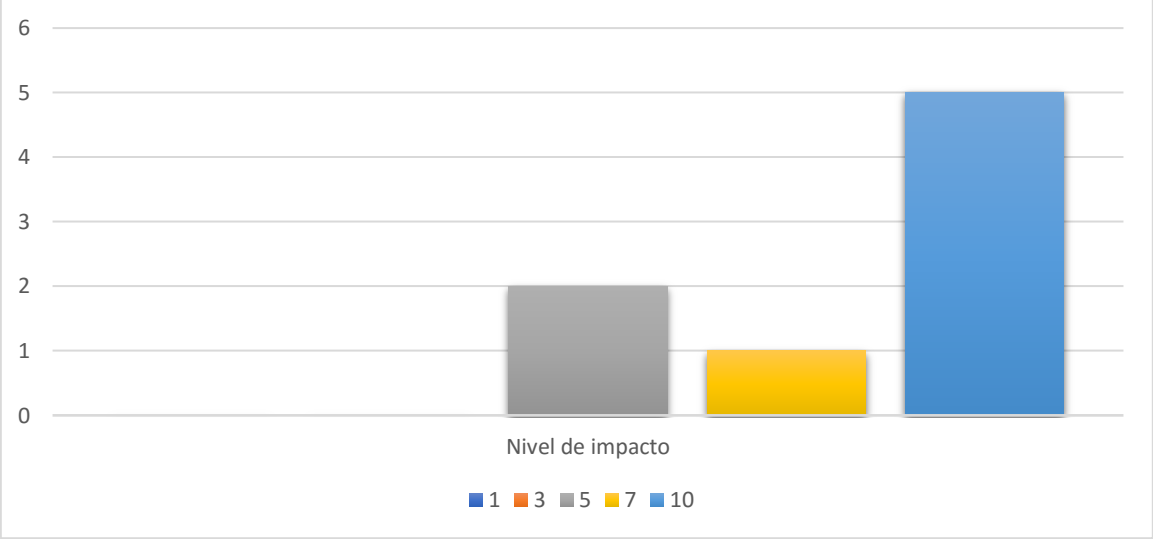
9.8.2.5. Desastre natural.

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.



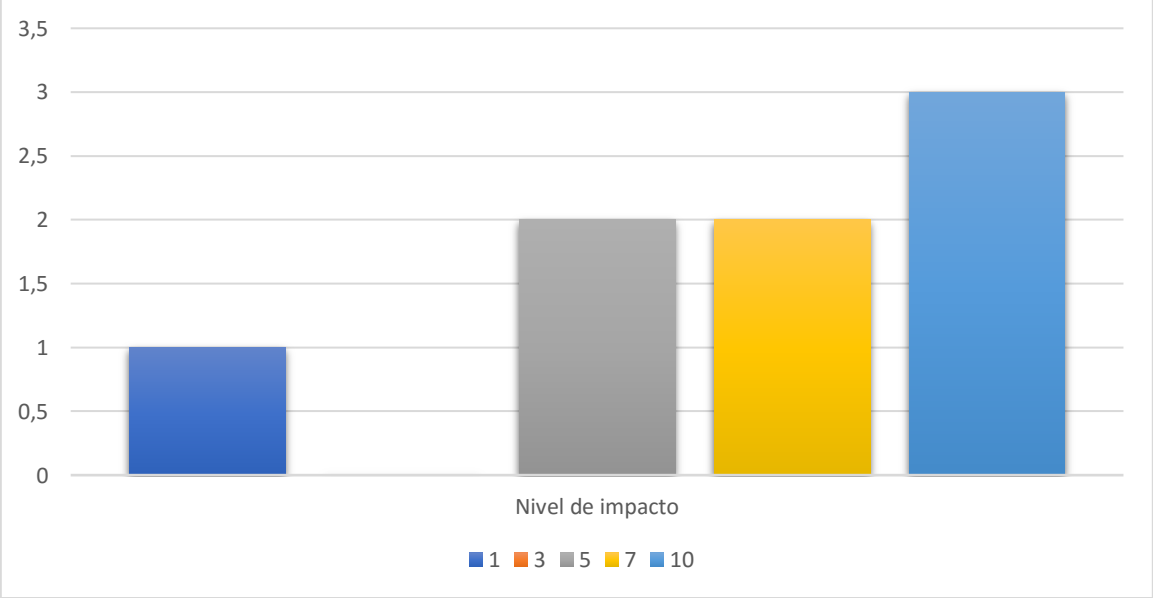
9.8.2.6. Incendio.

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.



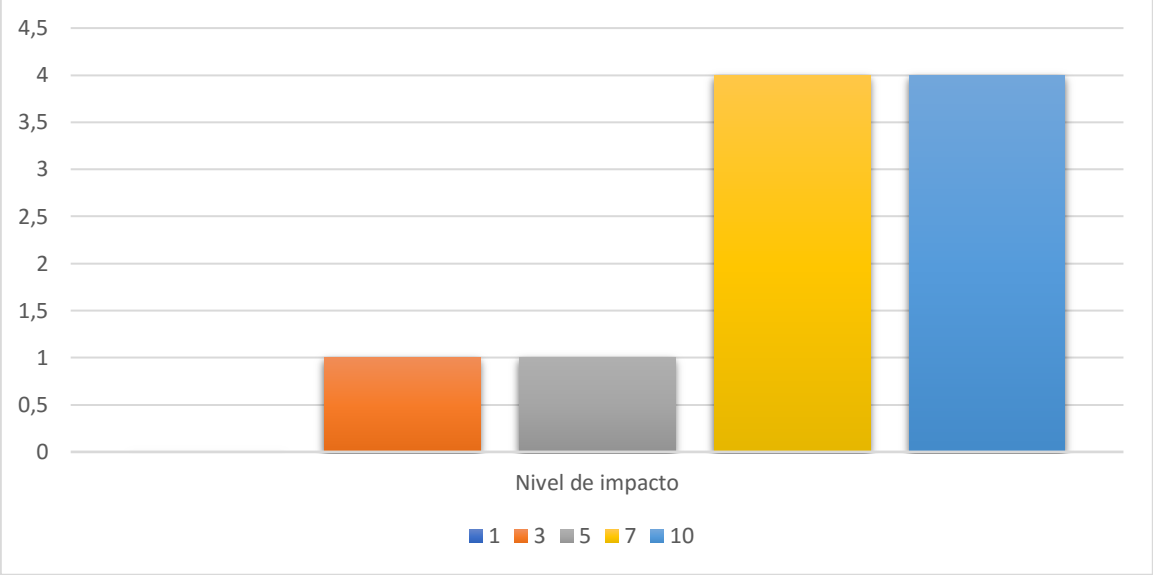
9.8.2.7. Fallos en respaldos.

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.



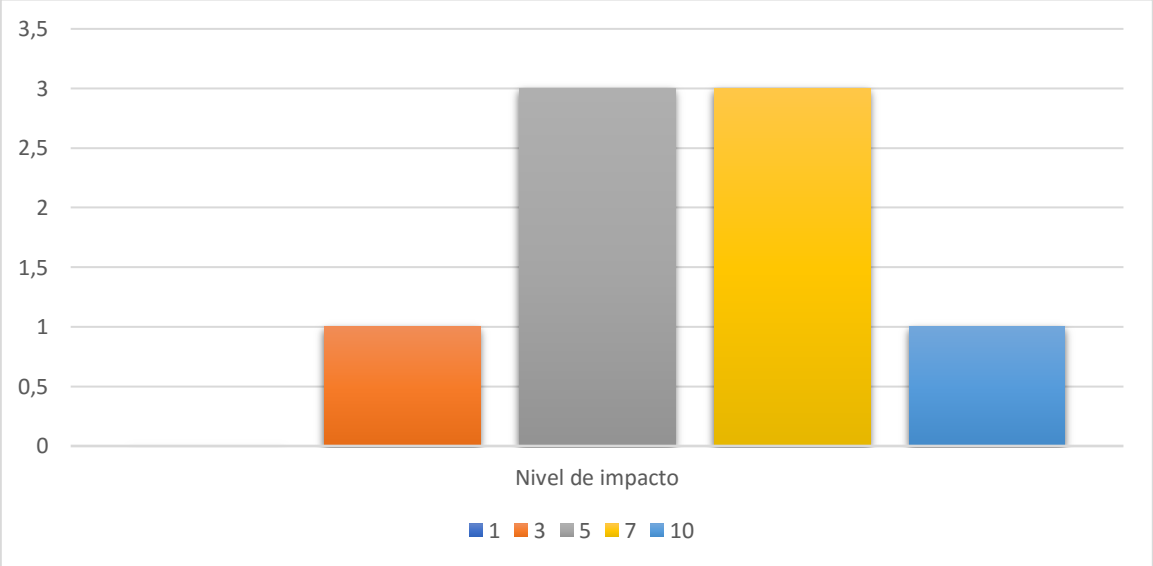
9.8.2.8. Virus.

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.



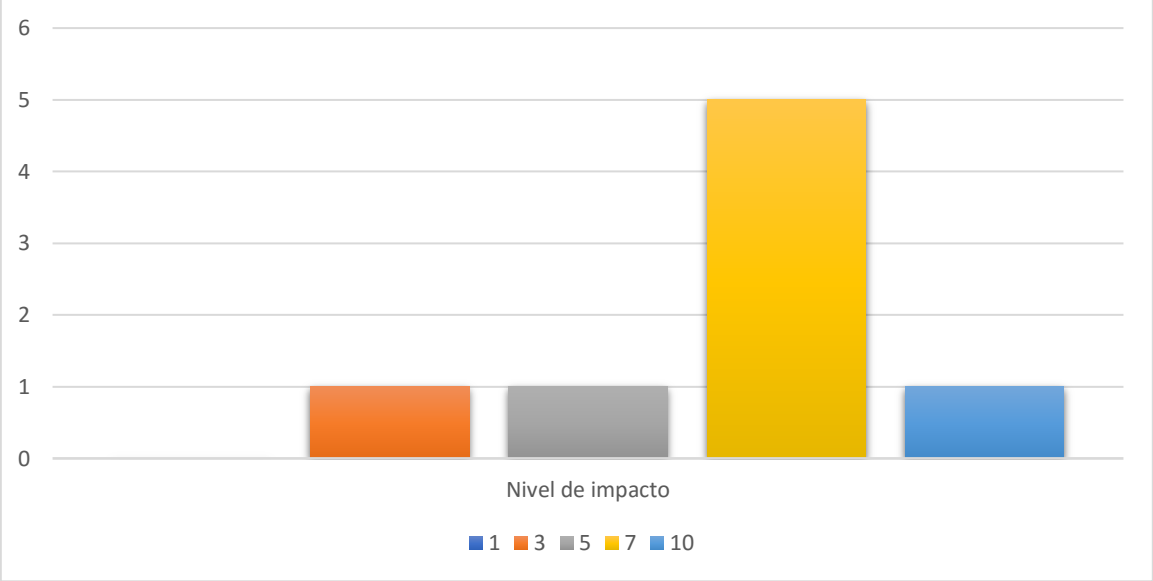
9.8.2.9. Violaciones a seguridad física.

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.



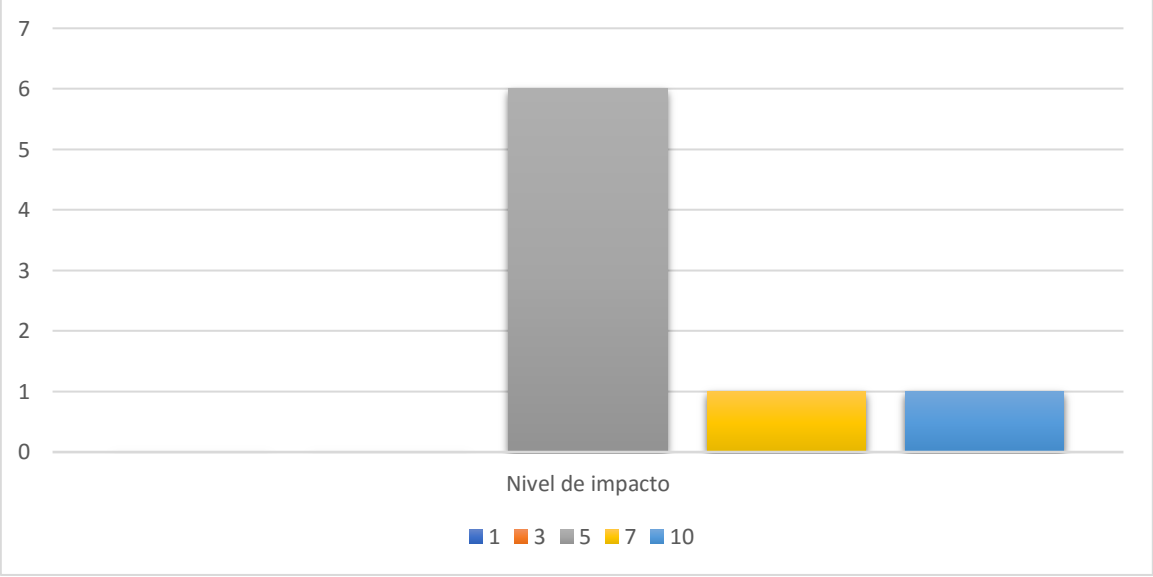
9.8.2.10. Intrusión.

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.



9.8.2.11. Recurso humano.

Nivel de impacto de los riesgos de TI, determinado por los colaboradores del área de TIC.

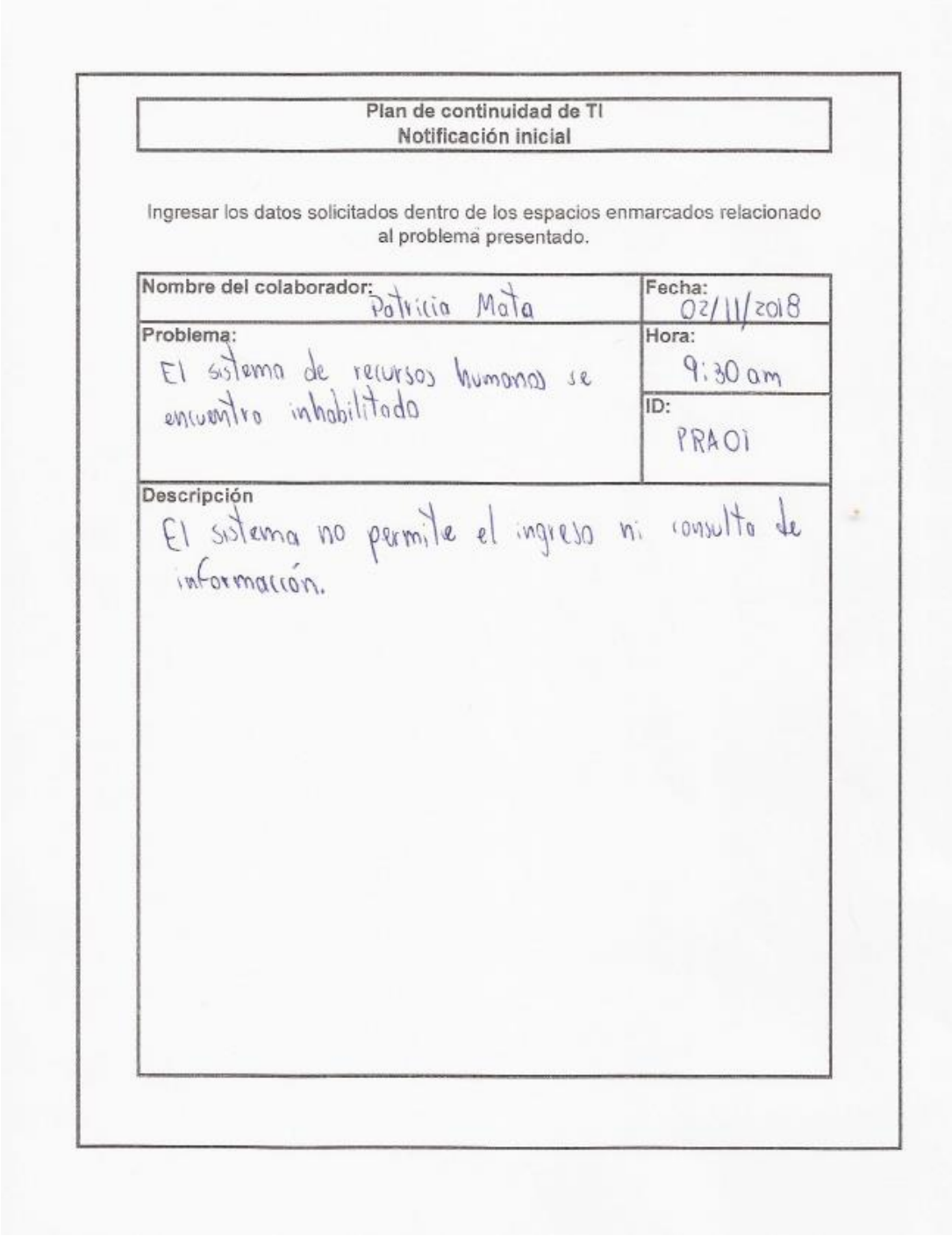


9.9. Apéndice I: Verificación de plan de continuidad.

En este apéndice se presentan los documentos generados como parte de la verificación del plan de continuidad.

9.9.1. Notificación inicial.

A continuación la notificación inicial presentada que activo el plan de continuidad y la ejecución de las estrategias reactivas correspondientes.



Plan de continuidad de TI
Notificación inicial

Ingresar los datos solicitados dentro de los espacios enmarcados relacionado al problema presentado.

Nombre del colaborador: Patricia Mata	**Fecha:** 02/11/2018
Problema: El sistema de recursos humanos se encuentra inhabilitado	**Hora:** 9:30 am
	ID: PRA01
Descripción El sistema no permite el ingreso ni consulta de información.	

9.9.2. Estrategia reactiva.

A continuación se presenta el documento de la plantilla que contiene la estrategia reactiva que permite el restablecimiento del activo.

Plan de continuidad de TI
Estrategia reactiva
Aplicativos: Oracle 10g.

Nombre del colaborador: Miguel Soto **Fecha:** 02/11/2018

Estrategia reactiva para habilitar algún aplicativo de Oracle 10g en caso de sufrir una interrupción.

Marque una ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Inspeccionar	Código: PR-07 Marque ✓
1) Ingresar a servidor de aplicativos.	✓
2) Ingresar Interfaz Gráfica de Servidor de Aplicaciones (OAS).	✓
3) ¿Interfaz no responde?	
a) Acceder por medio de acceso remoto al servidor de aplicaciones.	✓
b) Reiniciar la interfaz gráfica.	✓
c) ¿Interfaz no responde?	✓
i) Revisar servicios del servidor que utiliza la interfaz	✓
ii) ¿Servicios no responden?	✓
(1) Reiniciar los servicios.	✓
(2) ¿Servicios no pueden reiniciarse?	
(a) Reiniciar el servidor.	✓
4) Revisar estado del uso del servidor.	✓
5) ¿Fallan todos los servicios?	
a) Reiniciar el servicio de aplicaciones (gráfica).	
b) ¿Servicios no funcionan?	
i) Revisar conectividad de BD.	
ii) ¿Problemas con BD?	
(1) Realizar pasos anteriores.	✓
6) Revisar estado de cada aplicativo.	

Inspeccionar	Código: PR-07 Marque ✓
7) ¿Falla en un aplicativo?	
a) Reiniciar el aplicativo.	
b) ¿No funciona?	
i) Revisar conectividad de BD.	
ii) ¿Problemas con BD?	
(1) Revisar prioridad de servicios con otros aplicativos.	✓
(2) Terminar tareas del aplicativo que genera conflicto.	✓
(3) ¿No hay tareas con conflictos?	
(a) Realizar pasos anteriores.	
iii) Crear un nuevo archivo de ambiente para aplicativo.	
iv) ¿No funciona?	
(1) Respaldar carpeta del aplicativo en servidor de producción.	
(2) Respaldar carpeta Oracle\forms\server en servidor de producción.	
(3) Renombrar carpetas del aplicativo en servidor de contingencia.	
(a) Formas.	
(b) Reportes.	
(c) Recursos.	
(4) Redireccionar el aplicativo al servidor de contingencia.	
8) Realizar pruebas de conectividad y acceso.	✓
9) ¿Servidor de aplicaciones no responde?	
a) Respaldar carpeta de sistemas en servidor de producción.	

Inspeccionar	Código: PR-07 Marque ✓
b) Respaldar carpeta Oracle\forms\server en servidor de producción.	
c) Renombrar carpeta de sistemas en servidor de contingencia.	
d) Copiar carpetas de servidor de producción en servidor de contingencia.	
e) Redireccionar enlaces a equipo de contingencia (habilitar servicios).	
Observaciones. Se comprueba el correcto funcionamiento del sistema de recursos humanos	

9.9.3. Bitácora de estrategias reactivas.

A continuación se presenta la bitácora de las estrategias reactivas aplicadas.

Plan de continuidad de TI
Bitácora de estrategias reactivas.

Registrar los datos solicitados y detallar las estrategias reactivas implementadas.

Bitácora de estrategias reactivas.		ID problema: PRA01
Responsable: Miguel Soto		Fecha: 02/11/2018
Código de estrategia reactiva.	**Detalle**	**Completado (Si/No)**
PRO7	Se reinicia el servidor y se comprueba el correcto funcionamiento del sistema	Si

9.9.4. Cierre del plan de continuidad.

A continuación se presenta el documento de la plantilla que con las inspecciones realizadas para cerrar el plan de continuidad.

Plan de continuidad de TI
Cierre de plan de continuidad de TI
Software y acceso a información

Nombre del colaborador: Eddy Martínez **Fecha:** 02/11/2018

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intension de cerrar el plan de continuidad de TI.
Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PC-06 Marque ✓
1) Aplicaciones y servicios de la institución habilitados.	✓
2) Comunicación entre áreas operativas y centro de datos a nivel lógico (aplicaciones y bases de datos).	✓
3) Acceso controlado a los usuarios y nivel de acceso.	✓
4) Capacidad de procesamiento, desempeño e integridad.	✓
5) Seguridad de información.	✓
Observaciones.	

Plan de continuidad de TI
Cierre de plan de continuidad de TI
Activos de información

Nombre del colaborador: Eddy Martinez **Fecha:** 07/11/2018

Los siguientes elementos deben ser revisados por los responsables del plan de continuidad de TI con la intension de cerrar el plan de continuidad de TI.
Marque un ✓ en cada elemento inspeccionado, en caso de encontrar alguna anomalia que dificulte completarlo, detallarlo en la sección de observaciones.

Elementos a inspeccionar.	Código: PC-05
	Marqué ✓
1) Servidores en centro de datos disponible.	✓
2) Sistemas de almacenamiento de información y respaldos.	✓
3) Servicios de control de acceso y herramientas de seguridad de información.	✓
4) Dominio de la institución.	✓
5) Impresoras y centros de copiado.	
6) Activos de tecnología del personal operativo y administrativo.	
Observaciones.	

9.1. Apéndice J: Entrevistas realizadas.

En este apéndice se presentan los documentos generados como parte de las entrevistas realizadas.

9.1.1. Entrevista 01.

Se detalla el documento generado en la entrevista 01.

Entrevista

Proyecto: *Propuesta de plan de continuidad de TI para la Unidad de Tecnologías de Información y Comunicación de JASEC.*

Fecha:	27/07/2018	**Hora Inicio/Finalización:**	1:30 pm / 2:30 pm
Lugar:	JASEC		
Objetivo de la reunión:	Ampliar conocimiento sobre la organización.		
Participantes:	Eddy Martínez, Rodolfo Sanabria, Sonia Espinoza, Cristian Navarro.		

Temas Tratados

No.	Asunto	Comentarios
1	¿Cuál es el estado de la documentación existente?	Sitio en la intranet con documentos: • Formularios. • Instructivos. • Normativas.
2	¿Cuál es el estado del Inventario de TI actual?	Inventario desactualizado. Necesario realizar actualización.
3	¿Existen análisis previos dentro del área de TIC?	No existen, necesario realizar un análisis de impacto de negocio y un análisis de riesgos.

Uso Confidencial Pág. 1/2

9.2. Apéndice K: Grupos focales realizadas.

En este apéndice se presentan los documentos generados como parte de los grupos focales realizados.

9.2.1. Grupo focal 01.

Se detalla el documento generado del grupo focal 01.

Grupo focal

Proyecto: *Propuesta de plan de continuidad de TI para la Unidad de Tecnologías de Información y Comunicación de JASEC.*

Fecha:	03/08/2018	**Hora Inicio/Finalización:**	9:30 pm / 10:30 pm
Lugar:	JASEC		
Objetivo de la reunión:	Presentación de base teórica a aplicar y validación de propuesta metodológica a aplicar para el desarrollo del plan de continuidad.		
Participantes:	Eddy Martínez, Rodolfo Sanabria, Sonia Espinoza, Guillermo Gómez, Cristian Navarro.		

Temas Tratados

No.	Asunto	Comentarios	Cambios sugeridos.
1	Propuesta metodológica. Desarrollar un análisis de impacto de negocio, análisis de riesgos, desarrollo de estrategias para la continuidad de TI.	Aceptación de los colaboradores de JASEC participantes.	
2	Base teórica a aplicar. Seguir lo recomendado dentro del ISO 22301, 31000, y el manual desarrollado por la CCSS.	Aceptación de la base teórica.	Tomar como referencia lo recomendado dentro de las normas y guías, adaptar según la necesidad propia tanto de la organización como del proyecto.
3			

Uso Confidencial Pág. 1/1

9.2.2. Grupo focal 02.

Se detalla el documento generado del grupo focal 02.

Grupo focal

Proyecto: *Propuesta de plan de continuidad de TI para la Unidad de Tecnologías de Información y Comunicación de JASEC.*

Fecha:	05/10/2018	**Hora Inicio/Finalización:**	2:30 pm / 3:00 pm
Lugar:	JASEC		
Objetivo de la reunión:	Validar creación de estrategias proactivas y reactivas dentro del plan de continuidad.		
Participantes:	Eddy Martínez, Rodolfo Sanabria, Sonia Espinoza, Cristian Navarro.		

Temas Tratados

No.	Asunto	Comentarios	Cambios sugeridos.
1	Creación de estrategias proactivas y reactivas dentro del plan de continuidad.	Aprobación por parte de los colaboradores de JASEC.	Creación de inspecciones para cerrar el plan de continuidad.
2	Procedimientos de activación del plan de continuidad.	Aprobación por parte de los colaboradores de JASEC.	
3			

Uso Confidencial Pág. 1/1

9.2.3. Grupo focal 03.

Se detalla el documento generado del grupo focal 03.

Grupo focal

Proyecto: *Propuesta de plan de continuidad de TI para la Unidad de Tecnologías de Información y Comunicación de JASEC.*

Fecha:	10/10/2018	**Hora Inicio/Finalización:**	10:30 pm / 11:30 pm
Lugar:	JASEC		
Objetivo de la reunión:	Organización encargada del plan de continuidad y asignación de roles.		
Participantes:	Eddy Martínez, Rodolfo Sanabria, Sonia Espinoza, Cristian Navarro.		

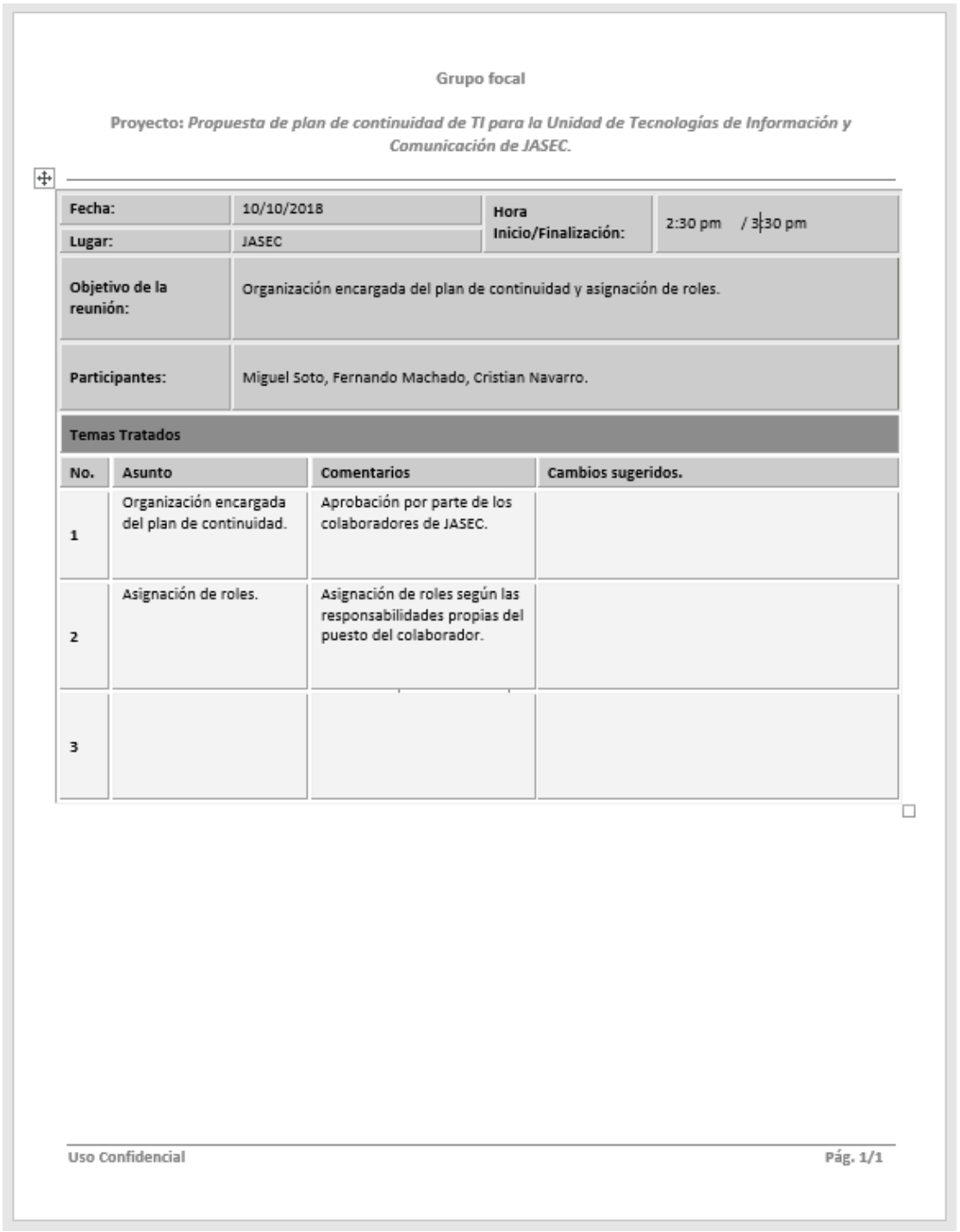
Temas Tratados

No.	Asunto	Comentarios	Cambios sugeridos.
1	Organización encargada del plan de continuidad.	Aprobación por parte de los colaboradores de JASEC.	
2	Asignación de roles.	Asignación de roles según las responsabilidades propias del puesto del colaborador.	
3			

Uso Confidencial Pág. 1/1

9.2.4. Grupo focal 04.

Se detalla el documento generado del grupo focal 04.



Grupo focal

Proyecto: *Propuesta de plan de continuidad de TI para la Unidad de Tecnologías de Información y Comunicación de JASEC.*

Fecha:	10/10/2018	**Hora Inicio/Finalización:**	2:30 pm / 3:30 pm
Lugar:	JASEC		
Objetivo de la reunión:	Organización encargada del plan de continuidad y asignación de roles.		
Participantes:	Miguel Soto, Fernando Machado, Cristian Navarro.		

Temas Tratados

No.	Asunto	Comentarios	Cambios sugeridos.
1	Organización encargada del plan de continuidad.	Aprobación por parte de los colaboradores de JASEC.	
2	Asignación de roles.	Asignación de roles según las responsabilidades propias del puesto del colaborador.	
3			

Uso Confidencial Pág. 1/1

9.2.5. Grupo focal 05.

Se detalla el documento generado del grupo focal 05.

Grupo focal

Proyecto: *Propuesta de plan de continuidad de TI para la Unidad de Tecnologías de Información y Comunicación de JASEC.*

Fecha:	23/10/2018	**Hora Inicio/Finalización:**	9:30 pm / 11:00 pm
Lugar:	JASEC		
Objetivo de la reunión:	Generación de estrategias reactivas y proactivas enfocadas a los aplicativos.		
Participantes:	Miguel Soto, Fernando Machado, Cristian Navarro.		

Temas Tratados

No.	Asunto	Comentarios	Cambios sugeridos.
1	Generación de estrategia reactiva.	Colaboración entre los participantes para la elaboración de las estrategias reactivas.	
2	Generación de estrategias proactivas.	Colaboración entre los participantes para la elaboración de las estrategias proactivas.	
3			

Uso Confidencial Pág. 1/1

9.2.6. Grupo focal 06.

Se detalla el documento generado del grupo focal 06.

Grupo focal

Proyecto: *Propuesta de plan de continuidad de TI para la Unidad de Tecnologías de Información y Comunicación de JASEC.*

Fecha:	24/10/2018	**Hora Inicio/Finalización:**	2:30 pm / 4:00 pm
Lugar:	JASEC		
Objetivo de la reunión:	Generación de estrategias reactivas y proactivas enfocadas a los comunicaciones y bases de datos.		
Participantes:	Eddy Martínez, Rodolfo Sanabria, Cristian Navarro.		

Temas Tratados

No.	Asunto	Comentarios	Cambios sugeridos.
1	Generación de estrategia reactiva.	Colaboración entre los participantes para la elaboración de las estrategias reactivas.	
2	Generación de estrategias proactivas.	Colaboración entre los participantes para la elaboración de las estrategias proactivas.	
3			

Uso Confidencial Pág. 1/1

9.2.7. Grupo focal 07.

Se detalla el documento generado del grupo focal 07.

Grupo focal

Proyecto: *Propuesta de plan de continuidad de TI para la Unidad de Tecnologías de Información y Comunicación de JASEC.*

Fecha:	25/10/2018	**Hora Inicio/Finalización:**	8:00 am / 9:00 am
Lugar:	JASEC		
Objetivo de la reunión:	Generación de estrategias reactivas y proactivas enfocadas a los comunicaciones y bases de datos.		
Participantes:	Marco Alvarado, Alejandra Chávez, Cristian Navarro.		

Temas Tratados

No.	Asunto	Comentarios	Cambios sugeridos.
1	Generación de estrategia reactiva.	Colaboración entre los participantes para la elaboración de las estrategias reactivas.	
2	Generación de estrategias proactivas.	Colaboración entre los participantes para la elaboración de las estrategias proactivas.	
3			

Uso Confidencial Pág. 1/1

9.2.8. Grupo focal 08.

Se detalla el documento generado del grupo focal 07.

Grupo focal

Proyecto: *Propuesta de plan de continuidad de TI para la Unidad de Tecnologías de Información y Comunicación de JASEC.*

Fecha:	31/10/2018	**Hora Inicio/Finalización:**	8:00 am / 9:00 am
Lugar:	JASEC		
Objetivo de la reunión:	Generación de Proceso de activación e inspecciones de cierre del plan de continuidad.		
Participantes:	Eddy Martínez, Rodolfo Sanabria, Cristian Navarro.		

Temas Tratados

No.	Asunto	Comentarios	Cambios sugeridos.
1	Proceso de activación de plan de continuidad.	Participación de los colaboradores de JASEC para desarrollar dicho proceso.	
2	Inspecciones de cierre.	Participación de los colaboradores de JASEC generar las inspecciones de cierre del plan.	
3			

Uso Confidencial Pág. 1/1

10. Capítulo IX: Anexos.

En este capítulo, se presenta los apéndices que contienen información complementaria.

10.1. Anexo A: Respaldo y recuperación de bases de datos.

Se detalla parte del procedimiento de respaldo y recuperación de bases de datos, por cuestión de confidencialidad se presenta únicamente la primera página.

RESPALDO Y RECUPERACIÓN DE
INFORMACIÓN DE BASE DE DATOS INFORMIX Y ORACLE

1. PROPÓSITO

1.1. Establecer las actividades requeridas para realizar el respaldo y la recuperación de la base de datos Informix y ORACLE.

2. DESCRIPCIÓN

2.1. El presente instructivo es responsabilidad de:

Coordinador Proyectos Apoyo
Coordinador Proyectos Sustantivos
Profesional Proyectos de Sustantivos
Profesional Proyectos de Apoyo

2.2. Lineamientos generales

2.2.1. El respaldo de las bases de datos de INFORMIX y ORACLE es ejecutado en forma automática y se establece un horario diario a media noche de cada día de la semana inclusive fines de semana.

2.2.2. El respaldo de las bases de datos se debe realizar fuera de las horas normales de oficina, entre las 12:00 de la noche y las 4:00 am, esto sin que interfiera con los procesos de carga de información para la gestión del cobro del área Administrativa Financiera.

2.2.3. Los respaldos al realizarse en forma diaria, deben de ser guardados en discos externos o DVD y almacenados, debidamente rotulados, una vez terminado el proceso debe de registrarse el respaldo del día en el Formulario **6F154 Registro diario de respaldo**.

2.2.4. Para cada fin de mes se debe de enviar un respaldo de todos los días lunes del mes y el día primero del mes siguiente a resguardo, a la empresa que brinda el servicio de custodia en San Jose llamada Retrievex (An Acces Copany), dicha empresa recoge el paquete en la oficina de JASEC donde se le indique.

2.2.5. Cada 6 meses deben de ser respaldados los discos duros del servidor de INFORMIX, será respaldo mediante el comando "respatotal" ejecutado desde la

10.1. Anexo B: Carta de aceptación del profesor tutor.

Se presenta la carta de aceptación brindada por el profesor tutor.

Aval de Entrega del Documento de Trabajo Final de Graduación

Nota aclaratoria:
Este documento se redacta de acuerdo a las disposiciones actuales de la Real Academia Española con relación al uso del género inclusivo (**https://goo.gl/ITVYiN**).
Al mismo tiempo, se aclara que estamos a favor de la igual de derechos entre los géneros.

Responsabilidad del Profesor Tutor:

1. A solicitud del estudiante, completar el formulario de Aval de Entrega del Documento de Trabajo Final de Graduación.
2. Devolver una respuesta al estudiante que realizó la solicitud de Aval de Entrega del Documento de Trabajo Final de Graduación. La respuesta debe ser por correo (en formato pdf).

Formulario de Aval de Entrega del Documento de Trabajo Final de Graduación:

Yo ___Gonzalo Delgado Leandro_ Profesor Tutor del Estudiante _Cristian Navarro Martínez carné ___2013034854_____, hago constar que he revisado exhaustivamente el documento académico final del Trabajo Final de Graduación, realizado en el II semestre del 2018. Asimismo, he verificado la atención de las correcciones realizadas en mi condición de Profesor Tutor. Por lo tanto, autorizo entregar este documento a la Coordinación de Trabajos Finales de Graduación para que se realicen las gestiones correspondientes para la programación de la defensa.

Nota Aclaratoria: Considerando el tiempo final de entrega de este documento, este aval está condicionado por la ejecución de los cambios solicitados, junto con la revisión de un profesional en Filología a más tardar para el día 09 de noviembre del 2018.

Responsabilidades del estudiante:

1. Solicitar al Profesor Tutor el Aval de Entrega del Documento de Trabajo Final de Graduación. Esta solicitud se debe realizar por correo al Profesor Tutor, después de haber enviado con al menos una semana hábil el documento académico completo para la respectiva revisión integral final.

2. Enviar a la Coordinación de Trabajos Finales de Graduación la respuesta otorgada por el Profesor Tutor según el formato indicado en este documento. Para esto, debe realizar un reenvío del correo a smora@itcr.ac.cr con copia:
   a. El correo del Profesor Tutor y
   b. Al correo soniamora0407@gmail.com

   No se requiere la firma del Profesor Tutor, dado que el reenvío del correo del Profesor Tutor garantiza la identidad del Profesor.

ati Área Académica de Administración de Tecnologías de Información
Lic. Administración de Tecnología de Información

10.2. Anexo C: Carta filóloga.

Se presenta la carta de la revisión filológica.

Cartago, 09 de noviembre de 2018

Instituto Tecnológico de Costa Rica
Área de Administración de Tecnologías de Información

Estimados señores:

Por este medio yo, Lic. Beatriz Ramírez Montero, mayor, filóloga de profesión, incorporada al Colegio de Licenciados y Profesores, con el número de carné 012143, domiciliada en el Carmen de Cartago, portadora de la cédula de identidad 3 255 316, hago constar:

1. Que he revisado el Trabajo Final de Graduación para optar por el grado de Licenciatura en Administración de Tecnología de Información que lleva como título *Propuesta de plan de continuidad de TI para el Área de Tecnologías de Información y Comunicación de JASEC.*
2. Que el Trabajo final de Graduación para optar por el grado académico de Licenciatura en Administración de Tecnología de Información es presentado por el sustentante Cristian Navarro Martínez, portador de la cédula número 304760476.
3. Que en al trabajo se le han hecho las correcciones en acentuación, ortografía, puntuación, concordancia gramatical y otras pertinentes del campo filológico, por ello doy fe de que se encuentra listo para ser presentado.

En espera de que mi participación satisfaga los requerimientos del Instituto Tecnológico de Costa Rica, se suscribe atentamente

3-255-316

Licda. Beatriz Ramírez Montero
Carné No. 012143
Filóloga