Universidad Hispanoamericana

Facultad de Ingeniería

Escuela de Ingeniería Informática

Proyecto de graduación para optar por el grado de Licenciatura en Ingeniería Informática con Énfasis en Administración

Plan de Continuidad en TIC

Subárea Gestión de Pagos-Tesorería General

Caja Costarricense de Seguro Social

Nombre del Estudiante:

Heilyn Méndez Alvarado

Tutor:

Ing. Cynthia López Valerio; Msc

II Cuatrimestre, 2021

ÍNDICES

Índice de Contenido

Índice de Figuras

Índice de tablas

Índice de gráficos

DECLARACIÓN JURADA

DECLARACIÓN JURADA

Yo, Heilyn Méndez Alvarado, mayor de edad, portadora de la cédula de identidad 1-1044-0176, egresado de la carrera de Ingeniería Informática de la Universidad Hispanoamericana, hago constar por medio de este acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código penal el delito de perjurio, ante quienes se constituyen en el Tribunal examinador de mi trabajo de tesis para optar por el título de Licenciatura en Ingeniería Informática con Énfasis en Administración, juro solemnemente que mi trabajo de investigación titulado: Plan de Continuidad en TIC para la Subárea Gestión de Pagos de la Tesorería General de la Caja Costarricense de Seguro Social, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982; incluyendo el numeral 70 de dicha ley que advierte, artículo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Así mismo, quedo advertido, que la Universidad se reserva el derecho de protocoliza este documento ate Notario Público.

En fe de lo anterior, firmo en la ciudad de Heredia, a los 17 días del mes de diciembre del año dos mil veintiuno.

HEILYN MENDEZ ALVARADO (FIRMA)

Firmado digitalmente por HEILYN MENDEZ ALVARADO (FIRMA)
Fecha: 2021.12.21 15:03:04 -06'00'

CARTAS DE APROBACIÓN

CARTA DEL TUTOR

San José, 21 de diciembre de 2021

Sra. María Isabel Losilla Barrientos
Directora Carrera
Ingeniería Informática
Universidad Hispanoamericana

Estimado señora:

La estudiante Heilyn Méndez Alvarado, cédula de identidad número 1-1044-0176, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado: Plan de Continuidad del Negocio en TIC Subárea Gestión de Pagos de la Tesorería General de la Caja Costarricense de Seguro Social, el cual ha elaborado para optar por el grado académico de Licenciatura en Ingeniería Informática con Énfasis en Administración.
En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	10%
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20%
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	30%
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	20%
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	20%
	TOTAL		100%

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

Ing. Cynthia López Valerio; Msc
Cédula identidad 1-0970-0997
Carné Colegio Profesional 1445

CARTA DE LECTOR

San José, 10 de febrero de 2022

Universidad Hispanoamericana
Sede Llorente
Carrera de Ingeniería en Informática

Estimada señora

La estudiante **HEILYN MÉNDEZ ALVARADO**, cédula de identidad 1010440176, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado **"Plan de Continuidad en TIC Subárea Gestión de Pagos-Tesorería General Caja Costarricense de Seguro Social"**, el cual ha elaborado para obtener su grado de Licenciatura.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación. He verificado que se han hecho las modificaciones correspondientes a las observaciones indicadas.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atentamente,

JULIAN RAQUEL CORDOBA SANABRIA (FIRMA)

firmado digitalmente por JULIAN RAQUEL CORDOBA SANABRIA (FIRMA)
fecha: 2022.02.10 13:03:16 -06'00'

Lic. Julián Córdoba Sanabria
Cédula identidad 109640134
Carné 3272

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 16 de febrero de 2022.

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Heilyn Méndez Alvarado, con número de identificación 110440176 autor (a) del trabajo de graduación titulado Plan de Continuidad en TIC Subárea Gestión de Pagos - Tesorería General - Caja Costarricense de Seguro Social, presentado y aprobado en el año 2022 como requisito para optar por el título de Licenciatura en Ingeniería Informática con Énfasis en Administración; (**SI** / NO) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

HEILYN MENDEZ ALVARADO (FIRMA)

Firmado digitalmente por HEILYN MENDEZ ALVARADO (FIRMA)
Fecha: 2022.02.16 17:32:56 -06'00'

Firma y Documento de Identidad

DEDICATORIA

DEDICATORIA

Primeramente, a Dios por nunca soltarme de su mano, y sostenerme para no caer, por permitirme cumplir este sueño guiando siempre mi caminar. A mi familia, por ser el motor que me impulsa a dar todo sin importar las dificultades.

Dedico este proyecto de graduación a mis hijos y a mi novio, por motivarme a culminar este proyecto de vida, por cada abrazo y por acompañarme en este proceso, brindándome todo el apoyo, pero sobre todo por creer en mí.

AGRADECIMIENTO

AGRADECIMIENTO

Agradezco a Dios por ser mi escudo y mi fortaleza, por caminar a mi lado siempre y ayudarme a cumplir mis sueños.

A cada uno de los profesores de mi querida Universidad Hispanoamericana, así como al personal administrativo por su trato de calidad y calidez, a mi Directora de carrera María Isabel Losilla Barrientos por su guía en este proceso y por atenderme siempre que lo necesité, a mi tutora Cynthia López Valerio, por la paciencia y por compartir todos sus conocimientos para que pudiera aplicarlos a mi proyecto.

A los funcionarios de la Subárea Gestión de Pagos, de la Tesorería General de la Caja Costarricense de Seguro Social, por toda la colaboración brindada.

RESUMEN

RESUMEN

La Caja Costarricense de Seguro Social, es una Institución que se dedica a la seguridad social, proporciona el Seguro de Salud y de Pensiones a los costarricenses y extranjeros que coticen para sus regímenes SEM e IVM, teniendo como base sus tres pilares Estado, Patronos y Trabajadores. Además, brinda subsidios a sus asegurados en caso de incapacidad por enfermedad, maternidad y accidentes.

El objetivo general de este proyecto es Desarrollar el Plan de Continuidad de la Subárea Gestión de Pagos del Área de Tesorería General para el año 2021 de acuerdo con los lineamientos de la Dirección de Tecnologías de Información y Comunicaciones y con base al Plan de Continuidad actual, elaborado desde junio del 2018, para que la Subárea de Gestión de Pagos cuente con las herramientas necesarias y encargados directos para mitigar sus riesgos en caso de que se materialicen.

Para determinar el diagnóstico de la situación actual, se identifican claramente los procesos de la Subárea Gestión de Pagos y se determina el ámbito en que se desarrolla. Además, se analiza el diagnóstico que actualmente presenta dicha Subárea en términos de la infraestructura de TI.

Posteriormente se analizan todos los riesgos, utilizando herramientas de medición y se concluye que todos los riesgos detectados entran dentro de la categoría críticos para poder mantener la continuidad. Se realiza entrevista a la jefatura de la Subárea y encuestas a los colaboradores de la misma.

Se plantea una propuesta de Plan de Continuidad en TIC, donde se apliquen las mejores prácticas, entre ellas, el análisis y evaluación de riesgos y las estrategias de mitigación , de manera que este sea un modelo para seguir; la propuesta describe los pasos a seguir para que la Subárea cuente con las herramientas para reaccionar ante una amenaza, se crean plantillas para los mantenimientos, indispensables en este tipo de plan, con el fin de minimizar el impacto que pueda causar la materialización de uno o varios riesgos.

CAPÍTULO I
PROBLEMA DEL PROYECTO

1. Capítulo 1: Problema del proyecto

1.1 ANTECEDENTES Y JUSTIFICACIÓN DEL PROYECTO

1.1.1 Marco de Referencia Empresarial y Contextual

Información general de la empresa

• Nombre de la empresa: Caja Costarricense de Seguro Social, Área de Tesorería General, Subárea Gestión de Pagos.

• Año de fundación: 1941

• Estrategia:

Misión

"Proporcionar los servicios de salud en forma integral al individuo, la familia y la comunidad, y otorgar la protección económica, social y de pensiones, conforme la legislación vigente, a la población costarricense, mediante:
El respeto a las personas y a los principios filosóficos de la CCSS: Universalidad, Solidaridad, Unidad, Igualdad, Obligatoriedad, Equidad y Subsidiaridad.
El fomento de los principios éticos, la mística, el compromiso y la excelencia en el trabajo en los funcionarios de la Institución.
La orientación de los servicios a la satisfacción de los clientes.
La capacitación continua y la motivación de los funcionarios.

La gestión innovadora, con apertura al cambio, para lograr mayor eficiencia y calidad en la prestación de servicios.
El aseguramiento de la sostenibilidad financiera, mediante un sistema efectivo de recaudación.
La promoción de la investigación y el desarrollo de las ciencias de la salud y de la gestión administrativa".

Visión

"Seremos una Institución articulada, líder en la prestación de los servicios integrales de salud, de pensiones y prestaciones sociales en respuesta a los problemas y necesidades de la población, con servicios oportunos, de calidad y en armonía con el ambiente humano".

Principios

"Equidad: Pretende una verdadera igualdad de oportunidades para que todos los ciudadanos puedan ser atendidos en el sistema nacional de salud, de una manera oportuna, eficiente y de buena calidad.
Igualdad: Propicia un trato equitativo e igualitario para todos los ciudadanos sin excepción.
Obligatoriedad: Es la contribución forzosa del Estado, patronos y trabajadores, a fin de proteger a éstos contra los riesgos de enfermedad, invalidez, maternidad, vejez, muerte y demás contingencias que la ley determine.
Solidaridad: Cada individuo contribuye económicamente en forma proporcional a sus ingresos para el financiamiento de los servicios de salud que otorga la CCSS.
Subsidiariedad: Es la contribución solidaria del Estado para la universalización del seguro social en su doble condición (patrono y Estado). Se crearán a favor de la CCSS, rentas suficientes para atender las necesidades actuales y futuras de la institución, en caso de déficit algunos de los regímenes, el Estado lo asumirá.

Unidad: Es el derecho de la población de recibir una atención integral en salud, para su protección contra los riesgos de enfermedad, maternidad, invalidez, vejez y muerte, mediante una institución que administra en forma integral y coordinada los servicios.
Universalidad: Garantiza la protección integral en los servicios de salud, a todos los habitantes del país sin distinción de ninguna naturaleza.
Responsabilidad: Asumir los deberes y obligaciones con dedicación, constancia y disciplina, aceptando las consecuencias de sus actos.
Compromiso: Adherirse al cumplimiento de una promesa común y compartida, para el desarrollo de los objetivos institucionales.
Respeto: Atender y escuchar a las personas y sus asuntos, reconociendo su dignidad como seres humanos, sin distinción de ninguna naturaleza.
Cortesía: Demostrar las normas de comportamiento que revelan la manera adecuada de relacionarse con los demás, en todos los ambientes en que se desarrolla.
Honestidad: Actuar con rectitud a partir de la razón; ser incapaz de engañar o defraudar a las personas. (Página WEB CCSS 2021)".

• Negocio al que se dedica:

La Caja Costarricense de Seguro Social, es una Institución que se dedica a la seguridad social, proporciona el Seguro de Salud y de Pensiones a los costarricenses y extranjeros que coticen para sus regímenes SEM e IVM, teniendo como base sus tres pilares Estado, Patronos y Trabajadores. Además, brinda subsidios a sus asegurados en caso de incapacidad por enfermedad, maternidad y accidentes.

• Historia de la organización:

"El 1º de noviembre de 1941 mediante Ley Nº17, se crea la C.C.S.S. como una Institución Semiautónoma del Estado, durante la administración del Dr. Rafael Ángel Calderón Guardia.

Sin embargo, el 22 de octubre de 1943 la Ley de la creación de la Caja fue reformada, constituyéndose en una Institución Autónoma del Estado, destinada a la atención del sector de la población obrera y mediante un sistema tripartito de financiamiento.

El Seguro de I.V.M. se crea en 1947, pero incluía a los trabajadores del Estado, Instituciones Autónomas, Semiautónomas y las Municipalidades. En julio de ese mismo año se incorporan trabajadores que laboraban para la empresa privada en el campo administrativo.

No fue sino hasta 1960 que el Seguro de I.V.M. amplió su cobertura a empleados del comercio, escuelas de enseñanza particular, consultorios profesionales y trabajadores municipales pagados por planillas de jornales. En 1962 se amplió a trabajadores manuales ocasionales (construcción), a los pagados por planillas de jornales en obras públicas, ferrocarriles y ya para 1971 cubre en general a todos los obreros del país.

El 12 de mayo de 1961 por Ley Nº 2738, se faculta a la C.C.S.S a la Universalización de los Seguros Sociales.

En 1973 se da el traspaso de hospitales a la C.C.S.S por medio de la Ley Nº 5349, proceso que tardó solo tres años y medio, hasta constituirse hoy en un sistema de 29 hospitales.

En 1975 se extiende el Seguro de Invalidez, Vejez y Muerte a los trabajadores del campo (agrícola) y la C.C.S.S. se hace cargo del Sistema de Pensiones del Régimen No Contributivo, esto con el fin de dar protección a los de más bajos recursos.

De un sistema de separación total de la fase preventiva a cargo del Ministerio de Salud, y la fase relativa correspondiente a la C.C.S.S., se pasa a la integración de servicios en algunos casos y al trabajo conjunto paralelo en otros: queda la C.C.S.S. facultada para llevar a cabo acciones de salud en materia de medicina preventiva.

Por el carácter de su función o fin principal la C.C.S.S. cuenta con el respaldo del Estado, Patronos y Trabajadores, quienes con sus cotizaciones constituyen el fundamento económico básico, sobre el cual giran todas sus actividades.”

1.2 JUSTIFICACIÓN DEL PROYECTO

La Caja Costarricense de Seguro Social es una Institución que se ha adaptado a los avances tecnológicos y constantes cambios en sus procesos con el fin de mantener la seguridad en todas sus áreas, parte de esta seguridad incluye el contar con un Plan de Continuidad en TIC, capaz de proporcionar las herramientas para la mitigación de riesgos.

En coordinación con el Centro de Gestión Informática de la Gerencia Financiera de la Caja Costarricense de Seguro Social y de acuerdo con la indicación de la Dirección de Tecnologías de Información y Comunicaciones existente en la Institución, se determina la necesidad de desarrollar el Plan de Continuidad en TIC de la Subárea Gestión de Pagos del Área de Tesorería General, ya que a la fecha existe información insipiente de algunas características resumidas en una hoja, razón por la cual se toma de decisión de desarrollar el plan con el propósito de fortalecer los diversos procesos que se ejecutan en la Subárea.

El Centro de Gestión Informática de la Gerencia Financiera ha concluido que la Subárea Gestión de Pagos requiere un Plan de Continuidad en TIC ya que actualmente tienen deficiencias en la valoración de riesgos y estrategias de mitigación que son importantes para que los riesgos no se lleguen a materializar y la continuidad del servicio se brinde de manera eficiente.

Al desarrollar el Plan de Continuidad en TIC se fortalecen los procesos críticos que se desarrollan, dado que son de gran impacto para para la Institución, en el sentido de que, si no se realizan los pagos a los proveedores en tiempo y forma, pueden ocasionar inconformidades, e incluso demandas a nivel judicial.

Al ser la Subárea Gestión de Pagos la encargada directa de realizar transacciones de pagos se debe prestar especial atención a contar con un Plan de Continuidad en TIC capaz de identificar eventos y presentar la solución en el menor tiempo, y debe ser del conocimiento de todos los

integrantes del equipo de trabajo, con el fin de que los colaboradores conozcan el proceder en caso de materializarse un riesgo.

El proyecto busca cumplir con la correcta elaboración del Plan de Continuidad en TIC, con esto se favorece la Subárea Gestión de Pagos ya que tendrá las herramientas para detectar sus riesgos y mitigar los mismos.

Por lo anterior, la importancia de realizar esta labor, para una correcta gestión, brindando a la Jefatura de la Subárea Gestión de Pagos, control y seguimiento, evitando atrasos y mostrando de forma clara las acciones a tomar en caso de un evento y los encargados directos en cada caso.

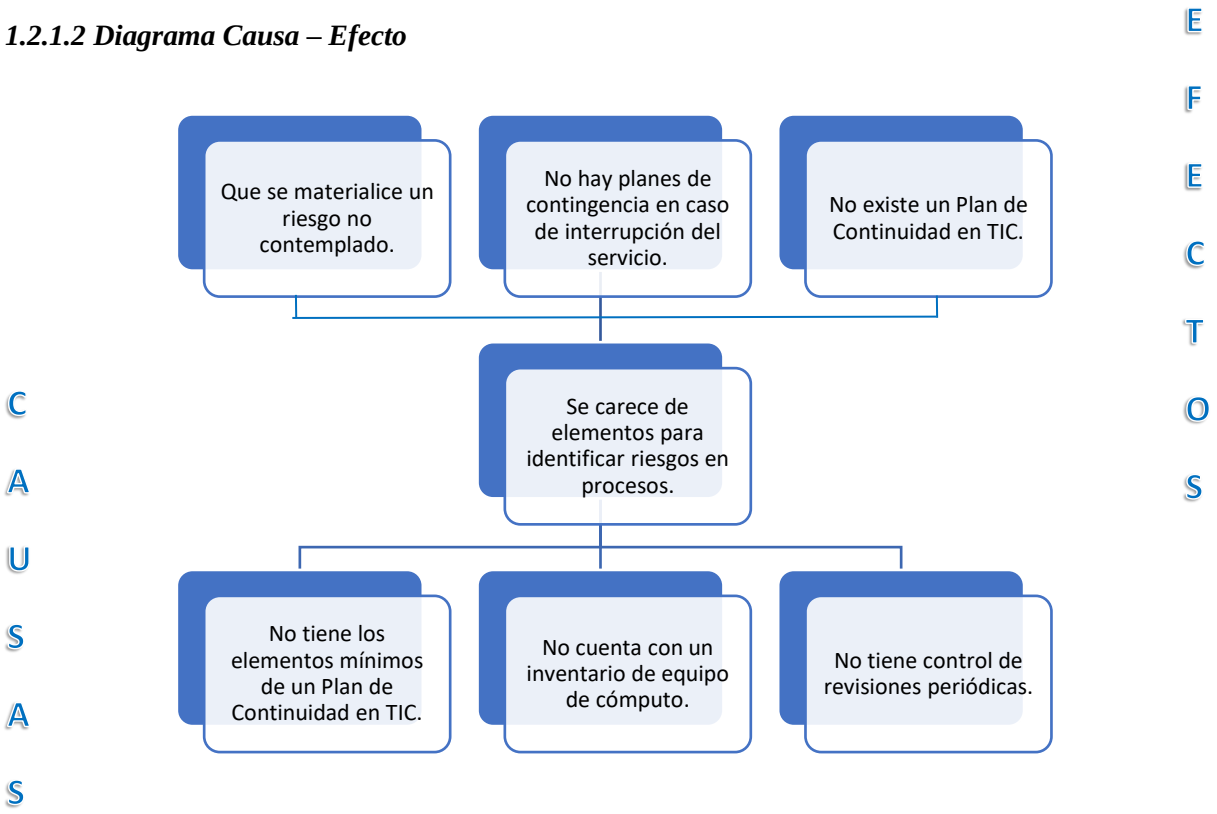
1.2.1 Definición del problema

La Subárea Gestión de Pagos requiere contar con un Plan de Continuidad en TIC, ya que en este momento existe información incipiente resumida en una hoja, con fecha junio 2018, además, dentro de esta información no se cuenta con riesgos inherentes de la Subárea y estos podrían materializarse sin tener una medida de mitigación sobre los mismos y se podría afectar la continuidad de las operaciones, por lo que se deben establecer las estrategias necesarias para garantizar la continuidad de los procesos.

1.2.1.1 Problemática

Analizando el resumen actual, el mismo carece de elementos necesarios para identificar los riesgos inherentes en los procesos de la Subárea Gestión de Pagos, por lo cual se requiere elaborar el Plan de Continuidad en TIC.

1.2.1.2 Diagrama Causa – Efecto



1.2.2 Problema General

- ¿Qué requiere la Subárea Gestión de Pagos del Área Tesorería General de la Caja Costarricense de Seguro Social para contar con un Plan de Continuidad en TIC efectivo?

1.2.3 Problemas Específicos

1. ¿Qué se debe hacer para contar con un buen Plan de Continuidad en TIC?
2. ¿Cuál sería la actividad por realizar para identificar riesgos inherentes en los procesos?
3. ¿De qué forma se mitigan los riesgos detectados?
4. ¿Cómo se deben realizar las revisiones periódicas?
5. ¿Cuál será la forma en la que culminará este proyecto?

1.3 OBJETIVOS DEL PROYECTO

El objetivo general se logrará desarrollando el Plan de Continuidad en TIC.

1.3.1 Objetivo general

Desarrollar el Plan de Continuidad de la Subárea Gestión de Pagos del Área de Tesorería General para el año 2021 de acuerdo con los lineamientos de la Dirección de Tecnologías de Información y Comunicaciones, para que la Subárea de Gestión de Pagos cuente con las herramientas necesarias y encargados directos para mitigar sus riesgos en caso de que se materialicen.

1.3.2 Objetivos específicos

1. Identificar los procesos críticos de la Subárea Gestión de Pagos de la Tesorería General de la Caja Costarricense de Seguro Social, por medio de una entrevista al encargado designado y mediante el análisis FODA y matrices para la determinación de los riesgos.

2. Realizar el diagnóstico de los riesgos de los procesos críticos, mostrando cada uno de forma clara, con su nivel de criticidad, para tenerlos claros e identificarlos en caso de que se estén materializando.

3. Determinar las estrategias de mitigación, tomando en cuenta cada uno de los riesgos detectados, con el fin de conocer el proceder en caso de materializarse alguno o varios de los riesgos y mostrando un responsable para cada uno de ellos al lado de la jefatura.

4. Desarrollar el Plan de Continuidad en TIC de la Subárea Gestión de Pagos de la Tesorería General de la Caja Costarricense de Seguro Social.

5. Comunicar el Plan de Continuidad en TIC a los funcionarios de la Subárea Gestión de Pagos, se realizará mediante una reunión virtual con los integrantes de la Subárea, para cumplir con lo establecido a nivel institucional sobre el conocimiento por parte de todo el equipo de trabajo y en especial por los responsables indicados por la jefatura en caso de materializarse un riesgo.

1.4. ALCANCES Y LIMITACIONES

1.4.1 Alcances

Mediante un proceso de diagnóstico en la Subárea de Gestión de Pagos se hace una numeración de los procesos y aspectos relevantes que se deben tener para la continuidad del negocio, para esto se debe realizar un análisis FODA con el fin de determinar fortalezas y debilidades en la unidad de trabajo.

Se deben identificar los procesos críticos de la Subárea Gestión de Pagos, una vez que se tienen identificados, se procede a realizar un análisis de estos procesos con el fin de identificar los riesgos, los cuales podrían ocasionar la interrupción del negocio en dicha Subárea, con esto se determinarán las estrategias de mitigación y se confeccionará el calendario de ensayos que refleje las fechas en las que este será verificado y actualizando por el encargado de la Unidad.

Una vez que se encuentre elaborado en su totalidad dicho Plan, se realizará el comunicado oficial a los funcionarios que conforman la Subárea Gestión de Pagos, ya que el comunicado al equipo de trabajo es un requisito obligatorio para las unidades de la Caja Costarricense de Seguro Social.

Este Plan de Continuidad en TIC, contempla los procesos sustantivos de la Subárea de Gestión de Pagos, sin embargo; no contempla los procesos que son complementarios o de apoyo de la Subárea porque son procesos que se relacionan con unidades externas.

Tomando en cuenta la Jerarquía Institucional, el Plan de Continuidad en TIC se limita a la Subárea Gestión de Pagos únicamente.

Durante el proceso de actividades los siguientes serían los entregables:

1. Inventario de procesos: El mismo contiene el inventario de los procesos de la Subárea de Gestión de Pagos.

2. Análisis de riesgos: Se realizará la identificación de los riesgos por medio del semáforo, siendo rojo para identificar el riesgo alto, amarillo para identificar el riesgo medio y verde para identificar un riesgo bajo.

3. Tabla de riesgos identificados y estrategias de mitigación: Del resultado del análisis, se brindará la descripción de los riesgos y su impacto, así como el nivel, la estrategia de mitigación y el responsable.

4. Entrega del Plan de Continuidad en TIC 2021 a la Subárea Gestión de Pagos: Contemplará los formularios DTIC, mostrará los riesgos identificados y su clasificación, además el plan de mitigación, procedimientos de recuperación ante desastres, inventario de activos, definición de controles para garantizar la continuidad, entre otros. Además, se hará una presentación de este, detallando cada punto, su distribución y sobre todo su importancia para el conocimiento de todos los funcionarios que conforman esta Subárea.

Exclusiones

- Existen sistemas externos a la Institución por medio de los cuales se realizan pagos a los proveedores, personas físicas o jurídicas, transacciones de pago utilizando principalmente la plataforma de pagos del Banco Central de Costa Rica, denominada SINPE, que, para efectos del Plan de Continuidad en TIC, no pueden ser contemplados, ya que no dependen de la Subárea, sino de una Institución independiente de la Caja Costarricense de Seguro Social.

1.4.2 Limitaciones

1. Una limitante es la Normativa Institucional, la Ley de control interno y la Ley de Administración Financiera, lo anterior, por ser una institución pública.

2. El tiempo es una limitante, ya que el Plan de Continuidad en TIC, se debe elaborar por completo en un lapso de seis meses.

Capítulo II
Marco Teórico

2. Capítulo II: Marco teórico

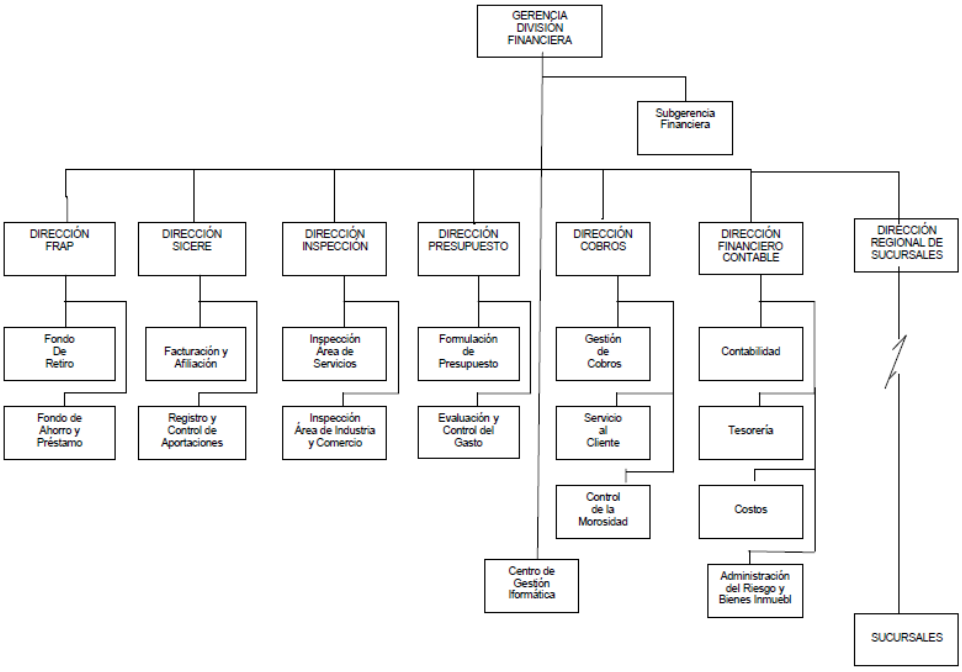
El presente capítulo contiene la base teórica para el sustento y entendimiento necesario en el desarrollo de este proyecto de graduación.

2.1 Subárea Gestión de Pagos

La Gerencia Financiera en la Caja Costarricense de Seguro Social, tiene dentro de sus unidades adscritas la Dirección Financiero Contable, la cual se divide en tres Áreas; el Área de Contabilidad Financiera, Área Contabilidad de Costos y Área de Tesorería General.

En el Área Tesorería General se encuentra la Subárea de Gestión de Pagos, la cual se encarga del pago a proveedores locales y extranjeros, empleados, pensionados y otros conceptos, por medio de SINPE del BCCR, internet banking BNCR, BCR comercial y por vía cheque. A continuación, se detalla el Organigrama de la Gerencia Financiera.

Figura 1-Organigrama de la Gerencia Financiera



Fuente:(Caja Costarricense de Seguro Social, 2007)

2.1.1 Procesos de negocio

Podemos explicar que un proceso de negocio, según indica Bravo Carrasco, consiste en:

> La gestión de procesos es una disciplina de gestión que ayuda a la dirección de la empresa a identificar, representar, diseñar, formalizar, controlar, mejorar y hacer más productivos los procesos de la organización para lograr la confianza del cliente. La estrategia de la organización aporta las definiciones necesarias en un contexto de amplia participación de todos sus integrantes, donde los especialistas en procesos son facilitadores. (Bravo Carrasco, 2005, pág. 9)

Por lo anterior, se puede indicar que 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.

2.1.2 Análisis de Impacto del Negocio

De acuerdo con lo indicado por MINTIC:

> La fase de Análisis de Impacto del Negocio BIA (Bussiness Impact Analysis) Por sus siglas en inglés), permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio. Como se ha venido mencionando, cada entidad debe disponer de un documento que permita identificar todas las áreas críticas del negocio y sea un instrumento para garantizar la medición de la magnitud del impacto operacional y financiero de la entidad, al momento de presentarse una interrupción. (MINTIC, 2015, pág. 12)

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.

2.1.2.1 Definición BIA

Un BIA es un análisis que permite estimar la afectación generada por la ocurrencia de un desastre o incidente dentro de una organización, según lo indica Kirvan:

> El BIA ayuda a identificar los procesos de negocios más críticos, y describe el impacto potencial que tendría una interrupción de esos procesos; y una evaluación de riesgo identifica situaciones internas y externas que podrían tener un impacto negativo en los procesos críticos. También intenta cuantificar la potencial gravedad de tales eventos, y la probabilidad de que ocurran. (Kirvan, 2013, pág. 1)

Como conclusión 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.

2.1.2.2 Guía para realizar el análisis de impacto de negocio

Corresponde a un documento, 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, pág. 13) 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”.

En conclusión, es un proceso metodológico utilizado para el desarrollo del BIA, tomando en consideración el alcance establecido para este proyecto de graduación.

2.1.2.2.1 Identificación de funciones y procesos

Según MINTIC, en lo que se refiere a la identificación de funciones y procesos, indica lo siguiente:

> En este paso se identifican las funciones del negocio útiles para apoyar la misión y los objetivos a alcanzar en el Sistema de Gestión de Seguridad de Información de la Entidad. Este punto tiene como resultado generar un listado de roles y procesos, que sirven de análisis para el cumplimiento de los siguientes pasos del BIA. (MINTIC, 2015, pág. 16)

Se identifican las funciones de la Subárea Gestión de Pagos, las cuales son útiles para alcanzar los objetivos planteados dentro del proyecto de graduación. Este paso tiene como resultado identificar todos los procesos de negocio, que sirven como base de análisis para los siguientes pasos del BIA.

2.1.2.2.2 Evaluación de impacto

Según lo indicado por MINTIC, en relación con la evaluación de impacto menciona:

> Teniendo en cuenta los elementos operacionales de la organización, se requiere evaluar el nivel de impacto de una interrupción dentro de la Entidad. El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C. • Nivel A: La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse. • Nivel B: La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica. • Nivel C: La operación no es una parte integral del negocio. (MINTIC, 2015, pág. 16)

Una vez identificados los procesos del negocio, se requiere evaluar el impacto de una posible interrupción dentro de las operaciones diarias de la Subárea Gestión de Pagos. La evaluación del impacto debe permitir evaluar el nivel negativo que genera una interrupción hacia la Subárea Gestión de Pagos, tomando en consideración aspectos relacionados al negocio.

2.1.2.2.3 Identificación de procesos críticos

Según MINTIC (2015) “La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones, según esta tabla” (pág. 17).

Figura 2-Identificación de procesos críticos

Valor	Interpretación del proceso crítico
A	Crítico para el Negocio, la función del negocio no puede realizarse
B	No es crítico para el negocio, pero la operación es una parte integral del mismo.
C	La operación no es parte integral del negocio.

Se identifican los procesos críticos del negocio, considerando como base la clasificación de los impactos operacionales dentro de la Subárea Gestión de Pagos. Dicha identificación permite conocer cuáles procesos son esenciales dentro del negocio.

2.1.2.2.4 Identificación de recursos

Basados en lo indicado por MINTIC, en relación con la identificación de recursos, se menciona:

> Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto, es clave en este punto, la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomas acciones para medir el impacto del negocio de las Entidades. (MINTIC, 2015, pág. 18)

Las actividades consideradas dentro de la Subárea Gestión de Pagos con función crítica del negocio deben ser valoradas como vitales, por lo tanto, la identificación de los recursos TIC que soportan los procesos críticos del negocio, permite la toma las decisiones con respecto al impacto.

2.1.2.2.5 Generación de informe de impacto de negocio

MINTIC señala que en la generación del informe de impacto de negocio:

> En este punto es necesario presentar un informe de impacto de negocio que corresponde a la guía para el BIA con los siguientes resúmenes: Listado de procesos críticos, Listado de prioridades de sistemas y aplicaciones, Listado de tiempos MTD, RTO y RPO, Listado de procedimientos alternos. (MINTIC, 2015, pág. 20)

Corresponde al paso final del proceso, genera un informe de impacto de negocio que contempla los siguientes puntos:

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

2.1.2.3 Recolección de datos

Según lo señalado por MINTIC (2015) "debe contener la información básica de los recursos requeridos y los tiempos de recuperación para que las entidades puedan poner en funcionamiento los servicios y por ende la continuidad del negocio". (pág. 21)

La recolección de datos es un paso clave dentro del análisis BIA, recomienda ciertos aspectos importantes para realizar la recolección de datos, los cuales se detallan a continuación:

2.1.2.4 Información necesaria

De acuerdo con lo indicado por MINTIC, en relación con la información:

> Es recomendable que las entidades posean un método estructurado que facilite la obtención de la información requerida, se debe disponer de encuestas, entrevistas y talleres. • Encuesta: Conjunto de preguntas que se envían a las distintas entidades de la organización. • Entrevistas: La información del Análisis de Impacto del Negocio (BIA), se obtiene personalmente, entrevistando a una o más personas. La información detallada puede obtenerse creando preguntas para cada entrevista, de acuerdo con las necesidades de la organización que hace las preguntas. • Talleres:

> Permite a un grupo de personas trabajar de forma colectiva para que de esta manera se provea de información para el análisis de impacto del negocio. (MINTIC, 2015, pág. 13)

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 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.

2.1.3 Valoración de impacto

De acuerdo con lo indicado en el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) “El impacto mide las consecuencias sobre el objetivo que puede ocasionar en la Unidad por la materialización del riesgo” (pág.34).

Dentro de un BIA, es necesario valorar el nivel de impacto que genera una posible interrupción de los procesos identificados de la Subárea Gestión de Pagos.

2.1.3.1 Categorías de impacto

De acuerdo con lo indicado en el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "El impacto de la interrupción de un proceso dentro de la organización puede representar una afectación que es posible categorizar, según: Operacional, Legal o regulatorio, Financiero y Reputación". (pág. 35)

2.1.3.2 Escenarios de impacto

Según indica el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "Existe escenarios en que se presenta durante la interrupción de un proceso y por consiguiente generan un determinado impacto (pág. 36).

2.1.4 Dependencias entre procesos

Según lo indicado por MINTIC, en cuanto a las dependencias entre procesos:

> En este paso se identifican las funciones del negocio útiles para apoyar la misión y los objetivos a alcanzar en el Sistema de Gestión de Seguridad de Información de la Entidad. Este punto tiene como resultado generar un listado de roles y procesos, que sirven de análisis para el cumplimiento de los siguientes pasos del BIA. (MINTIC, 2015, pág. 34)

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.

2.1.5 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, como lo indica MINTIC, en la 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. (MINTIC, 2015, pág. 14)

2.2 Riesgos

Para contextualizar el término de riesgo, se define como:

> El riesgo es un elemento consustancial a la propia actividad de la empresa y, aún más, en sus diferentes manifestaciones está presente en cualquier tipo de actividad; en la mayor parte de los casos no es posible establecer mecanismos para su completa eliminación, por lo que se hace absolutamente imprescindible gestionarlo de forma adecuada. Sin embargo, la naturaleza de estas indeterminaciones ha cambiado sustancialmente a lo largo de las dos últimas décadas. (Rodríguez López, Piñeiro Sánchez, & Llano Monelos, 2013, pág. 5)

Además, podemos indicar que riesgo significa lo siguiente:

> Cabe mencionar que el riesgo es la probabilidad de que un evento ocurra y cause consecuencias (daños o pérdidas) que afecten la habilidad de alcanzar los objetivos, se mide a través de la probabilidad de que una amenaza se materialice explotando en una vulnerabilidad ocasionando así un impacto. Dentro de la entidad el riesgo siempre estará presente aun cuando no se lo haya reconocido o detectado. (Alvarado & Zumba, 2015, pág. 85)

2.2.1 Riesgos tecnológicos

Tomando en cuenta lo indicado por Alvarado & Zumba, en riesgos tecnológicos:

> Los riesgos típicos incluyen pérdida de productividad o negocios debido al tiempo de inactividad, responsabilidad por brechas de seguridad que exponen la información de los clientes, multas por violaciones de normas y la imposibilidad de defenderse de demandas debido a la conservación inadecuada de registros. (Alvarado & Zumba, 2015, pág. 85)

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.

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, según se detalla a continuación:

> El análisis de riesgos se relaciona con la definición de escenarios de riesgos de TI conforme la estructura de la entidad, así como con los resultados de la información

> levantada, plasmando una calificación cualitativa y cuantitativa del nivel de riesgo. Para la calificación se deben clarificar conceptos relacionados, como: Frecuencia. - Número de veces que se repite un evento que afecta a la entidad. Magnitud.- Medida de las consecuencias que tiene un determinado evento para la entidad, ya sea de manera positiva o negativa. (Alvarado & Zumba, 2015, pág. 86)

La importancia del análisis de riesgos dentro del desarrollo de un plan de continuidad en TIC, 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.

2.2.3 Categorización del riesgo

Dentro de la sección de análisis de riesgos, el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones (CCSS, 2013) indica: "se categoriza los riesgos en: interrupción eléctrica, fallos en hardware, fallos en software, desastres naturales, incendio, fallos en respaldos, virus, violaciones en la seguridad física, intrusión, recurso humano (pág. 35).

Igualmente, dentro de dicho manual son considerados un conjunto de aspectos mínimos, que ayudan a mitigar la materialización de un riesgo asociado con cada categoría.

Tabla 1-Categorización del riesgo

Categorías 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.

Categorías de Riesgo	Consideraciones mínimas.
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. • 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.

Categorías de Riesgo	Consideraciones mínimas.
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. • 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.

Categorías de Riesgo	Consideraciones mínimas.
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, 2013, pág. 35)

2.2.4 Nivel de probabilidad de riesgos

En el manual para la elaboración de un plan de continuidad anteriormente mencionado, se indica lo siguiente:

> Medida o descripción de la posibilidad de ocurrencia de un evento; esta puede ser medida con criterios: - Frecuencia: si se ha materializado el riesgo, por ejemplo: No. de veces que ha sucedido un riesgo en un tiempo determinado; No. de robos al año en la Sucursal. - Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. (CCSS, 2013, pág. 34)

2.2.5 Nivel de impacto de riesgos

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, indica: CCSS (2013), "El

impacto mide las consecuencias sobre el objetivo que puede ocasionar en la Unidad por la materialización del riesgo" (pág. 34).

2.2.6 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

Figura 3-Matriz de rangos de riesgo

Probabilidad	Valor			
Alta	3	3- Zona de Riesgo Medio - Evitar Riesgo	6- Zona de Riesgo Alta - Reducir el Riesgo - Evitar el Riesgo - Compartir o transferir	9- Zona de Riesgo Alta - Reducir el Riesgo - Evitar el Riesgo - Compartir o transferir
Media	2	2- Zona de riesgo baja - Asumir el Riesgo - Reducir el riesgo	4- Zona de riesgo Medio - Reducir Evitar Compartir o transferir el riesgo	6- Zona de riesgo alta- Reducir Evitar Compartir o transferir el riesgo
Baja	1	1- Zona de riesgo Baja - Asumir el Riesgo	2- Zona de riesgo Baja - Reducir - Compartir o transferir el riesgo	3 Zona de riesgo Medio - Reducir compartir o transferir el riesgo
	Valor	1	2	3
	Impacto	**Bajo**	**Medio**	**Alto**

Fuente: (CCSS, 2013, pág. 39)

Este cuadro se interpreta de la siguiente manera: a) Al conocer la calificación Probabilidad del Riesgo (alta, media o baja), se ubica en el campo correspondiente en el margen izquierdo (probabilidad). b) Igualmente para el Impacto del Riesgo, se ubica en la parte inferior del cuadro (impacto), de acuerdo con la calificación dada (bajo, medio o alto). c) Luego en el punto donde se interceptan las respectivas calificaciones de la probabilidad y el impacto del riesgo (cuadros en color verde, amarillo o rojo), ese es el grado de Exposición del Riesgo. (CCSS, 2013, pág. 39).

2.2.7 Matriz de calor de riesgos

Según Mekhala en lo que se refiere a la matriz de calor de riesgos indica lo siguiente:

> Un mapa de riesgos, también conocido como mapa de calor de riesgos, es una herramienta de visualización de datos para comunicar los riesgos específicos que enfrenta una organización. Un mapa de riesgos ayuda a las empresas a identificar y priorizar los riesgos asociados con su negocio. (Mekhala, 2018, pág. 1)

2.3 Continuidad de negocio

Con el propósito de contextualizar el término de continuidad del negocio, se hace referencia a lo indicado por González Villalobos:

> Gestión de la Continuidad del Negocio (BCM): Disciplina que prepara a una organización para lo inesperado. Es un proceso de gestión que ofrece un marco de trabajo para darle resiliencia a la operación ante riesgos de interrupción, de tal manera que se garantice la continuidad en los servicios críticos. (González Villalobos, 2015, pág. 15)

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, contar con estrategias que permitan garantizar ante cualquier interrupción, la continuidad de las operaciones del negocio que son soportadas por TI.

2.3.1 Estrategia de continuidad del negocio

De acuerdo con lo indicado por MINTIC en su documento, indica que la estrategia de continuidad del negocio es:

> Diseñar una estrategia de continuidad de los servicios de TI, que tenga como base la reducción del impacto de una interrupción en los servicios críticos de TI del negocio, este debe estar difundido, aprobado y respaldado por los directivos de la entidad. (MINTIC, 2015, pág. 11)

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 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, según indica González Villalobos (2015)” Plan de Continuidad del Negocio (BCP): Principal salida del proceso de continuidad del negocio. Este documento describe un plan de tratamiento para ciertos riesgos y consecuencias que pueden afectar la operación de la organización”. (pág.15)

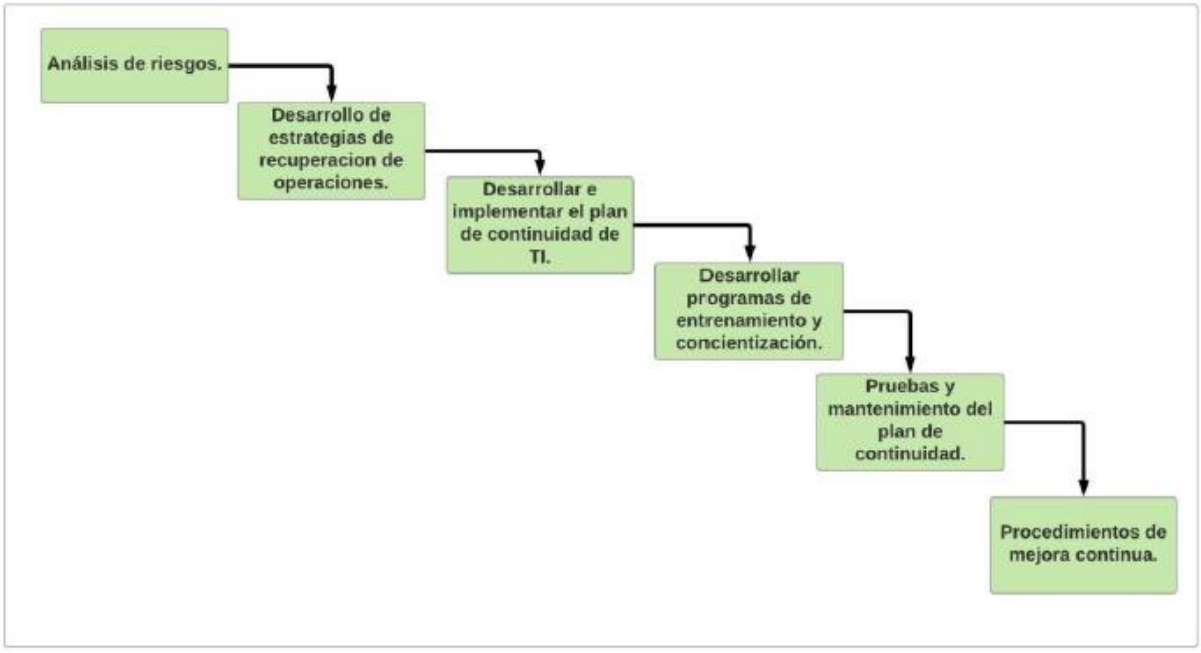
Dentro de sus objetivos, un plan de continuidad del negocio se enfoca en sostener las funciones del negocio durante y después de una interrupción a los procesos críticos de la

organización, identifica las amenazas potenciales y los impactos a las operaciones que esas amenazas podrían causar si se llegaran a materializar.

2.4.1 Etapas mínimas para elaborar un plan de continuidad

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "se especifica un conjunto de etapas mínimas para alcanzar con éxito la elaboración de un plan de continuidad" (pág.11).

Figura 4-Etapas mínimas para elaborar un plan de continuidad.



Etapas mínimas para elaborar un plan de continuidad de TI.
Fuente: CCSS (2013).

2.4.2 Componentes de un plan de Continuidad

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "incluye: Análisis de Riesgos, Análisis de Impacto

del Negocio, Desarrollo de Estrategias de Recuperación de las Operaciones, Desarrollar e implementar el Plan de Continuidad en TIC, Desarrollar programas de entrenamiento y concientización, Pruebas y mantenimiento, Procedimientos de mejora continua" (pág.12)

En conclusión, se requiere que un Plan de Continuidad en TIC contenga: identificación de amenazas, clasificación de riesgos, plan de acción y mitigación, procedimientos de recuperación ante desastres, inventario de activos, controles para garantizar la continuidad, tablas de recuperación de tiempos y análisis de vulnerabilidades, entre otros.

2.4.3 Tipo de estrategias del plan de continuidad

Dentro de un plan de continuidad especifican 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.

2.4.4 Organización y administración del plan de continuidad de TI

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "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" (pág.18)

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

2.4.4.1 Coordinador del plan de continuidad

Dentro del Manual para la elaboración del plan de continuidad en TIC de la CCSS, se señala que el coordinador del plan es:

> El Coordinador del Plan de Continuidad, adelante el CPC, es responsable de la supervisión y coordinación de todas las actividades de recuperación establecidas en este plan. Conforme se implante el Plan, será el responsable de acumular y administrar toda la información que esté incluida en el mismo. El CPC es responsable de obtener copias de este Plan y distribuirlas a los líderes de los equipos y a sus suplentes. Debe además encargarse de mantener copias de este Plan seguras en los sitios alternos que se mencionan. (CCSS, 2013, pág. 13)

El coordinador del plan de continuidad es responsable de supervisar y coordinar todas las actividades de recuperación establecidas dentro del plan de continuidad en TIC. Igualmente, es responsable de acumular y administrar toda la información generada una vez iniciado el plan de continuidad.

2.4.4.2 Líder de equipo del plan de continuidad

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "En cada equipo de recuperación deber definirse un Líder, quien debe ser una persona con liderazgo natural, para un grupo particular, donde los demás esperan que dirija y tenga la capacidad para realizar decisiones durante el periodo de recuperación" (pág. 20).

En resumen, 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.

2.4.4.3 Suplente del líder de equipo del plan de continuidad

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "El suplente sirve como Líder de Equipo si el líder de equipo designado está imposibilitado o no disponible para administrar el equipo. Por lo tanto, debe disponer del mismo perfil que el líder y cumplir con las mismas funciones" (pág.20).

En conclusión, 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.

2.4.4.4 Miembros de equipo del plan de continuidad

Dentro del Manual para la elaboración del plan de continuidad en TIC de la CCSS, se señala que los miembros de equipo del plan de continuidad cumplen las siguientes funciones:

> Los miembros de equipo son responsables de ejecutar las acciones de recuperación. Debido a que las actividades son usualmente desarrolladas por múltiples personas, quienes pueden variar dependiendo de las circunstancias y recursos disponibles, es mejor evitar la identificación de tareas con individuos específicos. En su lugar, la planeación se limita a experiencias y requerimientos específicos, los cuales son necesarios para realizar tareas particulares (CCSS, 2013, pág. 21)

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.

2.4.4.5 Equipos para el plan de continuidad

Dentro del Manual para la elaboración del plan de continuidad en TIC de la CCSS, se señala que los equipos para el plan de continuidad son los siguientes:

> En el caso particular del área de TI, y como parte de la organización se podrá definir los equipos siguientes: a- Equipo de Tecnología de Información (EATI), b- Equipo de Comunicaciones (EC), c- Equipo de Operaciones (EO), d- Equipo de Aplicaciones (EA) (CCSS, 2013, pág. 21)

Para la gestión de un plan de continuidad en TIC, es necesario la conformación de equipos que logren brindar su soporte. Como parte de la organización dentro de un plan de continuidad en TIC, se pueden definir los cuatro equipos con un respectivo alcance y responsabilidades, según se indica a continuación:

2.4.4.5.1 Equipo de tecnología de información

Dentro del Manual para la elaboración del plan de continuidad en TIC de la CCSS, se señala que el equipo de tecnología de información realiza las siguientes funciones:

> Una vez que la recuperación ha iniciado, el equipo EATI supervisa y coordina todas las actividades internas de recuperación, y monitorea el avance de las acciones realizadas por el personal de los equipos de Operaciones (EO), Comunicaciones (EC) y Aplicaciones (EA) (CCSS, 2013, pág. 21)

Como conclusión, es el 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.

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.

2.4.4.5.2 Equipo de comunicación

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "Este equipo de trabajo se encarga de las acciones de recuperación de las comunicaciones y debe informar al líder del EATI de la interrupción en el servicio y el avance en la recuperación" (pág. 21).

En resumen, este equipo 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.

2.4.4.5.3 Equipo de operación

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "Este equipo de trabajo coordina con el Líder del EATI el avance de la restauración de las operaciones de las plataformas críticas" (pág. 22)

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.

2.4.4.5.4 Equipo de aplicaciones

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "Este equipo coordina con el Líder del EATI y supervisa la restauración de las aplicaciones que residen en el computador principal (pág.22).

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.

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

De acuerdo con lo indicado en la Norma (ISO, 2012) un plan de continuidad es la "Principal salida del proceso de continuidad del negocio y describe un plan de tratamiento para ciertos riesgos y consecuencias que pueden afectar la operación de la organización".

La Dirección de Tecnologías de Información y Comunicaciones de la CCSS crea un Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones dentro de las unidades con que cuenta.

Según dicho manual CCSS (2013), El enfoque principal de un Plan de Continuidad en TIC considera recuperar las operaciones de los procesos sustantivos de una organización, dentro de un espacio de tiempo determinado, buscando equilibrar el costo y viabilidad de éste (pág. 7), en este sentido el enfoque que debe mantener un plan de continuidad debe ser la recuperación de las operaciones de los procesos de una organización, dentro del menor tiempo y buscando equilibrio entre las partes.

2.6 Desarrollo de estrategias de recuperación de las operaciones

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "En esta etapa se deberán establecer diversas estrategias orientadas a la recuperación de la plataforma tecnológica de acuerdo con los objetivos de tiempo de recuperación establecidos por el negocio" (pág. 14).

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.

2.7 Desarrollar e implementar el plan de continuidad de TIC

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) "En esta etapa se debe diseñar, desarrollar e implementar el plan de continuidad que proveerá de la información necesaria para recuperar las operaciones de TI dentro del marco de tiempo establecido por el negocio" (pág. 14).

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

- Determinar los requerimientos del plan de continuidad en TIC.
- Determinar la estructura del plan de continuidad en TIC.
- 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.

2.8 Procedimientos de recuperación

Según el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones CCSS (2013) “Los procedimientos de recuperación son documentos que apoyarán el proceso de recuperación de la plataforma de TI posterior a la manifestación de cualquier evento que los afecte parcial o totalmente (escenario de peor caso)” (pág. 15).

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.

2.9 Pruebas y dar mantenimiento al plan

Dentro del Manual para la elaboración del plan de continuidad en TIC de la CCSS, se señala lo siguiente con respecto a las pruebas y mantenimiento al plan:

> Esta etapa se orienta a probar con antelación y coordinar ejercicios, documentando y evaluando los resultados de ellos. Desarrollar procesos para mantener vigentes las capacidades para lograr una adecuada recuperación de las operaciones de TI, en acuerdo con la dirección estratégica del negocio (CCSS, 2013, pág. 16)

Como parte de las pruebas y mantenimiento del plan de continuidad de TIC, 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.

2.10 Procedimiento de mejora continua

Dentro del Manual para la elaboración del plan de continuidad en TIC de la CCSS, en cuanto al procedimiento de mejora continua, se señala:

> La Gestión de la Calidad Total (GCT) indica que el mejoramiento continuo del proceso es un aspecto vital. Durante muchos años se ha señalado que el mejoramiento del proceso es un factor muy importante. El modo de organizar y apoyar el esfuerzo de mejoramiento es esencial. (Ricardo Cabrera , 2009, pág. 27)

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

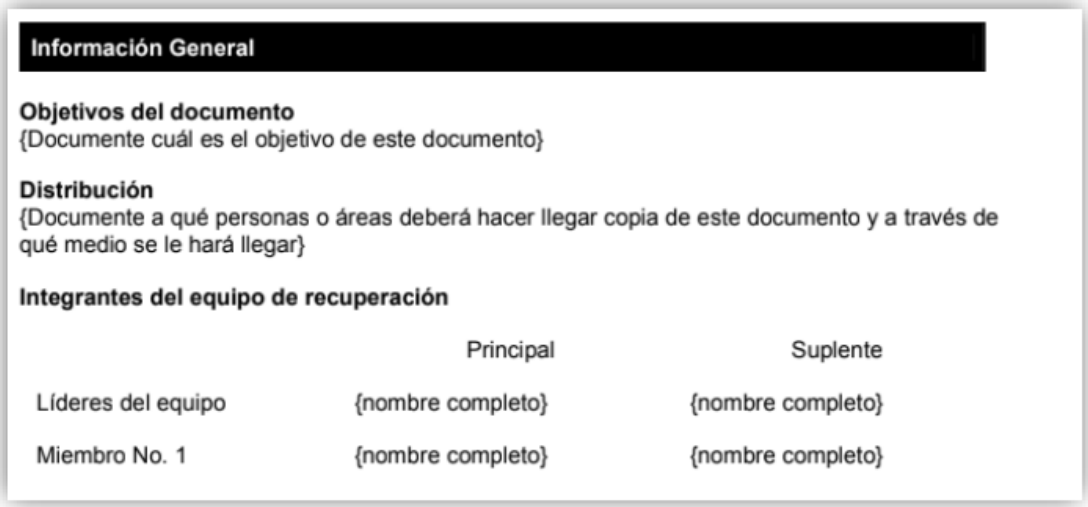
- Administración del cambio dentro de la organización y su impacto dentro del plan de continuidad.
- Capacitación del personal, fomentando su ejecución una vez al año.
- Ensayos del plan de continuidad en TIC, contando con el compromiso del personal relacionado al plan.
- Revisión constante de la organización, 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 en TIC, la Caja Costarricense de Seguro Social 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 en TIC.

2.11 Plantillas de control

Dentro del manual, la CCSS (2013) establece plantillas con el objetivo de gestionar el control y documentación de los procedimientos de recuperación aplicados dentro de la organización.

Figura 5-Plantillas de control



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

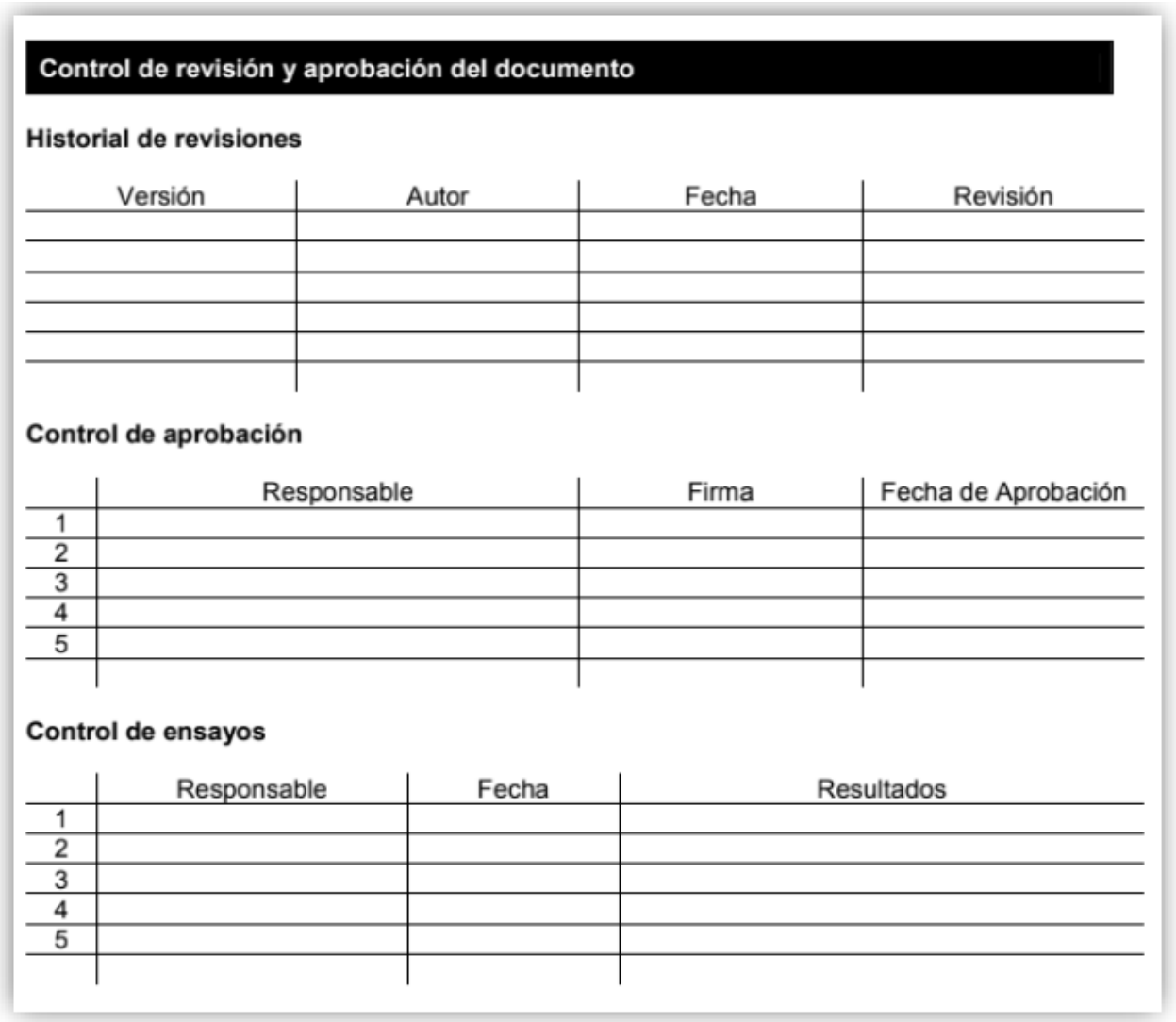
	Principal	Suplente
Líderes del equipo	{nombre completo}	{nombre completo}
Miembro No. 1	{nombre completo}	{nombre completo}

Información general del documento

Fuente: CCSS (2013)

Además, gestiona una plantilla con información general sobre las versiones generadas del plan de continuidad en TIC, donde detalla el responsable a cargo de la aprobación y los ensayos realizados que respaldan dicho plan:

Figura 6-Control de revisión y aprobación del documento



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

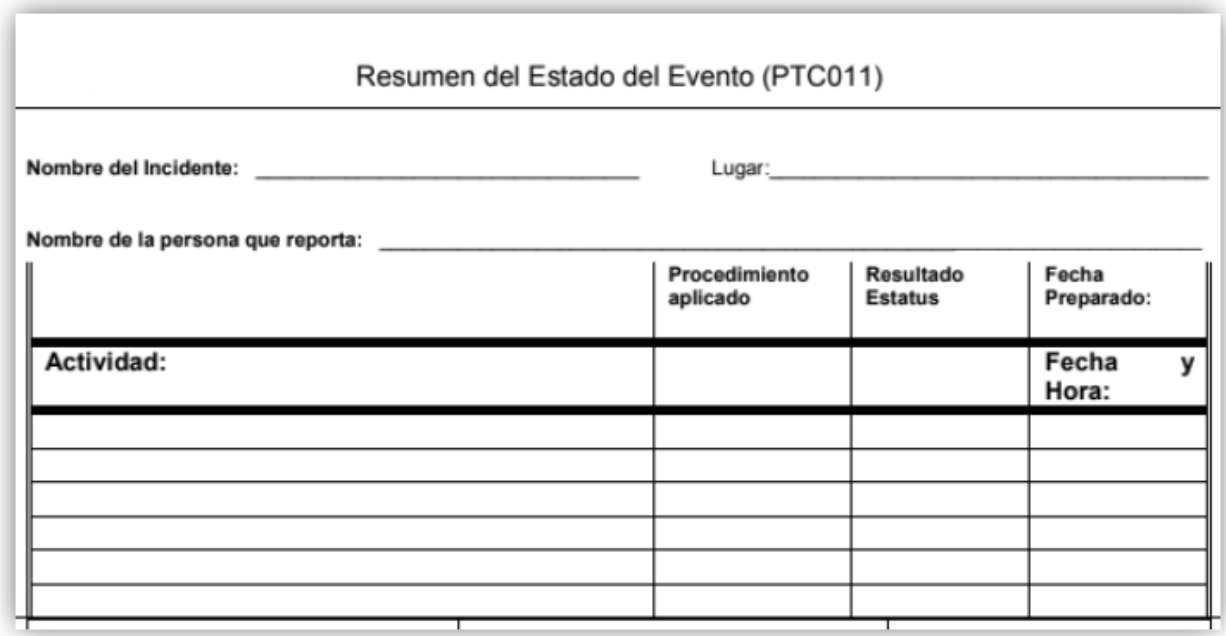
	Responsable	Fecha	Resultados
1			
2			
3			
4			
5			

Control de revisión y aprobación del documento.
Fuente: CCSS (2013)

2.12 Plantilla resumen del evento

La CCSS (2013) dentro de su manual para la creación del plan de continuidad, establece una plantilla como bitácora con el objetivo de documentar las actividades realizadas:

Figura 7-Plantilla resumen del evento



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:**

Plantilla de recuperación de resumen del estado del evento.
Fuente: CCSS (2013)

2.13 Normas

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

2.13.1 Norma ISO 22301

> La normativa ISO 22301 es un estándar publicado por la ISO en 2012, con el fin de brindar un documento que ofrezca soporte a las organizaciones para protegerse, mitigar o recuperarse de cualquier evento disruptivo a las operaciones, dicho documento se convierte en un instrumento para canalizar los esfuerzos de los grupos estratégicos para prolongar la supervivencia de la organización (GONZÁLEZ VILLALOBOS, 2015, pág. 17)

La norma ISO 22301, 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.

2.13.1.1. Modelo PDCA

De acuerdo con lo indicado en Progress el modelo de procedimiento metodológico de la investigación es:

> El ciclo planear-hacer-revisar-actuar (plan-do-check-act "PDCA") es un modelo muy bien conocido para mejoramiento continuo de procesos (continuous process improvement "CPI"). Enseña a organizaciones a planear una acción, hacerla, revisarla para ver cómo se conforma al plan y actuar en lo que se ha aprendido. (Progress, 2002, pág. 1)

En base a lo anterior, 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, los cuales permiten a las organizaciones mejorar integralmente a nivel de competitividad, calidad, productividad y rentabilidad

Dentro de la normativa ISO 22301, se propone el modelo PDCA para la mejora continua de un sistema de gestión de la continuidad, 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.

Dentro de Progress, expone cuatro pasos del modelo PDCA que plantea un objetivo específico que apoya tanto el desarrollo como la gestión de un sistema de gestión de continuidad de negocio, a continuación, los detallamos:

> a) Planear: Establecer una política de continuidad del negocio, objetivos, metas y procedimientos relevantes para la mejorar de la continuidad del negocio. b) Hacer: Implementar y operar la política de continuidad de negocio, controles, procesos y procedimientos. c) Verificar: Monitorear y evaluar el desempeño de la política de continuidad del negocio. Determinar y autorizar acciones de remediación y mejora. d) Actuar: Mantener y mejorar el sistema de gestión de continuidad de negocio mediante acciones correctivas, basadas en resultados de evaluaciones gerenciales. (Progress, 2002, pág. 1)

2.13.2 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 este proyecto de graduación, que a continuación indica:

> En la actualidad, la guía ISO 31000 enfocada en la gestión de riesgos, es utilizada como una herramienta destinada a proporcionar a las empresas criterios y estándares que permiten una más eficiente de los eventos de riesgo y procesos, efectuado en las diversas fases organizacionales, tales como estratégicas y operativas (Lizarzaburu, Barriga Ampuero, Noriega Febres, & Mejía, 2017, pág. 1)

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

> Incrementar la posibilidad de alcanzar los objetivos. Dar una fuente confiable para decidir y la planificar. Optimizar tanto el aprendizaje como la flexibilidad organizacional. Fomentar e incentivar una gestión proactiva. Cumplir las exigencias legales y normativas pertinentes y con las reglas internacionales. Perfeccionar la presentación de informes obligatorios y voluntarios. Mejorar la eficacia y la eficiencia operativa. Mejorar el gobierno. Optimizar los procesos de control.

> Mejorar la eficacia y la eficiencia operativa. Reformar la gestión de incidencias. Reducir el impacto de las pérdidas. (Lizarzaburu, Barriga Ampuero, Noriega Febres, & Mejía, 2017, pág. 5)

El proceso que recomienda la norma ISO 31000, 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 la Subárea de Gestión de Pagos.

2.13.3 Norma ISO 27000

Según lo indicado por Orrego, V.M. la Norma ISO 27000 significa:

> ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por la ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que brindan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización de tipo público o privada, grande o pequeña. (Orrego, 2013, pág. 22)

De acuerdo con la cita anterior esta ISO comprende una serie de normas de seguridad que para efectos de este proyecto de graduación se enfocará en la ISO 270001 y la ISO 27002.

2.13.3.1 Norma ISO 27001

Según (Advisera, 2021) “el ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa”. (pág. 1)

Esta norma nos aporta un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa.

2.13.3.1.1 Sistema de Gestión de la Seguridad de la Información (SGSI)

Según (Gómez Orozco, 2013) "Es el conjunto de procesos para gestionar eficientemente la accesibilidad integridad y disponibilidad de los activos de información minimizando a la vez los riesgos a los que están expuestos". (pág. 1)

El objetivo del SGSI es establecer las especificaciones estableciendo controles y medidas para mantener la seguridad de la información mediante la confiabilidad, integridad y disponibilidad.

A la hora de implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001, debemos considerar como eje central de este sistema la Evaluación de Riesgos. Lo primero, es elegir una metodología de evaluación del riesgo apropiada para los requerimientos del negocio.

Las fases de esta metodología son los siguientes:

1.- Identificar los Activos de Información y sus responsables, entendiendo por activo todo aquello que tiene valor para la organización, incluyendo soportes físicos (edificios o equipamientos), intelectuales o informativas (Ideas, aplicaciones, proyectos ...) así como la marca, la reputación etc. 2.- Identificar las Vulnerabilidades de cada activo: aquellas debilidades propias del activo que lo hacen susceptible de sufrir ataques o daños. 3.- Identificar las amenazas: Aquellas cosas que puedan suceder y dañar el activo de la información, tales como desastres naturales, incendios o ataques de virus, espionaje etc. 4.- Identificar los requisitos legales y contractuales que la organización está obligada a cumplir con sus clientes, socios o proveedores. 5.- Identificar los riesgos: Definir para cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información, en relación a su disponibilidad, confidencialidad e integridad del mismo. 6.- Cálculo del riesgo: Este se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización (Riesgo = impacto x probabilidad de

> la amenaza). Con este procedimiento determinamos los riesgos que deben ser controlados con prioridad. 7.- Plan de tratamiento del riesgo: En este punto estamos preparados para definir la política de tratamiento de los riesgos en función de los puntos anteriores y de la política definida por la dirección. En este punto, es donde seleccionaremos los controles adecuados para cada riesgo, los cuales irán orientados a: Asumir el riesgo, Reducir el riesgo, Eliminar el riesgo y Transferir el riesgo. (ISO, 2018, pág. 3)

2.13.1.2 ISO 27002

Según Gómez Orozco, 2013 la norma ISO 27002 es una "guía de buenas prácticas que describe los objetivos de control y controles recomendados en cuanto a seguridad de la información". (pág. 2)

La ISO 27002 se compone de diferentes elementos que a continuación se detallan:

> ISO/IEC 27002 proporciona 14 dominios, 35 objetivos de control y 114 controles. Dominios de ISO 27002: Políticas de seguridad, Aspectos organizativos de la Seguridad de la Información, Seguridad ligada a los Recursos Humanos, Gestión de activos, Control de accesos, Cifrado, Seguridad física y ambiental, Seguridad en la operativa, Seguridad en las telecomunicaciones, Adquisición, desarrollo y mantenimiento de los sistemas de información, Relaciones con proveedores, Gestión de incidentes en la Seguridad de la Información, Aspectos de la Seguridad de la Información en la gestión de la continuidad de negocio, Cumplimiento. (EALDE, 2017, pág. 1)

2.13.1.2.1 Controles de seguridad físicos

Sobre los controles de seguridad física detallados en la ISO 27002 se menciona:

> Consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. (MOSQUERA QUINTERO, 2015, pág. 25)

Por lo anterior, los controles físicos son medidas de seguridad en una determinada organización, con el propósito de prevenir o detener el acceso no autorizado a la información confidencial que salvaguarda los activos tangibles de la Subárea. Algunos ejemplos de este control son: cámaras de video vigilancia, alarmas en accesos restringidos, guardias de seguridad.

2.13.1.2.2 Controles de seguridad lógicos

Se entiende por controles de seguridad lógica:

> La seguridad lógica se refiere a los controles específicos establecidos para administrar el acceso a los sistemas informáticos y los espacios físicos dentro del centro de datos. Usar una puerta cerrada para salvaguardar la entrada de la sala de servidores del centro de datos puede ser una mejor práctica de seguridad física, pero tener que participar en la autenticación de dos factores para abrir la puerta es una forma de seguridad lógica. Este enfoque de la seguridad del centro de datos se extiende también a los sistemas informáticos. Las contraseñas y los perfiles de usuario son un enfoque común para restringir el acceso, asegurando que solo el personal autorizado pueda acceder a los sistemas clave, como los servidores. (AYUDALEY, 2020, pág. 1)

Así mismo, los controles lógicos son medidas de seguridad tomadas con el fin de prevenir el ingreso de personas no autorizadas a sistemas informáticos, requieren una identificación y contraseña por parte del usuario para autorizar el ingreso, estos controles están muy relacionados con el cifrado de datos y telecomunicaciones. Con ellos se trata de dar un uso correcto del software, sistemas operativos, acceso a sistemas institucionales, de acuerdo con sus funciones.

Capítulo III
Marco Metodológico

3. Capítulo 3: Marco Metodológico

En este capítulo se hace énfasis en el tipo de investigación y la metodología utilizada para el desarrollo de este proyecto 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 Tipo de investigación

En el presente proyecto de graduación, se seleccionaron variables que posteriormente fueron analizadas por el investigador, esto hace hincapié que el estudio en su primera fase es descriptivo, Sampieri lo define como: (Sampieri, 2014) “los estudios descriptivos son la base de las investigaciones correlacionales, las cuales a su vez proporcionan información para llevar a cabo estudios explicativos que generan un sentido de entendimiento y están muy estructurado”. (pág. 90)

De esta forma todos los procesos críticos de la organización pudieron identificarse y analizarse gracias al estudio descriptivo y así llegar a dar soluciones concretas y efectivas para el problema planteado.

Según (Sampieri, 2014) “un buen trabajo es aquel en el cual el equipo especialista ha puesto todo su empeño en la búsqueda de conocimiento o soluciones, manteniendo siempre la objetividad y la mente abierta para tomar las decisiones adecuadas” (pág. 125)

Esta investigación termina siendo del tipo aplicada ya que se empleó el conocimiento obtenido en la investigación descriptiva con el fin de diseñar un modelo de continuidad del negocio para que sea aplicado por la Subárea y así tener los mecanismos necesarios para afrontar las consecuencias en caso de que se materialice un desastre y se pueda dar la continuidad del negocio.

3.1.1 Enfoque de la investigación

Según (Sampieri, 2014) “los diseños investigación-acción también representan una forma de intervención y algunos autores los consideran diseños mixtos, pues normalmente recolectan datos cuantitativos y cualitativos, y se mueven de manera simultánea entre el esquema inductivo y el deductivo” (pág. 500)

Con respecto al enfoque de método mixto, de acuerdo con lo indicado por Sampieri:

> Representa un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (metainferencias) y lograr un mayor entendimiento del fenómeno bajo estudio (Hernández Sampieri y Mendoza, 2008). (Sampieri, 2014, pág. 534)

Partiendo de lo anterior, el enfoque del proyecto es mixto, ya que, en el transcurso de la investigación, resultan variables que se pueden cuantificar, además la meta es la descripción del problema. Al exponer cuántas cualidades presentan el problema de continuidad del negocio en la Subárea, se trata de acercar la realidad a través del contacto con la obligación de la entidad, partiendo de una metodología.

A través de este tipo de enfoque se da mayor solidez al método científico, así como mayor posibilidad de éxito al presentar los resultados, permite una mejor utilización de los datos y una mejor exploración.

3.2 Fuentes y sujetos de información

3.2.1 Fuentes primarias

Según (Silvestrini & Vargas, 2008) las fuentes primarias son: Contienen información original, que ha sido publicada por primera vez y que no ha sido filtrada, interpretada o evaluada por nadie más. Son producto de una investigación o de una actividad eminentemente creativa. (pág. 1)

Se coordina con la Dirección de Tecnologías de Información de la CCSS, así como con la Subárea Gestión de Pagos de la Institución para obtener información acerca de los procesos críticos que implementa dicha Subárea a través de los sistemas de información.

Así mismo se toma información para el desarrollo de este trabajo, proyectos de graduación anteriores realizados por estudiantes de universidades públicas y privadas.

Además, se estudió la norma ISO 22301: Societal security – Business continuity management systems, y la norma ISO 31000: para una correcta práctica de gestión de riesgos.

Se investiga 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.

3.2.2. Fuentes secundarias

Con respecto a las fuentes de información secundaria, (Silvestrini & Vargas, 2008) indica que: “Contienen información primaria, sintetizada y reorganizada. Están especialmente diseñadas para facilitar y maximizar el acceso a las fuentes primarias o a sus contenidos. Componen la colección de referencia de la biblioteca y facilitan el control y el acceso a las fuentes primarias”. (pág. 3)

Se tomaron en cuenta las siguientes fuentes secundarias:

Resultados del Índice de Gestión Institucional (IGI) de la Contraloría General de la República en el año 2019 en el área de tecnologías de información, específicamente el punto del Área de Tecnologías de Información que tiene como objetivo consultar la existencia de un plan formal que asegure la continuidad de los servicios de tecnologías de información en la organización en la Caja Costarricense de Seguro Social, para alcanzar la misión institucional. (Ver apéndice 1.1)

La Contraloría General de la Republica (CGR, 2019) indica que el Índice de Gestión Institucional (IGI) es: "un instrumento para medir los esfuerzos realizados por las instituciones para fortalecer determinados factores comunes para garantizar su capacidad de gestión, el cual ha permitido que las instituciones identifiquen sus brechas para el logro de las buenas prácticas evaluadas" (pág. 3)

3.2.3 Fuentes terciarias

Según (Silvestrini & Vargas, 2008), las fuentes terciarias son: "Son guías físicas o virtuales que contienen información sobre las fuentes secundarias. Forman parte de la colección de referencia de la biblioteca. Facilitan el control y el acceso a toda gama de repertorios de referencia, como las guías de obras de referencia o a un solo tipo, como las bibliografías". (pág. 4)

Entre estas fuentes se toman en cuenta:

• Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones de la Caja Costarricense de Seguro Social.

• Dirección de Tecnologías de Información y Comunicaciones CCSS.

3.2.4 Sujetos de información

Según (Cabrera Méndez, 2010), "se denominan fuentes de información a diversos tipos de documentos que contienen datos útiles para satisfacer una demanda de información o conocimiento. Las fuentes de información son convencionalmente, los documentos" (pág. 1)

Las personas de contacto para la recolección de información son los expertos de la Subárea Gestión de Pagos del Área de Tesorería General, así como las diferentes herramientas para análisis de riesgos, estos sujetos de información colaboran directamente con el proyecto de graduación, suministrando información o bien interactuando con el proyecto, estas personas son las que se detallan en la tabla siguiente:

Tabla 2-Sujetos de información

Descripción del puesto	Ocupación	Experiencia	Relación con el proyecto:
Jefe Subárea Control de Pagos	Jefe, Licenciado en Administración.	36 años como de experiencia en la Institución.	Conoce cada uno de los procesos de la Subárea Gestión de Pagos, así como las funciones de cada uno de los colaboradores.
Funcionario designado por la Jefatura.	Técnico Administrativo	34 años de experiencia en su puesto.	Como funcionario designado por la Jefatura, colabora con su conocimiento e interacción con todos los procesos.

Funcionario de la Subárea.	Profesional	10 años de experiencia en su puesto.	Encargado de pago de préstamos hipotecarios y depósitos judiciales por medio de SINPE y por cheque
Funcionario de la Subárea.	Profesional	9 años de experiencia en su puesto.	Pago a proveedores locales y extranjeros, empleados, pensionados y otros conceptos, por medio de SINPE del BCCR, Internet Banking BNCR, BCR comercial y por vía cheque.
Demás funcionarios de la Subárea.	Oficinista Secretaria Técnico Administrativo	Suman más de 40 años de experiencia en su puesto.	Otros procesos y servicios brindados por la Subárea Gestión de Pagos.

Fuente: Elaboración propia.

3.3 Técnicas y herramientas de recolección de datos

Según Sampieri las herramientas de recolección de datos implican lo siguiente:

> Una vez que seleccionamos el diseño de investigación apropiado y la muestra adecuada de acuerdo con nuestro problema de estudio e hipótesis (si es que se establecieron), la siguiente etapa consiste en recolectar los datos pertinentes sobre los atributos, conceptos o variables de las unidades de muestreo/ análisis o casos (participantes, grupos, fenómenos, procesos, organizaciones, etcétera). Recolectar los datos implica elaborar un plan detallado de procedimientos que nos conduzcan a reunir datos con un propósito específico. Este plan incluye determinar: a) ¿Cuáles son las fuentes de las que se obtendrán los datos? Es decir, los datos van a ser proporcionados por personas, se producirán de observaciones y registros o se encuentran en documentos, archivos, bases de datos, etcétera. b) ¿En dónde se localizan tales fuentes? Regularmente en la muestra seleccionada, pero es indispensable definir con precisión. c) ¿A través de qué medio o método vamos a recolectar los datos? Esta fase implica elegir uno o varios medios y definir los procedimientos que utilizaremos en la recolección de los datos. El método o métodos deben ser confiables, válidos y "objetivos". d) Una vez recolectados, ¿de qué forma vamos a prepararlos para que puedan analizarse y respondamos al planteamiento del problema? (Sampieri, 2014, pág. 198)

En conclusión, la recolección de datos consiste en obtener los datos pertinentes sobre los atributos, conceptos o variables de las unidades de análisis o casos (participantes, grupos, organizaciones, etcétera), implica elaborar un plan detallado de procedimientos que nos conduzcan a reunir con un propósito específico.

Para la recolección de datos se necesitan técnicas y herramientas que el investigador pueda utilizar para desarrollar de una mejor manera la solución a cada uno de los servicios críticos de la Subárea, todos los instrumentos se aplican en un momento determinado de la investigación, con la

finalidad de obtener la información en el instante preciso, las técnicas de recolección de datos usadas en este proyecto son:

- Entrevista.
- Encuesta.
- Observación.
- Documentos (normas y registros).
- Lluvia de ideas.

3.3.1 Entrevista

Según Sampieri, la entrevista implica:

> Que una persona calificada (entrevistador) aplica el cuestionario a los participantes; el primero hace las preguntas a cada entrevistado y anota las respuestas. Su papel es crucial, resulta una especie de filtro. El primer contexto que se revisará de una entrevista es el personal ("cara a cara"). (Sampieri, 2014, pág. 233)

Podemos concluir que una entrevista según (Sampieri, 2014) "se define una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (entrevistado) u otras (entrevistados)" (pág. 403)

Al hablar de entrevistado y entrevistador según (Etecé, 2020) se refiere a: "Entrevistador: Cumple la función de dirigir la entrevista y plantea el tema a tratar haciendo preguntas. A su vez, da inicio y cierre a la entrevista. Entrevistado: Es aquel que se expone de manera voluntaria al interrogatorio del entrevistador" (pág. 1)

En el caso de este proyecto de graduación la entrevista es un proceso de obtención de información oral que se da dentro de una situación cara a cara, y se aplicará directamente con la jefatura de la Subárea Gestión de Pagos y el funcionario que la jefatura ha asignado como encargado. Con esta se determinarán los procesos críticos en la Subárea, con el fin de obtener información importante sobre el plan de continuidad en TIC. (Ver apéndice 1.2)

Tabla 3-Definición de cuestionario de entrevista a jefatura y encargados de procesos

Sección	Objetivo del cuestionario	Descripción
Pregunta 1	Definir la cantidad de colaboradores de la Subárea Gestión de Pagos.	¿Cuántos funcionarios laboran en la Subárea Gestión de Pagos?
Pregunta 2	Conocer los servicios que se brindan en la Subárea.	¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?
Pregunta 3	Identificar el conocimiento de los funcionarios.	¿En caso de presentarse una interrupción a los servicios críticos, qué hacen y cómo lo hacen?
Pregunta 4	Conocer si existe un Plan de Continuidad en la Subárea Gestión de Pagos y en qué condiciones se encuentra.	¿Cuenta la Subárea Gestión de Pagos con un Plan de Continuidad en TIC, y cuándo fue su última actualización?
Pregunta 5	Conocer la probabilidad de que se presenten fallos en los servicios que brinda la Subárea.	¿Cuál es la probabilidad de fallo en los servicios?
Pregunta 6	Conocer los tiempos de respuesta en la atención de problemas críticos.	Por lo general, ¿cuánto tiempo se espera al momento de presentarse una interrupción en algún servicio?

Pregunta 7	Determinar la frecuencia con que se presentan interrupciones en los servicios.	¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?
Pregunta 8	Conocer los procesos que se llevan a cabo en la Subárea.	¿Cuáles procesos se ejecutan en la Subárea?
Pregunta 9	Conocer la población que se beneficia de los procesos que se realizan en la Subárea.	¿A quiénes benefician los procesos que se ejecutan en la Subárea?
Pregunta 10	Identificar el lugar de resguardo de los respaldos.	¿Dónde se guardan los respaldos de la Subárea?
Pregunta 11	Conocer si los funcionarios saben el proceder en caso de interrupción.	¿Conoce el proceder en caso de presentarse una interrupción en los procesos, sea por causas relacionadas con los sistemas o por desastre natural?
Pregunta 12	Conocer quién brinda soporte a la Subárea.	¿Existe un Departamento de TI asignado a la Subárea Gestión de Pagos para Soporte Técnico?
Pregunta 13	Determinar la calidad de los equipos que utilizan los colaboradores en los procesos que realizan.	¿Cómo considera la calidad del equipo de cómputo con que cuentan los funcionarios?

Pregunta 14	Conocer si la conectividad es efectiva para realizar los procesos de la Subárea.	¿Qué opina de la velocidad del internet para ejecutar los procesos en los sistemas?
Pregunta 15	Conocer la facilidad para utilizar los sistemas.	¿Qué tipo de sistemas operativos utilizan las computadoras?
Pregunta 16	Conocer si cuentan con algún tipo de seguridad contra ataques cibernéticos.	¿Dónde están ubicados los servidores? / ¿contemplan algún tipo de seguridad contra ataques cibernéticos?

Fuente: Elaboración propia.

3.3.2 Encuesta

De acuerdo con lo indicado por (Sampieri, 2014) con respecto a la encuesta, "generalmente utilizan cuestionarios que se aplican en diferentes contextos (entrevistas en persona, por medios electrónicos como correos o páginas web, en grupo, etc". (pág. 159). También deja saber que "las entrevistas, como herramientas para recolectar datos cualitativos, se emplean cuando el problema de estudio no se puede observar o es muy difícil hacerlo por ética o complejidad" (pág. 403)

Esta herramienta se aplica a todos los colaboradores de la Subárea Gestión de Pagos para medir el conocimiento acerca del Plan de Continuidad en TIC y los procesos que se ejecutan. La encuesta es del tipo mixta, ya que es necesario ponderar satisfacciones. (Ver apéndice 1)

3.3.3 Observación

El método de la observación consiste en recolectar datos mediante el proceso sistemático, válido y confiable de comportamientos y situaciones observables, a través de un conjunto de categorías y subcategorías.

> En la investigación cualitativa necesitamos estar entrenados para observar, que es diferente de ver (lo cual hacemos cotidianamente). Es una cuestión de grado. Y la

> “observación investigativa” no se limita al sentido de la vista, sino a todos los sentidos. (Sampieri, 2014, pág. 399)

Dicha técnica se emplea al visitar la Subárea de Gestión de Pagos y visualizar los diferentes procesos que se brindan, también se observa el funcionamiento de los diferentes sistemas de software utilizados por los usuarios.

3.3.4 Documentos y registros

Esta técnica de investigación Sampieri la define como:

> Una fuente muy valiosa de datos cualitativos son los documentos, materiales y artefactos diversos. Nos pueden ayudar a entender el fenómeno central de estudio. Prácticamente la mayoría de las personas, grupos, organizaciones, comunidades y sociedades los producen y narran, o delinean sus historias y estatus actuales. Le sirven al investigador para conocer los antecedentes de un ambiente, así como las vivencias o situaciones que se producen en él y su funcionamiento cotidiano y anormal. (Sampieri, 2014, pág. 415)

Con base en lo anterior se utilizará esta técnica para revisar el Índice de Gestión Institucional (IGI) de la Contraloría General de la República de la CCSS de los años anteriores, además las autoevaluaciones de control interno realizadas por la jefatura de la Subárea de periodos anteriores para verificar el grado de avance de los sistemas y/o servicios, es importante analizar estos datos y sacar conclusiones al respecto.

También interviene en este punto la aplicación de las Normas ISO 22301 y 31000, con el fin de tomar en cuenta las mejores prácticas.

3.3.5 Lluvia de ideas

Según lo indicado por Coworkingfy:

> Es una técnica utilizada en el trabajo en equipo para generar nuevas ideas o solucionar un determinado problema. Hoy día, es altamente empleada en las reuniones laborales o en debates. Lluvia de ideas significa pensar rápida y espontáneamente sobre un tema propuesto. (Coworkingfy, 2020)

Con esta técnica se realizarán reuniones y entrevistas con la jefatura de la Subárea Gestión de Pagos y el funcionario designado por la Jefatura, así como de la investigación y desarrollo del proyecto, se realiza una lluvia de ideas para seleccionar las preguntas más precisas relacionadas con los servicios críticos y las posibles soluciones, esta técnica permite representar de una mejor forma las preguntas planteadas.

3.4 Variables

Tabla 4-Variables

Titulo del Proyecto:	Plan de Continuidad en TIC de la Subárea Gestión de Pagos del Área de Tesorería General de la Caja Costarricense de Seguro Social.					
Objetivo General:	Desarrollar el Plan de Continuidad en TIC de la Subárea Gestión de Pagos del Área de Tesorería General.					
Objetivo Especifico	**Variable**	**Definición Conceptual**	**Indicador**	**Medida**	**Tipo de Variable**	**Instrumento**
1. Identificar los procesos críticos de la Subárea Gestión de Pagos de la Tesorería General de la Caja Costarricense de Seguro Social, por medio de una entrevista al encargado designado y mediante el análisis FODA y matrices para la determinación de los riesgos.	Identificar los procesos críticos.	Identificación de los procesos de la Subárea Gestión de Pagos.	Procesos que ejecuta la Subárea.	Enumerar los procesos.	Cualitativa	Entrevista y encuesta a los encargados de cada proceso.
2. Realizar el diagnóstico de los riesgos de los procesos críticos, mostrando cada uno de forma clara, con su nivel de criticidad, para tenerlos claros e identificarlos en caso de que se estén materializando.	Diagnóstico de riesgos de los procesos críticos.	Elaboración del Diagnóstico de Riesgos detectados.	Identificación de los riesgos por medio del semáforo	Enumerar los riesgos calificados según mapa de calor.	Cualitativa	Entrevista y encuesta con los funcionarios de la Subárea Gestión de Pagos.
3. Determinar las estrategias de mitigación, tomando en cuenta cada uno de los riesgos detectados, con el fin de conocer el proceder en caso de materializarse alguno o varios de los riesgos y mostrando un responsable para cada uno de ellos al lado de la jefatura	Estrategias de mitigación.	Estrategias de mitigación de cada uno de los riesgos detectados.	Estrategias de mitigación	Enumeración de estrategias de mitigación.	Cualitativa	Entrevista con el encargado asignado por la Jefatura de la Subárea Gestón de Pagos.

Titulo del Proyecto:	Plan de Continuidad en TIC de la Subárea Gestión de Pagos del Área de Tesorería General de la Caja Costarricense de Seguro Social.					
Objetivo General:	Desarrollar el Plan de Continuidad en TIC de la Subárea Gestión de Pagos del Área de Tesorería General.					
Objetivo Especifico	**Variable**	**Definición Conceptual**	**Indicador**	**Medida**	**Tipo de Variable**	**Instrumento**
4. Desarrollar el Plan de Continuidad en TIC de la Subárea Gestión de Pagos de la Tesorería General de la Caja Costarricense de Seguro Social.	Plan de Continuidad en TIC de la Subárea Gestión de Pagos del Área de Tesorería General.	Desarrollo del Plan de Continuidad en TIC de la Subárea Gestión de Pagos.	Plan de Continuidad en TIC 2021 a la Subárea Gestión de Pagos	Formularios DTIC, riesgos identificados y su clasificación, el plan de mitigación, procedimientos de recuperación ante desastres, inventario de activos, definición de controles para garantizar la continuidad.	Cualitativa	Cuestionario basado en las mejores prácticas y las normas ISO 22301 y 31000.
5.Comunicar el Plan de Continuidad en TIC a los funcionarios de la Subárea Gestión de Pagos e implementación de este, se realizará mediante una reunión virtual con los integrantes de la Subárea, para cumplir con lo establecido a nivel institucional sobre el conocimiento por parte de todo el equipo de trabajo y en especial por los responsables indicados por la jefatura en caso de materializarse un riesgo.	Hacer del conocimiento del equipo de trabajo el Plan de Continuidad en TIC.	Comunicación del Plan de Continuidad en TIC a la Subárea Gestión de Pagos.	Comunicar el Plan de Continuidad en TIC 2021 de la Subárea Gestión de Pagos	Reunión virtual.	Cualitativa	Reunión virtual con los integrantes de la Subárea.

3.5 Diseño de la investigación

De acuerdo con lo que indica Sampieri en relación al diseño de la investigación, menciona lo siguiente:

> Una vez que se precisó el planteamiento del problema, se definió el alcance inicial de la investigación y se formularon las hipótesis (o no se establecieron debido a la naturaleza del estudio), el investigador debe visualizar la manera práctica y concreta de contestar las preguntas de investigación, además de cumplir con los objetivos fijados. Esto implica seleccionar o desarrollar uno o más diseños de investigación y aplicarlos al contexto particular de su estudio. El término diseño se refiere al plan o estrategia concebida para obtener la información que se desea con el fin de responder al planteamiento del problema. (Sampieri, 2014, pág. 128)

En esta sección del documento se muestra el proceso que conlleva el trabajo de investigación, a continuación, se detallan las etapas y fases del proyecto, indicando las técnicas y herramientas empleadas por etapa, además de los resultados esperados.

Etapa 1-Investigación:

Se identifican las actividades que deben ser analizadas de forma previa. Elaboración del plan de continuidad en TIC que determine los objetivos y el alcance. Planificar el proyecto, programar y desarrollar el plan de trabajo el cual debe satisfacer los objetivos planteados.

- Técnica 1, Entrevista: se emplea está técnica para conocer como está actualmente el servicio brindado por la Subárea y antecedentes del conocimiento que poseen en temas relacionados al Plan de Continuidad en TIC.
- Técnica 2, Observación: está técnica se aplica con el objetivo de obtener datos de los servicios y procesos que realiza la Subárea, así como la interacción que los empleados realizan con los sistemas.

Etapa 2-Análisis de riesgos:

Se deben identificar los procesos claves de la Subárea y los riesgos a los que están expuestos. Examinar los servicios críticos de la Subárea, estimar el impacto de los posibles fallos en esos servicios, reconocer y valorar los riesgos que puedan interrumpir la continuidad del servicio.

- Técnica 3, Documentos y registros: se corroboran documentos y registros existentes para obtener información de los procesos y planes anteriores, así como las Normas ISO 22301 y 31000.

Etapa 3 Medidas preventivas:

Se implementan medidas de seguridad preventivas y proactivas para evitar o gestionar los incidentes graves. La Subárea debe identificar y aplicar controles o medidas de seguridad con el fin de:

▪ Reducir la probabilidad de que los procesos críticos sufran una interrupción.

▪ Disminuir el tiempo de una eventual interrupción.

▪ Limitar el impacto que puede causar una interrupción de los procesos críticos en la Institución.

▪ Incrementar la fortaleza de la Subárea eliminando puntos de fallo.

- Técnica 4, Lluvia de ideas: es aplicada con el fin de obtener diferentes soluciones a las reuniones provenientes de la jefatura respectiva, además para sintetizar de una mejor manera las opiniones expuestas.

Etapa 4 Estrategia de recuperación:

La idea principal es establecer objetivos y prioridades de recuperación en función de los riesgos que impactan los procesos de la Subárea, esta debe tener en cuenta los posibles daños potenciales a la hora de revisar y seleccionar las diferentes soluciones o alternativas de recuperación de sus actividades prioritarias.

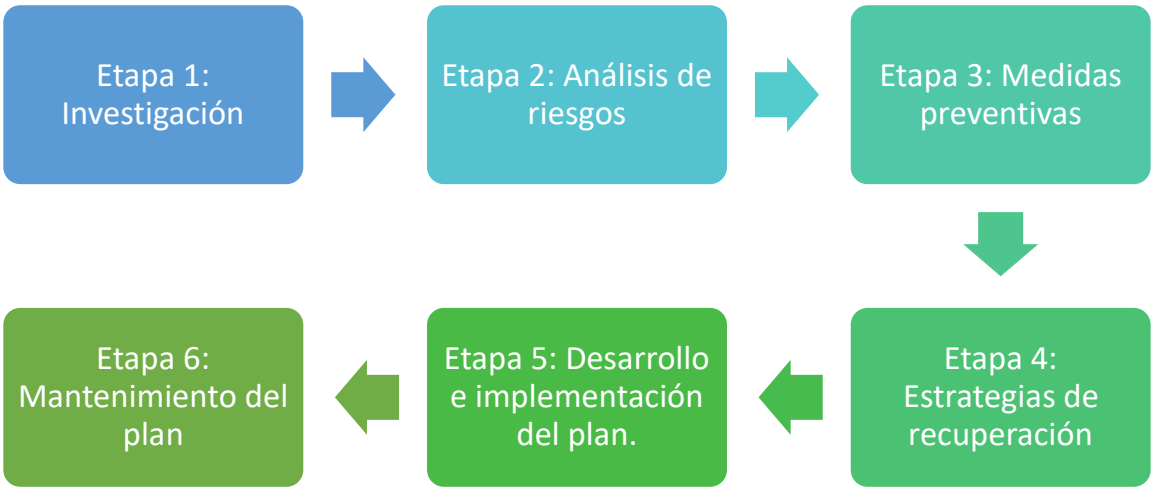
Etapa 5 Desarrollo e implementación del plan:

En esta etapa se dan todos los procedimientos a seguir para la recuperación de los servicios críticos al producirse una interrupción. Se deben identificar los procedimientos a seguir para la activación y ejecución del plan de continuidad. Se desarrollan los procedimientos de alerta y mitigación, se dispone de los medios y recursos necesarios para ejecutar el plan. En este caso en específico, solo se desarrolla el plan, ya que este será implementado en su momento por la Subárea Gestión de Pagos.

Etapa 6 Mantenimiento del plan:

En dicha etapa la Subárea Gestión de Pagos será la encargada de realizar el mantenimiento, siguiendo las recomendaciones brindadas, es importante comunicar la importancia del mantenimiento una vez que sea finalizado.

Figura 8-Flujo de las etapas del proyecto



Fuente: elaboración propia.

3.6 Matriz de coherencia

En la siguiente tabla se puede visualizar la relación entre los objetivos, los entregables, instrumentos y los temas del marco teórico con el fin de ordenar y entender de mejor forma el proceso metodológico de esta investigación.

Tabla 5-Relación matriz de coherencia

Objetivos	Entregable	Fase	Técnicas	Temas
Identificar los procesos críticos de la Subárea Gestión de Pagos de la Tesorería General de la Caja Costarricense de Seguro Social, por medio de una entrevista al encargado designado y mediante el análisis FODA y matrices para la determinación de los riesgos.	Inventario de procesos	Investigación	➤ Entrevista ➤ Encuesta ➤ Observación ➤ Lluvia de ideas	➤ Plan de continuidad. ➤ Proceso del negocio. ➤ Dependencias entre procesos.
Realizar el diagnóstico de los riesgos de los procesos críticos, mostrando cada uno de forma clara, con su nivel de criticidad, para tenerlos claros e identificarlos en caso de que se estén materializando	Matriz de análisis de riesgos	Análisis de riesgos	Documentos y registros	➤ Riesgos tecnológicos. ➤ Análisis de riesgos. ➤ Categorización del riesgo. ➤ Matriz de calor de riesgos.

Determinar las estrategias de mitigación, tomando en cuenta cada uno de los riesgos detectados, con el fin de conocer el proceder en caso de materializarse alguno o varios de los riesgos y mostrando un responsable para cada uno de ellos al lado de la jefatura.	Estrategias de mitigación	➢ Medidas preventivas ➢ Estrategias de recuperación	➢ Entrevista ➢ Observación ➢ Documentos y registros	➢ Estrategia de continuidad del negocio. ➢ Tipos de estrategias del plan de continuidad. ➢ Desarrollo de estrategias de recuperación. ➢ Requerimientos de recuperación.
Desarrollar el Plan de Continuidad en TIC de la Subárea Gestión de Pagos de la Tesorería General de la Caja Costarricense de Seguro Social.	Plan de Continuidad en TIC.	Desarrollo del plan	➢ Entrevista ➢ Encuesta ➢ Observación ➢ Documentos y registros	➢ Norma ISO 22301 ➢ Norma ISO 31000 ➢ Modelo PDCA ➢ Componentes de un plan de continuidad.

Comunicar el Plan de Continuidad en TIC a los funcionarios de la Subárea Gestión de Pagos	Entrega del Plan de Continuidad en TIC 2021 a la Subárea Gestión de Pagos	Comunicar el plan	Reunión virtual	➢ Organización y administración del plan. ➢ Procedimiento de mejora continua. ➢ Plantillas de control. ➢ Plantilla resumen del evento.

Fuente: elaboración propia

La tabla anterior complementa todo el marco teórico con los objetivos del proyecto, de esta forma determina la necesidad del plan de continuidad en TIC de la Subárea Gestión de Pagos.

CAPITULO IV

DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

4. Capítulo 4: Diagnóstico de la situación actual

4.1 Situación actual

El presente capítulo tiene como finalidad identificar claramente el proceso de diagnóstico de la Subárea Gestión de Pagos y determinar el ámbito en que se desarrolla. Además, se analiza el diagnóstico que actualmente presenta dicha Subárea en términos de la infraestructura de TI.

La labor de un diagnóstico se define como:

> Un estudio previo a toda planificación o proyecto y que consiste en la recopilación de información, su ordenamiento, su interpretación y la obtención de conclusiones e hipótesis. Consiste en analizar un sistema y comprender su funcionamiento, de tal manera de poder proponer cambios en el mismo y cuyos resultados sean previsibles. (Cauqueva, 2007)

De acuerdo con lo anterior y enmarcando la situación en la Subárea Gestión de Pagos, se reconoce que mediante el diagnóstico aplicado se permitirá brindar a la organización una proximidad, a la realidad que existe en la institución, todo esto con el objetivo de identificar los mecanismos que requieren mayor atención a fin de garantizar satisfactoriamente su debida gestión y funcionamiento. Los elementos que incluyen este diagnóstico son:

Administrativo: es un estudio sistemático en TI, que tiene como propósito conocer la organización administrativa de las jefaturas de acuerdo con entrevistas y el funcionamiento del área objeto de estudio con la finalidad de detectar las causas y efectos de los problemas administrativos de la Subárea. Las etapas que dividen al diagnóstico administrativo del proyecto son: políticas internas de seguridad, documentos existentes, e intranet interna.

Técnico: es la revisión de infraestructura física y lógica a nivel de TI en la Subárea Gestión de Pagos, se detalla en el inventario físico los equipos de la Subárea (computadoras e impresoras), servidores y dispositivos de red. En el inventario lógico se abarcan tres importantes datos como lo son: seguridad informática, servidores en la nube, enlace de internet y sistemas operativos.

Percepción: en este tipo de diagnóstico se analizan los resultados de las herramientas de aplicación (entrevistas y encuestas), se deben de plasmar los resultados obtenidos a partir de la

respuesta de los empleados o personas que estuvieron relacionadas con dichas aplicaciones. La entrevista se realizó a la jefatura de la Subárea Gestión de Pagos, se detallan las cuatro preguntas más sobresalientes. Para la sección de la encuesta se utilizó la herramienta Microsoft Word, donde se le envío vía correo electrónico para que completara la encuesta, todo el análisis se muestra en dicha sección.

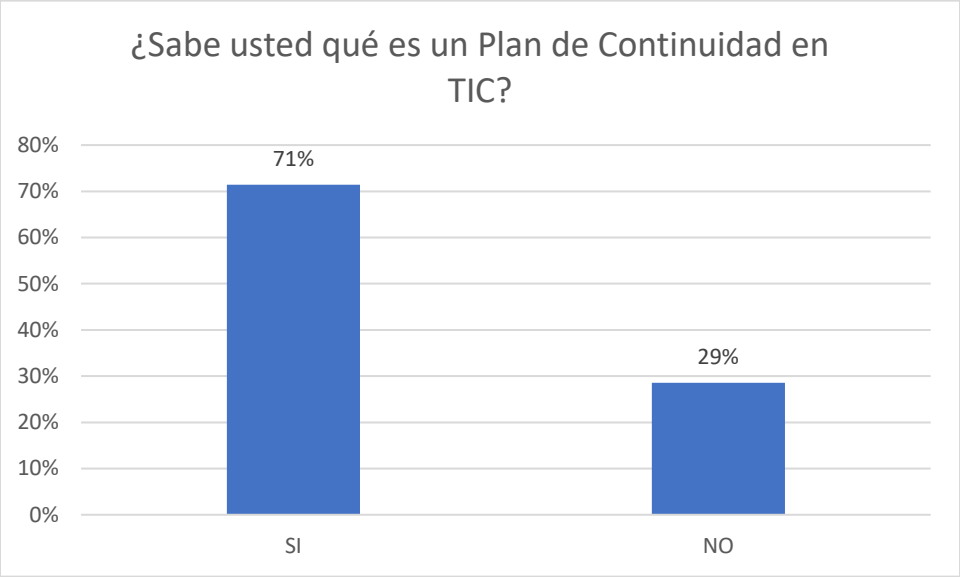
Conclusiones: se obtienen las brechas finales del diagnóstico donde se ve el impacto negativo que genera el no tener un Plan de Continuidad en TIC, se revelan los problemas potenciales de la Subárea Gestión de Pagos y de esta manera se determina como las distintas conclusiones implican en cómo se debe constituir para fundamentar el proyecto.

4.2. Diagnóstico administrativo

Se consulta a la jefatura sobre el conocimiento en materia del Plan de Continuidad en TIC, además se aplican entrevistas a un total de seis personas, que son los funcionarios de la Subárea Gestión de Pagos, se obtiene que la probabilidad de que los funcionarios conozcan lo que es un Plan de Continuidad en TIC es de un 71%, donde solamente cinco personas indican tener conocimiento acerca del tema.

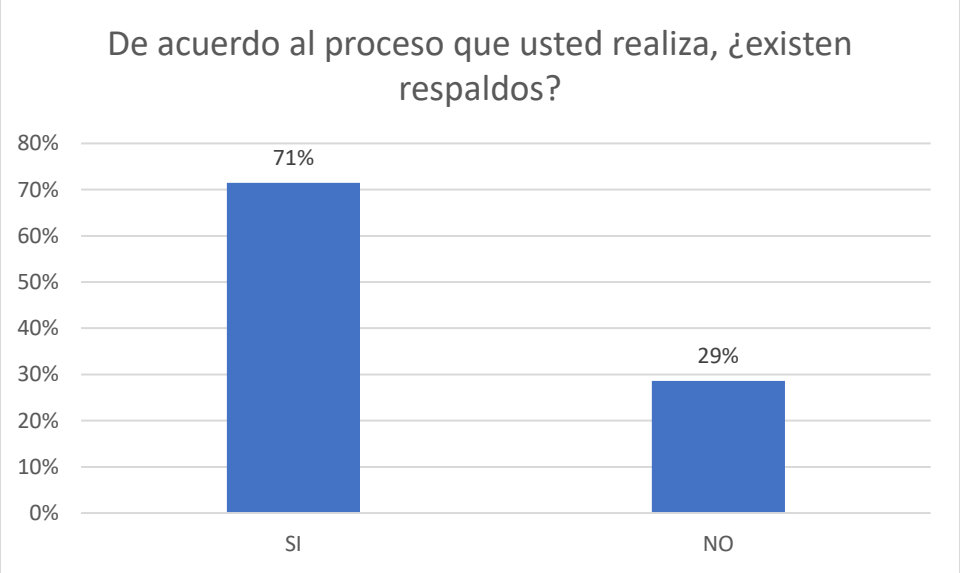
Existencia de procedimientos: como se observa en los siguientes gráficos se indica que el 29% del personal de la Subárea Gestión de Pagos, manifiesta que actualmente desconocen la existencia de un Plan de Continuidad en TIC implementado por la Subárea Gestión de Pagos, ni procedimientos que indiquen como proceder en caso de que alguno de los procesos de trabajo presente fallas y signifiquen un verdadero riesgo de continuidad en operaciones para la Subárea.

Gráfico 1-conocimiento sobre el Plan de Continuidad en TIC



Fuente: elaboración propia.

Gráfico 2-Existencia de respaldos de la información en la Subárea Gestión de Pagos



Fuente: elaboración propia.

4.2.1 Políticas internas de seguridad

La Subárea Gestión de Pagos no cuenta con un Plan de Continuidad en TIC, como parte de procesos o pasos que se deben realizar en caso de fallas que se den en sus sistemas, cuentan con una hoja de resumen incipiente con algunas características, el mismo se realizó en enero del 2018 por un funcionario de la Subárea que no tenía los conocimientos técnicos en TI, sin embargo la Institución cuenta con un Manual que lleva de nombre "Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones ASCI-UCG-0RG-002" donde se detallan todas las políticas que deben aplicarse en la organización, además se indica que como parte de las funciones de cada Área o Subárea de la Institución, se actualice el Plan de Continuidad en TIC, formalmente mínimo una vez cada dos años y cada modificación que se haga debe ser avalada por la Dirección de Tecnologías de Información y Comunicaciones.

4.2.2. Documentos existentes

Figura 9-Hoja resumen de la Subárea Gestión de Pagos

	Procedimiento alterno de trabajo (PTC019) número 1	Código de Procedimiento	Fecha de emisión 18/06/2018	
			Fecha de aprobación	Página 1
Escrito por: Juan Carlos Muñoz Jara		Aprobado por: Lic. Luis D. Bolaños Rojas		Versión: 3.1
Unidad de Negocio	Subarea Gestión de Pagos			
Proced. Relacionados	Emisión general de pagos cheque (**no critico)**			
Objetivos:	Tener un procedimiento manual de el proceso de emisión de pagos, para la continuidad de la gestión.			

Recursos críticos:

(1) Personal

Nombre	Puesto	Teléfono o correo electrónico
Luis Diego Bolaños Rojas	Jefatura	lubola@ccss.sa.cr
Luis Daniel Rodriguez Arce	Digitador	lrodrigueza@ccss.sa.cr
Juan Carlos Muñoz Jara	Aprobador	jcmunozj@ccss.sa.cr
Gabriela Aymerich Blem	Técnico Adm 1	gaymerich@ccss.sa.cr

(2) Comunicación:

Detalle del procedimiento

Acciones en orden de secuencia	Responsable	Recursos
Con la información de la factura, se emite el cheque mediante máquina de escribir o en forma manual	Luis Daniel Rodriguez Arce	Factura y Máquina de escribir
Al cheque se le adjunta la factura y se traslada para distribuir copias y ordenar cheques	Gabriela Aymerich Blem	Sellos con numeración y sellos de cancelado
Se traslada a la persona que revisa que toda la información de la factura sea congruente con el cheque emitido	Juan Carlos Muñoz Jara	Revisión y VB°
Sumar los montos de las facturas por cuentas bancarias para el cierre del día	Gabriela Aymerich Blem y Juan Carlos Muñoz Jara.	Sumadora, maquina de escribir o excel
Elaborar el listado diario en excel o máquina de escribir con el número de cheque, nombre de proveedor para ser entregada a la Subarea Caja Custodia de Valores	Gabriela Aymerich Blem y Juan Carlos Muñoz Jara.	Máquina de escribir o excel
Trastalar a la Subarea de Contabilidad la papelería, para realizar los asientos correspondientes	Juan Carlos Muñoz Jara	Máquina de escribir o excel

	Informar al Area de Contabilidad de IVM y al Area de Gestión Informática, de la Gerencia de Pensiones los pagos emitidos y las fechas del primer pago mediante listados manuales	Luis Daniel Rodriguez Arce	Máquina de escribir o excel
Código Área: Subarea Gestión de Pagos		Versión:3.1	Fecha: 18-06-2018
Plan de Continuidad TIC		Autor: Juan Carlos Muñóz Jara	

Fuente: Subárea Gestión de Pagos.

	Procedimiento alterno de trabajo (PTC019) número 2	Código de Procedimiento	Fecha de emisión 18/06/2018	
			Fecha de aprobación	Página 1
Escrito por: Jorge Araya Flores		Aprobado por: Lic. Luis D. Bolaños Rojas		Versión: 3.1

Unidad de Negocio Subarea Gestión de Pagos

Proced. Relacionados Emisión general de pagos SINPE(**no critico)**

Objetivos: Tener un procedimiento manual de el proceso de emisión de pagos, para la continuidad de la gestión.

-

Recursos críticos:

(1) Personal

Nombre	Puesto	Teléfono o correo electrónico
Luis Diego Bolaños Rojas	Jefatura	lubola@ccss.sa.cr
Luis Daniel Rodriguez Arce	Digitador	lrodrigueza@ccss.sa.cr
Maria Gabriela Arguello Perez	Digitador	marque@ccss.sa.cr
Juan Carlos Muñoz Jara	Aprobador	jcmunozj@ccss.sa.cr
Gabriela Aymerich Blem	Técnico Adm 1	gaymerich@ccss.sa.cr

Detalle del procedimiento **(2) Comunicación:**

Acciones en orden de secuencia	Responsable	Recursos
Con la información de la factura, se digita transferencia TEF Terceros por en nodo del SINPE, sea en la misma unidad o el SAO del BCCR	Luis Daniel Rodriguez Arce	Factura y plataforma SINPE (SAO)
Se traslada solicitud de transferencia con los adjuntos al funcionario aprobador de la misma en el SINPE	Juan Carlos Muñoz Jara	Factura, documentos adjuntos y plataforma SINPE(SAO)
Se traslada a la persona que emite la transferencia en SINPE	Luis Diego Bolaños Rojas	Plataforma SINPE
Arqueo diario de las operaciones, cotejar vrs listado de solicitud de recursos diarios	Gabriela Aymerich Blem	Sumadora, maquina de escribir o excel
Emitir al reestablecerse los servicios afectados,lo correspondiente a las solicitudes de pago en SIPA , con el objetivo de realizar la afectación contable y presupuestaria.	Maria Gabriela Arguello Perez	equipo computo, SIPA
Excluir de los archivos por credito directo a cancelar y que se remiten mediante el servicio CCD del BCCR, los pagos cancleados manualmente vía SINPE tef terceros, con el objetivo de evitar duplicidad de pago	Luis Diego Bolaños Rojas	equipo computo, archivos . Datos SINPE

Código Área: Subarea Gestión de Pagos	Versión:3.1	Fecha: 18-06-2018
Plan de Continuidad TIC	Autor: Juan Carlos Muñóz Jara	

Fuente: Subárea Gestión de Pagos.

En las figuras anteriores se evidencia el documento con el que cuenta actualmente la Subárea Gestión de Pagos, sin embargo, en el archivo no se indican los procesos críticos detallados, la estrategia de mitigación, ni los responsables directos de cada proceso, por tal motivo la necesidad de desarrollar el Plan de Continuidad en TIC de la Subárea.

4.2.3. Intranet interna

La Caja Costarricense de Seguro Social utiliza una intranet, donde todos los colaboradores comparten recursos importantes y de conocimiento, políticas, manuales y formularios entre otros, al alcance de todos los colaboradores, con algunas restricciones de acuerdo al lugar de trabajo o las funciones que se realizan, una intranet es un sitio web interno generalmente restringido por IP, el objetivo principal es que la información que se almacena reside como objetivo asistir a los trabajadores en la generación de valor en la organización.

En la Subárea Gestión de Pagos, la intranet no posee documentos importantes, no existen archivos ordenados por carpetas, cualquier colaborador puede visualizarlo. A continuación, se detallan pantallazos:

Figura 10-Intranet de la Subárea Gestión de Pagos

Figura 11-Intranet de la Subárea Gestión de Pagos-Documentos compartidos

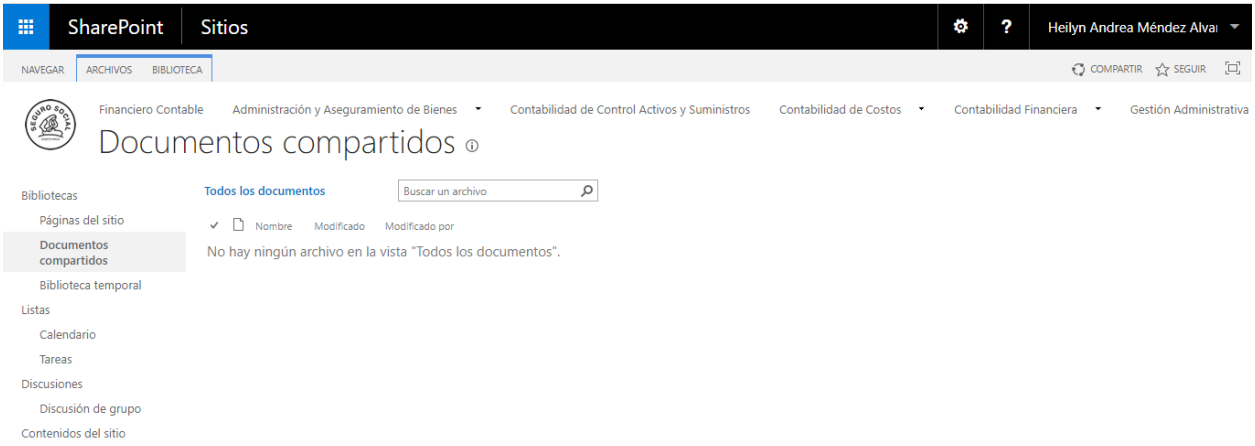
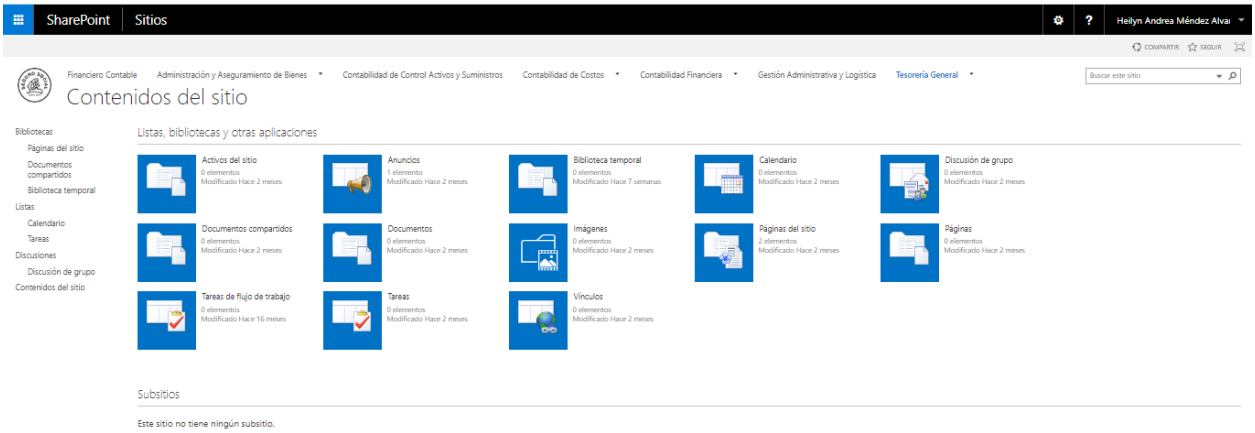


Figura 12-Intranet de la Subárea Gestión de Pagos-Contenido del sitio



Como se logra visualizar en las imágenes anteriores no existen documentos, políticas de seguridad, no hay modelos operativos, procedimientos ni reglamentos internos.

4.3 Diagnóstico técnico

El departamento de TI de toda organización, es un área clave ya que, tiene sus responsabilidades que básicamente se enfocan en cuatro campos que son: infraestructura, aplicativos, operaciones y servicio a los clientes internos como externos tales como: soporte a los empleados, servicios de red, mantenimiento preventivo y soporte entre otros. La Subárea Gestión de Pagos no cuenta con su propio Centro de Gestión Informática (CGI), depende del CGI de la Gerencia Financiera, que, en caso de requerir soporte, son quienes lo brindan.

4.3.1 Dispositivos físicos TI

El hecho de analizar todos los componentes de hardware es importante para brindar un panorama de la situación que se vive en la actualidad. Se analizarán los componentes de la infraestructura física de la Subárea Gestión de Pagos, dividiendo dicho análisis en computadoras, impresoras y teléfonos IP; se eligieron estos elementos porque son los que predominan en la Subárea, además es más sencillo subdividir la categoría en estos elementos.

La tabla mostrará el estado del equipo, además de su capacidad de almacenamiento, procesamiento y demás especificaciones.

Tabla 6-Inventario del equipo cómputo de la Subárea Gestión de Pagos

Nombre PC	Placa CPU	Placa Monitor	Disco Duro	Marca	Memoria RAM	Procesador
1121-1038127	1038127	1038175	1 Tb	HP	8 Gb	Core i5
1121-1314574	1314574	1167189	475 Gb	HP	8 Gb	Core i7
1121-975524	975524	975524	464 Gb	HP	6 Gb	Core i5
1121-1102940	1102940	1102939	915 Gb	HP	8 Gb	Core i5
1121-1102938	1102938	1102937	1 Tb	HP	8 Gb	Core i5
1121-1102936	1102936	1102935	1 Tb	HP	8 Gb	Core i5
1121-920285	920285	848181	465 Gb	HP	4 Gb	Core i5
1121-1167188	1167188	953126	1 Tb	HP	8 Gb	Core i5
1121-953104	953104	953111	465 Gb	HP	4 Gb	Core i5

Fuente: elaboración propia.

Tabla 7-Inventario impresoras de la Subárea Gestión de Pagos

Número de placa	Descripción
1167158	Impresora

Fuente: elaboración propia.

Tabla 8-Inventario teléfonos IP de la Subárea Gestión de Pagos

Placa	Descripción
1038252	Teléfono IP
1038250	Teléfono IP
1124456	Teléfono IP
1167101	Teléfono IP
1167175	Teléfono IP
1038251	Teléfono IP
1167176	Teléfono IP

Fuente: elaboración propia.

4.3.1.1 Computadoras

Tabla 9-Inventario computadoras de la Subárea Gestión de Pagos

Nombre PC	Placa CPU	Placa Monitor	Disco Duro	Marca	Memoria RAM	Procesador	Sistema operativo
1121-1038127	1038127	1038175	1 Tb	HP	8 Gb	Core i5	Windows 10
1121-1314574	1314574	1167189	475 Gb	HP	8 Gb	Core i7	Windows 10
1121-975524	975524	975524	464 Gb	HP	6 Gb	Core i5	Windows 10
1121-1102940	1102940	1102939	915 Gb	HP	8 Gb	Core i5	Windows 10
1121-1102938	1102938	1102937	1 Tb	HP	8 Gb	Core i5	Windows 10
1121-1102936	1102936	1102935	1 Tb	HP	8 Gb	Core i5	Windows 10
1121-920285	920285	848181	465 Gb	HP	4 Gb	Core i5	Windows 10
1121-1167188	1167188	953126	1 Tb	HP	8 Gb	Core i5	Windows 10
1121-953104	953104	953111	465 Gb	HP	4 Gb	Core i5	Windows 10

Fuente: elaboración propia.

4.3.1.2 Impresoras

Tabla 10-Inventario impresoras de la Subárea Gestión de Pagos

Número de placa	Descripción
1167158	Impresora

Fuente: elaboración propia.

Con respecto al cuadro anterior, la Subárea Gestión de Pagos cuenta con una única impresora, que está compartida por direccionamiento IP para el uso de todos los integrantes de la Subárea.

4.3.1.3 Conexión a internet

La conexión a internet es bastante buena, sin embargo, existen algunas quejas de los funcionarios, ya que la conexión a internet cuando falla tarda en restablecerse afectando la labor de las personas. En la revisión que se realiza a toda la instalación de red, se logra visualizar que los puertos de red se encuentran en buenas condiciones de uso y funcionamiento, tal y como se muestra en la siguiente figura.

Figura 13-Puntos de red

Se puede observar un poco de desorden de cables, además de diferentes tipos sin ningún etiquetado, lo que indica que el mantenimiento es mínimo, en la imagen se puede visualizar mucho polvo en la superficie de los equipos, todos los artefactos están conectados a una sola terminal, sin embargo, se rescata que los equipos cuentan con UPS, por lo que al haber un corte de corriente los funcionarios tienen la posibilidad de guardar la información.

Figura 14-Condiciones del equipo

En la figura anterior se muestra la falta de mantenimiento preventivo como correctivo que presentan los equipos de red en la Subárea Gestión de Pagos y es que, de acuerdo con lo investigado, no tienen fechas definidas para hacer mantenimientos, sino que cada vez que falle algún equipo de red o alguna computadora de los colaboradores, se solicita la corrección inmediatamente.

Figura 15-Cableado del equipo

La instalación de los equipos en los puestos de trabajo muestra los cables expuestos, enredados, no hay aseo por parte de los colaboradores según la imagen anterior, al consultar acerca del escaso mantenimiento que se observa en cada equipo comentan que el tiempo que dedican para realizar estas funciones es mínimo, por lo que el mantenimiento queda sin reparación hasta que ocurre la falla inminente en los equipos.

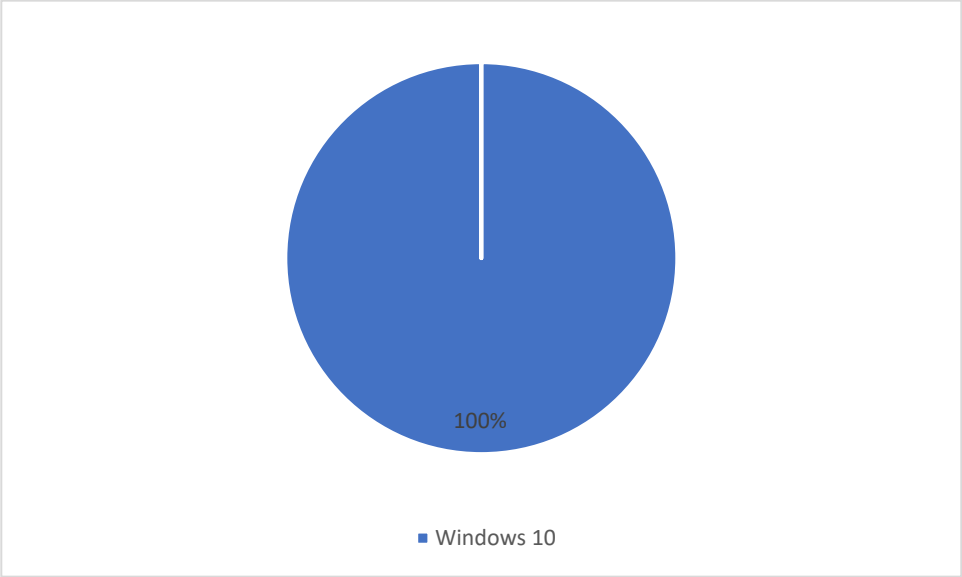
4.3.2 Dispositivos lógicos TI

En el diagnóstico lógico efectuado en la Subárea Gestión de Pagos, se detecta los siguiente:

4.3.2.1 Sistemas operativos de las computadoras

Los equipos poseen el sistema operativo Windows 10.

Gráfico 3-Sistema operativo de las computadoras de la Subárea Gestión de Pagos



Fuente: elaboración propia.

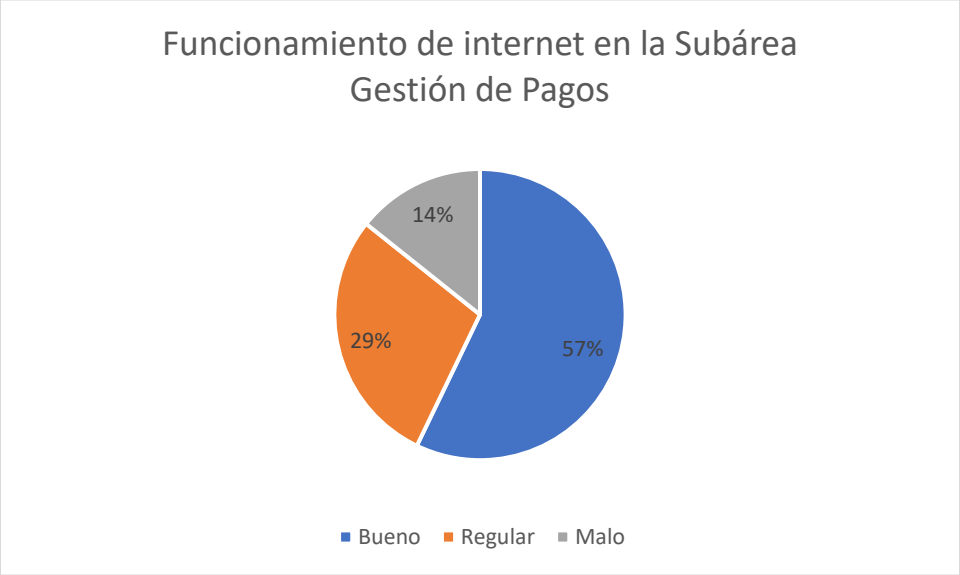
La gráfica muestra que todos los equipos la Subárea Gestión de Pagos, poseen el sistema operativo Windows 10.

Con respecto a los paquetes de ofimática utilizados, todos los equipos tienen versiones distintas de Microsoft Office, que van desde la 2010, hasta Office 365.

4.3.2.2 Conexión a internet

La conexión a internet funciona bastante bien, sin embargo, según mencionan los empleados que laboran dentro de la Subárea, en ocasiones sufre interrupciones.

Gráfico 4-Funcionamiento de internet en la Subárea Gestión de Pagos



Fuente: elaboración propia.

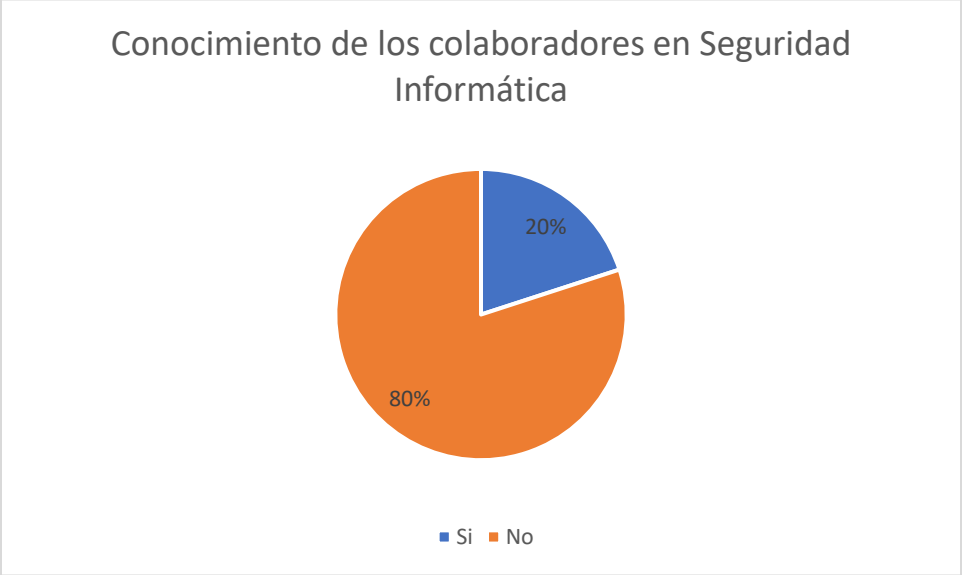
Con el estudio del gráfico anterior podemos determinar la opinión de los funcionarios, donde la mayoría indica que el internet es bueno, sin embargo, un porcentaje importante menciona que es regular y en menor grado, pero significativo, un porcentaje no responde a las expectativas de los funcionarios.

4.3.2.3 Seguridad informática

En la Subárea Gestión de Pagos, laboran 7 personas, todas ellas con funciones administrativas; su equipo de cómputo y sus herramientas para desarrollar cada una de sus funciones.

Se realizó una consulta a los empleados sobre el conocimiento de los roles y limitaciones que tienen dentro de la red, en cuanto accesos a documentos, instalación de aplicaciones e incluso el uso de la red inalámbrica y es que la mayoría de los funcionarios no conocen sobre las medidas de seguridad con las que cuenta, tales como accesos y uso de equipo de cómputo.

Gráfico 5-Conocimiento de los colaboradores de la Subárea Gestión de Pagos en Seguridad Informática



Fuente: elaboración propia.

Además, en consulta realizada a los colaboradores se identificó que no poseen conocimiento acerca de si están expuestos a ataques cibernéticos y sus afectaciones a documentos confiables que se manejan en la institución, además se perjudica por una posible intrusión.

Además, desconocen si se realiza algún tipo de respaldo para las configuraciones base de switches, routers, firewall.

4.3.2.4 Servidores

Al no contar con un encargado directo en el Área de Informática y depender de otra área para brindar soporte, desconocen sobre respaldos en los servidores de aplicaciones, lo cual no garantiza la continuidad ante los clientes y los sistemas o aplicaciones que se encuentran instalados en ellos.

Tampoco están enterados de si diariamente o cada cuánto tiempo se realiza una copia de seguridad en cada una de las bases de datos y archivos que están guardadas en un sitio alterno y el mantenimiento que les dan a los dispositivos es muy poca.

Todos los programas instalados en cada uno de los equipos cuentan con su respectiva licencia, no obstante, en estos equipos hay instalados aplicativos que no se utilizan por lo que esto puede ocasionar problemas de almacenamiento, memoria RAM e inclusive ataques cibernéticos, si no cuentan con ningún tipo de software de defensa ante ataques de este tipo.

4.4. Diagnóstico de percepción

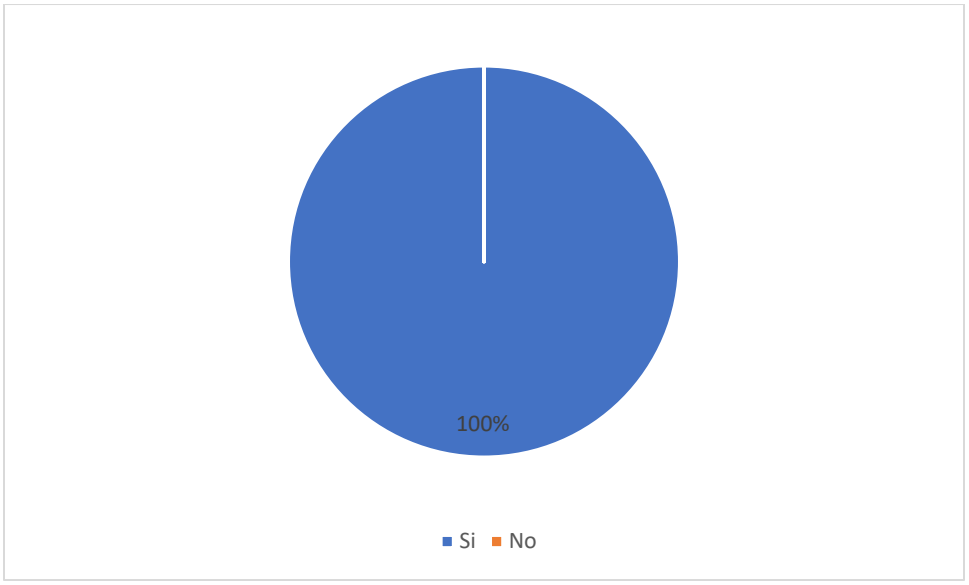
En el diagnóstico de percepción de la Subárea Gestión de Pagos, se efectúa por medio de los resultados de las entrevistas y encuesta realizados a los colaboradores de la Subárea, estos instrumentos, se muestran en este apartado, en el que se grafican los resultados obtenidos.

4.4.1 Entrevista

La entrevista se aplica a la jefatura de la Subárea Gestión de Pagos. La misma consta de 16 preguntas. A continuación, se exponen las 9 más relevantes para el diagnóstico de percepción:

1. ¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?

Gráfico 6-Servicios críticos de la Subárea Gestión de Pagos

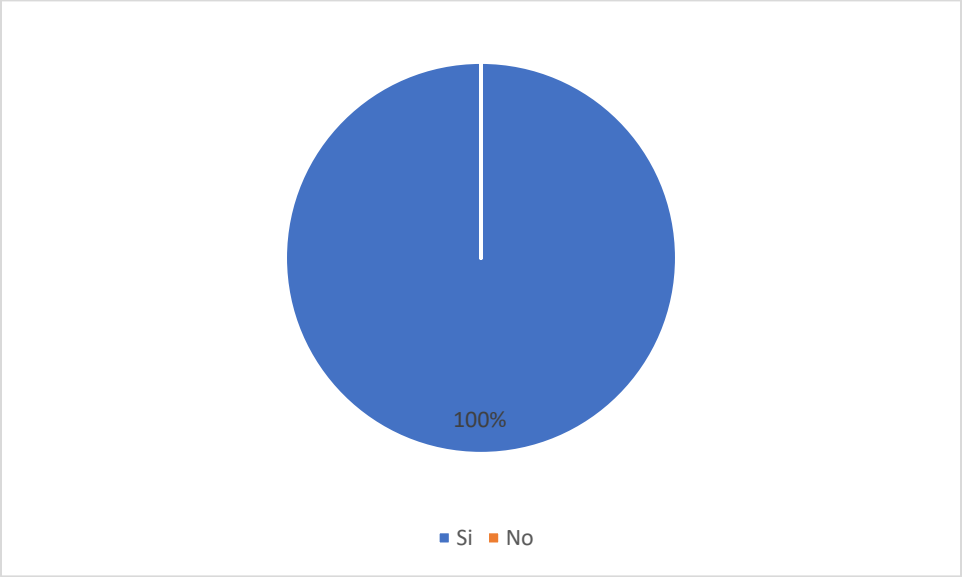


Fuente: elaboración propia.

Consultada la jefatura de la Subárea Gestión de Pagos, indica que si conoce los procesos críticos y menciona: Emitir pagos por bienes y servicios por medio de transferencias electrónicas de fondos o cheques.

2. ¿Cuenta la Subárea Gestión de Pagos con un Plan de Continuidad en TIC?

Gráfico 7-Existencia del Plan de Continuidad Subárea Gestión de Pagos

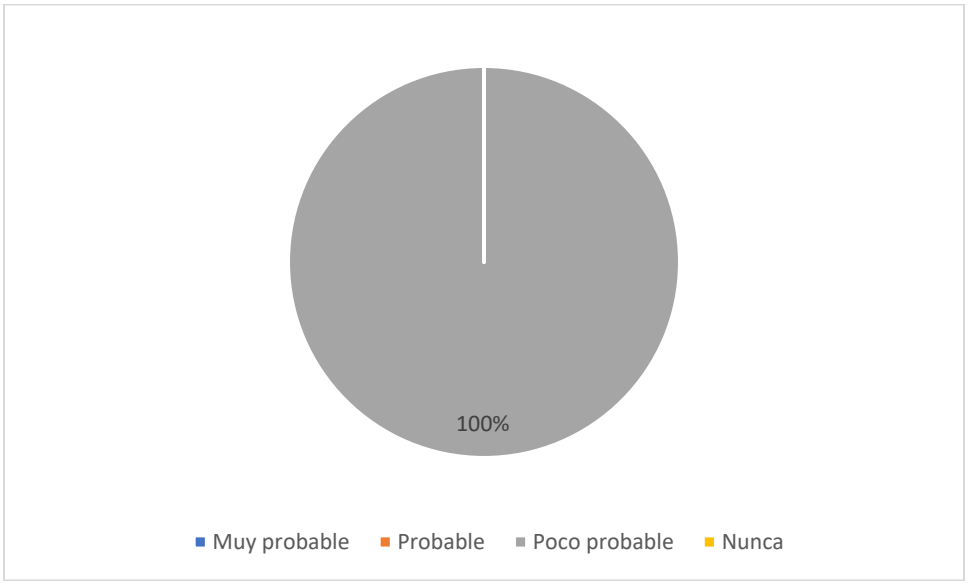


Fuente: elaboración propia.

La jefatura de la Subárea Gestión de Pagos indica que, si cuentan con un Plan de Continuidad en TIC, sin embargo, el mismo se encuentra desactualizado, lo cual no satisface las expectativas en cuanto a darle continuidad a los procesos que se realizan.

3. ¿Cuál es la probabilidad de fallo en los servicios?

Gráfico 8-Probabilidad de fallo en los servicios de la Subárea Gestión de Pagos

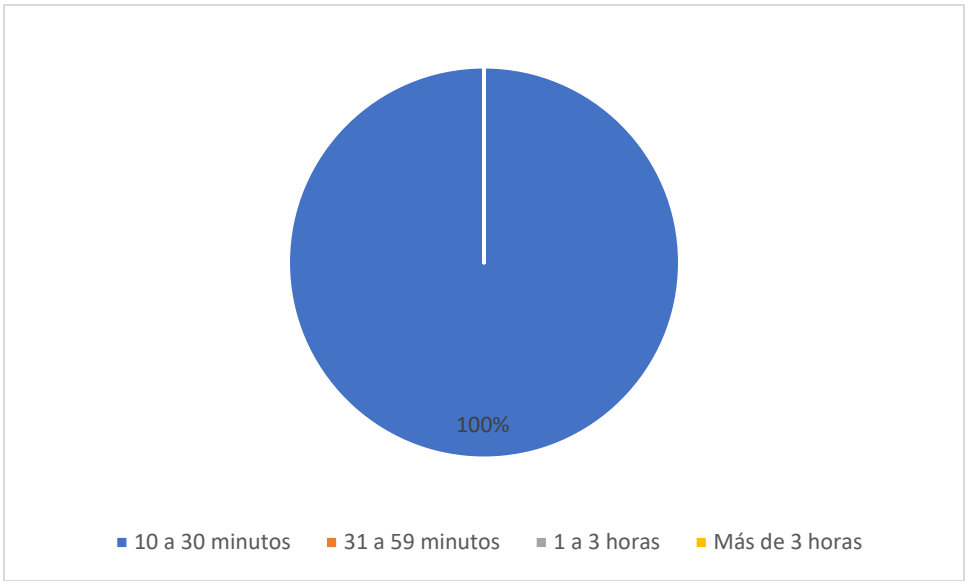


Fuente: elaboración propia.

Cuando se consulta sobre la probabilidad de fallo en los servicios, se indica que es poco probable que se presente. Sin embargo, siempre existe la probabilidad de que se dé un fallo sin tener un plan actualizado.

4. Por lo general, ¿cuánto tiempo se espera al momento de presentarse una interrupción en algún servicio?

Gráfico 9-Tiempo de interrupción en los servicios de la Subárea Gestión de Pagos

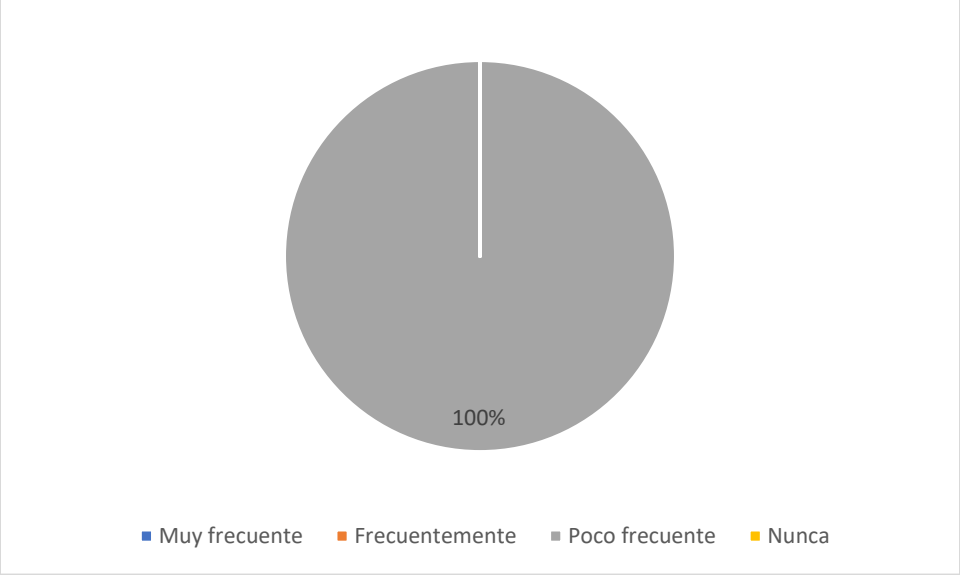


Fuente: elaboración propia.

Ante la consulta del tiempo de espera al presentarse una interrupción en algún servicio, ser indica que de 10 a 30 minutos. Sin embargo, algunos colaboradores indican que el tiempo de interrupción es mayor.

5. ¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?

Gráfico 10-Frecuencia con que se presentan interrupciones en los servicios

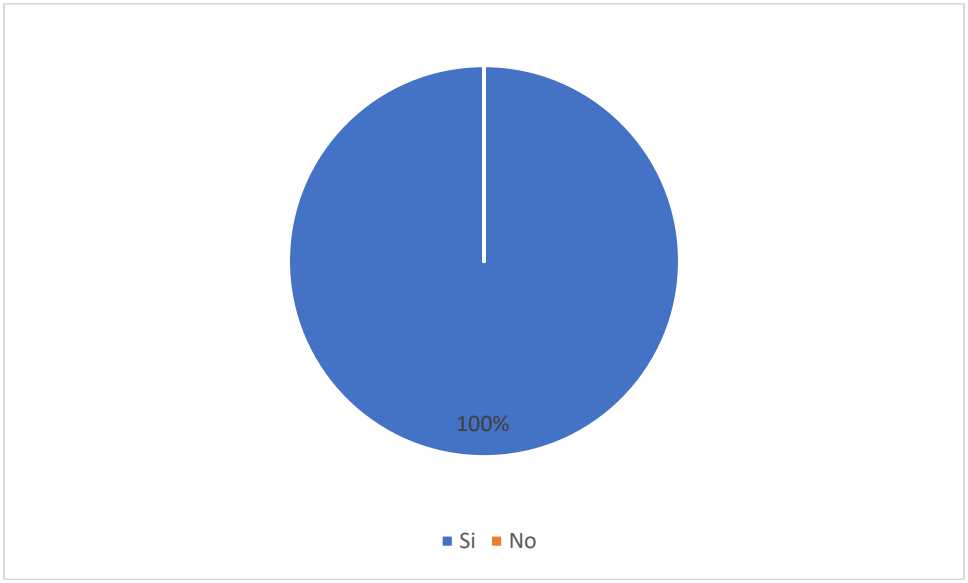


Fuente: elaboración propia.

Se indica que es poco frecuente que se presente interrupción en los servicios que brinda la Subárea Gestión de Pagos, sin embargo, se debe contemplar una interrupción como un riesgo.

6. ¿Conoce el proceder en caso de presentarse una interrupción en los procesos, sea por causas relacionadas con los sistemas o por desastre natural?

Gráfico 11-Conocimiento de procedimientos en caso de interrupción de los procesos

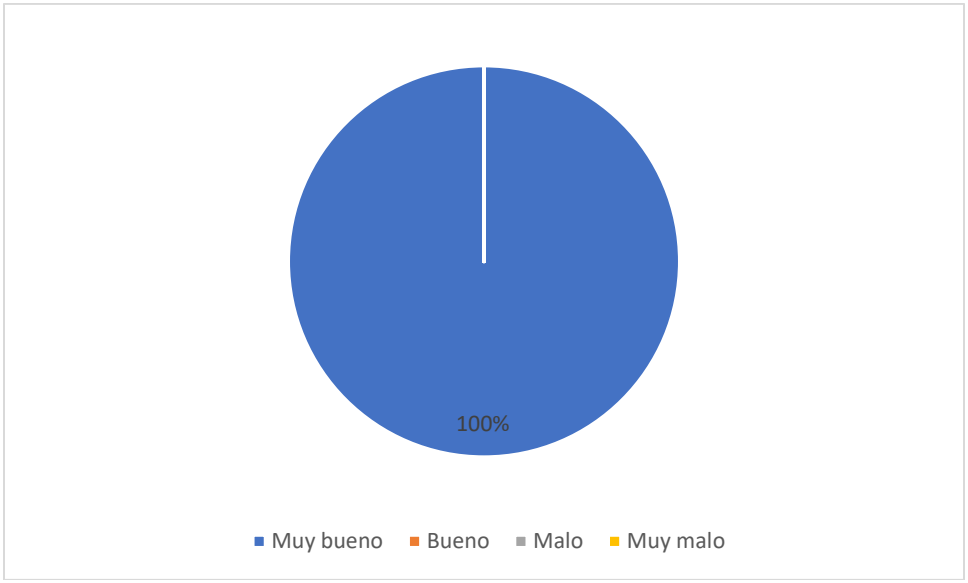


Fuente: elaboración propia.

En este caso se indica conocer el proceder en caso de presentarse una interrupción en los procesos, sin embargo, no está documentada en lugares de fácil acceso a los colaboradores para tomar las medidas necesarias en caso de que se den sucesos de este tipo.

7. ¿Cómo considera la calidad del equipo de cómputo con que cuentan los funcionarios?

Gráfico 12-Calidad del equipo de cómputo de la Subárea Gestión de Pagos

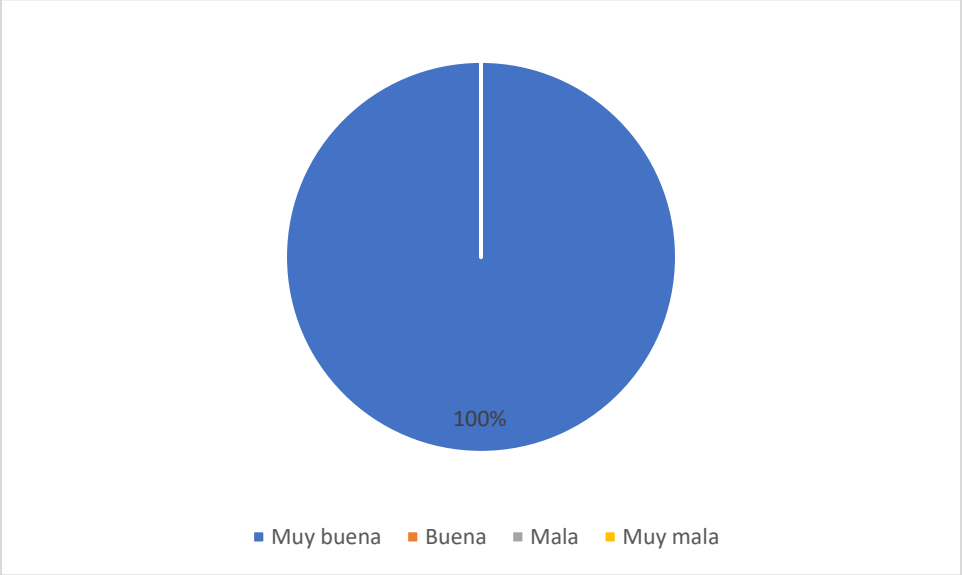


Fuente: elaboración propia.

El equipo de cómputo es la herramienta de trabajo de cada colaborador, se indica que la calidad es muy buena, sin embargo, algunos colaboradores indican que cuentan con el mismo equipo desde hace más de seis años.

8. ¿Qué opina de la velocidad del internet para ejecutar los procesos en los sistemas?

Gráfico 13-Velocidad de internet para ejecutar procesos en los sistemas

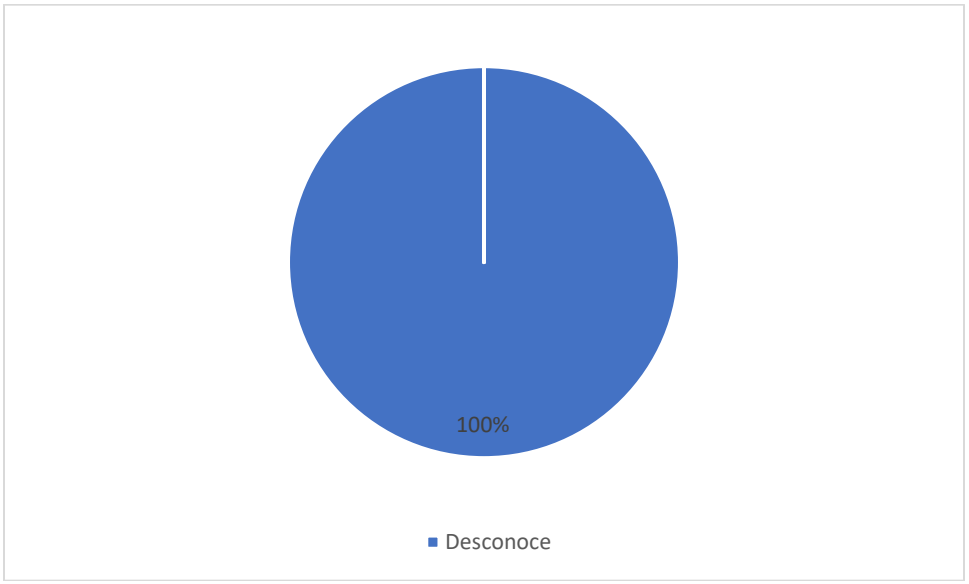


Fuente: elaboración propia.

Aunque la percepción de la velocidad del internet es muy buena, se resalta que algunos colaboradores no piensan de igual forma, ya que inclusive mencionan interrupciones frecuentes.

9. ¿Contemplan algún tipo de seguridad contra ataques cibernéticos?

Gráfico 14-Plan de seguridad contra ataques cibernéticos



Fuente: elaboración propia.

Ante la consulta sobre ataques cibernéticos, desconocen sobre el tema, lo cual, aunque no forma parte de sus funciones, deberían de conocer los riesgos que estos conllevan y que podrían poner en riesgo la continuidad del servicio que se brinda.

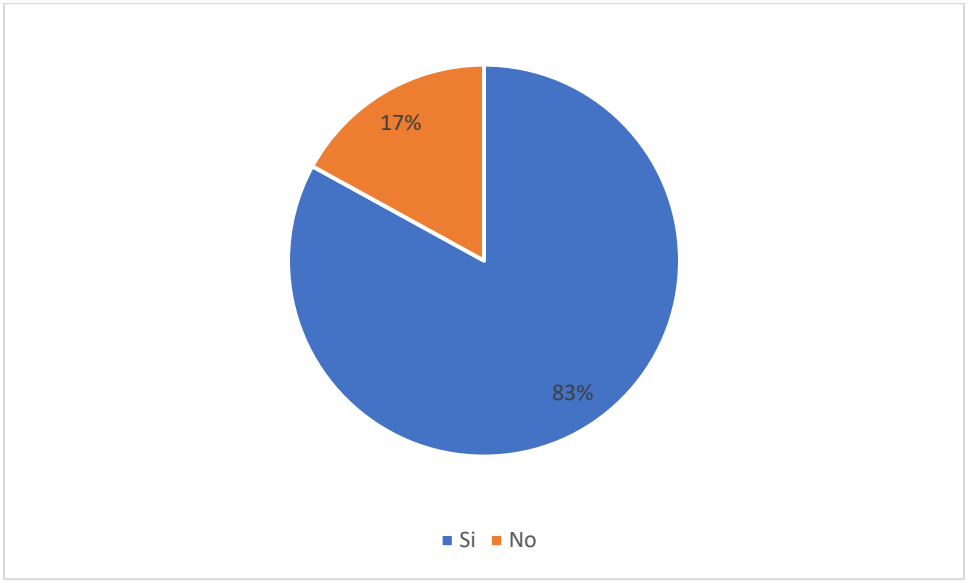
4.4.2 Encuestas

La encuesta se realizó por medio de Microsoft Word, vía correo electrónico a todos los colaboradores de la Subárea Gestión de Pagos, la cual cuenta con un total de 7 funcionarios incluyendo la Jefatura. Se grafican únicamente las preguntas más trascendentales relacionadas al Plan de Continuidad en TIC de la Subárea, todas las preguntas con sus respectivas respuestas se pueden visualizar en el Apéndice.

Pregunta 1: “¿Sabe usted qué es un plan de continuidad en TIC?”.

De los colaboradores encuestados, el 83% indica saber qué es un Plan de Continuidad en TIC y el 17% indica no saber de qué se trata.

Gráfico 15-Conocimiento sobre el Plan de Continuidad en TIC

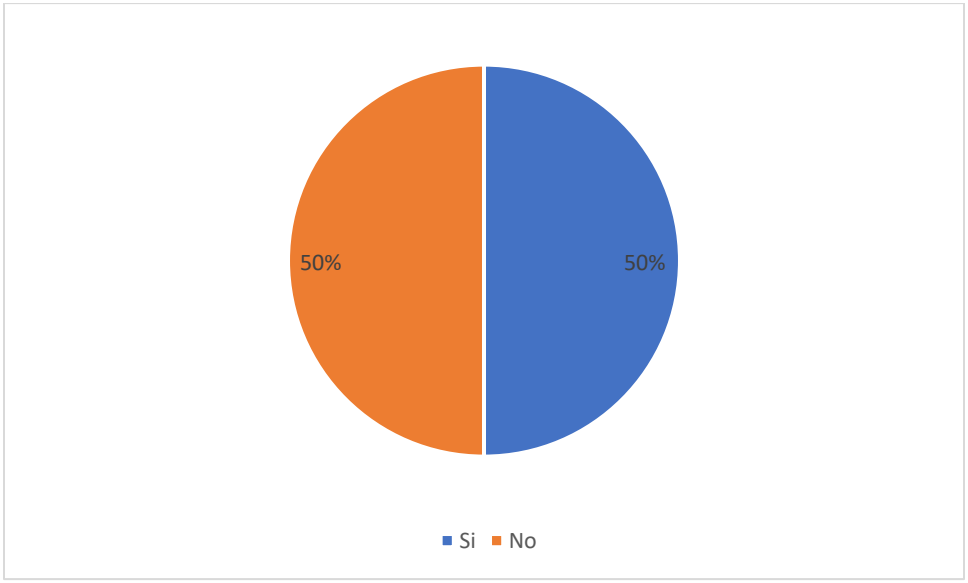


Fuente: elaboración propia.

Pregunta 2: “¿En la Subárea Gestión de Pagos existe un Plan de Continuidad en TIC?”

El 50% de los colaboradores indican que no existe un Plan de Continuidad en TIC y el restante 50% indica que si existe.

Gráfico 16-Plan de Continuidad en TIC existente en la Subárea Gestión de Pagos

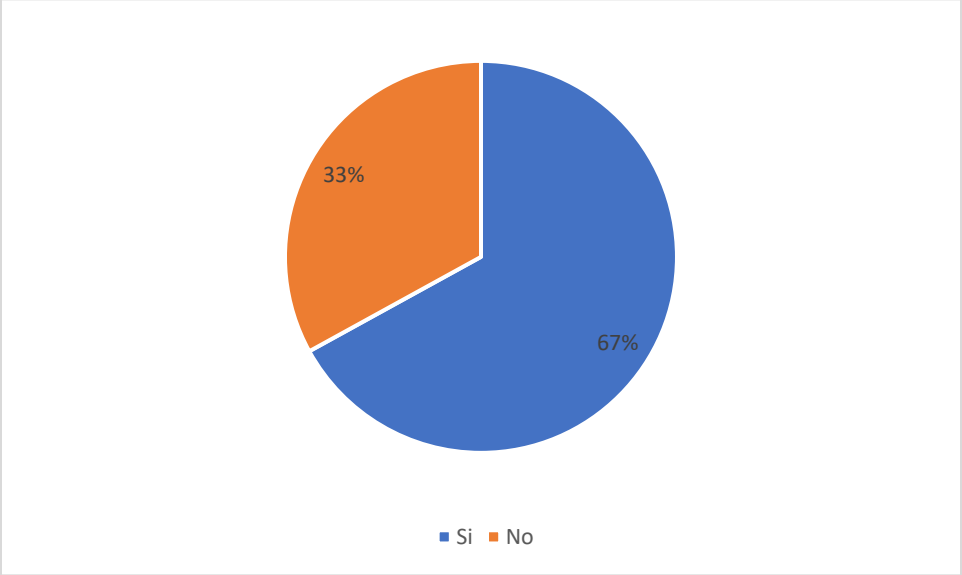


Fuente: elaboración propia.

Pregunta 3: “De acuerdo al proceso que usted realiza, ¿existen respaldos?”

El 33% de los colaboradores indican que no existe ningún tipo de procedimiento de respaldo y el 67% de ellos señala que existen procedimientos de respaldo.

Gráfico 17-Respaldos de la información

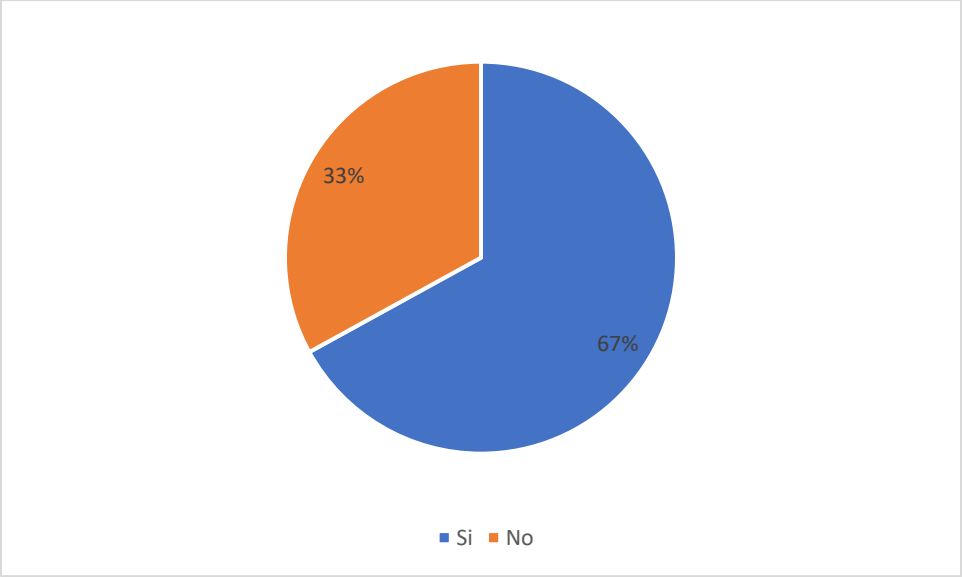


Fuente: elaboración propia.

Pregunta 4: “¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?”

En esta pregunta, el 67% de los colaboradores indican que si saben cuáles son los servicios críticos, sin embargo, no todas las respuestas son claras y concisas, es importante tomar en consideración que algunos funcionarios no están seguros acerca de cuáles son sus funciones más críticas, por lo que se debe trabajar en identificar estos servicios en los funcionarios de la Subárea. El 33% de los colaboradores indican no saber cuáles son los servicios críticos.

Gráfico 18-Servicios críticos de la Subárea Gestión de Pagos



Fuente: elaboración propia.

Pregunta 5: De la pregunta 8, que se puede visualizar completa en el Apéndice, se extrae "Si los procesos sufren una interrupción, ¿qué otras Áreas se pueden afectar?"

Es importante mencionar que de darse una interrupción en los servicios que brinda la Subárea Gestión de Pagos, se ve afectada tanto la Institución como otras entidades, por lo que se evidencia la importancia de mantener la continuidad de los procesos.

A continuación, se detallan las instituciones que se pueden ver afectadas de acuerdo a lo indicado por los colaboradores de la Subárea.

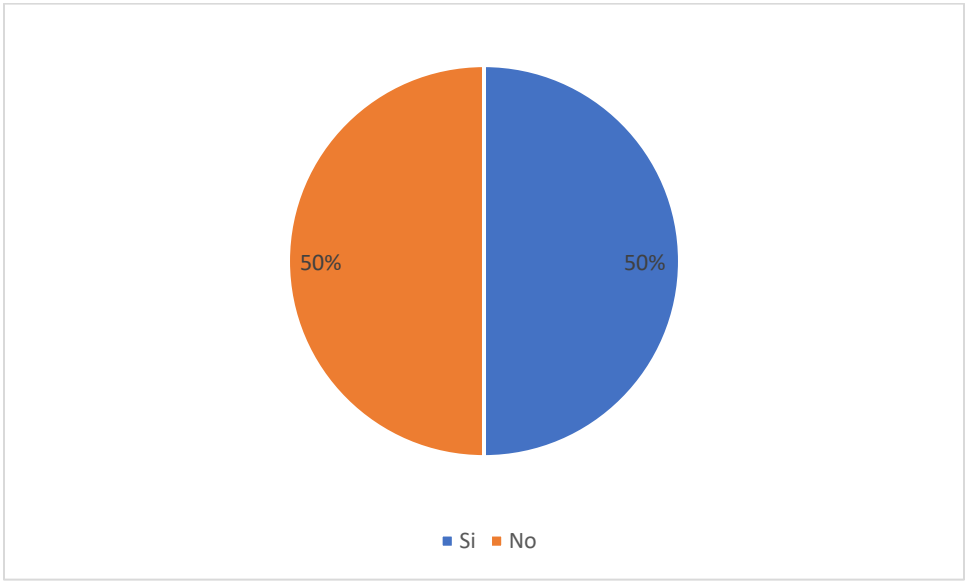
Gráfico 19-Lugares afectados por una interrupción en los servicios de la Subárea Control de Pagos

Fuente: elaboración propia.

Pregunta 6: “¿Sabe qué son controles físicos?”

El 50% de los colaboradores dicen saber que son controles físicos y el 50% indican no saber que son.

Gráfico 20-Conocimiento en controles físicos

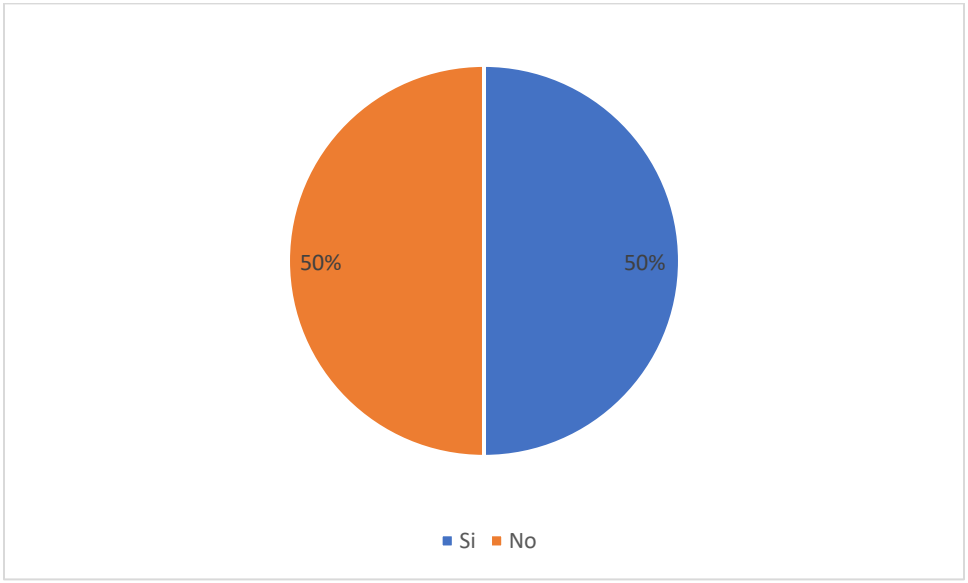


Fuente: elaboración propia.

Pregunta 7: “¿Sabe qué son controles lógicos?”

Con respecto a los controles lógicos, el 50% de los colaboradores dicen saber que son y el 50% indican no saber. Sin embargo, los colaboradores que indican saber de qué se trata no brindan una respuesta que realmente muestre tener el conocimiento de qué se tratan dichos controles.

Gráfico 21-Conocimiento en controles lógicos

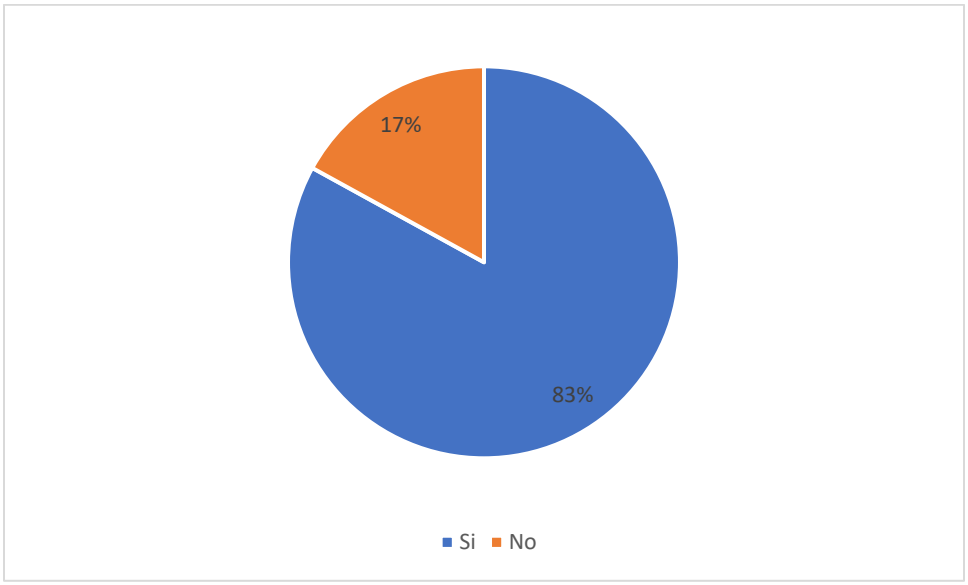


Fuente: elaboración propia.

Pregunta 8: “¿Sabe qué son activos de información?”

En lo que se refiere a activos de información, el 83% de los colaboradores dicen saber que son y el 17% indican no saber de qué se trata. A pesar de que el 83% de los colaboradores indican saber de qué se trata no brindan una respuesta que muestre realmente su conocimiento en el tema.

Gráfico 22-Conocimiento sobre activos de información

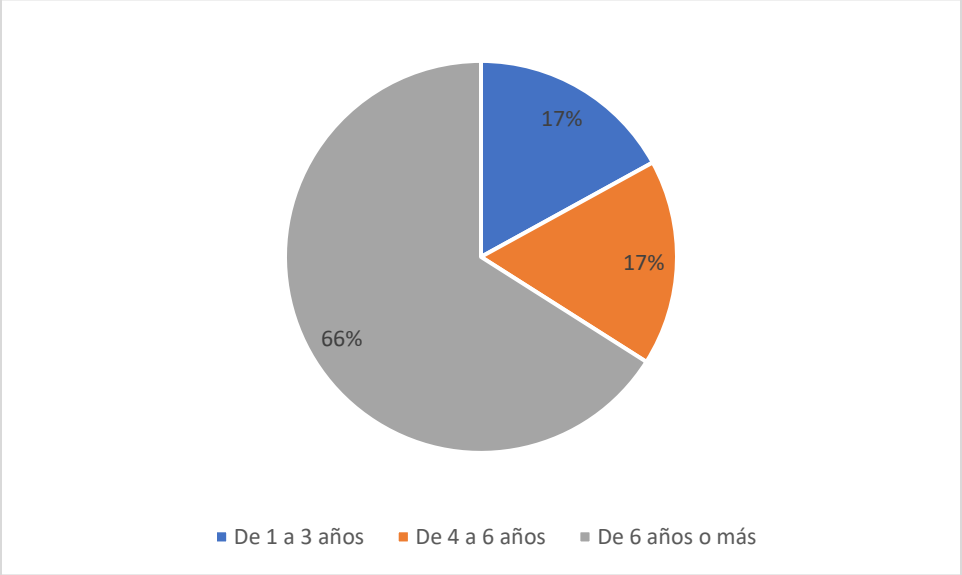


Fuente: elaboración propia.

Pregunta 9: “¿Hace cuánto tiempo utiliza su equipo de cómputo?”

Del total de funcionarios de la Subárea Gestión de Pagos, el 66% de los colaboradores poseen su equipo de cómputo desde hace seis años o más, el 17% tiene su equipo hace aproximadamente 4 o 6 años y el 17% tiene de 1 a 3 años con el mismo equipo.

Gráfico 23-Antigüedad del equipo de cómputo

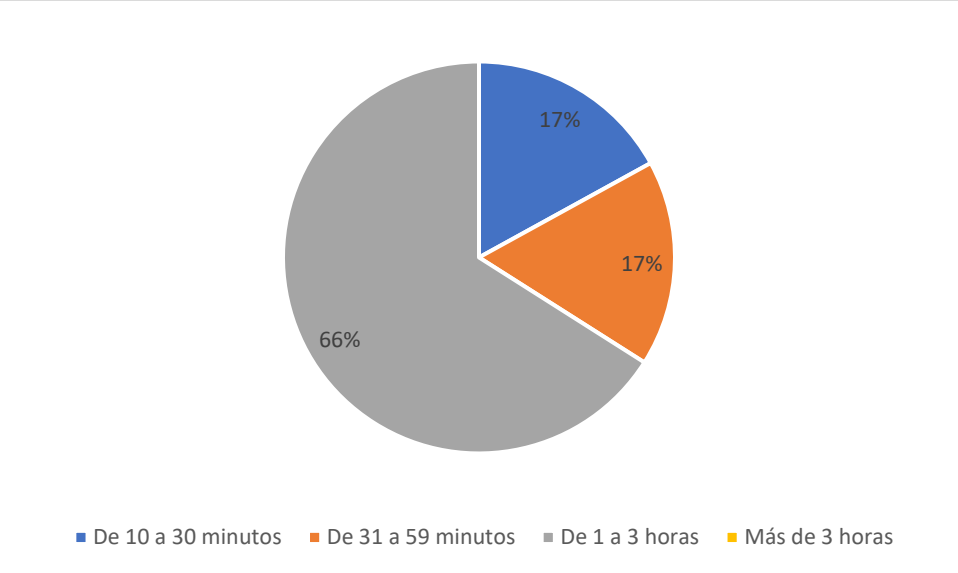


Fuente: elaboración propia.

Pregunta 10: “¿Por lo general cuánto tiempo espera al momento de presentarse una interrupción en alguno de los procesos?”

El tiempo de espera al momento de presentarse una interrupción de acuerdo a lo indicado por los colaboradores de la Subárea Gestión de Pagos es la siguiente: El 66% indica que va de 1 a 3 horas, el 17% indica que va de 31 a 59 minutos, el 17% indica que el tiempo de espera es de 10 a 30 minutos y en ninguno de los casos se indica que sea de más de tres horas.

Gráfico 24-Tiempos de interrupción

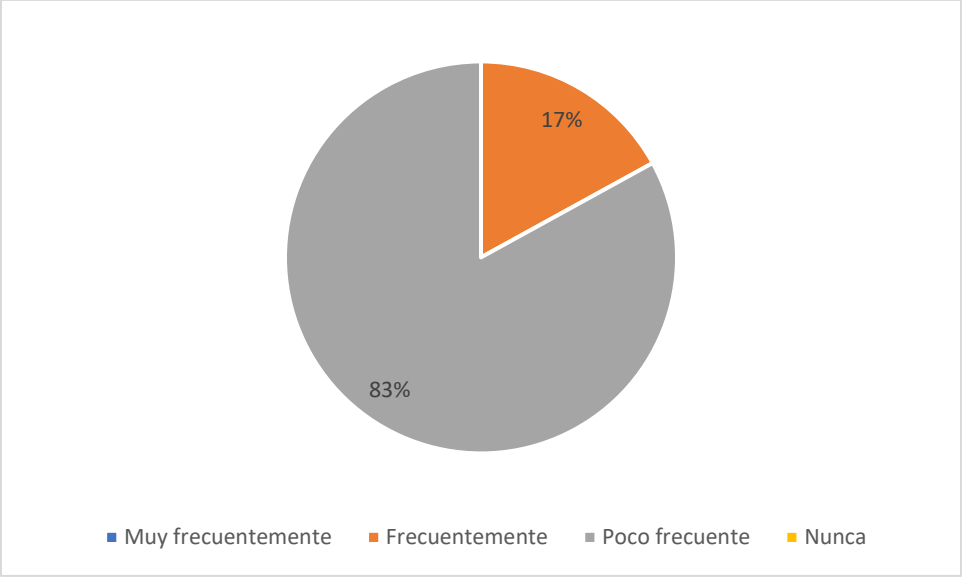


Fuente: elaboración propia.

Pregunta 11: “¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?”

En atención a la frecuencia con que se presentan interrupciones en los servicios que brinda la Subárea Gestión de Pagos, el 83% de los colaboradores indican que se dan con poca frecuencia y el 17% indica que se dan frecuentemente.

Gráfico 25-Frecuencia con que se presentan interrupciones



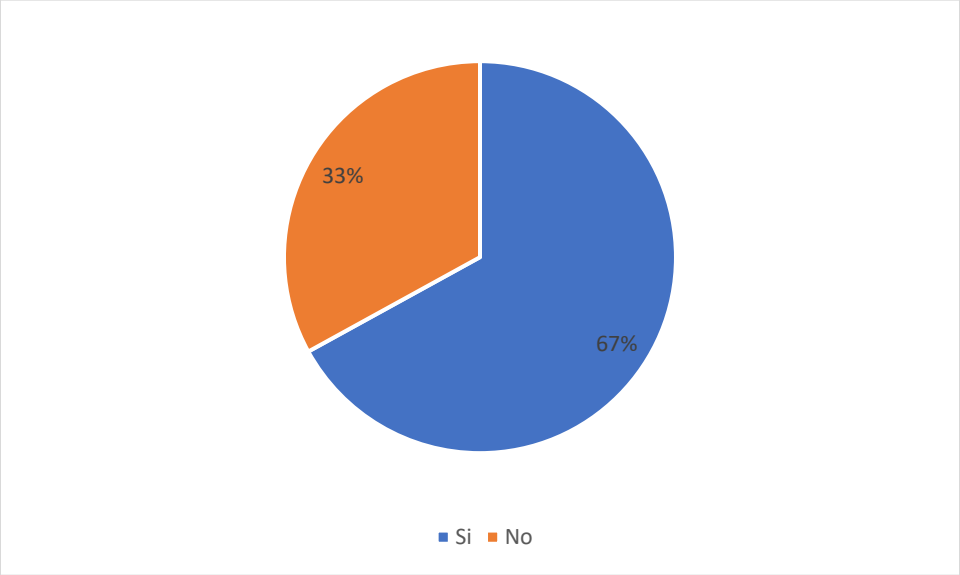
Fuente: elaboración propia.

Pregunta 12: “¿Conoce qué hacer en caso de presentarse una interrupción o daño en su equipo?”

En caso de presentarse una interrupción o daño en el equipo de un colaborador, el 67% indica saber qué hacer y el 33% no sabe qué se hace en estos casos.

A pesar de que el 67% de los funcionarios dicen saber qué hacer, al analizar las respuestas de la encuesta en su totalidad, se identifica que no existe un conocimiento real del actuar en caso de interrupción o daño en el equipo.

Gráfico 26-Acciones en caso de interrupción



Fuente: elaboración propia.

4.5 Brechas y recomendaciones del diagnóstico

Tabla 11-Brechas y recomendaciones

Análisis de la situación actual			
#	**Brecha**	**Estándares**	**Recomendación**
1	En la Subárea Gestión de Pagos, no cuentan con procesos de contingencia definidos para brindar continuidad al servicio.	ISO 22301: 1.Los procesos críticos de la organización, entradas, resultados, la relación con otros procesos de la organización. 2.Desarrollar el plan de continuidad de TIC, diseñado para reducir el impacto de una interrupción.	1.Identificar los procesos críticos del servicio, mediante un diagnóstico de la situación actual para determinar falencias en el proceso y el servicio que brinda la Subárea. 2.Comunicar los planes de contingencia. 3.Desarrollar el Plan de Continuidad en TIC de la Subárea Gestión de pagos.
2	No se visualiza dentro de la Subárea un análisis de riesgos e impacto para brindar la continuidad del servicio.	ISO 22301: 1.Establecer e implementar documentalmente un análisis de valoración de riesgos e impacto del servicio	1.Se recomienda realizar el análisis de impacto, que muestre las amenazas, vulnerabilidades y riesgos.
3	Los colaboradores no tienen conocimiento del Plan de Continuidad en TIC, en caso de interrupción del servicio.	ISO 22301: 1.Todos los colaboradores deben tener conocimiento del Plan de Continuidad en TIC.	1.Comunicar el Plan de Continuidad en TIC a todos los colaboradores de la Subárea Gestión de Pagos. 2.Debe existir un responsable de actualizar periódicamente el Plan de Continuidad en TIC.

4	No se visualiza que los colaboradores realicen el respaldo de la información en caso de dañarse los equipos.	ISO 22301: 1.La Subárea debe implementar el almacenamiento, conservación y recuperación de la información resguardada.	1.Comunicar a los colaboradores de la Subárea Gestión de Pagos, la importancia de respaldar la información en forma periódica. 2.Configurar un servidor para realizar los respaldos de los colaboradores.
5	Se visualiza desconocimiento en materia de vulnerabilidades en los sistemas de la Subárea Gestión de Pagos.	ISO 22301: 1.Se debe contar con revisiones periódicas, pruebas y reportes después de incidentes.	1.Tener conocimiento del firewall que se aplica en la red de la Subárea Gestión de Pagos para tener seguridad de que se bloqueen los accesos no autorizados, es de vital importancia para evitar ataques cibernéticos.
6	Analizar la posibilidad de adquirir equipo de cómputo e impresoras.	ISO 22301: 1.Se debe contar con el equipo idóneo para brindar una continuidad del servicio.	1.Analizar la factibilidad de compra de equipos desactualizados. 2.Analizar la factibilidad de compra de una impresora, en vista de que solo cuentan con una.

Fuente: elaboración propia.

CAPITULO V
PROPUESTA DEL PROYECTO

5. Capítulo V: Propuesta del Proyecto

5.1 Propuesta del proyecto

Se plantea una propuesta como una solución de desarrollo del Plan de Continuidad en TIC, donde se pueda aplicar un modelo a seguir, el presente capítulo se compone de: situación actual, análisis de riesgos y desarrollo de la propuesta.

La situación actual en la Subárea Gestión de Pagos comprende la realidad actual de la unidad de trabajo en donde se evidencian deficiencias en tecnología y sistemas. Así como la capacitación de los funcionarios para manejar contingencias en la interrupción de los procesos.

En el análisis de riesgos se presentan los procesos de mayor vulnerabilidad que requieren planes de acción para enfrentar diferentes situaciones que se presentan en el transcurso de un siniestro.

Es importante identificar los procesos de mayor importancia que tienen riesgos elevados para evitar interrupciones en el servicio y que los pagos que se realicen a los diferentes proveedores no causen quejas ni inconformidades en el servicio, lo que puede generar pagos de intereses adicionales.

Por último, se desarrolla el Plan de Continuidad en TIC de la Subárea Gestión de Pagos, aplicando las mejores prácticas, con base en la situación actual, riesgos, vulnerabilidad y amenazas que se indicaron anteriormente, con esto se busca proponer y generar una mayor confianza en las soluciones integrales en la gestión de incidentes que puedan presentarse en la Subárea y que impiden el curso normal en los procesos.

5.2 Situación actual de Subárea Gestión de Pagos

5.2.1 Análisis PESTEL

Según Chapman, un análisis PESTEL es:

> El análisis PESTEL es una herramienta de gran utilidad para comprender el crecimiento o declive de un mercado, y, en consecuencia, la posición, potencial y dirección de un negocio. Es una herramienta de medición de negocios. PESTEL está compuesto por las iniciales de factores Políticos, Económicos, Sociales y Tecnológicos, utilizados para evaluar el mercado en el que se encuentra un negocio o unidad. (Chapman, 2004, pág. 5)

A continuación, se muestra el Análisis PESTEL de la Subárea Gestión de Pagos:

Tabla 12-Análisis PESTEL

Aspecto	Características	Impacto		
		Alto	Medio	Bajo
Político	-Riesgo país	**X**		
	-Reforma a la Normativa Institucional	**X**		
Económico	-Inestabilidad en la política monetaria (tipo de cambio)	**X**		
	-Cambio en los diferentes impuestos a nivel nacional.	**X**		
Social	-No satisfacer las necesidades de los usuarios.	**X**		

Tecnológico	-Fallos en los sistemas.	**X**		
	-Ataques cibernéticos.	**X**		
Ecológico	-Incendios	**X**		
	-Terremotos	**X**		
Legal	-Demandas a la Institución por gestiones de pago mal realizadas.	**X**		

Fuente: Elaboración propia

5.2.2 Análisis FODA de la Subárea Gestión de Pagos

Con el objetivo de identificar el estado de la situación actual de la Subárea Gestión de Pagos, se procede a realizar un análisis FODA, con el análisis no solo se trata de identificar las fortalezas, debilidades, oportunidades y amenazas, sino cómo generar algún tipo de valor agregado para la Subárea.

De acuerdo con lo indicado por Chapman:

> El análisis FODA es una evaluación subjetiva de datos organizados en el formato FODA, que los coloca en un orden lógico que ayuda a comprender, presentar, discutir y tomar decisiones. Puede ser utilizado en cualquier tipo de toma de decisiones, ya que la plantilla estimula a pensar pro-activamente, en lugar de las comunes reacciones instintivas. (Chapman, 2004, pág. 1)

A continuación, se presenta el Análisis FODA realizado en la Subárea Gestión de Pagos:

Tabla 13-Análisis FODA de la Subárea Gestión de Pagos

FORTALEZAS	DEBILIDADES
Garantiza el pago oportuno de los diferentes conceptos (facturas, salarios, pensiones, cesantías, etc.) una vez recibida la documentación	Atrasos en la remisión de información para la gestión de pagos.
Funcionario con amplia experiencia en los diferentes puestos y comprometidos con las metas de la Subárea.	Poco mantenimiento a los equipos necesarios para llevar a cabo las labores podría provocar un mal funcionamiento y retraso en los procesos de pagos.

OPORTUNIDADES	AMENAZAS
Promueve que las declaraciones informativas de impuestos, así como el pago de las obligaciones tributarias al Ministerio de Hacienda, se realicen dentro del plazo establecido por Ley.	Atrasos en los pagos por fallos en los sistemas de pagos (SIPA, SINPE CCSS)
Garantiza los pagos por cheque y traslado de los mismos al Banco de Costa Rica por reintegros de pensión alimenticia, pago de embargos, derechos laborales en forma oportuna. Además, prevé realizar los pagos a las diferentes organizaciones sindicales, colegios, cooperativas, se realicen antes que finalice el mes calendario a la aplicación de la deducción a los empleados por su afiliación a estas organizaciones.	Fallos en los sistemas de Hacienda, así como falta de liquidez en las cuentas bancarias, ocasionado un atraso en la presentación y pago de los impuestos, que provocaría sanciones económicas a la Institución.
Traslado de títulos valores en el menor tiempo.	Peligro (robo, extravío) de traslado de los títulos valores (cheques) de la Subárea al Banco de Costa Rica, por medio de mensajería.

Fuente: elaboración propia.

Una vez realizado el análisis FODA, se debe prestar especial atención a las oportunidades, para generar por medio de estas estrategias importantes para la Subárea. Además, por medio de las amenazas se puede estudiar cómo mitigar eventos que perjudiquen los procesos cotidianos.

Al detectar las debilidades, es importante mencionar que estas se pueden convertir en fortalezas, definiendo buenas estrategias que las contrarresten.

5.2.3 Análisis CAME

Una vez elaborada la matriz FODA con el análisis interno, se definen las estrategias de acción mediante el análisis CAME, que de acuerdo con Samanes lo define como:

> El método complementario que permite en paralelo al diagnóstico, la formulación de propuestas para superar los factores limitantes y poner en valor los factores positivos. Es pues una técnica complementaria y suplementaria a la del FODA, que da pautas para actuar sobre los aspectos hallados en el diagnóstico de situación. Consiste en valorar cada una de las deficiencias, amenazas, fortalezas y oportunidades, seleccionadas previamente en el FODA, y formular estrategias y acciones asociadas para: - Corregir las Deficiencias (C-D), con el fin de superar o disminuir las deficiencias detectadas. - Afrontar las Amenazas (A-A), enfocadas a eliminar las amenazas o minimizar su impacto. - Mantener las Fortalezas (M-F), para conservar lo que hace fuerte a IFPE y le distingue del - Explotar las Oportunidades (E-O), encaminada a explorar oportunidades y convertirlas en fortalezas. Posteriormente las estrategias de acción se jerarquizan en función de las prioridades marcadas en el FODA. Han de ser realistas, consistentes y cuantificables. (Samanes, 2021, pág. 17)

Tabla 14-Análisis CAME de la Subárea Gestión de Pagos

DEBILIDADES	**Corregir**
Atrasos en la remisión de información para la gestión de pagos.	Realizar planes de recordatorio a las unidades que remiten información necesaria para la adecuada gestión de los pagos a nivel institucional.
Poco mantenimiento a los equipos necesarios para llevar a cabo las labores podría provocar un mal funcionamiento y retraso en los procesos de pagos.	Implementar una cultura de uso adecuado de los equipos, brindándoles limpieza y verificando que las partes se encuentren en óptimas condiciones.
AMENAZAS	**Afrontar**
Atrasos en los pagos por fallos en los sistemas de pagos (SIPA, SINPE CCSS)	Contar con el plan de contingencia en caso de presentarse fallo en alguno de los sistemas de pagos.
Fallos en los sistemas de Hacienda, así como falta de liquidez en las cuentas bancarias, ocasionado un atraso en la presentación y pago de los impuestos, que provocaría sanciones económicas a la Institución.	Coordinación con las entidades de manera que exista una comunicación efectiva en todo momento para subsanar cualquier inconveniente.
Peligro (robo, extravío) de traslado de los títulos valores (cheques) de la Subárea al Banco de Costa Rica, por medio de mensajería.	Establecer las estrategias necesarias para evitar que se ponga en riesgo el traslado de títulos valores o cualquier otro documento de importancia.
FORTALEZAS	**Mantener**
Garantiza el pago oportuno de los diferentes conceptos (facturas, salarios, pensiones, cesantías, etc) una vez recibida la documentación	Mantener los procesos actuales, incorporando la mejora continua.
Funcionario con amplia experiencia en los diferentes puestos y comprometidos con las metas de la Subárea.	Capacitación constante para que los conocimientos sean transmitidos a nuevos colaboradores que se integran al equipo de trabajo.
OPORTUNIDADES	**Explotar**
Promueve que las declaraciones informativas de impuestos, así como el pago de las obligaciones tributarias al Ministerio de Hacienda, se realicen dentro del plazo establecido por Ley.	Llevar mecanismos de control para que los pagos se realicen de acuerdo con un cronograma definido desde el inicio del año.
Garantiza los pagos por cheque y traslado de los mismos al Banco de Costa Rica por reintegros de pensión	Llevar mecanismos para que los pagos por cheque se realicen de forma oportuna.

alimenticia, pago de embargos, derechos laborales en forma oportuna. Además, prevé realizar los pagos a las diferentes organizaciones sindicales, colegios, cooperativas, se realicen antes que finalice el mes calendario a la aplicación de la deducción a los empleados por su afiliación a estas organizaciones.	

Fuente: Elaboración propia.

5.2.4 Análisis de riesgos para la Subárea Gestión de Pagos según ISO 27001

El análisis de riesgo valora la posibilidad de que se produzca un daño que afecte a los activos de toda institución. En un Plan de Continuidad en TIC, el análisis de riesgos debe valorar los elementos que soportan a los procesos críticos y los diversos riesgos que pueden afectar dichos procesos, tanto eventos sistemáticos como naturales. Al valorar los riesgos, se logra establecer la probabilidad de que estos ocurran y las consecuencias asociadas al evento, de esta forma se clasifican, con el propósito de establecer el nivel de criticidad y las acciones que se deben implementar para su mitigación.

En la siguiente tabla se muestra una comparación entre vulnerabilidades, amenazas y riesgos de seguridad más frecuentes según la norma ISO 27001 / 27002 que más adelante se comprueban mediante pruebas documentales.

Tabla 15-Vulnerabilidades, amenazas y riesgos de seguridad según ISO 27001 / 27002

	Vulnerabilidades	Amenazas	Riesgo potencial
Hardware	Equipo de cómputo	Condiciones físicas y ambientales (limpieza, humedad, temperatura)	Fallo y obsolescencia
Software	Desarrollo local de aplicaciones (metodologías/ estándares);	Cambios y configuración en aplicaciones	Trascendencia de los sistemas incluidos en el estudio
Seguridad física	Soporte técnico de los equipos utilizados.	Poco mantenimiento preventivo y correctivo de	Fallo de los equipos

		los equipos de comunicación	
Seguridad lógica	Sistemas	Ataque cibernético	Pérdida de datos
Red de comunicaciones	Soporte técnico de los equipos utilizados;	Poco mantenimiento preventivo y correctivo de los equipos de comunicación	
Personal	Los colaboradores	Enfermedades y accidentes laborales	Ausencia de los colaboradores

Escala para cuantificar los activos informáticos:

Tabla 16-Cuantificación de activos según ISO 27002

NIVEL	Muy alto	Alto	Medio	Muy bajo
VALOR	Monto > ₡10.000.000	₡10.000.000 < Monto > ₡5.000.000	₡5.000.000 < Monto > ₡1.000.000	₡1.000.000 < Monto > ₡500.000

Fuente: Elaboración propia

Una vez evaluados los criterios se procede a la valoración de riesgos en la escala de probabilidad e impacto según norma ISO 27002

Tabla 17-Valoración de activos según ISO 27002

DAÑO	**VALOR**
Daño catastrófico	10
Daño grave	7-9
Daño moderado	4-6
Daño leve	1-3
Daño irrelevante	0

Fuente: Elaboración propia

Tabla 18-Criterios de evaluación de seguridad de la información

Tipo de activo	Nombre del activo	Confidencialidad / Daño	Integridad / perjuicio	Disponibilidad / perjuicio	Autenticidad / Perjuicio	Trazabilidad / Daño
Hardware	Equipo Internet	-	-	-	-	-
Software	Licencias	-	10 / ALTO	-	-	-
Activo de información	Proveedores Instituciones	8 / ALTO	8 / ALTO	5 / BAJO	7 / MEDIO	-
Funcionarios	Usuarios de sistemas	9 / ALTO	9 / ALTO	8 / ALTO	8 / ALTO	-
Instalaciones eléctricas	Normas establecidas	-	8 / ALTO	8 / ALTO	-	8 / ALTO

Fuente: Elaboración propia

Una vez evaluados los criterios, lo siguiente es la valoración de riesgos en la escala de probabilidades e impacto según la norma 27002.

Tabla 19-Escala de valoración de ocurrencia según ISO 27002

Frecuencia	Simbología	Ocurrencia
Frecuencia muy baja	MB	Una vez cada seis meses
Frecuencia baja	B	Una vez cada dos meses
Frecuencia media	M	Una vez cada mes
Frecuencia alta	A	Una vez a la semana
Frecuencia muy alta	MA	Una o más veces a la semana

Fuente: Elaboración propia

Según los resultados obtenidos en la valoración se evidencia que los problemas de seguridad en la Subárea Gestión de Pagos se relacionan con el desconocimiento sobre la aplicación de normas, seguridad informática, recursos disponibles, lo que puede comprometer la imagen de la Subárea. Las posibles causas se asocian a poco conocimiento en el tema de seguridad de la información, no hay responsables en cada uno de los procesos, al no conocer, existe falta de cumplimiento de políticas y procedimientos internos de seguridad y de esto depende la protección de los activos informáticos frente a las amenazas y riesgos que se presenten.

A continuación, se describen los pasos a realizar para la identificación general y el análisis de riesgos para la Subárea Gestión de Pagos.

1. Se toma la clasificación de los riesgos presentes en la Subárea.

Figura 16-Clasificación de riesgos

Fuente: Elaboración propia

2. Una vez que se realiza la clasificación de los riesgos, se debe determinar para cada uno de estos el impacto que puede tener si se materializa, este impacto se obtiene por medio de la entrevista y encuestas realizadas a los colaboradores de la Subárea Gestión de Pagos.

Tabla 20-Descripción de los riesgos, fuentes y áreas de impacto

Riesgos	Fuentes	Áreas de Impacto
Recurso Humano	Falta de capacitación Accidentes laborales Incapacidades	Servicio a proveedores Atraso general en procesos y atención a usuarios internos y externos
Interrupción eléctrica	Compañía de servicios públicos	Sistemas y aplicaciones Servicios a proveedores
Incendio	Cableado eléctrico	Sistemas y aplicaciones Servicios a proveedores Equipo
Terremoto	Región sísmica	Sistemas y aplicaciones Servicios a proveedores Equipo

Fuente: Elaboración propia.

Por las funciones que realiza la Subárea Gestión de Pagos, los riesgos están orientados a los proveedores y sistemas.

3. Al establecer los riesgos y las fuentes generadoras de los mismos, seguidamente se realizar el análisis, tomando en cuenta el impacto que tendrían si llegan a materializarse y el impacto que produciría.

Figura 17-Califiación del Impacto

Impacto	Abreviatura	Valor	Descripción
Alto	A	3	Perdida Financiera Mayor porque existen perjuicios extensivos
Medio	M	2	Perdida Financiera media porque se le contuvo a tiempo requiere de un tratamiento especifico
Bajo	B	1	Sin perjuicio, perdida financiera relativamente baja

Fuente: Dirección Tecnologías de Información y Comunicaciones. Caja Costarricense de Seguro Social

Figura 18-Calificación de la probabilidad

Probabilidad	Abreviatura	Valor	Descripción
Alto	A	3	Se espera que el evento ocurra en la mayoría de los casos
Medio	M	2	Puede ocurrir en algún momento bajo ciertas circunstancias
Bajo	B	1	Puede ocurrir el evento solamente en circunstancias excepcionales.

Fuente: Dirección Tecnologías de Información y Comunicaciones. Caja Costarricense de Seguro Social

4. Para la determinación del nivel de riesgo se utiliza el impacto y versus la probabilidad.

Figura 19-Nivel de riesgo

Probabilidad	Valor			
Alta	3	3- Zona de Riesgo Medio - Evitar Riesgo	6- Zona de Riesgo Alta - Reducir el Riesgo - Evitar el Riesgo - Compartir o transferir	9- Zona de Riesgo Alta - Reducir el Riesgo - Evitar el Riesgo - Compartir o transferir
Media	2	2- Zona de riesgo baja - Asumir el Riesgo - Reducir el riesgo	4- Zona de riesgo Medio - Reducir Evitar Compartir o transferir el riesgo	6- Zona de riesgo alta- Reducir Evitar Compartir o transferir el riesgo
Baja	1	1- Zona de riesgo Baja - Asumir el Riesgo	2- Zona de riesgo Baja - Reducir - Compartir o transferir el riesgo	3 Zona de riesgo Medio - Reducir compartir o transferir el riesgo
	Valor	1	2	3
	Impacto	**Bajo**	**Medio**	**Alto**

Fuente: Dirección Tecnologías de Información y Comunicaciones. Caja Costarricense de Seguro Social

La tabla anterior se interpreta de la siguiente forma:

a) Al conocer la calificación Probabilidad del Riesgo (alta, media o baja), se ubica en el campo correspondiente en el margen izquierdo (probabilidad).

b) Igualmente para el Impacto del Riesgo, se ubica en la parte inferior del cuadro (impacto), de acuerdo con la calificación dada (bajo, medio o alto).

c) Luego en el punto donde se interceptan las respectivas calificaciones de la probabilidad y el impacto del riesgo (cuadros en color verde, amarillo o rojo), ese es el grado de Exposición del Riesgo. (CCSS, 2013, pág. 39)

5. Con las matrices anteriores, se realiza el análisis de riesgos y de este análisis, se determina cuál será la prioridad para mitigar o si entran en lo aceptable. De esta forma se tomarán en cuenta los procesos que muestren un nivel Alto de ocurrencia.

   Anteriormente se mencionaron los riesgos a nivel global, a partir de la siguiente matriz se tomarán en cuenta los riesgos detallados uno a uno, que giran a través de los ya mencionados.

Tabla 21-Matriz Análisis de riesgos

Riesgo	Fuente	Impacto	Probabilidad	Resultado
Interrupción de servicio crítico	Falta de mantenimiento, error humano.	Alto	Baja	Medio
Errores Humanos	Falta de capacitación	Medio	Baja	Bajo
Incumplimiento de normas	Legislaciones	Medio	Medio	Medio
Incendios	Cableado eléctrico	Alto	Baja	Bajo
Sismos	Región sísmica	Alto	Baja	Medio
Robos	Mala intención de las personas	Alto	Baja	Medio
Daños al equipo	Manipulación incorrecta	Alto	Baja	Medio
Pérdidas Humanas	Accidentes, pandemias, enfermedades terminales	Alto	Baja	Medio
Accidentes laborales y enfermedades	Desacato a procedimientos de seguridad	Medio	Baja	Bajo

Ausencia de personal	Incapacidades	Medio	Baja	Bajo
Incumplimiento de legislaciones	Falta de capacitación	Medio	Baja	Bajo
Demandas externas	Proveedores	Alto	Baja	Medio
Mala calidad	Fallo en especificaciones.	Medio	Baja	Bajo
Especificaciones erróneas	Errores humanos	Medio	Baja	Bajo

Fuente: Elaboración propia.

Se pueden visualizar los riesgos presentes en la Subárea Gestión de Pagos y las fuentes que pueden hacer que se materialice el riesgo, además se muestran los resultados de impacto y probabilidad, y de esta forma se clasifica el riesgo, mostrando la magnitud que puede tener para la Subárea.

5.2.5 Riesgos presentes en los procesos

Una interrupción de los procesos de TI afecta grandemente las operaciones de cualquier departamento, provocando daños irreparables, por esta razón se debe tener un tiempo máximo establecido para la no ejecución de los procesos. Tomando en cuenta el diagnóstico se evidencian los riesgos que tiene la Subárea Gestión de Pagos con respecto a la continuidad de los servicios, por lo que se tomando en cuenta la ISO 22301; se realiza la siguiente lista de riesgos enumerados y de estos se desprenderá el mapa de calor:

1. Corte de energía prolongado.
2. Caída de los sistemas automatizados.
3. Suspensión de servicios de proveedor de internet.
4. Incendio o sismo en el edificio.
5. Robo de información
6. Pérdida de información por ataque cibernético.
7. Manipulación sensible sin autorización.

8. Falla en bases de datos.
9. Vencimiento de licencias de software.
10. Personal no capacitado para sus funciones.
11. Caídas de los equipos informáticos o medios de comunicación (dispositivos de red, servidores, UPS).
12. Pérdida de credibilidad en los servicios de TI debido a que no se han definido los servicios críticos de TI.
13. Pérdidas económicas importantes debido a la no realización de mantenimientos preventivos.

5.2.5.1 Valoración de los riesgos

Los riesgos se evalúan de acuerdo con escalas y de acuerdo con el impacto, se realiza un cálculo para obtener el nivel del riesgo inherente, el cual consiste en una multiplicación entre ambos resultados:

(Valor del impacto * Valor de la probabilidad = Valor del riesgo)

Tabla 22-Valoración del riesgo

#	Riesgo	Valor Impacto	Valor Probabilidad	Valor del Riesgo	Probabilidad	Impacto	Nivel del Riesgo
1	Corte de energía prolongado	3	1	3	A	B	MEDIO
2	Caída de los sistemas automatizados	3	1	3	A	M	MEDIO
3	Suspensión de servicios de	3	1	3	A	B	MEDIO

	proveedor de internet.						
4	Incendio o sismo en el edificio	3	1	3	M	B	MEDIO
5	Robo de información	3	2	6	A	M	ALTO
6	Pérdida de información por ataque cibernético	3	2	6	A	A	ALTO
7	Manipulación sensible sin autorización	3	1	3	A	M	MEDIO
8	Falla en bases de datos	3	1	3	M	M	MEDIO
9	Vencimiento de licencias de software	2	1	2	M	A	BAJO
10	Personal no capacitado para sus funciones	2	2	2	M	M	BAJO
11	Caídas de los equipos informáticos o medios de comunicación (dispositivos de red, servidores, UPS).	3	2	6	A	A	ALTO
12	Pérdida de credibilidad en los servicios de TI debido a que no se han definido los	3	1	3	A	A	MEDIO

	servicios críticos						
13	Pérdidas económicas debido a la no realización de mantenimientos preventivos	2	1	2	B	A	BAJO
		Cálculo			Valoración		

Fuente: Elaboración propia.

5.2.5.2 Mapa de calor

De acuerdo con la valoración de riesgos anterior, se obtienen los siguientes resultados:

1. Valor de nivel del riesgo = 3
2. Valor de nivel del riesgo = 3
3. Valor de nivel del riesgo = 3
4. Valor de nivel del riesgo = 3
5. Valor de nivel del riesgo = 6
6. Valor de nivel del riesgo = 6
7. Valor de nivel del riesgo = 3
8. Valor de nivel del riesgo = 3
9. Valor de nivel del riesgo = 2
10. Valor de nivel del riesgo = 2
11. Valor de nivel del riesgo = 6
12. Valor de nivel del riesgo = 3
13. Valor de nivel del riesgo = 2

A continuación, se muestra el mapa de calor, de acuerdo con la numeración dada anteriormente, los riesgos se encuentran ordenados ascendentemente según su impacto en la Subárea, con el propósito de obtener un panorama más claro y sencillo acerca de los riesgos más críticos.

Tabla 23-Mapa de calor

Matriz de exposición			**Impacto**		
Mapa de calor			**Alto**	**Medio**	**Bajo**
Probabilidad	**Estimación**	**Valor**	**3**	**2**	**1**
Alta	>60% y <100%	**3**			
Media	>30% y <60%	**2**	5, 6, 11	10	
Baja	>0% y <30%	**1**	1, 2, 3, 4, 7, 8, 12	9, 13	

Fuente: Elaboración propia.

Tabla 24-Riesgos de forma ascendente

#	Riesgo	Valor resultante	Nivel de riesgo inherente
5	Robo de información	6	ALTO
6	Pérdida de información por ataque cibernético	6	ALTO
11	Caídas de los equipos informáticos o medios de comunicación (dispositivos de red, servidores, UPS).	6	ALTO
1	Corte de energía prolongado	3	MEDIO
2	Caída de los sistemas automatizados	3	MEDIO
3	Suspensión de servicios de proveedor de internet.	3	MEDIO
4	Incendio o sismo en el edificio	3	MEDIO
7	Manipulación sensible sin autorización	3	MEDIO
8	Falla en bases de datos	3	MEDIO

12	Pérdida de credibilidad en los servicios de TI debido a que no se han definido los servicios críticos	3	MEDIO
9	Vencimiento de licencias de software	2	BAJO
10	Personal no capacitado para sus funciones	2	BAJO
13	Pérdidas económicas debido a la no realización de mantenimientos preventivos	2	BAJO

Fuente: Elaboración propia.

5.3 Servicios críticos según norma ISO 22301

Este apartado busca determinar cuáles son los servicios críticos de la Subárea, que de llegar a verse interrumpidos por alguna circunstancia provocaría la interrupción de los procesos y con esto se afectaría la continuidad.

5.3.1. Procesos críticos de la Subárea Gestión de Pagos

De acuerdo con las encuestas realizadas a todos los funcionarios de la Subárea Gestión de Pagos se logra obtener información referente a los procesos que realiza la Subárea, los cuales se detallan a continuación:

Tabla 25-Procesos críticos de la Subárea Gestión de Pagos

Procesos
1. Pago a proveedores locales y extranjeros, empleados, pensionados y otros conceptos, por medio de SINPE del BCCR, Internet Banking BNCR, BCR Comercial y por vía cheque.
2. Presentaciones de declaraciones y pagos de impuestos al Ministerio de Hacienda por BCR Comercial.
3. Pago a Organizaciones Sindicales, Colegios, Universidades, Cooperativa y entidades financieras por deducciones a empleados CCSS por SINPE
4. Pagos por caja única de Hacienda de Bienestar Social.

5. Pagos a diferentes dependencias de la CCSS como el FRIP-FRAP-FOCARE-FRE por medio de Internet Banking BNCR.
6. Pago de préstamos hipotecarios y depósitos judiciales por medio de SINPE y por cheque.
7. Custodia y control de fórmulas de cheques para uso de la Subárea.
8. Elaboración de certificaciones por requerimientos del Ministerio de Hacienda o proveedores en general.

Los procesos anteriormente descritos se interrelacionan, por esta razón es importante identificar los servicios más críticos para posteriormente estimar los tiempos de recuperación, en razón a las posibles alteraciones de los procesos considerados de alta prioridad.

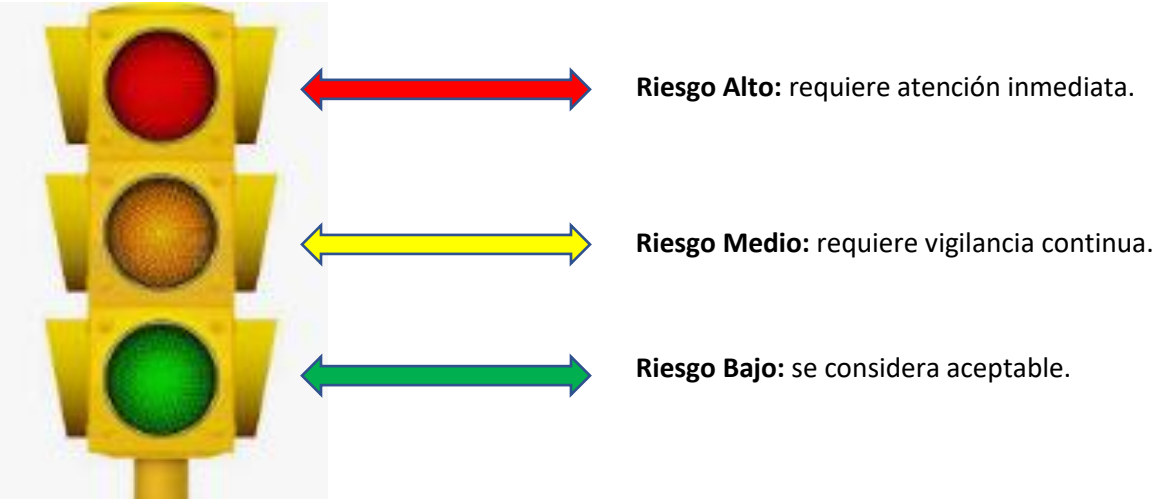
Una vez que se tiene la claridad de los servicios más críticos de la Subárea, se procede a realizar una clasificación de los riesgos.

La clasificación de riesgos se realizó mediante entrevista con las jefaturas y conversaciones con los colaboradores de la Subárea. En la figura del siguiente punto se muestran los riesgos de los servicios críticos de la organización clasificados según la metodología de semáforo de riesgos.

5.3.2 Semáforo de servicios críticos

El semáforo es utilizado para clasificar los servicios críticos de toda organización y con esto establecer el nivel de riesgo de cada proceso. Los riesgos se miden en una escala de Alto, Medio y Bajo, como se muestra en la siguiente figura:

Figura 20-Semáforo de servicios críticos



Fuente: Elaboración propia.

Tabla 26-Matriz herramienta de riesgos de la Subárea Gestión de Pagos

Procesos	Valoración de acuerdo con el semáforo
1. Pago a proveedores locales y extranjeros, empleados, pensionados y otros conceptos, por medio de SINPE del BCCR, Internet Banking BNCR, BCR Comercial y por vía cheque.	ALTO
2. Presentaciones de declaraciones y pagos de impuestos al Ministerio de Hacienda por BCR Comercial.	MEDIO
3. Pago a Organizaciones Sindicales, Colegios, Universidades, Cooperativa y entidades financieras por deducciones a empleados CCSS por SINPE	ALTO
4. Pagos por caja única de Hacienda de Bienestar Social.	ALTO

5. Pagos a diferentes dependencias de la CCSS como el FRIP-FRAP-FOCARE-FRE por medio de Internet Banking BNCR.	MEDIO
6. Pago de préstamos hipotecarios y depósitos judiciales por medio de SINPE y por cheque.	ALTO
7. Custodia y control de fórmulas de cheques para uso de la Subárea.	MEDIO
8. Elaboración de certificaciones por requerimientos del Ministerio de Hacienda o proveedores en general.	MEDIO

La tabla anterior muestra los procesos que representan riesgo y el nivel de cada uno de estos, de acuerdo con el semáforo, indicando de esta forma si este nivel es alto, medio o bajo. Con esto se le presta atención de acuerdo con el nivel mostrado, su materialización y mitigación, con el fin de que no se detenga la continuidad de los procesos que se ejecutan en la Subárea Gestión de Pagos. A la vez de esta forma se podrá visualizar a futuro los procesos que han cambiado su nivel en el tiempo, llevando un control de los mismos.

5.3.3 Procedimiento que establece Good Practice Guidelines

Después de identificar los procesos críticos, se deben establecer los tiempos de recuperación que se refieren al tiempo disponible para recuperarse de una suspensión o falla de los procesos; al entender lo fundamental del establecimiento de los tiempos de recuperación, se comprende realmente el BIA. Los tiempos de recuperación se describen en el análisis de impacto BIA de la norma ISO 22301.

En lo que se refiere a los procedimientos establecidos por la guía de buenas prácticas es importante señalar que el Business Continuity Institute, (Guidelines, 2013) en su código de buenas prácticas para la gestión de continuidad del negocio, especifica algunas herramientas que se ajustan

a cada etapa del ciclo de vida de la gestión de continuidad del negocio, las cuales son: "-RTO: Establecimiento de parámetros como el recovery time objetive -RPO: Recovery point objetive -MTPD: Maximum tolerable period of disruption, para la determinación de las estrategias. -BIA: Business impact analisys"

Se identifica el período máximo de inactividad que puede tolerar una organización en un servicio crítico antes de llegar al colapso y se hace la clasificación a fin de priorizar la recuperación del servicio. Esto muestra que si un proceso tiene un periodo máximo de tiempo de inactividad (MTD) de un (1) día, este debe tener mayor prioridad para iniciar el evento de recuperación, en razón al poco tiempo de tolerancia de la inactividad, frente a los de mayor tolerancia.

En el caso de la Subárea Gestión de Pagos se muestra el MTD en minutos:

Tabla 27-Prioridad de recuperación de procesos críticos de la Subárea Gestión de Pagos

Procesos	MTD (en minutos)	Prioridad de recuperación
1. Pago a proveedores locales y extranjeros, empleados, pensionados y otros conceptos, por medio de SINPE del BCCR, Internet Banking BNCR, BCR Comercial y por vía cheque.	10	1
2. Presentaciones de declaraciones y pagos de impuestos al Ministerio de Hacienda por BCR Comercial.	60	2
3. Pago a Organizaciones Sindicales, Colegios, Universidades, Cooperativa y entidades financieras por deducciones a empleados CCSS por SINPE	10	1
4. Pagos por caja única de Hacienda de Bienestar Social.	10	1
5. Pagos a diferentes dependencias de la CCSS como el FRIP-FRAP-FOCARE-FRE por medio de Internet Banking BNCR.	60	2
6. Pago de préstamos hipotecarios y depósitos judiciales por medio de SINPE y por cheque.	10	1

7. Custodia y control de fórmulas de cheques para uso de la Subárea.	60	2
8. Elaboración de certificaciones por requerimientos del Ministerio de Hacienda o proveedores en general.	60	2

De acuerdo con los resultados en la tabla anterior, se muestra que los servicios críticos de la Subárea Gestión de Pagos no pueden esperar más de tres horas para solucionarlos, ya que tienen prioridad uno (1).

Por lo anterior la importancia de tomar acciones para medir el impacto, ya que de acuerdo con los datos obtenidos sería grave que los procesos de la Subárea Gestión de Pagos sufran una interrupción.

Al determinar las necesidades temporales (RTO), limitaciones de pérdida de datos (RPO) para cada uno de los procesos de la empresa desde el punto de vista de la continuidad, será poca o nula la materialización de un riesgo

5.4 Implementación de Plan de Continuidad de Negocio (BCP)

En este apartado se realiza la propuesta de implementación del Plan de Continuidad en TIC para la Subárea de Gestión de Pagos del Área de Tesorería General de la Caja Costarricense de Seguro Social, una vez efectuado el diagnóstico y análisis de la organización. La implementación del plan de continuidad, la realizará en su momento la Subárea Gestión de Pagos, siguiendo la recomendación de analizar los resultados y ejecutar una evaluación de aceptación, colaboración y cumplimiento de los objetivos del plan.

En la realización del plan de continuidad en TIC para la Subárea de Gestión de Pagos, una vez que se ha efectuado el diagnóstico y análisis de la unidad, se recoge la información necesaria, se crean nuevas plantillas, de acuerdo con lo estipulado en las normas ISO 22301. Para la implementación

del plan, la Subárea Gestión de Pagos, utilizará los criterios de los entregables de este documento, los cuáles son explicados y entregados a la jefatura de la Subárea. A continuación, se detallan los entregables:

- Diagnóstico y análisis de la situación actual.
- Diseño de la metodología y plantillas a considerar.

Ahora bien, se le indica a la jefatura los pasos para la implementación del plan de continuidad en TIC para la Subárea Gestión de Pagos, que son:

1. Diagnosticar y analizar la situación actual de la Subárea de Gestión de Pagos, este punto se desarrolla en la sección 5.2.5 de este documento. Se debe tomar en cuenta:

    - Análisis de impacto
    - Análisis de riesgos
    - Identificación de riesgos
    - Evaluación de los riesgos

2. Diseñar la metodología y definir las necesidades de la Subárea Gestión de Pagos. Se realiza en el capítulo 3 de este documento, este punto se desarrolla según diagnóstico hecho en la Subárea y se toma como referencia el marco de trabajo y la norma ISO 22301.

3. Cuando se llega a este punto la situación de la Subárea Gestión de Pagos, posee un panorama más claro, al tener conocimiento sobre todos los riesgos, identificación de los procesos críticos para la Subárea en caso de una interrupción. Se determinan los riesgos relevantes que pueden generar una brecha importante en la unidad de trabajo en caso de ocurrir y se determina la estrategia a utilizar. La ISO 22301 menciona las operaciones a seguir para implementar los procedimientos.

    a. Establecer protocolo de comunicación interna y externa.
    b. Ser específicos a las medidas inmediatas que deben tomarse durante caída del servicio.
    c. Ser flexible para poder responder a amenazas imprevistas y cambiantes.

d. Centrarse en el impacto de los eventos que podrían generar una mayor afectación en el servicio que se brinda.
e. Desarrollar en base a los supuestos establecidos.

5.4.1. Fase I – Recopilación de datos

En este punto se reúnen los datos necesarios tales como: actividades, activos y medidas de defensa de cada proceso que es tomado en cuenta para el caso de aplicación.

En la tabla siguiente se resume una ficha técnica referente a la Valoración de impacto según ISO 27002 con información de la Subárea Gestión de Pagos.

Tabla 28-Ficha técnica Subárea Gestión de Pagos

Nombre de la Unidad	Subárea de Gestión de Pagos
Razón de ser	Gestionar pago a proveedores
Unidades relacionadas	5
Dirección	Oficinas Centrales de la Caja Costarricense de Seguro Social, Área de Tesorería
Teléfono	25390000 ext.7193
Nombre de la Jefatura	Lic. Luis Diego Bolaños Rojas
Número de colaboradores	7
Número de laptops instaladas	2
Número desktops instaladas	4
Número de servidores	1
Número de aplicaciones	10
Servicios Críticos	• Corte de energía prolongado. • Caída de los sistemas automatizados. • Suspensión de servicios de internet. • Incendio o sismo en el edificio.

	• Robo de información. • Pérdida de información por ataque cibernético. • Manipulación sensible sin autorización. • Falla en bases de datos. • Vencimiento de licencias de software. • Personal no capacitado para sus funciones. • Caídas de los equipos informáticos (dispositivos de red, servidores, UPS). • No realización de mantenimientos preventivos.

Fuente: elaboración propia.

5.4.1.1. Corte de energía prolongado

Tabla 29-Corte de energía prolongado

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr					Versión 1.0 Servicio crítico: corte de energía prolongado
Responsable	Lic. Luis Diego Bolaños					
Puesto	Jefe de Subárea					
Simbología						
Cumple las mejoras		Necesita Mejorar		Carencias Severas		
Listado de medidas de defensa	Estado	Actividad del proceso				
Infraestructura		El edificio es antiguo, debe mejorar en infraestructura física en la Subárea.				
Aplicaciones		Aplicaciones de recuperación y restauración de datos.				

Operaciones		Mínimo mantenimiento a las UPS e inclusive actualmente la fuente de corriente principal está dañada.
Personal		Directrices con recursos humanos.
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?	
☐ Irrecuperable ☑ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☐ > 24 horas	1. Verificar estado del generador eléctrico en la Subarea de Gestión de Pagos. 2. Velar por el funcionamiento de las UPS. 3. Revisar que la falla sea externa y no un tema de tomacorrientes de la institución.	

¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?	¿Hay pérdidas económicas en dinero?
☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
Todos los equipos físicos de la Subárea.	xxxxx	2 horas.
Tiempo total de recuperación del proceso	3☑ horas ☐ días ☐ semanas ☐ meses	

Fuente: Elaboración propia.

5.4.1.2. Caída de los sistemas automatizados

Tabla 30-Caída de los sistemas automatizados

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr				Versión 1.0 Servicio crítico: caída de los sistemas automatizados
Responsable	Lic. Luis Diego Bolaños				
Puesto	Jefe de Subárea				
Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura		Equipo de empleados que utilizan los sistemas están obsoletos.			
Aplicaciones		Aplicaciones con poco mantenimiento.			
Operaciones		No se brinda un mantenimiento a las bases de datos ni a los archivos de los sistemas automatizados.			
Personal		Requisitos de seguridad, empleados reportan problema hasta que sistema deja de funcionar.			
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?				
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☑ 8-24 horas ☐ > 24 horas	1. Reportar incidente al departamento de TI. 2. Asignar un técnico al problema reportado. 3. El técnico asignado revisa la falla y soluciona, en caso de que no pueda solucionar lo reporta al Centro de Gestión de Informática y a la Jefatura de la Subárea. 4. Jefatura coordina con el Centro de Gestión de Informática para resolver y se hacen las pruebas para verificar el funcionamiento.				
¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?		¿Hay pérdidas económicas en dinero?		
☐ 2-5 horas ☐ 5-12 horas ☑ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante		☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx		

	☐ Sin importancia	colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
Equipo del colaborador afectado de acuerdo con el sistema crítico caído.	xxxxx	15 horas.
Tiempo total de recuperación del proceso	24☑ horas ☐ días ☐ semanas ☐ meses	

Fuente: Elaboración propia.

5.4.1.3. Suspensión de servicios de proveedor de internet

Tabla 31-Suspensión de servicios de proveedor de internet

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr				Versión 1.0 Servicio crítico: suspensión de servicios proveedor de internet
Responsable	Lic. Luis Diego Bolaños				
Puesto	Jefe de Subárea				
Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura		El equipo físico de red de la Subárea no se renueva desde el año 2018, no se hacen mantenimientos. .			
Aplicaciones		No aplica directamente con el servicio crítico.			
Operaciones		Dependencia de un solo proveedor.			
Personal		Conocimiento de seguridad, directrices por parte de TI.			
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?				

☐ Irrecuperable ☑ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☐ > 24 horas	1. Reportar incidente al departamento de TI. 2. Asignar un técnico al problema reportado por el empleado. 3. El técnico asignado revisa la falla y soluciona, en caso de que no pueda solucionar lo reporta a la jefatura. 4. Coordinador llama al proveedor de servicios de internet, por ser una línea empresarial el problema debería de resolverse en las primeras 2 horas, de no ser algún problema con cableado externo de la Subárea.	
¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?	¿Hay pérdidas económicas en dinero?
☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
Todos los equipos físicos conectado a la red de CENECOOP R.L.	xxxxx	2 horas.
Tiempo total de recuperación del proceso	3 ☑ horas ☐ días ☐ semanas ☐ meses	

Fuente: Elaboración propia.

5.4.1.4. Desastre natural en el edificio

Tabla 32-Desastre natural en el edificio

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr				Versión 1.0 Servicio crítico: desastre natural en el edificio (incendios, inundaciones o terremotos)
Responsable	Lic. Luis Diego Bolaños				
Puesto	Jefe de Subárea				
Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura		El edificio es antiguo, debe mejorar en infraestructura física en la Subárea de Gestión de Pagos. .			
Aplicaciones		No aplica directamente con el servicio crítico.			
Operaciones		Velar por el cumplimiento en las medidas de seguridad impuestas por la comisión de brigadistas de la Institución.			
Personal		Se debe mejorar en los requisitos e instrucciones de seguridad en la Subárea de Gestión de Pagos.			
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?				
☑ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☐ > 24 horas	1. Reportar el desastre al equipo de brigadistas que lo conforman compañeros del mismo edificio. 2. Iniciar proceso de evacuación y control del desastre. 3. Verificar que todas las personas se encuentren bien, posteriormente revisar las instalaciones. 4. Reportar al departamento de TI los posibles fallos en equipos o sistemas. 5. Realizar las reparaciones de los equipos de ser posible.				
¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?	¿Hay pérdidas económicas en dinero?			

☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
Infraestructura física de Subárea	----	3 días
Infraestructura físico y lógica de la red en la subárea	xxxxx	2 días.
Tiempo total de recuperación del proceso	☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: Elaboración propia.

5.4.1.5. Robo de información

Tabla 33-Robo de información

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr				Versión 1.0 Servicio crítico: robo de información
Responsable	Lic. Luis Diego Bolaños				
Puesto	Jefe de Subárea				
Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura		Mejorar el equipo de red de la Subárea de Gestión de Pagos. .			
Aplicaciones		Las computadoras de los empleados no cuentan con software especializado para la prevención de pérdida de datos, además no hay cortafuegos en equipos de red.			

Operaciones		Cifrar la información confidencial que viaja a través de la red, mantener siempre actualizadas las aplicaciones que usa la organización.
Personal		El personal de la Subárea de Gestión de Pagos no se ha capacitado en aspectos de seguridad de la información, deben conocer la información sensible que gestiona en la unidad de trabajo.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☑ > 24 horas	1. Reportar o anticipar el incidente al departamento de TI. 2. La jefatura analiza el caso. 3. Examina el tipo de robo de información tecnológica para identificar criticidad. 4. Definir acciones tanto preventivas como correctivas para evitar este tipo de operaciones.

¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?	¿Hay pérdidas económicas en dinero?
☐ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☑ > 2 días	☐ Irremplazables ☑ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.

Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
PC o servidor	xxxxx	3 días.

Tiempo total de recuperación del proceso	☐ horas ☑ días ☐ semanas ☐ meses

Fuente: Elaboración propia.

5.4.1.6. Pérdida de información por ataque cibernético

Tabla 34-Pérdida de información por ataque cibernético

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr				Versión 1.0 Servicio crítico: pérdida de información por ataque cibernético
Responsable	Lic. Luis Diego Bolaños				
Puesto	Jefe de Subárea				
Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura		El equipo de red es bastante obsoleto. . .			
Aplicaciones		Actualización de equipo de red y software en servidores.			
Operaciones		No realización de copias de seguridad en computadoras de los colaboradores de la Subárea.			
Personal		No se advierte al personal de posibles peligros informáticos, no poseen restricciones de páginas web o enlaces sospechosos.			
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?				
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☑ 8-24 horas ☐ > 24 horas	1. Reportar o anticipar el incidente al departamento de TI. 2. Todo el departamento de TI se reúne y responden lo más rápido posible ante el ataque. 3. Examina el tipo de robo de información tecnológica para identificar criticidad. 4. Definir acciones tanto preventivas como correctivas para evitar este tipo de operaciones. 5. Solicitar restauración en servidores o computadoras atacadas con base en respaldos realizados.				
¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?		¿Hay pérdidas económicas en dinero?		
			☑ Sí		

☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
PC o servidor	xxxxx	2 días.
Tiempo total de recuperación del proceso	☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: Elaboración propia.

5.4.1.7. Manipulación sensible sin autorización

Tabla 35-Manipulación sensible sin autorización

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr				Versión 1.0 Servicio crítico: manipulación sensible sin autorización
Responsable	Lic. Luis Diego Bolaños				
Puesto	Jefe de Subárea				
Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura		No aplica directamente con el servicio crítico. . .			
Aplicaciones		Se puede mejorar en aspectos de software especializado de auditoría informática para la información.			
Operaciones		Informar a los colaboradores acerca documentos sensibles.			

Personal		Mínimas directrices del departamento de Tecnologías de la Información.
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?	
☐ Irrecuperable ☑ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☐ > 24 horas	1. Reportar o anticipar el incidente al departamento de TI. 2. Verificar que el colaborador sin autorización no haya reenviado la información confidencial. 3. Suprimir la información de la persona sin autorización. 4. Crear política para garantizar la no transferencia de información consideradas como confidenciales sin autorización previa.	
¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?	¿Hay pérdidas económicas en dinero?
☐ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☑ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
Cualquier dispositivo móvil o computador de donde salió la información	xxxxx	1 hora.
Tiempo total de recuperación del proceso	1 ☑ horas ☐ días ☐ semanas ☐ meses	

Fuente: Elaboración propia.

5.4.1.8. Falla en bases de datos

Tabla 36-Falla en base de datos

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr	Versión 1.0 Servicio crítico: falla en base de datos
Responsable	Lic. Luis Diego Bolaños	
Puesto	Jefe de Subárea	

Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	

Listado de medidas de defensa	Estado	Actividad del proceso
Infraestructura		No aplica en el proceso ya que las bases de datos de la Subárea de Gestión de Pagos están en Servidores Seguros. . .
Aplicaciones		Se debe actualizar las bases de datos SQL y MySQL, además de darle un mantenimiento constante a cada una de ellas.
Operaciones		No se realizan respaldos a todas las bases de datos de la Subárea de Gestión de Pagos.
Personal		Mínima capacitación a empleados sobre la utilización de sistemas de la Subárea de Gestión de Pagos.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☑ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☑ 8-24 horas ☐ > 24 horas	1. Reportar la falla al departamento de TI. 2. Asignar un técnico al problema para que revise la falla. 3. El técnico reporta la falla a la jefatura. 4. El coordinador repara la falla en la base de datos en caso de no ser así obtener respaldos para proceder con la restauración de la base de datos. 5. Hacer pruebas para comprobar que el problema ha sido solventado.

¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?	¿Hay pérdidas económicas en dinero?
☑ 2-5 horas	☑ Irremplazables	☑ Sí

☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐> 2 días	☐ Importantes ☐ Algo importante ☐ Sin importancia	☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
Servidor	xxxxx	8 hora.
Tiempo total de recuperación del proceso	1 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: Elaboración propia.

5.4.1.9. Vencimiento de licencias de software

Tabla 37-Vencimiento de licencias de software

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr					Versión 1.0 Servicio crítico: vencimiento de licencias de software
Responsable	Lic. Luis Diego Bolaños					
Puesto	Jefe de Subárea					
Simbología						
Cumple las mejoras		Necesita Mejorar		Carencias Severas		
Listado de medidas de defensa	Estado	Actividad del proceso				
Infraestructura		Algunas computadoras de empleados obsoletas por lo que es difícil la actualización de sistemas. .				
Aplicaciones		Escasa actualización del personal de TI en los sistemas administrativos instalados en las computadoras de los colaboradores.				
Operaciones		El personal de TI debe tener un mayor control sobre el software que se instala en la Subárea de Gestión de Pagos, además es				

		necesario la implementación de un software para limitar la descarga de programas en la red interna. .
Personal		Poca capacitación al personal, para que alerte del tema y conozca de los peligros.
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?	
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☑ 8-24 horas ☐ > 24 horas	1. Reportar o anticipar el incidente al departamento de TI. 2. Asignar un técnico a la computadora o servidor con licencia caducada o próxima a vencer y revisar la información de esta. 3. Solicitar a la jefatura de la Subárea de Gestión de Pagos boleta para adquisición de compra de licenciamiento. 4. Instalación de software y verificación que problema sea resuelto	
¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?	¿Hay pérdidas económicas en dinero?
☐ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☑ 1-2 días ☐> 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
PC o Servidor	xxxxx	1- 12 horas
Tiempo total de recuperación del proceso	1 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: Elaboración propia.

5.4.1.10. Personal no capacitado para sus funciones

Tabla 38-Personal no capacitado para sus funciones

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr				Versión 1.0 Servicio crítico: personal no capacitado para sus funciones
Responsable	Lic. Luis Diego Bolaños				
Puesto	Jefe de Subárea				
Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura		No aplica directamente con el servicio crítico. .			
Aplicaciones		No aplica directamente con el servicio crítico.			
Operaciones		Escasa planificación, directrices y políticas de capacitaciones de los altos mandos a los colaboradores de la Subárea de Gestión de Pagos			
Personal		Falta de conocimiento ante cualquier eventualidad del departamento de TI y los colaboradores de la Subárea de Gestión de Pagos.			
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?				
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☑ > 24 horas	1. El técnico debe reportar a la jefatura de la Subárea su inexperiencia en la tarea asignada. 2. Es responsabilidad de la jefatura mantener actualizados los entrenamientos de los colaboradores. 3. El técnico en TIC debe lograr resolver el inconveniente inicial.				
¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?		¿Hay pérdidas económicas en dinero?		
☐ 2-5 horas	☐ Irremplazables		☑ Sí		

☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☑> 2 días	☐ Importantes ☑ Algo importante ☐ Sin importancia	☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
Computadoras de Colaboradores	xxxxx	15 días
Tiempo total de recuperación del proceso	1 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: Elaboración propia.

5.4.1.11. Caídas de los equipos informáticos

Tabla 39-Caídas de los equipos informáticos

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr				Versión 1.0 Servicio crítico: personal no capacitado para sus funciones
Responsable	Lic. Luis Diego Bolaños				
Puesto	Jefe de Subárea				
Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura		El edificio es antiguo, por lo que hay mucho polvo que cae en los equipos de la Subárea de Gestión de Pagos. .			
Aplicaciones		Mínima actualización de software en los equipos de red y computadoras que pueden repercutir en el fallo de equipos informáticos.			
Operaciones		Este es el principal problema de las caídas, el último mantenimiento que realizó el departamento de TI al equipo de			

		red fue en el año 2019, por lo que las caídas pueden ser de alto riesgo.
Personal		El personal de TIC no está comprometido con los mantenimientos preventivos, ya que estos problemas son continuos y solamente lo resuelven momentáneamente.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☑ 8-24 horas ☐> 24 horas	1. La Jefatura reporta el daño al departamento de TI. 2. Seguimiento a que se designe un técnico al problema reportado. 3. El técnico asignado revisa el equipo y reporta el tipo y la gravedad del daño. (Jefatura verifica si el equipo posee garantía) 4. Si no aplica la garantía el técnico de TI puede reparar el equipo o el proveedor lo repara con un costo adicional. 5. Hacer pruebas para verificar que la falla sea resuelta.

¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?	¿Hay pérdidas económicas en dinero?
☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐> 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.

Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
Computadoras de Colaboradores	xxxxx	1 día

Tiempo total de recuperación del proceso	1 ☐ horas ☑ días ☐ semanas ☐ meses

Fuente: Elaboración propia.

5.4.1.12 No se han definido los servicios críticos de TI

Tabla 40-No se han definido los servicios críticos de TI

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr				Versión 1.0 Servicio crítico: no se han definido los servicios críticos de TI
Responsable	Lic. Luis Diego Bolaños				
Puesto	Jefe de Subárea				
Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura		No aplica directamente con el servicio crítico. .			
Aplicaciones		No aplica directamente con el servicio crítico.			
Operaciones		No se tienen definidos los servicios críticos vinculados con la continuidad del TIC			
Personal		El personal de TI no le ha dado la atención que requiere los servicios críticos de la Subárea.			
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?				
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☑> 24 horas	1. Los altos mandos deben programar una reunión con todo el personal de la Subárea de Gestión de Pagos 2. Se le indica a la jefatura para que se reúna internamente con los colaboradores de la Subárea para que determinen los servicios críticos que desarrollan. 3. La jefatura debe generar un documento formal con todos los riesgos descritos por cada proceso. 4. La jefatura debe dar seguimiento a los servicios críticos.				
¿Tiempo en recibir pérdidas económicas?	¿Tiempo en recibir pérdidas económicas?		¿Hay pérdidas económicas en dinero?		
☐ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas	☑ Irremplazables ☐ Importantes		☑ Sí ☐ No		

☐ 1-2 días ☑> 2 días	☐ Algo importante ☐ Sin importancia	Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración
Computadoras de Colaboradores	xxxxx	No aplica
Tiempo total de recuperación del proceso	1 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: Elaboración propia.

5.4.1.13 No realización de mantenimientos preventivos

Tabla 41-No realización de mantenimientos preventivos

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr				Versión 1.0 Servicio crítico: no realización de mantenimientos preventivos
Responsable	Lic. Luis Diego Bolaños				
Puesto	Jefe de Subárea				
Simbología					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura		No aplica directamente con el servicio crítico. .			
Aplicaciones		Algunas aplicaciones utilizadas por la Subárea son obsoletas por lo que su mantenimiento se vuelve difícil,			
Operaciones		Debido al mínimo mantenimiento muchos equipos presentan fallos que pudieron haberse reparado con el soporte adecuado.			

<table>
<tr><td>Personal</td><td>  </td><td colspan="2">El personal de TI no saca el tiempo adecuado para actualizar equipos físicos tanto de los colaboradores, como red interna ni mucho menos una limpieza o actualización en las versiones.</td></tr>
<tr><td>¿Tiempo estimado en la recuperación de la información?</td><td colspan="3">¿Cómo se procede para combatir el servicio crítico?</td></tr>
<tr><td>☐ Irrecuperable
☐ 0-4 horas
☐ 4-8 horas
☐ 8-24 horas
☑> 24 horas</td><td colspan="3">1. La jefatura debe comunicar a los colaboradores como proceder con la solicitud de mantenimientos preventivos.
2. La jefatura comunica a los colaboradores acerca de la necesidad de los riesgos por la no realización de mantenimiento.
3. Asignar a un responsable por semana (incluida la jefatura) para la ejecución de cada uno de los mantenimientos propuestos (impresoras, computadoras, equipo de red, servidores).
4. Informar a la jefatura la labor completada para que sea anotada en bitácora.</td></tr>
<tr><td>¿Tiempo en recibir pérdidas económicas?</td><td>¿Tiempo en recibir pérdidas económicas?</td><td colspan="2">¿Hay pérdidas económicas en dinero?</td></tr>
<tr><td>☐ 2-5 horas
☐ 5-12 horas
☐ 12-24 horas
☐ 1-2 días
☑> 2 días</td><td>☐ Irremplazables
☐ Importantes
☑ Algo importante
☐ Sin importancia</td><td colspan="2">☑ Sí
☐ No
Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: xxx colones por hora, multiplicado por la cantidad de horas que no hubo servicio.</td></tr>
<tr><td colspan="4">Recursos tecnológicos que soportan este proceso:
(Información se completa con ayuda de personal de TI)</td></tr>
<tr><td>Nombre de equipos</td><td>Placa de Activo del equipo</td><td colspan="2">Tiempo de restauración</td></tr>
<tr><td>Computadoras de Colaboradores y equipos de red</td><td>xxxxx</td><td colspan="2">4 horas</td></tr>
<tr><td colspan="2">Tiempo total de recuperación del proceso</td><td colspan="2">☑ horas ☐ días ☐ semanas ☐ meses</td></tr>
</table>

Fuente: Elaboración propia.

5.4.2 Fase II – Aplicación del plan de continuidad en TIC

Esta aplicación la realizará la Subárea Gestión de Pagos, para esto debe tomar en cuenta los procesos críticos identificados, que tienen medidas de defensa que necesitan ser mejoradas y en otros casos implementadas debido a la nula existencia, en el siguiente punto se describen las medidas de defensa que se deben tomar en cuenta para garantizar la continuidad del servicio.

5.4.3 Medidas de defensa para garantizar la continuidad del servicio

Al llegar este proyecto hasta la etapa de desarrollo, el objetivo de este apartado del documento es emitir un criterio sobre el cumplimiento de los controles, además de recomendar oportunidades de mejora y agregar valor, para garantizar de manera razonable la efectividad, eficiencia y disponibilidad de los servicios críticos de la Subárea Gestión de Pagos. A continuación, se detalla cada uno de los objetivos de control donde se señala la recomendación o estructura de plantilla que se debe tomar en cuenta para una efectiva aplicación del plan de continuidad en TIC.

5.4.3.1 Mantenimiento del Plan de Continuidad de TI

Esta etapa será aplicada por la Subárea Gestión de Pagos, ya que este proyecto comprende hasta el desarrollo del plan, el mantenimiento se orienta a probar con antelación y coordinar ejercicios, documentando y evaluando los resultados de ellos. Desarrollar procesos para mantener vigentes las capacidades para lograr una adecuada recuperación de las operaciones de TI, en acuerdo con la dirección estratégica del negocio. Para el logro de los objetivos se deberá:

- Establecer y ejercitar el Plan.
- Determinar los requerimientos de ejercitación.
- Desarrollar escenarios realistas para las pruebas.
- Preparar reportes y procedimientos de control de los ejercicios.
- Ejecutar ejercicios.
- Obtener retroalimentación de los resultados de las pruebas e implementar las mejoras requeridas.

El propósito es mantener actualizada la documentación cada vez que se produce un cambio importante en la organización a nivel de infraestructura, operaciones, personal, aplicaciones de TI o de cualquier otro proceso implicado en los procesos críticos de la Subárea. Esto permite que la documentación se utilice ante una situación de crisis, que se refleje la información de distintos actores involucrados en los procesos que se deben tener en cuenta en una situación de contingencia.

Tabla 42-Mantenimiento de los servicios críticos

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr	Fecha y Hora:
Responsable		
Puesto		

Diagnóstico del Servicio					
Cumple las mejoras		Necesita Mejorar		Carencias Severas	

Impacto en la Subárea	Estado	Causas
Infraestructura		
Aplicaciones		
Operaciones		
Personal		
Solución:		

¿El servicio se encuentra detenido actualmente?	SI ☐ NO ☐
¿Se han reportado fallas en el servicio crítico recientemente?	SI ☐ NO ☐

Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	Placa de Activo del equipo	Tiempo de restauración

Tiempo total de recuperación del proceso	☑ horas ☐ días ☐ semanas ☐ meses

Fuente: Elaboración propia.

5.4.3.2 Pruebas del Plan de Continuidad de TI

Estas pruebas las debe realizar la Subárea Gestión de Pagos, una vez que realice la implementación del plan. Se realiza la estructura del plan de pruebas, que es probar el plan de continuidad en TIC de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción.

Se aplica una plantilla para la documentación del plan de pruebas, se conforma por datos generales, participantes, detalles de pruebas, programación, revisión y autorización; estos campos son los sugeridos para la Subárea de Gestión de Pagos.

• Datos generales: se le debe poner un id a cada prueba, registro de fecha de creación, alcance que consiste en lo que se va a realizar, donde y para qué.

• Recursos necesarios: son los recursos necesarios que dependen de la prueba, puede ser desde una computadora hasta un servidor.

• Participantes del equipo: es el punto más importante de la plantilla se completa el nombre del personal y documentar las funciones durante la ejecución de la prueba.

• Detalles de la prueba: objetivo principal de la prueba, fecha y hora de inicio, tipo de prueba y la existencia de alguna condición para el cumplimiento de la prueba (opcional) y en caso de que haya cierta observación.

• Programación: listado de actividades para realizar en cada prueba, fecha y hora, el responsable de la ejecución de cada actividad y en caso de que haya alguna observación.

• Revisión: quién revisa y autoriza.

Tabla 43-Diseño del plan de pruebas

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr	Fecha y Hora: ID:

Realizado por:		Firma:
Revisado por:		Firma:

Participantes		
Nombre Completo	Colaborador	Actividades por ejecutar:

Detalles de la prueba	
Objetivo de la prueba	
Fecha y hora programada	
Hora de retorno	
Tipo de prueba	
Condiciones para cancelar prueba	
Observaciones	

Programación de actividades	
Nombre de la Actividad	
Fecha de Inicio	
Responsable	
Observaciones	

Fuente: Elaboración propia.

5.4.3.3 Entrenamiento del Plan de Continuidad de TI

Para asegurarse de que todas las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Se debe verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

Se muestra la estructura de la plantilla para los servicios de capacitación en la Subárea de Gestión de Pagos, en el entendido de que esta parte será de aplicación por parte de la Subárea a futuro.

Tabla 44-Propuesta de capacitación a la continuidad de los servicios tecnológicos

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr	Fecha y Hora: ID:

Expositor		Duración
Datos de la Capacitación		
Objetivo	Cantidad de Colaboradores	Capacitación Virtual o Presencial
Contenidos		
Listado de Contenidos		
Asistencia		
Nombre		
Revisión		
Realizado por:		
Revisado por		
Autorizado por:		
Observaciones		

Fuente: Elaboración propia.

5.4.3.4 Distribución del Plan de Continuidad en TIC

La distribución del plan de continuidad en TIC se realiza con una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.

Para el caso de la Subárea de Gestión de Pagos al existir solamente 7 colaboradores, cada uno de los miembros debe cumplir con varias tareas por lo que el equipo se distribuye de la siguiente manera:

- Equipo de administración de crisis: Jefatura.
- Equipo de notificación: Funcionario designado.
- Coordinador de la continuidad del negocio: Jefatura.
- Equipo de recuperación de backups: Funcionario designado.

- Equipo de coordinación de soporte: Funcionarios designados.
- Equipo de redes y telecomunicaciones: Funcionarios designados.
- Equipo de respuesta de emergencia: Funcionario designado.
- Equipo de aplicaciones: Funcionario designado.
- Equipo de evaluación y daños: Funcionario designado.
- Equipo de recuperación de respaldos de registros críticos: Funcionario designado.
- Equipo de integración y pruebas: Funcionario designado.
- Equipo de controles de seguridad: Funcionario designado.
- Equipo de logística y suministro de recursos: Funcionario designado.
- Equipo de coordinación y soporte: Jefatura.

Tabla 45-Distribución de roles por actividades de negocio

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr	Fecha y Hora:

Conformación de Roles		
Riesgo Critico	Equipos Responsables	Personas Responsables
Corte de energía prolongado.	Equipo de administración de crisis. Equipo de notificación. Coordinador de la continuidad del negocio. Equipo de recuperación de backups.	
Caída de los sistemas automatizados.	Equipo de administración de crisis. Equipo de notificación. Coordinador de la continuidad del negocio. Equipo de coordinación de soporte Equipo de aplicaciones	
Suspensión de servicios de proveedor de internet.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de notificación. Equipo de redes y telecomunicaciones.	
Incendio o sismo en el edificio.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de notificación.	

	Equipo de respuesta de emergencia Equipo de evaluación y daños	
Robo de información.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de controles de seguridad Equipo de integración y pruebas. Equipo de recuperación de respaldos de registros críticos. Equipo de evaluación y datos	
Pérdida de información por ataque informático.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de controles de seguridad Equipo de integración y pruebas. Equipo de recuperación de respaldos de registros críticos. Equipo de evaluación y daños	
Manipulación sensible sin autorización.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de controles de seguridad Equipo de evaluación y daños	
Falla en bases de datos.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de evaluación y daños Equipo de recuperación de backups de registros críticos y datos.	
Vencimiento de licencias de software.	Equipo de notificación. Equipo de coordinación y soporte Equipo de integración y pruebas	
Personal no capacitado para sus funciones.	Coordinador de la continuidad del negocio. Equipo de notificación. Equipo de logística y suministro de recursos.	
Caídas de los equipos informáticos (dispositivos de red, central telefónica, servidores, UPS).	Coordinador de la continuidad el negocio. Equipo de notificación. Equipo de controles de seguridad. Equipo de evaluación y riesgos. Equipo de sistemas de backups. Equipo de integración y pruebas.	
No se han definido los servicios críticos de TI.	Coordinador de la continuidad del negocio. Equipo de notificación. Equipo de logística y suministro de recursos.	

No realización de mantenimientos preventivos.	Equipo de coordinación y soporte. Equipo de evaluación y daños.	
Observaciones		

Fuente: Elaboración propia.

5.4.3.5 Recuperación y Reanudación de los Servicios de TI

Para planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a usuarios y colaboradores, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

Se crea una plantilla donde jefatura de la Subárea de Gestión de Pagos avala el procedimiento.

Tabla 46-Recuperación y reanudación de los servicios de TI

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr	Fecha y Hora: ID:
Reanudación del Servicio		
Puesto	Encargado	Sustituye
Revisión de Lista (cuando un servicio falla)		
Se activa procedimiento de respaldo		Si ☐ No ☐
Se comunica a los equipos respectivos de la continuidad		Si ☐ No ☐
Empleados continúan utilizando el servicio caído		Si ☐ No ☐
Se reanuda el servicio de manera correcta		Si ☐ No ☐
Observaciones		

Fuente: Elaboración propia.

5.4.3.6 Almacenamiento de Respaldos

Se almacenan fuera de la institución todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y la jefatura. La administración del sitio de almacenamiento externo a las instalaciones debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la institución.

Se crea una estructura de plantilla para la restauración de respaldos, como lo menciona el ISO 22301 en referencia a la importancia de los procesos. Se recomienda tomar en cuenta los siguientes aspectos:

- Nombre del encargado del puesto.
- Mencionar el tipo de respaldo, puede ser de configuración de equipos o de base de datos, también es importante tomar en cuenta el ambiente en el cual se aplica el respaldo, ya sea de producción o desarrollo, tiempos calculados para efectuar dicha acción.

Tabla 47-Restauración de respaldos

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr	Fecha y Hora: ID:
Restauración de Respaldos		
Puesto	Encargado	Sustituye
Detalle de Respaldos		
Tipo de Respaldo		

Ambiente Destino	
Tiempo de restauración	
Descripción	
Observaciones	

Fuente: Elaboración propia.

5.4.3.7 Revisión Post Reanudación

Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, se determina si la jefatura de la Subárea ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

Se crea una plantilla donde jefatura de la Subárea se encarga de distribuir la información y hacer una revisión de lista donde se colocan los servicios y procesos que brinda la Subárea de Gestión de Pagos, para verificar que la unidad se encuentre en un correcto funcionamiento.

Tabla 48-Reanudación de servicio

	CAJA COSTARRICENSE DE SEGURO SOCIAL Gerencia Financiera Subárea Gestión de Pagos Teléfono: 2539-0000 Ext. 200000 Correo electrónico: coinccss@ccss.sa.cr	Fecha y Hora: ID:
Reanudación del Servicio		
Puesto	Encargado	Sustituye
Revisión de Lista (cuando un servicio falla)		
Los servicios que brinda la Subárea están arriba		Si ☐ No ☐
Los datos que brinda la Subárea están arriba		Si ☐ No ☐
Validación con los interesados del funcionamiento del equipo		Si ☐ No ☐
Observaciones		

Fuente: Elaboración propia.

5.4.4 Fase III – Análisis de resultados

Una vez aplicado el plan de continuidad en TIC se procede a aplicar las respectivas pruebas, ejercicios y ensayos, para analizar los resultados de acuerdo con el factor tiempo y factor procesos.

5.4.4.1 Factor tiempo

A continuación, se detallan los parámetros y el tiempo de duración para recuperar el servicio:

Tabla 49-Factor tiempo

Parámetro de referencia	Tiempo Registrado
Promedio que un servicio pasa detenido	60 minutos
Promedio que toma en reportar un incidente	5 minutos
Promedio de revisión de los equipos para determinar el problema	30 minutos
Promedio que tarda el proveedor de los equipos para dar una solución (solo en caso de que aplique)	180 minutos
Promedio que tarda el técnico del departamento de TI en dar una solución	120 minutos
Promedio necesario para conseguir un servidor de características similares al equipo que presenta problemas	120 minutos
Promedio necesario para instalar y configurar las aplicaciones del servidor	180 minutos
Promedio necesario de instalación y configuración de servicios y aplicaciones críticas de TI	180 minutos
Promedio necesario para reiniciar un servidor e iniciar la aplicación	15 minutos
Promedio necesario para verificar que los estados de los servicios sean óptimos para los usuarios	10 minutos
Promedio necesario para levantar el internet en caso de fallo interno	60 minutos
Promedio de imprevistos	60 minutos
Promedio de Tiempo de Fallas	**85 minutos**

Fuente: Elaboración propia.

En base con el factor tiempo el parámetro que representa un mayor problema es el tiempo que se necesita para instalar y configurar las aplicaciones en el servidor lo que implica restaurar las aplicaciones tomaría mínimo 3 horas. Los demás parámetros son tiempos asequibles para la Subárea de Gestión de Pagos, el tiempo promedio de una falla es de 85 minutos.

5.4.4.2 Factor organizacional

En el factor organizacional se define el recurso humano que es necesario para la implementación del plan de continuidad en TIC. El equipo de gestión de riesgos está conformado los colaboradores de la Subárea de Gestión de Pagos.

Es importante aclarar que la implementación de un equipo de seguridad de salud ocupacional es importante en la Subárea de Gestión de Pagos, con el fin de tener un nivel de operación aceptable y seguro de las actividades dentro de la unidad de trabajo y de esta manera prevenir los riesgos para garantizar la integridad de los colaboradores; se debe involucrar a todo el personal para la capacitación constante.

Para la implementación del equipo de seguridad de salud ocupacional se puede utilizar la Norma OHSAS 18001 que puede ser aplicada a cualquier tipo de unidad de trabajo, porque ayuda a fomentar ambiente laborales seguros, estables y confortables. Con dicha norma, se garantiza una respuesta ante situaciones de emergencia como:

✓ Creación de una política de salud ocupacional.

✓ Identificar riesgos de salud.

✓ Análisis, evaluación y mejora del sistema de salud y seguridad ocupacional.

Al identificar los procesos críticos que contribuyen más a la misión de Subárea de Gestión de Pagos, se analiza el impacto que podría tener cualquiera de estos eventos que impida el correcto funcionamiento y pérdidas potenciales que podría acarrear esa interrupción. Como resultado, se desarrolla las tres fases: análisis de servicios críticos, aplicación del plan y análisis de resultados.

Se identifican los servicios y se establece la magnitud de los impactos potenciales tanto operativos como financieros.

El BCP involucra acciones complejas ante los servicios críticos mencionados anteriormente que son salvavidas ante eventualidades en la unidad de trabajo, es de vital importancia que la Subárea conozca su naturaleza de negocio para la recuperación, de esto depende la identificación acertada de los riesgos para establecer las estrategias más eficientes para su implementación, permitiendo de esta manera la correcta estimación de recursos. Además de esto los altos mandos deben demostrar su compromiso con el proceso, pues la implementación de la administración de la continuidad de servicios de TI es compleja y costosa sin un retorno de inversión. Sin embargo, como se ha mencionado a lo largo de este proyecto, esta etapa la realizará la Subárea Gestión de Pagos cuando lo considere pertinente.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6. Capítulo VI: Conclusiones y Recomendaciones

6.1 Conclusiones

Por medio de los análisis FODA, PESTEL y CAME se establecieron varias debilidades y fortalezas, así como las oportunidades y amenazas de la Subárea Gestión de Pagos; además, se concluyó que la Subárea contaba con un tipo de resumen que no aplicaba lo requerido en un plan de continuidad en TIC, lo cual no es efectivo para afrontar los riesgos inherentes de la unidad de trabajo, siendo necesario el desarrollo del Plan de Continuidad en TIC, para garantizar la efectiva y óptima continuidad del servicio que se brinda. La propuesta consideró estándares y normas internacionales, para la disminución de vulnerabilidades y riesgos, entre ellos diferentes normas ISO.

Además, se lograron detectar los procesos con los riesgos críticos que pueden materializarse, tanto a nivel de la Subárea de Gestión de Pagos. así como los riesgos informáticos, a los que están expuestos los colaboradores, así mismo se evidencian los riesgos altamente potenciales, mediante matrices para la determinación de riesgos (análisis de riesgos cualitativo, probabilidad, impacto, nivel de riesgo inherente, valoración de riesgos y semáforo de riesgos), lo cual afirma la prevención en cualquier tipo de interrupción, que pueden traer consigo la no continuidad del servicios que se brinda en la Subárea, tanto materiales, como humanos, generando seguridad en la unidad de trabajo.

Se elabora el Plan de Continuidad en TIC aplicado a los procesos con mayor riesgo y son necesarios para dar una solución breve y dar continuidad a los procesos, ante cualquier tipo de incidente, reduciendo el impacto sobre la Subárea y la Institución. Se define un proceso que permite aplicar los pasos necesarios, en caso de que se presente alguna contingencia en el lugar de trabajo; este proceso permite identificar cada uno de los riesgos a los que se enfrenta la Subárea

Gestión de Pagos y con base en lo anterior, se elabora un plan de acción para disminuir el impacto de dichos riesgos. Además, se confeccionaron plantillas para evitar las vulnerabilidades que se puedan presentar, por ejemplo: respaldos, mantenimiento del plan, roles y responsables, capacitaciones y post reanudación de servicios críticos.

Al finalizar este proyecto de graduación, se evidencia que la Subárea Gestión de Pagos no está exenta a sufrir incidentes que afecten los procesos de sus servicios más importantes, lo que puede generar daño a la imagen a nivel institucional. Finalmente, la Subárea Gestión de Pagos está anuente a mejorar y ofrecer la continuidad en sus servicios, sin embargo, hasta el momento no contaba con un Plan de Continuidad en TIC, por lo que al ocurrir un acontecimiento grave no se podrían levantar los servicios en un tiempo óptimo, lo que repercute en clientes insatisfechos con respecto a los servicios brindados por la institución.

6.2 Recomendaciones

1) Llevar a cabo la implementación del plan de continuidad en TIC, tomando como referencia la propuesta elaborada y utilizando como base las plantillas entregadas, ya que se encuentran enfocadas en la Subárea de Gestión de Pagos y alineadas a los estándares ISO 22301.

2) Solicitar los servicios de un técnico de la institución certificado en telecomunicaciones, para que realice un análisis de estructura de redes y cableado estructurado, además que verifique la topología actual, para garantizar el buen funcionamiento de la red y que la seguridad de la información sea integra, esté disponible y sea confidencial.

3) Actualizar al menos una vez al año el Plan de Continuidad en TIC, por lo que se debe revisar la valoración de riesgos, con el propósito de no afectar los procesos y la continuidad del servicio.

4) El jefe de la Subárea de Gestión de Pagos debe velar porque los colaboradores estén comprometidos con el plan, buscando la asignación de responsables ante nuevos riesgos de los procesos, además, se aconseja implementar políticas de control asociadas al plan, siendo la jefatura quien debe dar el seguimiento oportuno.

5) Capacitación continua a los colaboradores de la Subárea de Gestión de Pagos involucrados en el Plan de Continuidad en TIC, para que los resultados que se presenten garanticen una calidad en los procesos que se realizan, alcanzando con ello las metas de la unidad de trabajo.

6) Cuando el Plan de Continuidad en TIC, haya sido ejecutado e implementado, es importante mantener una evaluación del mismo para identificar cualquier tipo de ajuste que se deba realizar y con esto evitar que se vea afectado el correcto funcionamiento de los procesos de la Subárea.

BIBLIOGRAFIA

BIBLIOGRAFÍA

Advisera. (01 de 01 de 2021). *Advisera Expert Solutions Ltd.* Obtenido de Advisera Expert Solutions Ltd: https://advisera.com/27001academy/es/que-es-iso-27001/

Alvarado, D. F., & Zumba, L. (1 de enero de 2015). *dspace.ucuenca.edu.ec.* Obtenido de dspace.ucuenca.edu.ec: http://dspace.ucuenca.edu.ec/handle/123456789/22342

AYUDALEY. (01 de 01 de 2020). *ayudaleyprotecciondatos*. Obtenido de ayudaleyprotecciondatos: https://ayudaleyprotecciondatos.es/2020/12/30/seguridad-logica/#Que_es_la_seguridad_logica

Bravo Carrasco, J. (2005). *Gestión de Procesos.* Santiago, Chile: Evolución.

Cabrera Méndez, M. (2010). Introducción a las fuentes de información. *Universidad Politécnica de Valencia*, 8.

Caja Costarricense de Seguro Social, D. D. (2007). *Estudio Organizacional Integral de la Gerencia de División Financiera.* San José: Primera.

Cauqueva, J. R. (01 de 05 de 2007). *Google Académico*. Obtenido de Google Académido: Rodríguez, J. (2007). Guía de elaboración de diagnósticos. Línea). Consultado, 22.

CCSS. (01 de Mayo de 2013). *https://www.ccss.sa.cr.* Obtenido de https://www.ccss.sa.cr: https://www.academia.edu/9225021/Caja_Costarricense_de_Seguro_Social_Tabla

CGR. (31 de 12 de 2019). *Contraloría General de la Republica CR.* Obtenido de Contraloría General de la Republica CR: https://www.cgr.go.cr/03-documentos/publicaciones/igi.html

Chapman, A. (01 de 08 de 2004). *Google Académico*. Obtenido de Google Académico: https://d1wqtxts1xzle7.cloudfront.net/45320229/AnalisisFODAyPEST-with-cover-page-v2.pdf?Expires=1639444997&Signature=UGh7XYU~eRyuUsFGkaG-VjeOUCL632wLXogsSs0Z2~AAF-GwXFBxRzDpAI6-Mu6ofNNhuU6loKK6t~w9N7xyHiB7wChPf-ooRYDSMsdPldhMukIR4ntFXicF1ZoWm4pD5Z3FZDJ6gG

Coworkingfy. (enero de 01 de 2020). *Coworkingfy .* Obtenido de Coworkingfy : https://coworkingfy.com/lluvia-de-ideas/

EALDE. (07 de 09 de 2017). *Gestión de Riesgos.* Obtenido de Gestión de Riesgos: https://www.ealde.es/gestion-de-riesgos-seguridad-de-la-informacion/

Etecé, E. (25 de setiembre de 2020). *Concepto.* Obtenido de Concepto: https://concepto.de/entrevista/

Gómez Orozco, A. (01 de 01 de 2013). Sistema de gestión de seguridad de la información SGSI. Colombia, Colombia, Colombia. Obtenido de Google Académico.

González Villalobos, J. A. (1 de enero de 2015). *Google Académico.* Obtenido de Google Académico: https://core.ac.uk/download/pdf/67720071.pdf

GONZÁLEZ VILLALOBOS, J. A. (01 de enero de 2015). *www.kerwa.ucr.ac.cr.* Obtenido de www.kerwa.ucr.ac.cr: https://www.kerwa.ucr.ac.cr/bitstream/handle/10669/27824/MATI-TFG-JAGV-B29148.pdf?sequence=1&isAllowed=y

Guidelines, B. C. (01 de 01 de 2013). *Google Académico*. Obtenido de Google Académico: https://scholar.google.es/scholar?hl=es&as_sdt=0,5&qsp=2&q=business+continuity+institute+%22good+practice+guidelines%22&qst=ib

ISO, N. (01 de 01 de 2018). *Normas ISO.* Obtenido de Normas ISO: https://www.normas-iso.com/iso-27001/

Kirvan, P. (14 de Nov de 2013). *searchdatacenter.techtarget.com.* Obtenido de searchdatacenter.techtarget.com: https://searchdatacenter.techtarget.com/es/tutoriales/Guia-de-evaluacion-de-riesgos-de-TI

Lizarzaburu, E. R., Barriga Ampuero, G., Noriega Febres, L. E., & Mejía, P. Y. (05 de setiembre de 2017). Gestión de Riesgos Empresariales: Marco de revisión ISO 31000. *Espacios*, 8. Obtenido de Google académico: http://revistaespacios.com/a17v38n59/a17v38n59p08.pdf

Mekhala, R. (1 de abril de 2018). *searchdatacenter.techtarget.com.* Obtenido de searchdatacenter.techtarget.com: https://searchdatacenter.techtarget.com/es/definicion/Mapa-de-riesgos-mapa-de-calor-de-riesgos

MINTIC. (12 de mayo de 2015). *mintic.gov.co.* Obtenido de mintic.gov.co: https://mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

MOSQUERA QUINTERO, G. C. (30 de 10 de 2015). *Google Académico.* Obtenido de Google Académico: http://repositorio.ufpso.edu.co/xmlui/bitstream/handle/123456789/2862/27980.pdf?sequence=1&isAllowed=y

Orrego, V. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Revista Pensamiento Americano*, 21-23.

Progress, Q. (01 de mayo de 2002). *Google Académico.* Obtenido de Google Académico: http://rube.asq.org/quality-progress/2002/05/problem-solving/los-beneficios-de-pdca.html

Ricardo Cabrera , H. (01 de octubre de 2009). *www.eumed.net.* Obtenido de www.eumed.net: https://www.eumed.net/libros-gratis/2010a/650/650.pdf

Rodríguez López, M., Piñeiro Sánchez, C., & Llano Monelos, P. (1 de Enero de 2013). *Google Académico.* Obtenido de Google Académico: https://scholar.google.es/scholar?hl=es&lr=lang_es&as_sdt=0%2C5&q=riesgos&btnG=

Samanes, B. E.-C. (01 de 01 de 2021). *Google Académico*. Obtenido de Google Académico: file:///C:/Users/Heilyn%20(Mamita)/Downloads/eavila,+1%20(2).pdf

Sampieri, R. H. (2014). *Metodología de la investigación, Sexta Edición.* México: Editorial McGraw Hill.

Silvestrini, M., & Vargas, J. (01 de 01 de 2008). *Fuentes de información primaria, secundaria y terciarias.* Obtenido de Fuentes de información primaria, secundaria y terciarias: https://ponce.inter.edu/cai/manuales/FUENTES-PRIMARIA.pdf

APÉNDICES

1. **Índice de Gestión Institucional (IGI) de la Contraloría General de la República**

CRITERIOS COMUNES	
6	**TECNOLOGÍAS DE LAS INFORMACIÓN**
6.1	¿La institución ha establecido un departamento de TI; mediante una estructura formal, que contemple el establecimiento de los roles y las responsabilidades de sus funcionarios?
6.2	¿Existen en la institución funcionarios formalmente designados para que conformen una representación razonable que como parte de sus labores, asesoren y apoyen al jerarca en la toma de decisiones estratégicas en relación con el uso y el mantenimiento de tecnologías de información?
6.3	¿La institución cuenta con un plan estratégico de tecnologías de información vigente que al menos cumpla los siguientes requisitos?: a Describir la forma en que los objetivos estratégicos de TI están alineados con los objetivos estratégicos de la institución b Disponer de un método para evaluar el impacto de TI en los objetivos estratégicos de la institución c Incluir fuentes de financiamiento, estrategias de adquisiciones y un presupuesto que esté vinculado con el presupuesto institucional (LA RESPUESTA AFIRMATIVA REQUIERE QUE EL PLAN CONTEMPLE LOS TRES PUNTOS, COMO MÍNIMO)
6.4	¿La institución cuenta con un modelo de arquitectura de la información que: a Sea conocido y utilizado por el nivel gerencial de la institución? b Caracterice los datos de la institución, aunque sea a nivel general? (LA RESPUESTA AFIRMATIVA REQUIERE QUE SE CUMPLAN AMBOS PUNTOS)
6.7	¿La institución cuenta con un modelo de entrega de servicio de TI que defina los acuerdos de nivel de servicio con los usuarios?
6.8	¿Se ha oficializado en la institución un marco de gestión de la calidad en la entrega de productos y servicios asociados a las tecnologías de información?
6.9	¿La institución cuenta con directrices (o políticas) orientadas a lo siguiente?: a La identificación de información en soporte digital, gestionada por la institución, que deba ser compartida con otras instituciones o que deba ser del conocimiento de la ciudadanía en general b La implementación de mecanismos tecnológicos para comunicar dicha información a sus destinatarios (LA RESPUESTA AFIRMATIVA REQUIERE QUE SE CUMPLAN AMBOS PUNTOS)
6.10	La institución ha oficializado un marco de gestión para la seguridad de la información (tanto física como lógica), alineado al Plan Estratégico de TI, que identifique al menos lo siguiente: a Políticas y procedimientos de seguridad de la información b Gestión de riesgos asociados a la seguridad de la información c Marco legal y regulatorio relacionado con seguridad de la información, que la entidad debe cumplir (LA RESPUESTA AFIRMATIVA REQUIERE QUE SE IDENTIFIQUEN LOS TRES ASUNTOS, COMO MÍNIMO)

6.11	¿La institución ha definido, oficializado y comunicado políticas y procedimientos de seguridad lógica? (LA RESPUESTA AFIRMATIVA REQUIERE QUE SE CUMPLAN AMBOS TIPOS DE REGULACIÓN HAYAN SIDO DEFINIDOS, OFICIALIZADOS Y COMUNICADOS)
6.12	¿Se han definido e implementado procedimientos para otorgar, limitar y revocar el acceso físico al centro de cómputo y a otras instalaciones que mantienen equipos e información sensibles?
6.13	¿Se aplican medidas de prevención, detección y corrección para proteger los sistemas contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento, etc)?
6.14	¿Se aplican políticas oficializadas que garanticen que la solicitud, el establecimiento, la emisión, la suspensión, la modificación y el cierre de cuentas de usuario y de los privilegios relacionados se hagan efectivas por el administrador de cuentas de usuario de manera inmediata?
6.15	¿Existe un plan formal que asegure la continuidad de los servicios de tecnologías de información en la organización?
6.16	¿Las políticas de TI se comunican a todos los usuarios internos y externos relevantes? (LA RESPUESTA AFIRMATIVA REQUIERE QUE SE CONSIDERE A LOS USUARIOS TANTO INTERNOS COMO EXTERNOS, SEGÚN CORRESPONDA)

2. Entrevista realizada a la Jefatura de la Subárea Gestión de Pagos

Entrevista a jefatura de la Subárea Gestión de Pagos

1. ¿Cuántos funcionarios laboran en la Subárea Gestión de Pagos?

2. ¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?

   ☐ Si, por favor detállelos: _____

   ☐ No

3. ¿En caso de presentarse una interrupción a los servicios críticos, qué hacen y cómo lo hacen?

4. Cuenta la Subárea Gestión de Pagos con un Plan de Continuidad en TIC, ¿y cuándo fue su última actualización?

   ☐ Si

   ☐ No

   Última actualización: _____

5. ¿Cuál es la probabilidad de fallo en los servicios?

   ☐ Muy probable

   ☐ Probable

   ☐ Poco probable

   ☐ Nunca

6. Por lo general, ¿cuánto tiempo se espera al momento de presentarse una interrupción en algún servicio?

☐ De 10 a 30 minutos

☐ De 31 a 59 minutos

☐ De 1 a 3 horas

☐ Más de 3 horas

7. ¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?

   ☐ Muy frecuentemente
   ☐ Frecuentemente
   ☐ Poco frecuentemente
   ☐ Nunca

8. ¿Cuáles procesos se ejecutan en la Subárea?

9. ¿A quiénes benefician los procesos que se ejecutan en la Subárea?

10. ¿Dónde se guardan los respaldos de la Subárea?

11. ¿Conoce el proceder en caso de presentarse una interrupción en los procesos, sea por causas relacionadas con los sistemas o por desastre natural?

    ☐ Si

    ☐ No

12. ¿Existe un Departamento de TI asignado a la Subárea Gestión de Pagos para Soporte Técnico?

    ☐ Si

    ☐ No

13. ¿Cómo considera la calidad del equipo de cómputo con que cuentan los funcionarios?

    ☐ Muy bueno

    ☐ Bueno

    ☐ Malo

    ☐ Muy malo

14. ¿Qué opina de la velocidad del internet para ejecutar los procesos en los sistemas?

    ☐ Muy buena

    ☐ Buena

    ☐ Mala

    ☐ Muy mala

15. ¿Qué tipo de sistemas operativos utilizan las computadoras?

16. En caso de falla en herramientas (hardware-software) como equipo de cómputo o sistemas de información ¿existe un plan para solucionarlo?

17. ¿Dónde están ubicados los servidores? _____, ¿contemplan algún tipo de seguridad contra ataques cibernéticos?

☐ Si

☐ No

3. Encuestas realizadas a los colaboradores de la Subárea Gestión de Pagos

Subárea Gestión de Pagos	**Encuesta "Plan de Continuidad en TIC"**

Saludos estimados colaboradores:

Por medio de este formulario se desea recopilar su opinión sobre el Plan de Continuidad en TIC.

Por favor conteste el siguiente cuestionario con toda sinceridad. Sus respuestas son confidenciales.

Marque una ☒ en el espacio que corresponda o conteste de forma amplia cada pregunta.

Fecha: _____/_____/_____

Encargado del proceso: _____

1) ¿Sabe usted qué es un plan de continuidad en TIC?

   ☐ Si

   ☐ No

2) ¿Qué es para usted un Plan de Continuidad en TIC?

   _____
   _____
   _____

3) ¿En la Subárea Gestión de Pagos existe un Plan de Continuidad en TIC?

   ☐ Si

☐ No

4) De acuerdo al proceso que usted realiza, ¿existen respaldos?

☐ Si, indique donde se encuentran _____

☐ No

5) Describa con sus propias palabras, qué es un riesgo y cómo mitigarlo.

_____
_____
_____
_____

6) ¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?

☐ Si, por favor detállelos: _____

☐ No

7) Dentro de los procesos a su cargo, cuáles considera son críticos

_____
_____
_____
_____

8) Si los procesos anteriores sufren una interrupción, ¿qué otros procesos pueden verse afectados y a qué otras Áreas se puede afectar?

_____
_____
_____

9) ¿Qué herramientas (hardware-software) necesita para llevar a cabo sus funciones?

- ☐ Monitor-Teclado-CPU
- ☐ Sistemas de información
- ☐ Impresora
- ☐ Aplicaciones de Office
- ☐ Otros _____

10) ¿Sabe qué son controles físicos?

- ☐ Si, amplíe su respuesta_____
- ☐ No

11) ¿Sabe qué son controles lógicos?

- ☐ Si, amplíe su respuesta_____
- ☐ No

12) ¿Sabe qué son activos de información?

- ☐ Si, por favor detállelos_____
- ☐ No

13) Ante una amenaza a un activo de información, ¿qué controles aplicaría?

_____

14) ¿Hace cuánto tiempo utiliza su equipo de cómputo?

- ☐ De 1 a 3 años
- ☐ De 4 a 6 años
- ☐ De 6 años o más

15) ¿Por lo general cuánto tiempo espera al momento de presentarse una interrupción en alguno de los procesos?

- ☐ De 10 a 30 minutos
- ☐ De 31 a 59 minutos
- ☐ De 1 a 3 horas
- ☐ Más de 3 horas

16) ¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?

- ☐ Muy frecuentemente
- ☐ Frecuentemente
- ☐ Poco frecuentemente
- ☐ Nunca

17) ¿Conoce qué hacer en caso de presentarse una interrupción o daño en su equipo?

- ☐ Si
- ☐ No

Muchas gracias por su cooperación.

ANEXOS

1. **Resultado de la entrevista a Jefatura de la Subárea Gestión de Pagos**

Entrevista a jefatura de la Subárea Gestión de Pagos

1. ¿Cuántos funcionarios laboran en la Subárea Gestión de Pagos?
   Siete¿

   Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?

   ☐ Si, por favor detállelos: Emitir pagos por bienes y servicios por medio de transferencias electrónicas de fondos o cheques.

   ☐ No

2. ¿En caso de presentarse una interrupción a los servicios críticos, qué hacen y cómo lo hacen?
   En el caso de transferencias se tiene una sala alterna ubicada en la Dirección Financiera Contables y otra que ofrece el Banco Central de Costa Rica para atender las transferencias electrónicas de Fondos. En el caso de cheques se tienen dos máquinas de escribir para emitirlos.

3. Cuenta la Subárea Gestión de Pagos con un Plan de Continuidad en TIC, ¿y cuándo fue su última actualización?

   ☐**X** Si

   ☐ No

   Última actualización: __2019_____

4. ¿Cuál es la probabilidad de fallo en los servicios?

   ☐ Muy probable

   ☐ Probable

   ☐**X** Poco probable

☐ Nunca

5. Por lo general, ¿cuánto tiempo se espera al momento de presentarse una interrupción en algún servicio?

☐X De 10 a 30 minutos

☐ De 31 a 59 minutos

☐ De 1 a 3 horas

☐ Más de 3 horas

6. ¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?

   ☐ Muy frecuentemente

   ☐ Frecuentemente

   ☐X Poco frecuentemente

   ☐ Nunca

7. ¿Cuáles procesos se ejecutan en la Subárea?
   Emisión de pagos por medio del Sistema Institucional de Pagos (SIPA) en forma paralela con el Sistema Nacional de Pagos.
   Autorizaciones de pagos por planillas de pensiones del IVM y pensiones alimenticias del RNC judiciales, utilizando la plataforma del Banco de Costa Rica, denominada BCR-COMERCIAL.

8. ¿A quiénes benefician los procesos que se ejecutan en la Subárea?
   A todos los usuarios externos e internos, con lo que la Institución tiene algún compromiso financiero.

9. ¿Dónde se guardan los respaldos de la Subárea?
   Los archivos propios de gestión de la Subárea en la nube y los generados por los sistemas, no sabría contestar con exactitud, ese tema lo administra el Área de Soporte Técnico.

10. ¿Conoce el proceder en caso de presentarse una interrupción en los procesos, sea por causas relacionadas con los sistemas o por desastre natural?

    ☐ XSi

    ☐ No

11. ¿Existe un Departamento de TI asignado a la Subárea Gestión de Pagos para Soporte Técnico?

    ☐ XSi

    ☐ No

12. ¿Cómo considera la calidad del equipo de cómputo con que cuentan los funcionarios?

    ☐ XMuy bueno

    ☐ Bueno

    ☐ Malo

    ☐ Muy malo

13. ¿Qué opina de la velocidad del internet para ejecutar los procesos en los sistemas?

    ☐ XMuy buena

    ☐ Buena

    ☐ Mala

    ☐ Muy mala

14. ¿Qué tipo de sistemas operativos utilizan las computadoras?
    Window 10

15. En caso de falla en herramientas (hardware-software) como equipo de cómputo o sistemas de información ¿existe un plan para solucionarlo?
    Se procede a llenar un reporte especialmente formulado por el Centro de Gestión Informático (CGI), para su atención.

16. ¿Dónde están ubicados los servidores? Centro Gestión Informática de la Dirección Financiero Contable, ¿contemplan algún tipo de seguridad contra ataques cibernéticos?

☐ Si

☐ No

Los servidores se ubican en el CGI, Área de Soporte Técnico.
Respecto a los ataques cibernéticos, no sabría contestar.

2. **Resultado de las encuestas efectuadas a los colaboradores de la Subárea Gestión de Pagos**

Subárea Gestión de Pagos	**Encuesta "Plan de Continuidad en TIC"**

Saludos estimados colaboradores:

Por medio de este formulario se desea recopilar su opinión sobre el Plan de Continuidad en TIC.

Por favor conteste el siguiente cuestionario con toda sinceridad. Sus respuestas son confidenciales.

Marque una ☒ en el espacio que corresponda o conteste de forma amplia cada pregunta.

Fecha: 10 _/11__/2021_

Encargado del proceso: Jorge M. Araya Flores

1) ¿Sabe usted qué es un plan de continuidad en TIC?

   X Si

   ☐ No

2) ¿Qué es para usted un Plan de Continuidad en TIC?

   Es el plan que se realiza para mitigar los problemas que se pueden presentar en el lugar de trabajo, en lo relacionado a lo informático

3) ¿En la Subárea Gestión de Pagos existe un Plan de Continuidad en TIC?

X Si

☐ No

4) De acuerdo al proceso que usted realiza, ¿existen respaldos?

X Si, indique donde se encuentran SE encuentran en la NUBE

☐ No

5) Describa con sus propias palabras, qué es un riesgo y cómo mitigarlo.

Un riesgo es cuando algo está en peligro de perderlo. Para mitigar el riesgo, deben de tomarse medidas preventivas o de acción inmediata para protegerlo.

6) ¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?

X Si, por favor detállelos: Custodia de fórmulas de cheques y traslado de los mismos a otras unidades de trabajo, perdida de información sensible de datos, por desconocimiento de lugares de respaldo (Nube) o por mal manejo de los datos;

☐ No

7) Dentro de los procesos a su cargo, cuáles considera son críticos

El pago de las obligaciones de la Institución al Ministerio de Hacienda, debido a que existe un plazo, y si se incumple en el plazo, ocasionaría sanciones millonarias para la C.C.S.S.
La presentación de las declaraciones informativas al Ministerio de Hacienda, tiene un plazo de entrega, de igual forma un incumpliendo, la C.C.S.S. queda expuesta a sanciones económicas.
Presentación de requerimientos solicitados por la Administración Tributaria, tienen plazo de entrega, si la C.C.S.S. incumple se expone a sanciones económicas.
Pago de las diferentes organizaciones (sindicatos, cooperativas, asociaciones, entidades financieras) tienen una fecha establecida, la cual se debe de respetar, de lo contrario muchos funcionarios que tienen compromisos con estas organizaciones, quedaría en los sistemas financieros en estado moroso.
Un fallo en los sistemas SINPE CCSS y del SIPA, atrasaría los pagos de los proveedores locales y beneficiarios.

8) Si los procesos anteriores sufren una interrupción, ¿qué otros procesos pueden verse afectados y a qué otras Áreas se puede afectar?

La Institución, la Gerencia Financiera, la Dirección Financiero Contable y el Area de Tesoreria General quedan expuesta a sanciones económicas fuertes por parte del Ministerio de Hacienda.
El Area de Pensiones, la Subarea de Caja Custodia de Valores, diferentes sucursales de la C.C.S.S, que distribuyen los pagos por cheques del Régimen No Contributivo

9) ¿Qué herramientas (hardware-software) necesita para llevar a cabo sus funciones?

X☐ Monitor-Teclado-CPU

X☐ Sistemas de información

X☐ Impresora

X☐ Aplicaciones de Office

X☐Otros Sistemas Web del Ministerio de Hacienda y de entidades financieras.

10) ¿Sabe qué son controles físicos?

☐ Si, amplíe su respuesta_____

X☐ No

11) ¿Sabe qué son controles lógicos?

☐ Si, amplíe su respuesta_____

X☐ No

12) ¿Sabe qué son activos de información?

X☐ Si, por favor detállelos Todo lo que son software y datos

☐ No

13) Ante una amenaza a un activo de información, ¿qué controles aplicaría?

Hacer respaldos de la información constantemente, sea esta en la Nube o en un servidor

14) ¿Hace cuánto tiempo utiliza su equipo de cómputo?

☐ De 1 a 3 años

☐ De 4 a 6 años

X De 6 años o más

15) ¿Por lo general cuánto tiempo espera al momento de presentarse una interrupción en alguno de los procesos?

☐ De 10 a 30 minutos

☐ De 31 a 59 minutos

X De 1 a 3 horas

☐ Más de 3 horas

16) ¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?

☐ Muy frecuentemente

☐ Frecuentemente

X Poco frecuentemente

☐ Nunca

17) ¿Conoce qué hacer en caso de presentarse una interrupción o daño en su equipo?

X Si

☐ No

Muchas gracias por su cooperación.

Subárea Gestión de Pagos	**Encuesta “Plan de Continuidad en TIC”**

Saludos estimados colaboradores:

Por medio de este formulario se desea recopilar su opinión sobre el Plan de Continuidad en TIC.

Por favor conteste el siguiente cuestionario con toda sinceridad. Sus respuestas son confidenciales.

Marque una ☒ en el espacio que corresponda o conteste de forma amplia cada pregunta.

Fecha: 16-11-2021

Encargado del proceso: Esteban Romero

1) ¿Sabe usted qué es un plan de continuidad en TIC?

   ☐ ❹ Si

   ☐ No

2) ¿Qué es para usted un Plan de Continuidad en TIC?

   Continuidad en los procesos durante cualquier evento no planificado

3) ¿En la Subárea Gestión de Pagos existe un Plan de Continuidad en TIC?

   ☐ ❹ Si

   ☐ No

4) De acuerdo al proceso que usted realiza, ¿existen respaldos?

   ☐ ❹ Si, indique donde se encuentran One Drive (nube CCSS)

☐ No

5) Describa con sus propias palabras, qué es un riesgo y cómo mitigarlo.

Un evento que puede generar peligros en las actividades laborales.
Realizar un plan de contingencia puede mitigar el riesgo de gran manera.

6) ¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?

☐ XSi, por favor detállelos: Falla en los servicios del SINPE

☐ No

7) Dentro de los procesos a su cargo, cuáles considera son críticos

Falla de conectividad.
Falla en los sistemas de pago.

8) Si los procesos anteriores sufren una interrupción, ¿qué otros procesos pueden verse afectados y a qué otras Áreas se puede afectar?

Afecta a todos los proveedores a nivel nacional, además de las Subáreas que nos facilitan los documentos de pago.

9) ¿Qué herramientas (hardware-software) necesita para llevar a cabo sus funciones?

☐ ❹ Monitor-Teclado-CPU

☐ XSistemas de información

☐ XImpresora

☐ XAplicaciones de Office

☐ Otros Sistema Nacional de Pagos Electrónicos SINPE

10) ¿Sabe qué son controles físicos?

☐ XSi, amplíe su respuesta camaras, equipo de seguridad

☐ No

11) ¿Sabe qué son controles lógicos?

☐ Si, amplíe su respuesta_____

☐ XNo

12) ¿Sabe qué son activos de información?

☐ XSi, por favor detállelos Base de datos, archivos

☐ No

13) Ante una amenaza a un activo de información, ¿qué controles aplicaría?

Pérdida de información o de base de datos, se puede controlar realizando varias copias a otro servidor.

14) ¿Hace cuánto tiempo utiliza su equipo de cómputo?

☐ De 1 a 3 años

☐ De 4 a 6 años

☐ ❹ De 6 años o más

15) ¿Por lo general cuánto tiempo espera al momento de presentarse una interrupción en alguno de los procesos?

☐ De 10 a 30 minutos

☐ De 31 a 59 minutos

☐ XDe 1 a 3 horas

☐ Más de 3 horas

16) ¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?

☐ Muy frecuentemente

☐ Frecuentemente

☐ XPoco frecuentemente

☐ Nunca

17) ¿Conoce qué hacer en caso de presentarse una interrupción o daño en su equipo?

☐ XSi

☐ No

Muchas gracias por su cooperación.

Subárea Gestión de Pagos	**Encuesta "Plan de Continuidad en TIC"**

Saludos estimados colaboradores:

Por medio de este formulario se desea recopilar su opinión sobre el Plan de Continuidad en TIC.

Por favor conteste el siguiente cuestionario con toda sinceridad. Sus respuestas son confidenciales.

Marque una ☒ en el espacio que corresponda o conteste de forma amplia cada pregunta.

Fecha: 15 / 11 / 2021

Encargado del proceso: Omaira Gabriela Oymacch Blen

1) ¿Sabe usted qué es un plan de continuidad en TIC?

☒ Si

☐ No

2) ¿Qué es para usted un Plan de Continuidad en TIC?

Son las Transacciones en desarrollar cuando se presenta en función en la parte de Informática

3) ¿En la Subárea Gestión de Pagos existe un Plan de Continuidad en TIC?

☒ Si

☐ No

4) De acuerdo al proceso que usted realiza, ¿existen respaldos?

☐ Si, indique donde se encuentran _____

☒ No

5) Describa con sus propias palabras, qué es un riesgo y cómo mitigarlo.

Pérdida de información o factores negativos a lo que me veo expuesta al desarrollo de mis funciones.

6) ¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?

☐ Si, por favor detállelos: _____

☒ No

7) Dentro de los procesos a su cargo, cuáles considera son críticos

la emisión de los pagos.

8) Si los procesos anteriores sufren una interrupción, ¿qué otros procesos pueden verse afectados y a qué otras Áreas se puede afectar?

El suministro de insumos de la Caja Costarricense Seguro Social por parte de los proveedores.

9) ¿Qué herramientas (hardware-software) necesita para llevar a cabo sus funciones?

- [x] Monitor-Teclado-CPU
- [ ] Sistemas de información
- [x] Impresora
- [ ] Aplicaciones de Office
- [ ] Otros _____

10) ¿Sabe qué son controles físicos?

- [ ] Si, amplíe su respuesta _____
- [x] No

11) ¿Sabe qué son controles lógicos?

- [x] Si, amplíe su respuesta uso de contraseña y datos a nivel informático
- [ ] No

12) ¿Sabe qué son activos de información?

- [x] Si, por favor detállelos base de datos, claves, software, correo
- [ ] No

13) Ante una amenaza a un activo de información, ¿qué controles aplicaría?

uso de antivirus y software de seguridad

14) ¿Hace cuánto tiempo utiliza su equipo de cómputo?

- ☐ De 1 a 3 años
- ☒ De 4 a 6 años
- ☐ De 6 años o más

15) ¿Por lo general cuánto tiempo espera al momento de presentarse una interrupción en alguno de los procesos?

- ☐ De 10 a 30 minutos
- ☐ De 31 a 59 minutos
- ☒ De 1 a 3 horas
- ☐ Más de 3 horas

16) ¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?

- ☐ Muy frecuentemente
- ☐ Frecuentemente
- ☒ Poco frecuentemente
- ☐ Nunca

17) ¿Conoce qué hacer en caso de presentarse una interrupción o daño en su equipo?

- ☒ Si
- ☐ No

Muchas gracias por su cooperación.

Subárea Gestión de Pagos	**Encuesta “Plan de Continuidad en TIC”**

Saludos estimados colaboradores:

Por medio de este formulario se desea recopilar su opinión sobre el Plan de Continuidad en TIC.

Por favor conteste el siguiente cuestionario con toda sinceridad. Sus respuestas son confidenciales.

Marque una ☒ en el espacio que corresponda o conteste de forma amplia cada pregunta.

Fecha:11 _____/_11____/_____2021__

Encargado del proceso:

Melanie Orias Garbanzo

1) ¿Sabe usted qué es un plan de continuidad en TIC?

   X Si

   ☐ No

2) ¿Qué es para usted un Plan de Continuidad en TIC?

   _Un plan de acción en caso de alguna situación de urgencia ocurra y se necesite accesar a servicios o plataformas software de las tecnologías de infamación
   _____
   _____
   _____

3) ¿En la Subárea Gestión de Pagos existe un Plan de Continuidad en TIC?

☐ Si

X No

4) De acuerdo al proceso que usted realiza, ¿existen respaldos?

X Si, indique donde se encuentran _____ONE DRIVE_____

☐ No

5) Describa con sus propias palabras, qué es un riesgo y cómo mitigarlo.

Posibilidad constante que se pierda o interrupción de un servicio. Ausencia a programas institucionales instalados en computadoras

Yo siento que todo debe estar en plataforma web_____
_____
_____
_____

6) ¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?

X Si, por favor detállelos: _____Pagos créditos directos, _____

☐ No

7) Dentro de los procesos a su cargo, cuáles considera son críticos

Pagos a procesos judiciales y procesos hipotecarios_____
_____
_____
_____
_____

8) Si los procesos anteriores sufren una interrupción, ¿qué otros procesos pueden verse afectados y a qué otras Áreas se puede afectar?

Dirección Jurídica y la Subárea Gestión de Crédito IVM_____

9) ¿Qué herramientas (hardware-software) necesita para llevar a cabo sus funciones?

X Monitor-Teclado-CPU

X Sistemas de información

X Impresora

X Aplicaciones de Office

☐ Otros _____

10) ¿Sabe qué son controles físicos?

☐ Si, amplíe su respuesta_____

X No

11) ¿Sabe qué son controles lógicos?

☐ Si, amplíe su respuesta_____

X No

12) ¿Sabe qué son activos de información?

X Si, por favor detállelos_____CPU, LAPTOS , Monitores, UPS, Impresora

☐ No

13) Ante una amenaza a un activo de información, ¿qué controles aplicaría?

un virus, antivirus, un riesgo externo un robo o estén en un ambiente delicado sin aire acondicionado, no Conectados a UPS, darle las condiciones adecuadas físicas en lo posible.

14) ¿Hace cuánto tiempo utiliza su equipo de cómputo?

X De 1 a 3 años

☐ De 4 a 6 años

☐ De 6 años o más

15) ¿Por lo general cuánto tiempo espera al momento de presentarse una interrupción en alguno de los procesos?

☐ De 10 a 30 minutos

X De 31 a 59 minutos

☐ De 1 a 3 horas

☐ Más de 3 horas

16) ¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?

☐ Muy frecuentemente

X Frecuentemente

☐ Poco frecuentemente

☐ Nunca

17) ¿Conoce qué hacer en caso de presentarse una interrupción o daño en su equipo?

☐ Si

X No

Muchas gracias por su cooperación.

Subárea Gestión de Pagos	**Encuesta "Plan de Continuidad en TIC"**

Saludos estimados colaboradores:

Por medio de este formulario se desea recopilar su opinión sobre el Plan de Continuidad en TIC.

Por favor conteste el siguiente cuestionario con toda sinceridad. Sus respuestas son confidenciales.

Marque una ☒ en el espacio que corresponda o conteste de forma amplia cada pregunta.

Fecha:noviembre18 _____/11_____/2021_____

Encargado del proceso: ___Jorge Rolando Rivera Porras _____

1) ¿Sabe usted qué es un plan de continuidad en TIC?

☐ Si

X☐ No

2) ¿Qué es para usted un Plan de Continuidad en TIC?
Es una ayuda para pequeñas y medianas empresas
_____
_____
_____

3) ¿En la Subárea Gestión de Pagos existe un Plan de Continuidad en TIC?

☐ Si

X☐ No

4) De acuerdo al proceso que usted realiza, ¿existen respaldos?

☐ Si, indique donde se encuentran _____

☐**X** No

5) Describa con sus propias palabras, qué es un riesgo y cómo mitigarlo.
Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra pérjuicio o daño
_____
_____
_____
_____
_____

6) ¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?

☐ Si, por favor detállelos: _____

☐**X** No

7) Dentro de los procesos a su cargo, cuáles considera son críticos

__ninguno_____
_____
_____
_____
_____

8) Si los procesos anteriores sufren una interrupción, ¿qué otros procesos pueden verse afectados y a qué otras Áreas se puede afectar?

_____no
sabria_____
_____
_____

9) ¿Qué herramientas (hardware-software) necesita para llevar a cabo sus funciones?

X☐ Monitor-Teclado-CPU

☐ Sistemas de información

☐ Impresora

☐ Aplicaciones de Office

☐ Otros _____

10) ¿Sabe qué son controles físicos?

X☐ Si, amplíe su respuesta es la implementación de medidas de seguridad en una estructura definida usada para prevenir o detener el acceso no autorizado a material confidencial. _____

☐ No

11) ¿Sabe qué son controles lógicos?

X☐ Si, amplíe su respuesta_es un dispositivo electrónico que recibe n varialbles binarias de entrada y produce m variables binarias de salida diseñado con el objetivo de controlar productos y procesos industriales _____

☐ No

12) ¿Sabe qué son activos de información?

☐ Si, por favor detállelos_____

☐X No

13) Ante una amenaza a un activo de información, ¿qué controles aplicaría?

_no se
_____

14) ¿Hace cuánto tiempo utiliza su equipo de cómputo?

☐ De 1 a 3 años

☐ De 4 a 6 años

☐X De 6 años o más

15) ¿Por lo general cuánto tiempo espera al momento de presentarse una interrupción en alguno de los procesos?

☐ De 10 a 30 minutos

☐ De 31 a 59 minutos

☐X De 1 a 3 horas

☐ Más de 3 horas

16) ¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?

☐ Muy frecuentemente

☐ Frecuentemente

☐X Poco frecuentemente

☐ Nunca

17) ¿Conoce qué hacer en caso de presentarse una interrupción o daño en su equipo?

☐ Si

☐X No

Muchas gracias por su cooperación.

Subárea Gestión de Pagos	**Encuesta “Plan de Continuidad en TIC”**

Saludos estimados colaboradores:

Por medio de este formulario se desea recopilar su opinión sobre el Plan de Continuidad en TIC.

Por favor conteste el siguiente cuestionario con toda sinceridad. Sus respuestas son confidenciales.

Marque una ☒ en el espacio que corresponda o conteste de forma amplia cada pregunta.

Fecha: _15___/__11___/_2021_____

Encargado del proceso: Paulina Brenes Quesada

1. ¿Sabe usted qué es un plan de continuidad en TIC?

   X Si NO

1. ¿Qué es para usted un Plan de Continuidad en TIC?

   Es un documento o un plan logístico, para la práctica de cómo se debe recuperar y restaurar las funciones parcial o totalmente interrumpidas

1. ¿En la Subárea Gestión de Pagos existe un Plan de Continuidad en TIC?

   ☐ Si
   X No

1. De acuerdo al proceso que usted realiza, ¿existen respaldos?

   X Si, indique donde se encuentran

   ☐ No

1. Describa con sus propias palabras, qué es un riesgo y cómo mitigarlo.

Riesgo es la posibilidad una amenaza que se convierta en un desastre, pero si se juntan se convierte en un riesgo, admitiendo que un riesgo si se puede solucionar

1. ¿Sabe cuáles son los servicios críticos de la Subárea Gestión de Pagos?

   X Si, por favor detállelos: Accidentes, Caídas físicas y de objetos, contactos eléctricos fatiga mental, golpes o choques contra objetos

1. Dentro de los procesos a su cargo, cuáles considera son críticos

   Las caídas accidentales, golpes, fatiga mental

1. Si los procesos anteriores sufren una interrupción, ¿qué otros procesos pueden verse afectados y a qué otras Áreas se puede afectar?

   La electricidad, computadoras, ascensores y otros

1. ¿Qué herramientas (hardware-software) necesita para llevar a cabo sus funciones?

   ☐ Monitor-Teclado-CPU

   ☐ Sistemas de información

   ☐ Impresora

   ☐ Aplicaciones de Office

   ☐ Otros Todas las anteriores

1. ¿Sabe qué son controles físicos?

   ☐ Si, amplíe su respuesta, Es la implementación de medidas dé seguridades una estructura o edificio

   ☐ No

1. ¿Sabe qué son controles lógicos?

X Si, amplíe su respuesta: Dispositivo electrónico, que recibe varias entradas y produce varias salidas

☐ No

1. ¿Sabe qué son activos de información?

X Si por favor detállelos Base de datos , archivos físicos, sistemas de información cableado, redes, dispositivos, etc.

☐ No

1. Ante una amenaza a un activo de información, ¿qué controles aplicaría?

Riesgos físicos, riesgos biológicos, riesgos químicos

Salto de página

1. ¿Hace cuánto tiempo utiliza su equipo de cómputo?

☐ De 1 a 3 años

☐ De 4 a 6 años

X De 6 años o más

1. ¿Por lo general cuánto tiempo espera al momento de presentarse una interrupción en alguno de los procesos?

X De 10 a 30 minutos

☐ De 31 a 59 minutos

☐ De 1 a 3 horas

☐ Más de 3 horas

1. ¿Con qué frecuencia se presenta una interrupción en los servicios de la Subárea?

☐ Muy frecuentemente

☐ Frecuentemente

X Poco frecuentemente

☐ Nunca

1. ¿Conoce qué hacer en caso de presentarse una interrupción o daño en su equipo?

X Si

☐ No

Muchas gracias por su cooperación.