PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

Anexos

Stephany Candy Canchari Pastor

ASESOR: Moisés Antonio Villena Aguilar

Lima, abril de 2014

Tabla de contenido

Anexos

1. Anexo1: Principales Desastres Naturales 2006 – 2011

PRINCIPALES DESASTRES NATURALES - AÑO 2006							
FENÓMENO	EMERGENCIA	DAÑOS PERSONALES				DAÑOS MATERIALES	
		DAMNIFICADOS	AFECTADOS	HERIDOS	FALLECIDOS	VIVIENDAS AFECTADAS	VIVIENDAS DESTRUIDAS
TOTAL	627.000	1,364.595	230.080	99.000	17.000	1,185.501	514.315
Aluvión	4.000	12.000	9.000		3.000	2.000	3.000
Desplazamiento	158.000	1.267	21.450	4.000	1.000	266.000	235.000
Huayco	73.000	908.000	69.335	1.000	3.000	293.000	55.000
Inundación	348.000	6.328	115.648		9.000	12.501	1.315
Maretazo	12.000	71.000	13.031			230.000	10.000
Sismo	32.000	366.000	1.616	94.000	1.000	382.000	210.000

Figura 1.1. Principales Desastres Naturales en el 2006. (INDECI 2007)

PRINCIPALES DESASTRES NATURALES - AÑO 2007							
FENÓMENO	EMERGENCIA	DAÑOS PERSONALES				DAÑOS MATERIALES	
		DAMNIFICADOS	AFECTADOS	HERIDOS	FALLECIDOS	VIVIENDAS AFECTADAS	VIVIENDAS DESTRUIDAS
TOTAL	654.000	1,967.037	324.647	97.046	539.000	1,235.518	1,721.683
Aluvión	2.000	75.000					14.000
Desplazamiento	126.000	1,468.000	17.093		2.000	474.000	296.000
Huayco	53.000	3.302	7.236	83.000	9.000	712.000	474.000
Inundación	272.000	4.517	64.535	12.000	4.000	8.308	848.000
Maretazo	1.000						
Sismo	200.000	416.218	235.783	2.046	524.000	41.210	89.683

Figura 1.2. Principales Desastres Naturales en el 2007. (INDECI 2008)

PRINCIPALES DESASTRES NATURALES - AÑO 2008							
FENÓMENO	EMERGENCIA	DAÑOS PERSONALES				DAÑOS MATERIALES	
		DAMNIFICADOS	AFECTADOS	HERIDOS	FALLECIDOS	VIVIENDAS AFECTADAS	VIVIENDAS DESTRUIDAS
TOTAL	450.000	964.504	1,656.838	47.000	9.000	234.124	421.816
Aluvión	5.000	171.000	417.000			5.000	152.000
Desplazamiento	128.000	1.333	82.524	8.000	6.000	68.000	39.000
Huayco	50.000	492.000	76.106	4.000	1.000	99.000	147.000
Inundación	242.000	8.171	105.208	10.000	1.000	1.124	19.816
Maretazo	1.000		44.000				10.000
Sismo	24.000	292.000	932.000	25.000	1.000	61.000	54.000

Figura 1.3. Principales Desastres Naturales en el 2008. (INDECI 2009)

PRINCIPALES DESASTRES NATURALES - AÑO 2009							
FENÓMENO	EMERGENCIA	DAÑOS PERSONALES				DAÑOS MATERIALES	
		DAMNIFICADOS	AFECTADOS	HERIDOS	FALLECIDOS	VIVIENDAS AFECTADAS	VIVIENDAS DESTRUIDAS
TOTAL	412.000	2,148.000	41,026.000	244.000	114.000	655.000	9,432.000
Aluvión	5.000	18.000	12.000	1.000			148.000
Desplazamiento	116.000	459.000	382.000	92.000	31.000	152.000	1,879.000
Huayco	64.000	188.000	530.000	3.000	17.000	76.000	932.000
Inundación	219.000	1,309.000	39,581.000	136.000	66.000	427.000	5,792.000
Maretazo							
Sismo	8.000	174.000	521.000	12.000			681.000

Figura 1.4. Principales Desastres Naturales en el 2009. (INDECI 2010)

PRINCIPALES DESASTRES NATURALES - AÑO 2010							
FENÓMENO	EMERGENCIA	DAÑOS PERSONALES				DAÑOS MATERIALES	
		DAMNIFICADOS	AFECTADOS	HERIDOS	FALLECIDOS	VIVIENDAS AFECTADAS	VIVIENDAS DESTRUIDAS
TOTAL	402.000	20,059.000	103,312.000	94.000	60.000	2,877.000	14,983.000
Aluvión	10.000	1,375.000	2,584.000	1.000	7.000	280.000	518.000
Desplazamiento	92.000	2,542.000	7,329.000	59.000	47.000	462.000	
Huayco	60.000	6,090.000	22,626.000	32.000	3.000	336.000	924.000
Inundación	216.000	9,720.000	68,964.000	1.000	3.000	1,750.000	13,126.000
Maretazo	7.000	160.000					35.000
Sismo	17.000	172.000	1,809.000	1.000		49.000	380.000

Figura 1.5. Principales Desastres Naturales en el 2010. (INDECI 2011)

PRINCIPALES DESASTRES NATURALES - AÑO 2011							
FENÓMENO	EMERGENCIA	DAÑOS PERSONALES				DAÑOS MATERIALES	
		DAMNIFICADOS	AFECTADOS	HERIDOS	FALLECIDOS	VIVIENDAS AFECTADAS	VIVIENDAS DESTRUIDAS
TOTAL	406.000	117,548.000	284,449.000	76.000	37.000	10,964.000	53,694.000
Aluvión	5.000	67.000	600.000			14.000	120.000
Desplazamiento	141.000	614.000	8,861.000	51.000	27.000	426.000	1,065.000
Huayco	43.000	945.000	35,422.000	7.000	8.000	190.000	380.000
Inundación	156.000	113,100.000	224,464.000	18.000	2.000	10,315.000	48,643.000
Maretazo	20.000		1,839.000				447.000
Sismo	41.000	2,822.000	13,263.000			19.000	3,039.000

Figura 1.6. Principales Desastres Naturales en el 2011. (INDECI 2012)

2. Anexo 2: Líneas de Negocio Genéricas para empresas de Seguros

NIVEL 1	NIVEL 2	Definición
Ramos generales	Incendio y Domiciliario	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Incendios - Líneas Aliadas Incendio - Lucro Cesante - Cristales - Terremoto - Domiciliario
	Ramos Técnicos	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Todo riesgo para contratistas - Rotura de maquinaria - Lucro cesante de Rotura de maquinaria - Montaje contra todo riesgo - Todo riesgo equipo electrónico - Todo riesgo equipo para contratistas - Calderas
	Robo, Bancos y 3D	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Robo y asalto - Deshonestidad frente a la empresa - Comprensivo contra deshonestidad - Seguro de Bancos
	Responsabilidad civil	Se refiere a pólizas emitidas por responsabilidad civil
	Cascos, Transportes y Aviación	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Transportes - Marítimo – Cascos

NIVEL 1	NIVEL 2	Definición
		- Aviación
	Autos y SOAT	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Vehículos - Líneas aliadas vehículos - SOAT
	Accidentes personales	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Accidentes personales - Escolares
	Asistencia médica	Se refiere a pólizas emitidas por asistencia médica
	Otros	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Cauciones - Crédito Interno - Crédito a la exportación - Multiseguros - Agrícola - Misceláneos - Animales
Ramos de vida	Seguros de Vida en Grupo	Se refiere a las siguientes pólizas: - Seguro de Vida en Grupo Particular - Seguro de Vida para Trabajadores - Seguro de Desgravamen - Seguro de Vida Individual de Corto Plazo - Sepelio de Corto Plazo
	Seguros de Vida Individual y Rentas	Se refiere a las siguientes pólizas: - Seguro de Vida Individual de Largo Plazo

NIVEL 1	NIVEL 2	Definición
		- Sepelio de Largo Plazo - Seguro de Vida para ex - Trabajadores - Renta Particular - Pensiones del Seguro Complementario de Trabajo de Riesgo - Renta de Jubilación - Pensión de Invalidez - Pensión de Sobrevivencia - Pensión de Invalidez-Régimen Temporal - Pensión de Sobrevivencia-Régimen Temporal
	Seguros Previsionales y SCTR	Se refiere a las siguientes pólizas: - Seguro Complementario de Trabajo de Riesgo - Invalidez - Sobrevivencia - Gastos de Sepelio
Finanzas corporativas	Finanzas corporativas	Deuda subordinada, emitir acciones, ofertas públicas iniciales y colocaciones en mercado secundario, fideicomiso
Negociación y ventas	Negociación y ventas	Renta fija, renta variable, divisas, posiciones propias en valores, operaciones con pacto de recompra.
Créditos	Créditos	Fianzas, créditos hipotecarios para trabajadores.

3. Anexo 3: Principios Básicos de la Superintendencia de Banca y Seguros

Principio de Regulación

A través de ésta, pretende crear un sistema de incentivos que propicie que las decisiones privadas de las empresas estén alineadas con el objetivo de lograr que los sistemas bajo supervisión adquieran solidez e integridad para mantener su solvencia y estabilidad. Para que este enfoque se pueda desarrollar en la práctica la SBS se apoya en 4 principios básicos relacionados:

La calidad de los participantes del mercado, Si se desea que los sistemas gocen de solidez e integridad, entonces es necesario asegurar que quienes operan en el mercado sean personas de solvencia moral, económica y que demuestren capacidad de gestión.

La calidad de la información y análisis que respalda las decisiones de las empresas supervisadas, poniendo énfasis en la necesidad de aplicar sistemas que les permitan identificar, medir, controlar y monitorear sus riesgos de una manera eficiente.

La información que revelan las empresas supervisadas para que otros agentes económicos tomen decisiones, basada en el principio de la transparencia con el propósito de que las decisiones sean óptimas y fomenten una disciplina de mercado, se requiere que la información sea correcta, confiable y oportuna.

La claridad de las reglas de juego, basada en el principio de la ejecutabilidad. Este principio persigue que las normas dictadas por la SBS sean de fácil comprensión, exigibles y que puedan ser supervisadas.

Principio de Supervisión

Significa que la SBS pretende implementar un enfoque de supervisión por tipo de riesgo. Este principio se orienta hacia una supervisión integral que genere una apreciación sobre la administración de los riesgos por parte de las empresas supervisadas. Por otro lado, una supervisión discrecional se refiere a que el contenido, alcance y frecuencia de la supervisión debe estar en función del diagnóstico de los riesgos que enfrenta cada empresa supervisada.

La estrategia de supervisión de la SBS se desarrolla en dos frentes. El primero consiste en la supervisión que ejerce directamente sobre las empresas y el segundo se basa en

participación de los colaboradores externos, tales como los auditores, las empresas clasificadoras de riesgo, supervisores locales y de otros países.

4. Anexo 4: Resolución SBS N° 2115 – Capítulos

Capítulo I – Principios generales, donde establece que las disposiciones de la presente norma son aplicables a las empresas comprendidas en el artículo 16° de la Ley General, los métodos para el cálculo del requerimiento patrimonial efectivo por riesgo operacional y el proceso de autorización ante la Superintendencia.

Capítulo II – Método del Indicador Básico, definiendo el indicador de exposición por riesgo operacional el "margen bruto operacional" de la empresa indicando las cuentas contables a ser usadas así como el proceso para el cálculo del requerimiento patrimonial y algunas consideraciones especiales para empresas con menos de 36 meses de operación.

Capítulo III – Método alternativo estándar, dividiendo las actividades de las empresas en líneas de negocio, y en función a ello, estableciendo los indicadores de exposición por riesgo operacional y el cálculo de requerimiento patrimonial así como algunas consideraciones especiales para empresa que cuenten con menos de 36 meses de operación.

Capítulo IV – Métodos avanzados, determinando que las empresas autorizadas a utilizar este método calcularán el requerimiento patrimonial mediante un sistema interno de medición del riesgo operacional. Especifica los requisitos cualitativos y cuantitativos para el uso éste método, así como las disposiciones para reconocer el efecto reductor del riesgo que generan los seguros en el cálculo del requerimiento patrimonial por riesgo operacional.

5. Anexo 5: Resolución SBS N° 2116 – Capítulos

Capítulo I – Disposiciones generales, donde establece que el reglamento será de aplicación a las empresas señaladas en el artículo 16° y 17° de la Ley General. Define el riesgo operacional, los factores que lo originan y los eventos de pérdida.

Capítulo II – Roles y responsabilidades, específicamente del Directorio, la Gerencia, Comité de riesgos y la Unidad de riesgos.

Capítulo III – La gestión de riesgo operacional, estableciendo los aspectos mínimos que deberá contemplar un manual de gestión de riesgo operacional. Define la metodología y los criterios a cumplirse además de la implicancia de la seguridad de la información para que la operatividad del negocio continúe de manera razonable ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Capítulo IV – Requerimientos de información, dando como referencia para el contenido mínimo del informe a la Superintendencia al “Manual del IG-ROp”, aclarando además que como ente regulador podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de la gestión del riesgo operacional.

Capítulo V – Colaboradores externos, definiendo a la Unidad de Auditoría Interna, las Sociedades de Auditoría Externa y las empresas Clasificadoras del Riesgo como entes que verifiquen y aseguren el cumplimiento del reglamento.

6. Anexo 6: Los 3 Pilares de Basilea II

<table>
<tr><td rowspan="6">Pilar I</td><td colspan="2">Requerimientos Mínimos de Capital</td><td colspan="2">Se calculan en base a los activos ponderados por su riesgo, con nuevos criterios que reflejen de manera más ajustada el cambio en el perfil de riesgo de las entidades.</td></tr>
<tr><td colspan="4">Los riesgos a considerar son tres:</td></tr>
<tr><td rowspan="3"></td><td rowspan="2">Riesgo de Crédito</td><td>Método Estandarizado (EE)</td><td>Similar al Acuerdo vigente, pero introduce más categorías de riesgo y posibilidad de evaluaciones de riesgo otorgadas por agencias externas (ECAIs y ECAs).</td></tr>
<tr><td>Método Basado en Calificaciones Internas (IR)</td><td>Se proponen dos variantes:
1) <u>Básico</u> (FIRB): Los bancos estiman sólo la probabilidad de incumplimiento (o default) para cada activo. Los otros indicadores y ecuaciones son provistos por el Comité de Basilea.
2) <u>Avanzado</u> (AIRB): los bancos estiman todos los indicadores cuantitativos que requieren las ecuaciones desarrolladas por el Comité de Basilea.</td></tr>
<tr><td>Riesgo de Mercado</td><td colspan="2">No se modifica el Acuerdo vigente</td></tr>
<tr><td>Riesgo Operativo</td><td colspan="2">Se considera en particular este riesgo que estaba implícito en los otros riesgos del Acuerdo vigente.
Se permiten tres métodos de cálculo:
1) Indicador básico,
2) Estándar y
3) Avanzado (AMA)</td></tr>
</table>

Pilar II	Proceso de Supervisión Bancaria	Se le otorga un rol fundamental y los principios básicos son: 1) Los bancos deberán contar con un proceso para evaluar la suficiencia de capital total en función de su perfil de riesgo y con una estrategia de mantenimiento de sus niveles de capital. 2) Los supervisores deberán examinar las estrategias y evaluaciones internas de la suficiencia de capital de los bancos así como la capacidad de estos para vigilar y garantizar su cumplimiento y deberán intervenir cuando no queden satisfechos con el resultado. 3) Los supervisores deberán esperar que los bancos operen por encima de los coeficientes mínimos de capital y deberán tener la capacidad de exigirles que mantengan capital por encima del mínimo. 4) Los supervisores deberán intervenir con prontitud para evitar que el capital descienda por debajo de los mínimos y deberán exigir la inmediata adopción de medidas correctivas.
Pilar III	Disciplina de Mercado	Se establecen requerimientos de divulgación de la información con el objetivo de permitir a los participantes del mercado evaluar el perfil de riesgo del banco. Esto por cuanto los nuevos métodos de estimación de riesgo que se introducen dependen en mayor medida de las estimaciones de las propias entidades.

7. Anexo 7: Formas aproximadas de resolver el problema

a. Deloitte Touche Tohmatsu Limited

Ofrece una gama completa de servicios objetivos de continuidad de negocio, aprovechando su red mundial, las iniciativas de investigación, buenas prácticas y su experiencia (DELOITTE TTL. 2012).

Cuenta con profesionales certificados a nivel mundial con componentes orientados a la seguridad y a la continuidad del negocio. Sus servicios incluyen:

- Análisis de la situación actual de la administración de la continuidad.
- Análisis de riesgos (RIA)
- Análisis de impacto en el negocio (BIA)
- Plan de recuperación de desastres (DRP)
- Plan de continuidad del negocio (BCP)

b. Protiviti – Risk and Business Consulting

Firma de consultoría global que asiste a las empresas en los siguientes ámbitos (PROTIVITI 2012):

Riesgos de negocio

Brinda a sus clientes herramientas y experiencia para entender los riesgos a través de las siguientes soluciones:

- Evaluación del Riesgo Operacional.
- Manejo del Riesgo Crediticio.
- Enterprise Risk Management.
- Gestión de Continuidad de Negocio.
- Soluciones para la Recuperación de Costos (Cost Recovery Solutions).
- Supply Chain Risk Consulting.

Riesgos de TI

Ayuda a sus clientes a identificar, localizar el origen, medir, manejar, implementar y monitorear los riesgos a través de las siguientes soluciones:

- Evaluación de Riesgo Tecnológico

- Plan de Recuperación ante Desastres
- Seguridad de la Información
- Auditoria de Sistemas de Información
- Auditoría en la Gestión de TI
- Administración de Riesgos en Proyectos
- ITIL - Information Technology Infrastructure Library
- Administración de cambios Tecnológicos
- Planificación de los Recursos de Infraestructura Tecnológica

c. IBM – Continuidad empresarial

Sus servicios ofrecen a las empresas diversas opciones que puedan construir la resiliencia adecuada con el objetivo de anticipar los impactos potenciales de una amplia gama de amenazas. Los especialistas en continuidad empresarial de IBM han identificado tres categorías de amenazas que deben ser abordadas en un programa de continuidad. Su portfolio aborda las tres categorías: dirigida a las empresas, a los datos y a los eventos (IBM 2012).

d. Business Development Association

Ofrece los siguientes servicios de planificación para la continuidad del negocio y operaciones (BUSINESS DEVELOPMENT ASSOCIATION 2012):

- **Evaluación de riesgo:**
  Para determinar el riesgo cuantitativo y cualitativo de una organización. Los consultores utilizan datos primarios, simulaciones y técnicas de modelaje para llevar a cabo la evaluación de riesgo.

- **Análisis de impacto de negocio (BIA):**
  Utiliza su herramienta CONTINUUM en el Análisis de Impacto del Negocio para realizar el BIA para los clientes. Continuum, una herramienta de encuesta, se utiliza para identificar funciones, procesos, vendedores, archivos vitales y recursos de mayor importancia.

- **Planificación de continuidad del negocio/Desarrollo de plan de continuidad de operaciones:**
  Un desarrollo robusto requiere un Plan de continuidad del negocio o Plan de continuidad de operaciones para un nivel corporativo o global tanto como para

un nivel departamental. Estos incluyen infraestructura de mando y control, respuesta a emergencia, procedimientos de intensificación para planes de activación o de departamentos.

- **Planificación de recuperación de desastres (DP):**
  Dictando cómo y cuándo se podrá restablecer la tecnología después de cualquier tipo de interrupción y define cómo continuar los sistemas informáticos más críticos y operaciones para preparar a responder a desastres.

- **Capacitación y promoción de conciencia de la planificación de la continuidad del negocio:**
  Los consultores desarrollan un plan de capacitación y de promoción de conciencia que sea apropiado para las necesidades específicas de cada organización. Los servicios varían de sesiones de capacitación para personal clave a técnicas innovadoras para asegurar que todos los empleados estén listos a responder y sepan seguir el protocolo de un plan después de cualquier tipo de interrupción.

- **Evaluación del plan de continuidad del negocio:**
  Ayudan a desarrollar e implementar ejercicios de evaluación que incluyen ejercicios de mesa, prácticas repetidas, evaluaciones funcionales para organizaciones y tenedores de apuestas y simulaciones. Además, diseñan evaluaciones para cumplir con los requisitos federales NIMS para el gobierno americano.

- **Auditoría del plan de continuidad del negocio:**
  En respuesta a la gran cantidad de agencias y empresas deciden enfocar su atención en el desarrollo de un plan extensivo para la continuidad del negocio o la continuidad de operaciones, los consultores ayudan a los clientes a desarrollar Planes de Continuidad del Negocio para cumplir con todas las regulaciones y estándares.

8. Anexo 8: Productos Comerciales para resolver el problema

a. Shadow - Planner

Paquete de software planificador diseñado para que la continuidad de negocio funcione en una organización. Este producto guía al usuario a través de todo el proceso de planificación de la continuidad del negocio además de la protección continua de los recursos de las organizaciones, ya sean tangibles o intangibles (ICM 2012).

b. Business Protector

Software de apoyo en el planeamiento que contiene un conjunto completo de plantillas basadas en metodologías estándar de la industria. Está basado en la web proporcionando una plataforma a la que se puede acceder de cualquier computadora conectada a internet (BPSi 2012). Cuenta con las siguientes ediciones: Standard Edition, Enterprise Edition, Credit Unions, Community Banks y Public Sector.

c. TAMP DRS – Smartphone App

Permite a sus usuarios acceder a la documentación del plan de gestión de la continuidad y otras funcionalidades clave como (TAMP SYSTEMS 2012)

- Acceder a la información publicada.
- Apoyo en la gestión de desastres.
- Apoyo en la respuesta ante incidentes.
- Comunicación en tiempo real.
- Gestión de las tareas de recuperación en tiempo real.

d. Continuum BCP

Software que incluye un módulo de encuesta que se puede personalizar para organizaciones de cualquier tamaño y les permite a los usuarios la posibilidad de agregar tantas unidades de negocios como sea necesario.

La herramienta permite a los propietarios del proceso el ingreso a la aplicación y a los datos sobre su unidad de negocio, incluyendo información sobre procesos, personal, vendedores, dependencias de archivos críticos, y recursos necesarios para seguir con las operaciones críticas en un sitio alternativo durante una interrupción.

Además, colecciona y almacena todos los datos de cada unidad de negocio y automáticamente desarrolla una serie de reportes que se puede descargar en formato

de Microsoft Word y Excel. También facilita el análisis de datos a través de algoritmos internos tanto como el uso estratégico de puntos asignados para las aportaciones del gerente. La aplicación tiene un mecanismo de seguimiento interno que le permite al gerente el monitoreo del progreso del análisis del impacto de negocio (BUSINESS DEVELOPMENT ASSOTIATION 2012).

9. Anexo 9: Cuadro comparativo de formas aproximadas de resolver el problema

Criterios	Shadow Planner	Business Protector	TAMP DRS	Continuum BCP
Etapa del proyecto que soportan	Planificación			
Tipo	✓ Web ✓ Móvil	✓ Web	✓ Móvil	✓ Móvil
Acceso a demo	✓ Sí	✓ No	✓ Sí	✓ Sí
Principales módulos	✓ Análisis de Impacto de Negocio. ✓ Planificación de Continuidad de Negocio. ✓ Comunicaciones. ✓ Móvil.	✓ Análisis de Impacto de Negocio. ✓ Planificación de Continuidad de Negocio. ✓ Gestión de Crisis. ✓ e-Learning. ✓ Gestión de Dashboards.	✓ Análisis de Impacto de Negocio. ✓ Planificación de Continuidad de Negocio. ✓ Gestión de Crisis.	✓ Análisis de Impacto de Negocio. ✓ Planificación de Continuidad de Negocio. ✓ Anásis de información. ✓ Reportes
Ventajas	✓ Accesible vía móvil y web. ✓ Incluye herramientas de notificación de alarmas.	✓ Infraestructura segura de datos. ✓ Incluye plantillas basadas en metodologías estándar.	✓ Transmisión de voz y texto en tiempo real.	✓ Uso de algoritmos para el análisis de información. ✓ Gracias a las encuestas, permite la participación activa de los integrantes

Criterios	Shadow Planner	Business Protector	TAMP DRS	Continuum BCP
				de la empresa. ✓ Escalabilidad, al permitir la creación de unidades de negocio dependiendo del tamaño de la empresa.

10. Anexo 10: Mapeo de los resultados esperados con las herramientas, métodos y procedimientos seleccionados

Resultados esperado	Herramientas a usarse
Resultado 1 para el OE1: Metodología para la identificación de procesos vitales de continuidad de negocio.	**ISO/IEC 22301:2012 "Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio"**, es una norma internacional que especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión de continuidad documentado.
Resultado 2 para el OE1: Listado de los procesos, productos y/o servicios críticos para la continuidad clasificados por líneas de negocio.	
Resultado 1 para el OE2: Modelado de los procesos de negocio identificados como críticos para la continuidad	**Business Process Modeling Notation** o **BPMN** (**Notación para el Modelado de Procesos de Negocio**) es una notación gráfica estandarizada que permite el modelado de procesos de negocio, en un formato de flujo de trabajo.
Resultado 1 para el OE3: Análisis de impacto de negocio definiendo los requerimientos de recuperación en caso de la ocurrencia de un sismo.	**ISO/IEC 22301:2012 "Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio"**, es una norma internacional que especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión de continuidad documentado.
Resultado 1 para el OE4: Análisis de riesgos considerando como escenario la ocurrencia de un sismo.	**ISO 31000: 2009**, Norma internacional que brinda un framework para el proceso de gestión de riesgo. Puede ser usada por cualquier organización sin importar su tamaño o sector. **NFPA 1600,** norma australiana creada por el Comité de Gestión de Desastres que proporciona una base estandarizada para la planificación y gestión de programas de

Resultados esperado	Herramientas a usarse
	continuidad de negocio en caso de desastres o emergencia en los sectores público y privado.
Resultado 1 para el OE5: Plan de manejo de crisis considerando como escenario la ocurrencia de un sismo.	**ISO/IEC 22301:2012 "Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio"**, es una norma internacional que especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión de continuidad documentado
Resultado 1 para el OE6: Plan de emergencia considerando como escenario la ocurrencia de un sismo.	**NFPA 1600,** norma australiana creada por el Comité de Gestión de Desastres que proporciona una base estandarizada para la planificación y gestión de programas de continuidad de negocio en caso de desastres o emergencia en los sectores público y privado.
Resultado 1 para el OE7: Plan de recuperación de desastres considerando como escenario la ocurrencia de un sismo.	**ISO/IEC 22301:2012 "Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio"**, es una norma internacional que especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión de continuidad documentado.
Resultado 1 para el OE8: Plan de pruebas considerando como escenario la ocurrencia de un sismo.	
Resultado 1 para el OE9: BCP considerando como escenario la ocurrencia de un sismo.	

11. Anexo 11: Plan de Actividades

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
Revisión de tema de tesis	**6 días**	**lun 19/08/13**	**lun 26/08/13**	
Elaboración del documento	2 días	lun 19/08/13	mar 20/08/13	
Revisión del asesor	2 días	mié 21/08/13	jue 22/08/13	2
Elaboración de presentación	2 días	vie 23/08/13	lun 26/08/13	3
Elaboración de metodología de identificación de procesos crítico	**4 días**	**mar 27/08/13**	**vie 30/08/13**	
Elaboración de metodología (R.E 1)	2 días	mar 27/08/13	mié 28/08/13	4
Análisis de resultados de metodología	1 día	jue 29/08/13	jue 29/08/13	6
Consolidado de lista de procesos vitales de continuidad de negoci	1 día	vie 30/08/13	vie 30/08/13	7
Validación de resultados	1 día	vie 30/08/13	vie 30/08/13	7
Entrega de resultado esperado 1 y 2	1 día	lun 02/09/13	lun 02/09/13	9
Elaboración de modelado de procesos	**15 días**	**mar 03/09/13**	**lun 23/09/13**	
Modelado del 30% de procesos	3 días	mar 03/09/13	jue 05/09/13	10
Validación de la empresa	1 día	vie 06/09/13	vie 06/09/13	12
Entrega de avance	1 día	lun 09/09/13	lun 09/09/13	13
Modelado del 60% de procesos	3 días	mar 10/09/13	jue 12/09/13	14
Validación de la empresa	1 día	vie 13/09/13	vie 13/09/13	15
Entrega de avance	1 día	lun 16/09/13	lun 16/09/13	16
Modelado del 100% de procesos	3 días	mar 17/09/13	jue 19/09/13	17
Validación de la empresa	1 día	vie 20/09/13	vie 20/09/13	18
Entrega del modelado de procesos al 100%	1 día	lun 23/09/13	lun 23/09/13	19
Elaboración de análisis de riesgos	**5 días**	**mar 24/09/13**	**lun 30/09/13**	
Entrevista con empresa	1 día	mar 24/09/13	mar 24/09/13	20
Elaboración de análisis	2 días	mié 25/09/13	jue 26/09/13	22
Validación de la empresa	1 día	vie 27/09/13	vie 27/09/13	23
Entrega de análsis de riesgos	1 día	lun 30/09/13	lun 30/09/13	24
Elaboración de BIA	**5 días**	**mar 24/09/13**	**lun 30/09/13**	
Entrevista con empresa	1 día	mar 24/09/13	mar 24/09/13	20
Elaboración de análisis	2 días	mié 25/09/13	jue 26/09/13	27
Validación de la empresa	1 día	vie 27/09/13	vie 27/09/13	28
Entrega de BIA	1 día	lun 30/09/13	lun 30/09/13	29
Elaboración de plan de manejo de crisis	**5 días**	**mar 01/10/13**	**lun 07/10/13**	
Entrevista con empresa	1 día	mar 01/10/13	mar 01/10/13	30
Elaboración de plan	2 días	mié 02/10/13	jue 03/10/13	32
Validación de la empresa	1 día	vie 04/10/13	vie 04/10/13	33
Entrega de análsis de plan	1 día	lun 07/10/13	lun 07/10/13	34
Elaboración de plan de manejo de emergencia	**5 días**	**mar 01/10/13**	**lun 07/10/13**	
Entrevista con empresa	1 día	mar 01/10/13	mar 01/10/13	30
Elaboración de plan	2 días	mié 02/10/13	jue 03/10/13	37
Validación de la empresa	1 día	vie 04/10/13	vie 04/10/13	38
Entrega de análsis de plan	1 día	lun 07/10/13	lun 07/10/13	39
Elaboración de plan de recuperación de desastres	**5 días**	**mar 08/10/13**	**lun 14/10/13**	
Entrevista con empresa	1 día	mar 08/10/13	mar 08/10/13	40
Elaboración de plan	2 días	mié 09/10/13	jue 10/10/13	42
Validación de la empresa	1 día	vie 11/10/13	vie 11/10/13	43
Entrega de análsis de plan	1 día	lun 14/10/13	lun 14/10/13	44
Elaboración de plan de pruebas	**5 días**	**mar 15/10/13**	**lun 21/10/13**	
Entrevista con empresa	1 día	mar 15/10/13	mar 15/10/13	45
Elaboración de plan	2 días	mié 16/10/13	jue 17/10/13	47
Validación de la empresa	1 día	vie 18/10/13	vie 18/10/13	48
Entrega de análsis de plan	1 día	lun 21/10/13	lun 21/10/13	49
Elaboración de BCP	**5 días**	**mar 22/10/13**	**lun 28/10/13**	
Entrevista con empresa	1 día	mar 22/10/13	mar 22/10/13	50
Elaboración de plan	2 días	mié 23/10/13	jue 24/10/13	52
Validación de la empresa	1 día	vie 25/10/13	vie 25/10/13	53
Entrega de análsis de plan	1 día	lun 28/10/13	lun 28/10/13	54

12. Anexo 12: Detalle de Metodología para la identificación de procesos críticos

a. Presentación

Identificación de Procesos Críticos de Continuidad

Objetivo:

Identificar los procesos críticos para la continuidad del negocio en base a los siguientes criterios: Tiempo de interrupción, rentabilidad neta, cumplimiento y reputación.

1. Dar click a ***"Ir al cuestionario"*** de esta hoja y se colocará en la hoja ***"Información"*** en donde encontrará un breve formulario para el registro de los procesos de la unidad/área a la que usted pertenece y/o gestiona.

2. Para empezar, seleccione la línea de negocio y producto asociado de la lista desplegable según el proceso a desarrollar.

3. Para el registro del proceso tiene una lista desplegable donde puede seleccionarlo.

4. A continuación, se realizarán 4 preguntas que nos permitirán evaluar el nivel de criticidad del proceso. Para esto, se pide por favor basarse en fuentes que sustenten la respuesta como por ejemplo:

- Estado de pérdidas y ganancias
- Fujo de Caja
- Balance General
- Contratos
- Dueños del proceso
- Otros relacionados

5. Finalmente podrá observar el resultado del cuestionario en la parte inferior del mismo, para que usted pueda validar si lo obtenido coincide con su criterio.

Ir a cuestionario

b. Información

Datos Generales

Línea de Negocio:	
Producto asociado:	
Nombre del proceso:	

Tiempo de Interrupción

1.¿Cuál es el tiempo máximo durante el cual el proceso puede dejar de funcionar?

a)	Hasta 1 mes.	
b)	Hasta 1 semana.	
c)	Hasta 48 horas.	
d)	Hasta 24 horas.	
e)	Hasta 6 horas.	
f)	El proceso no puede dejar de funcionar.	

Rentabilidad Neta

2. ¿Cuál es el impacto monetario que la empresa dejaría de transaccionar si el proceso sufre una interrupción en un horizonte temporal de aproximadamente un día (24 hrs)?

a)	S/.0 - S/.50,000	
b)	S/.50,001 - S/.100,000	
c)	S/.100,001 - S/.250,000	
d)	S/.250,001 - S/.500,000	
e)	S/.500,001 - S/.1,000,000	
f)	Más de S/.1,000,000	

Cumplimiento

3. En caso de la interrupción total o parcial del proceso, ¿Qué tipo de sanción(es) podría recibir la empresa?

a)	-Incumplimiento de normas internas de la empresa. -Amonestación leve a la empresa por parte de la SBS, SUNAT, MINTRA u otros entes reguladores (**Hasta S/.50,000**). - Incumplimiento de cláusulas contractuales con clientes o terceros con posibilidad de pérdidas menores (**Hasta S/.50,000**) para la empresa.	
b)	-Incumplimiento de normas internas de la empresa. -Amonestación leve a la empresa por parte de la SBS, SUNAT, MINTRA u otros entes reguladores (**Hasta S/.100,000**). - Incumplimiento de cláusulas contractuales con clientes o terceros con posibilidad de pérdidas menores **(Hasta S/.100,000**) para la empresa.	
c)	- Amonestación grave a la empresa por parte de la SBS, SMV, INDECOPI, SUNAT, MINTRA u otros entes reguladores (**Hasta S/.250,000**). - Multa a un director o empleado por parte de la SBS, u otro regulador. - Incumplimiento de cláusulas contractuales con clientes o terceros con posibilidad de demandas (**Hasta S/.250,00**) para la empresa.	
d)	- Amonestación grave a la empresa por parte de la SBS, SMV, INDECOPI, SUNAT, MINTRA u otros entes reguladores (**Hasta S/.500,000**). - Multa a un director o empleado por parte de la SBS, u otro regular. - Incumplimiento de cláusulas contractuales con clientes o terceros con posibilidad de demandas (**Hasta S/.500,000**) para la empresa.	
e)	-Amonestación muy grave a la empresa por parte de la SBS, SMV, INDECOPI, SUNAT, MINTRA u otros (**Hasta S/.1,000,000**). -Condena en proceso penal a directores, gerentes, funcionarios o empleados de la empresa, que podría o no llevarlos a prisión efectiva. -Remoción, suspensión o inhabilitación de directores o empleados de la empresa por parte de la SBS. -Suspensión o cancelación de la autorización de funcionamiento de la empresa, llevando incluso a su disolución y liquidación. -Intervención de la empresa y/o sometimiento a Régimen de Vigilancia.	
f)	-Amonestación muy grave a la empresa por parte de la SBS, SMV, INDECOPI, SUNAT, MINTRA u otros (**Más de S/.1,000,000**). -Condena en proceso penal a directores, gerentes, funcionarios o empleados de la empresa, que podría o no llevarlos a prisión efectiva. -Remoción, suspensión o inhabilitación de directores o empleados de la empresa por parte de la SBS. -Suspensión o cancelación de la autorización de funcionamiento de la empresa, llevando incluso a su disolución y liquidación. -Intervención de la empresa y/o sometimiento a Régimen de Vigilancia.	

Reputación

4. En caso de la interrupción total o parcial del proceso, ¿Qué personas o interesados se verían **más** afectados?

a)	Accionistas	
b)	Proveedores	
c)	Empleados	
d)	Organizaciones Reguladoras	
e)	Imagen Corporativa	
f)	Clientes	

Clasificación:

13. Anexo 13: Resultados de la Evaluación de Criticidad de los Procesos

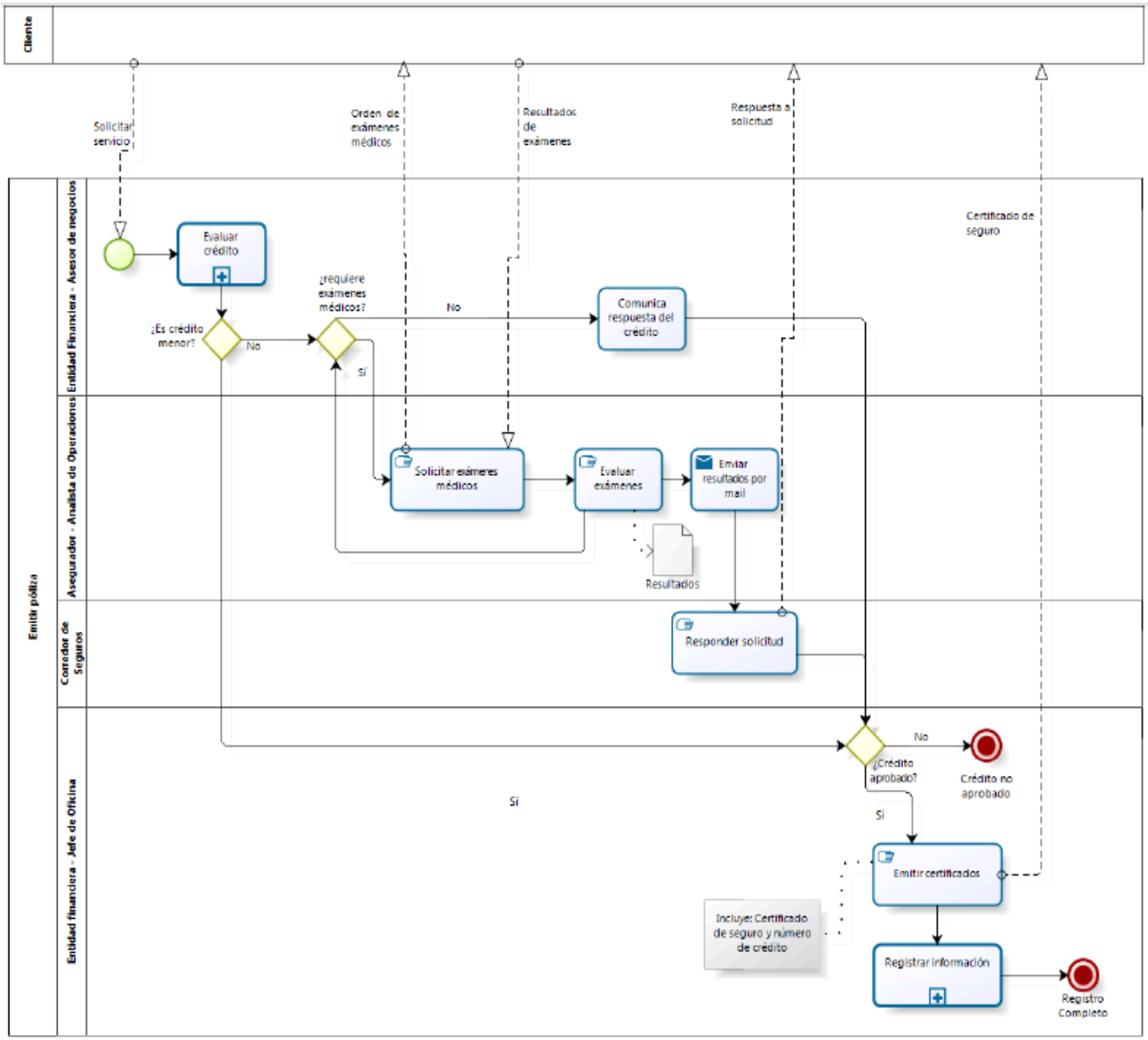
Línea de negocio	Producto	Proceso	Clasificación
Ramos de vida	Desgravamen	Atención de solicitudes de Cobertura	Muy Alto
Ramos de vida	Desgravamen	Suscripción, emisión y registro de información	Muy Alto
Ramos de vida	RV Pensión de Jubilación	Emisión de la póliza y endoso	Alto
Ramos de vida	No aplica	Gestión de servicio al cliente	Alto
Todos	No aplica	Gestión de Pagos	Alto
Ramos de vida	Desgravamen	Cálculo de reservas técnicas	Medio
Ramos de vida	Desgravamen	Comercialización	Medio
Ramos de vida	Desgravamen	Comisiones	Medio
Ramos de vida	Desgravamen	Diseño y desarrollo de productos y servicios	Medio
Ramos de vida	No aplica	Gestión de Cobranzas	Medio
Ramos de vida	No aplica	Gestión de Procesos Administrativos de Recursos Humanos	Medio
Ramos de vida	Renta Fija	Valorización de Inversiones	Medio
Ramos de vida	Renta Variable	Valorización de Inversiones	Medio
Ramos de vida	RV Pensión de Invalidez	Cálculo de reservas matemáticas	Medio
Ramos de vida	RV Pensión de Invalidez	Comercialización	Medio
Ramos de vida	RV Pensión de Invalidez	Emisión de la póliza y endoso	Medio

Línea de negocio	Producto	Proceso	Clasificación
Ramos de vida	RV Pensión de Invalidez	Pagos mensuales	Medio
Ramos de vida	RV Pensión de Jubilación	Comercialización	Medio
Ramos de vida	RV Pensión de Jubilación	Comercialización	Medio
Ramos de vida	RV Pensión de Jubilación	Pagos mensuales	Medio
Ramos de vida	RV Pensión de Sobrevivencia	Cálculo de reservas matemáticas	Medio
Ramos de vida	RV Pensión de Sobrevivencia	Comercialización	Medio
Ramos de vida	RV Pensión de Sobrevivencia	Emisión de la póliza y endoso	Medio
Ramos de vida	RV Pensión de Sobrevivencia	Pagos mensuales	Medio
Ramos de vida	Seguro de Vida Individual Corto Plazo	Atención de solicitudes de Cobertura	Medio
Ramos de vida	Sepelio Corto Plazo	Atención de solicitudes de Cobertura	Medio
Todos	No aplica	Gestión contable	Medio
Ramos de vida	RV Pensión de Invalidez	Comisiones	Bajo
Ramos de vida	RV Pensión de Jubilación	Cálculo de reservas matemáticas	Bajo
Ramos de vida	RV Pensión de Sobrevivencia	Comisiones	Bajo
Ramos de vida	Seguro de Vida Individual Corto Plazo	Cálculo de reservas técnicas	Bajo
Ramos de vida	Seguro de Vida Individual Corto Plazo	Comercialización	Bajo
Ramos de vida	Seguro de Vida Individual Corto Plazo	Comisiones	Bajo

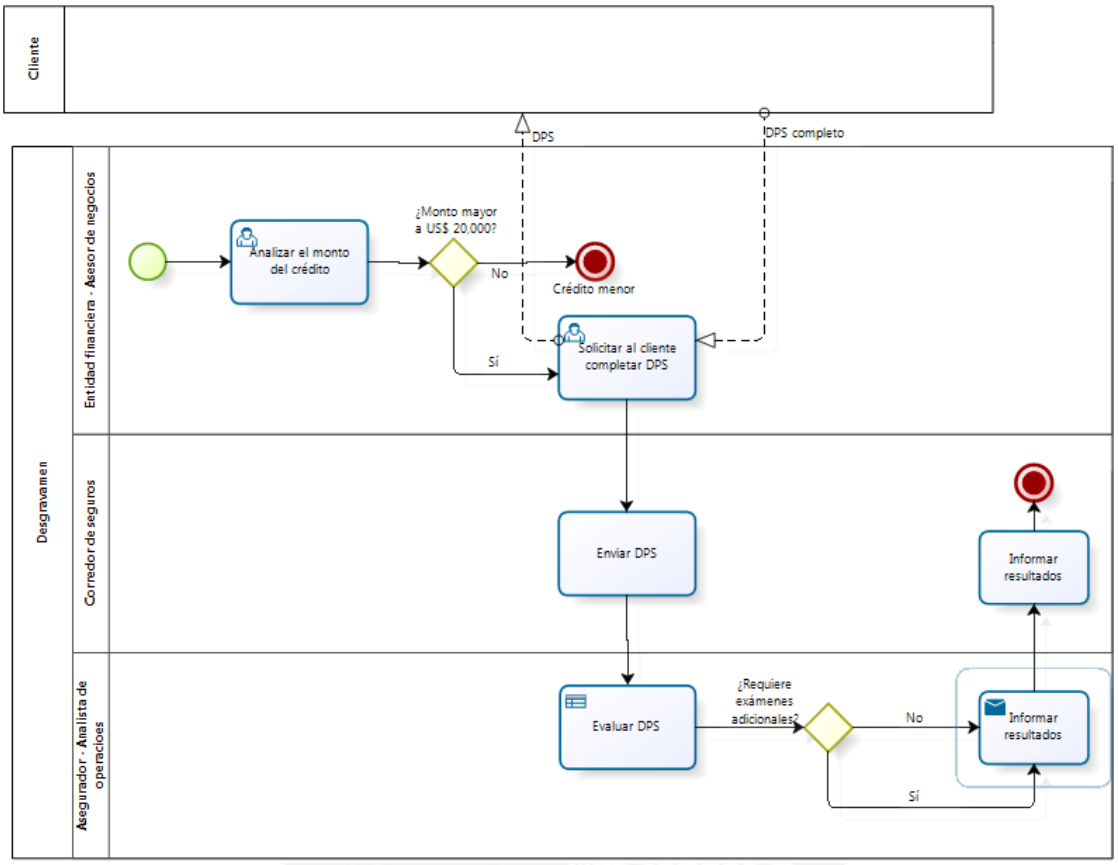
Línea de negocio	Producto	Proceso	Clasificación
Ramos de vida	Seguro de Vida Individual Corto Plazo	Diseño y desarrollo de productos y servicios	Bajo
Ramos de vida	Seguro de Vida Individual Corto Plazo	Suscripción, emisión y registro de información	Bajo
Ramos de vida	Sepelio Corto Plazo	Cálculo de reservas técnicas	Bajo
Ramos de vida	Sepelio Corto Plazo	Comercialización	Bajo
Ramos de vida	Sepelio Corto Plazo	Comisiones	Bajo
Ramos de vida	Sepelio Corto Plazo	Diseño y desarrollo de productos y servicios	Bajo
Ramos de vida	Sepelio Corto Plazo	Suscripción, emisión y registro de información	Bajo
Todos	No aplica	Desarrollo	Bajo
Todos	No aplica	Desarrollo del Talento Humano	Bajo
Todos	No aplica	Producción	Bajo
Todos	No aplica	Redes y Comunicaciones	Bajo
Todos	No aplica	Seguridad de la Información TI	Bajo

14. Anexo 14: Modelado de Procesos

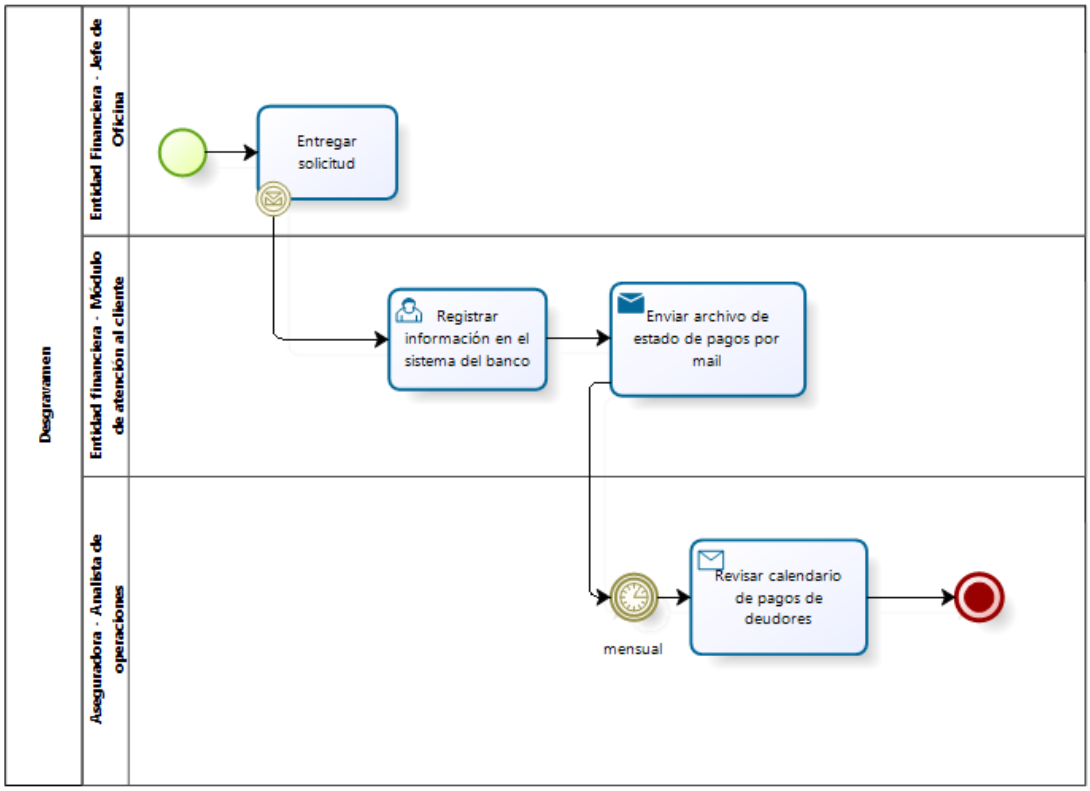
Modelado 1: Desgravamen - Suscripción, emisión y registro de información



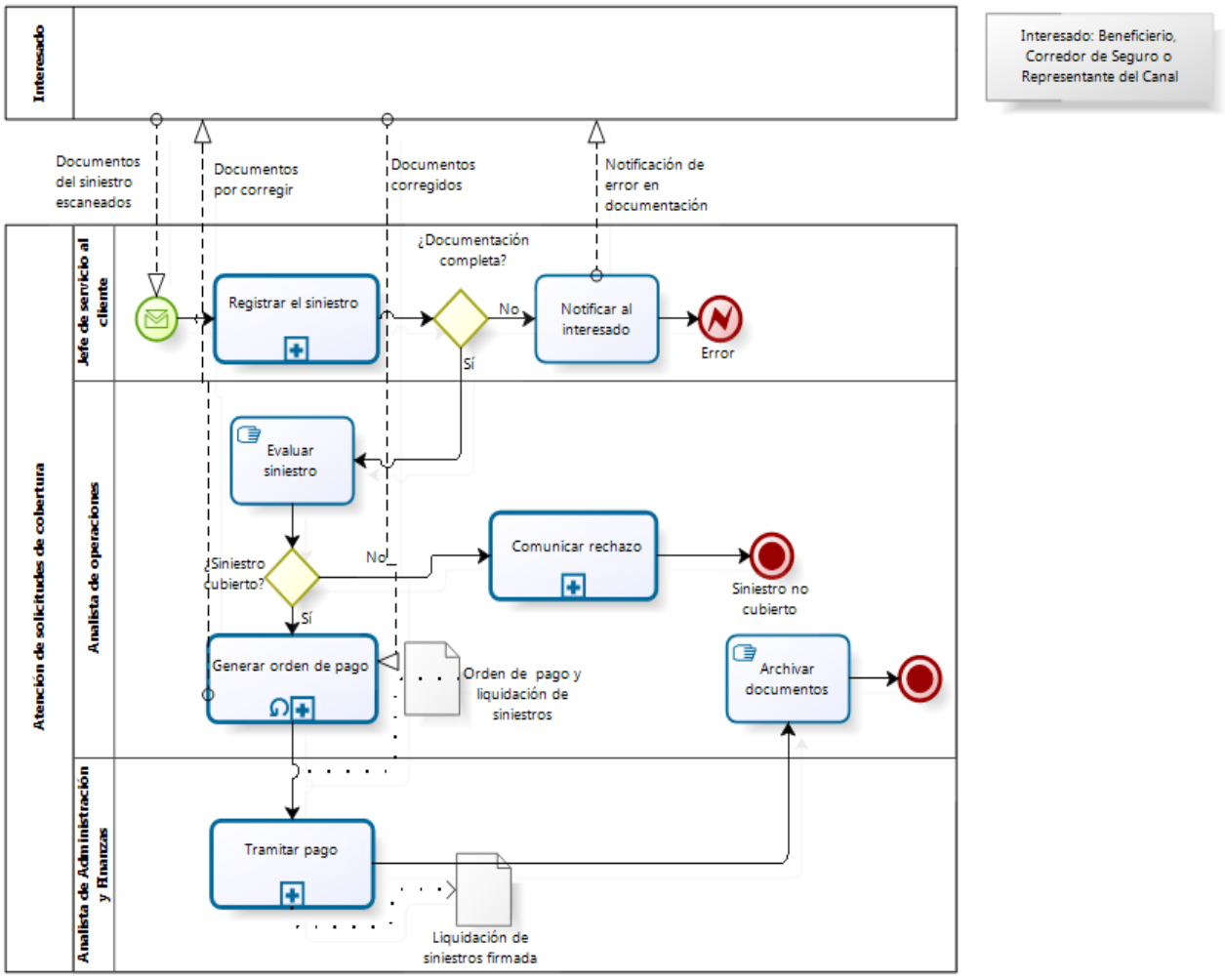
Subproceso: Evaluar Crédito



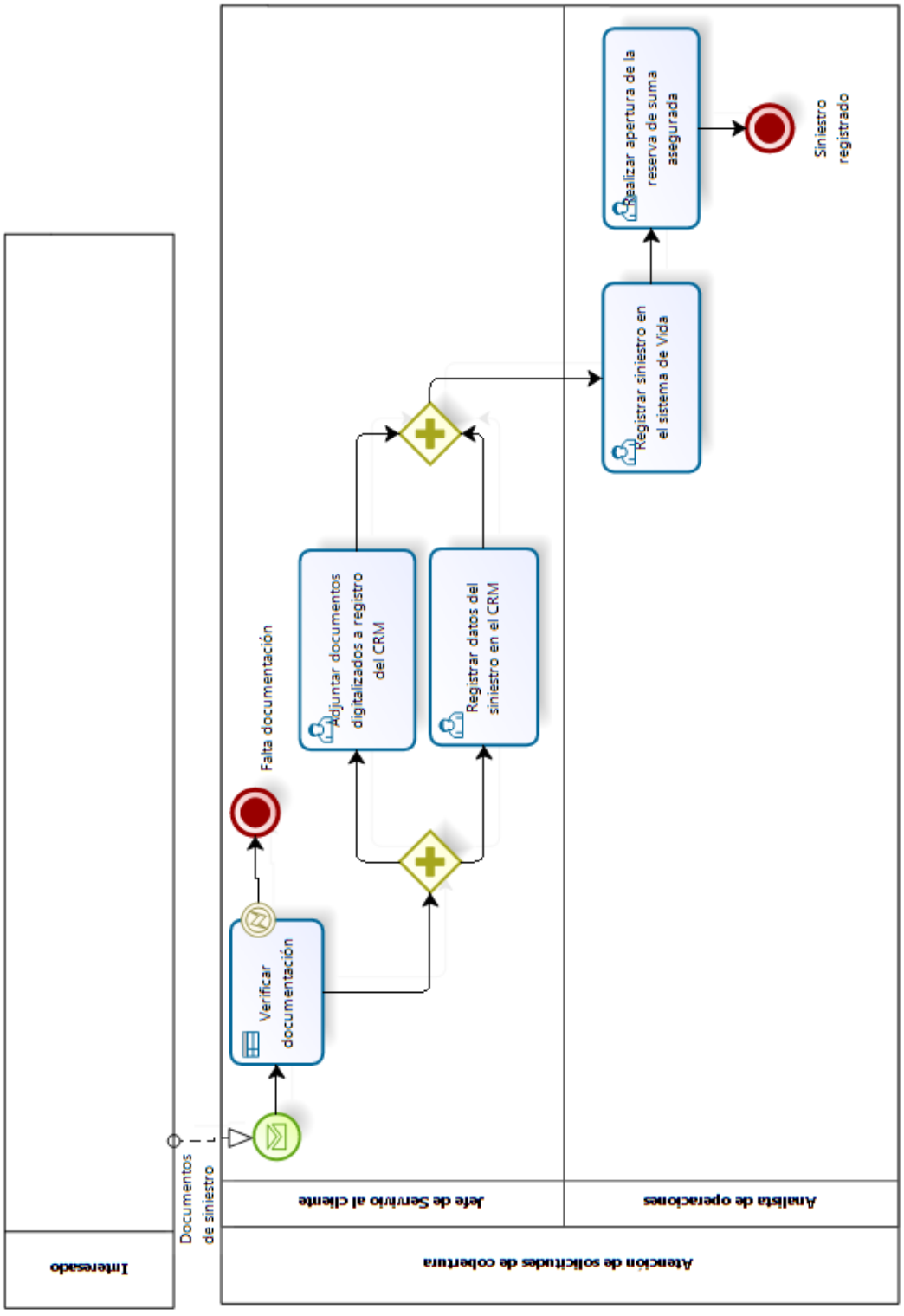
Registrar información



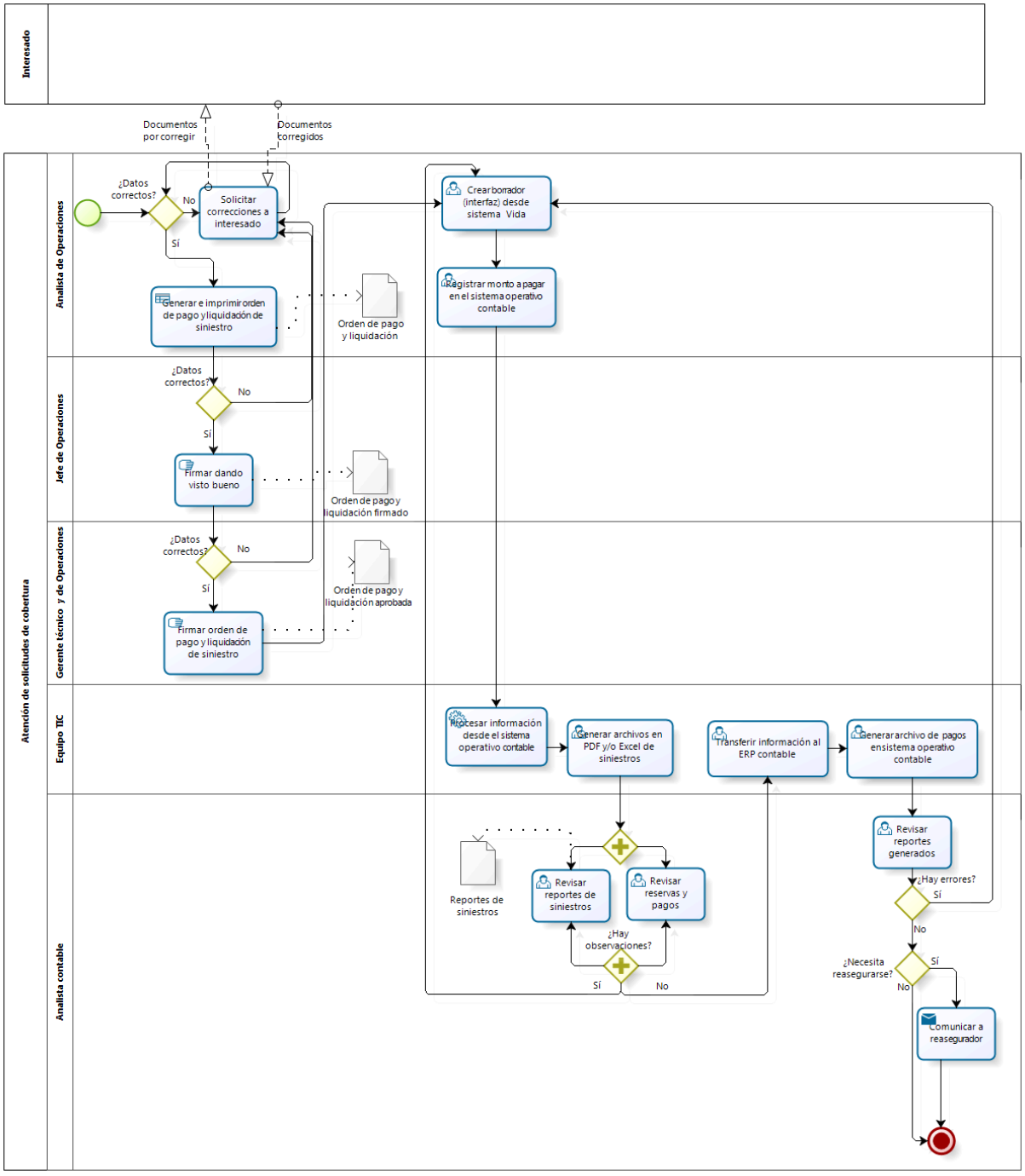
Modelado 2: Desgravamen - Atención de solicitudes de Cobertura



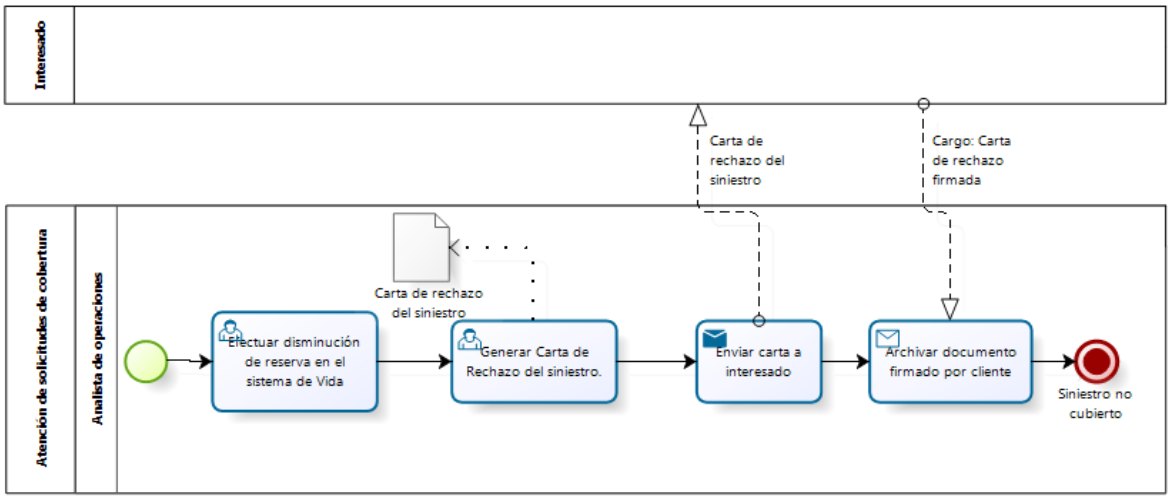
Registrar el siniestro



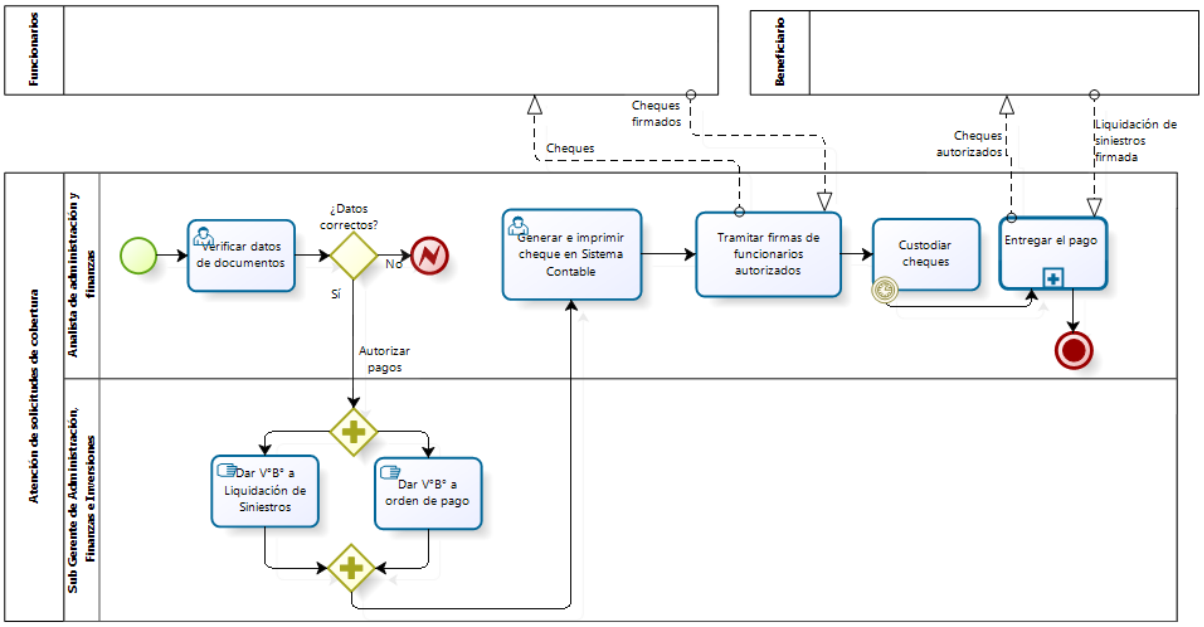
Generar orden de pago



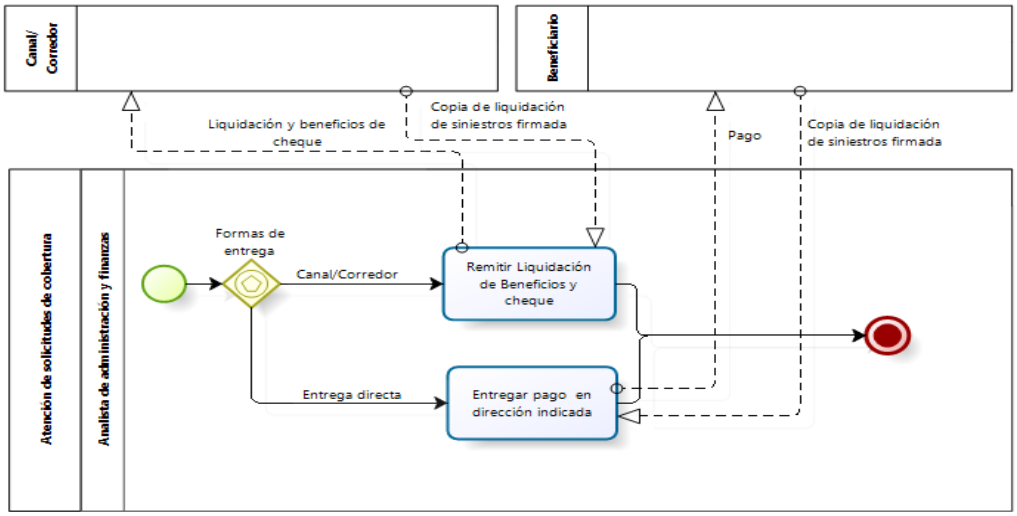
Comunicar rechazo



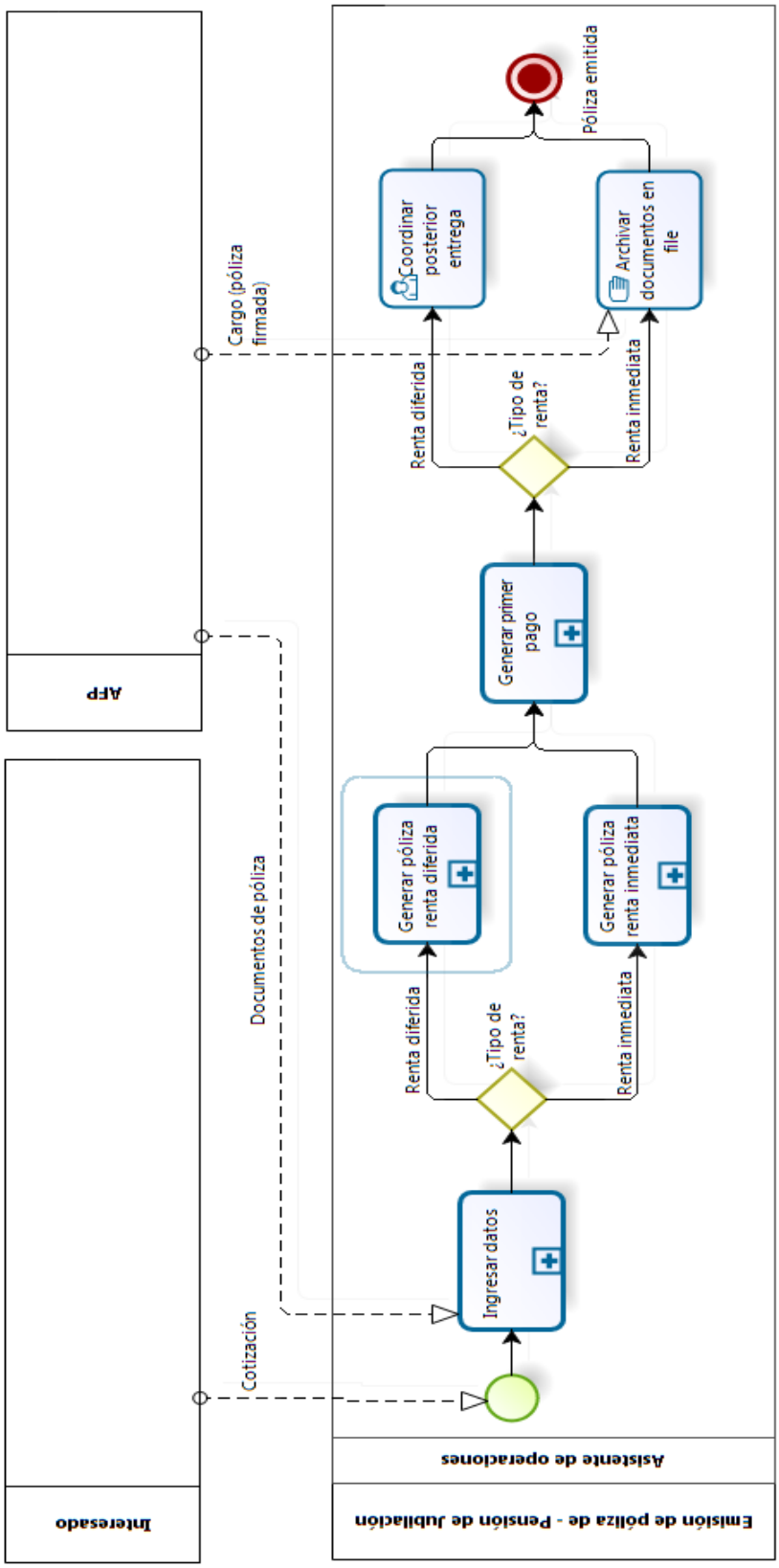
Tramitar pago



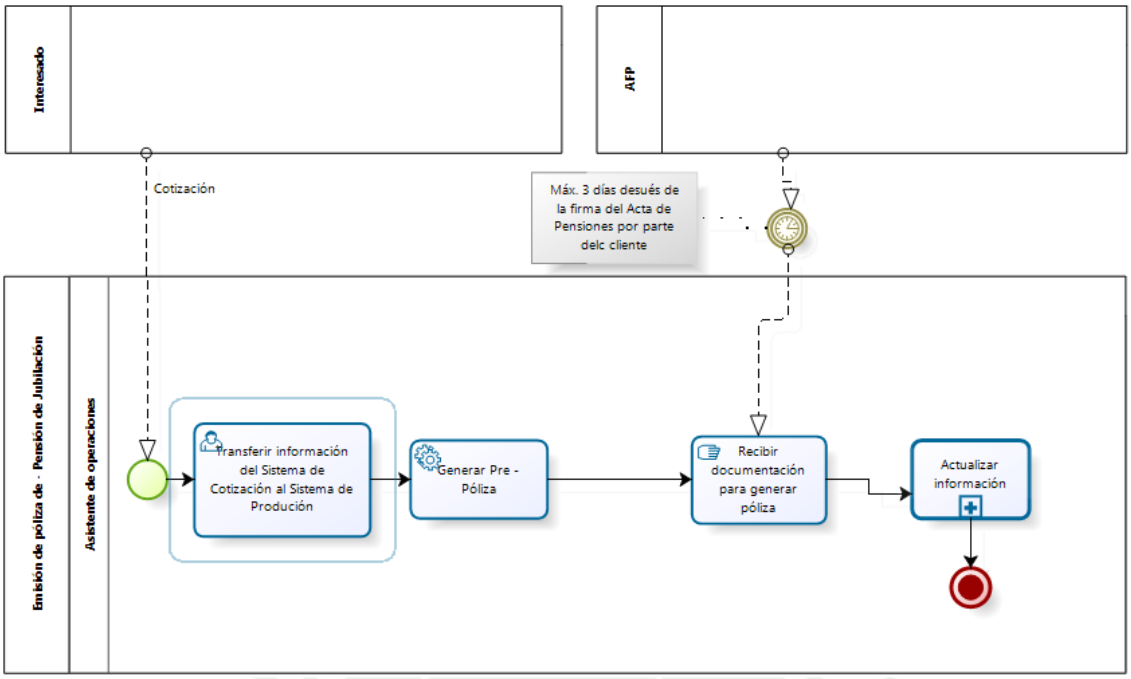
Entregar pago



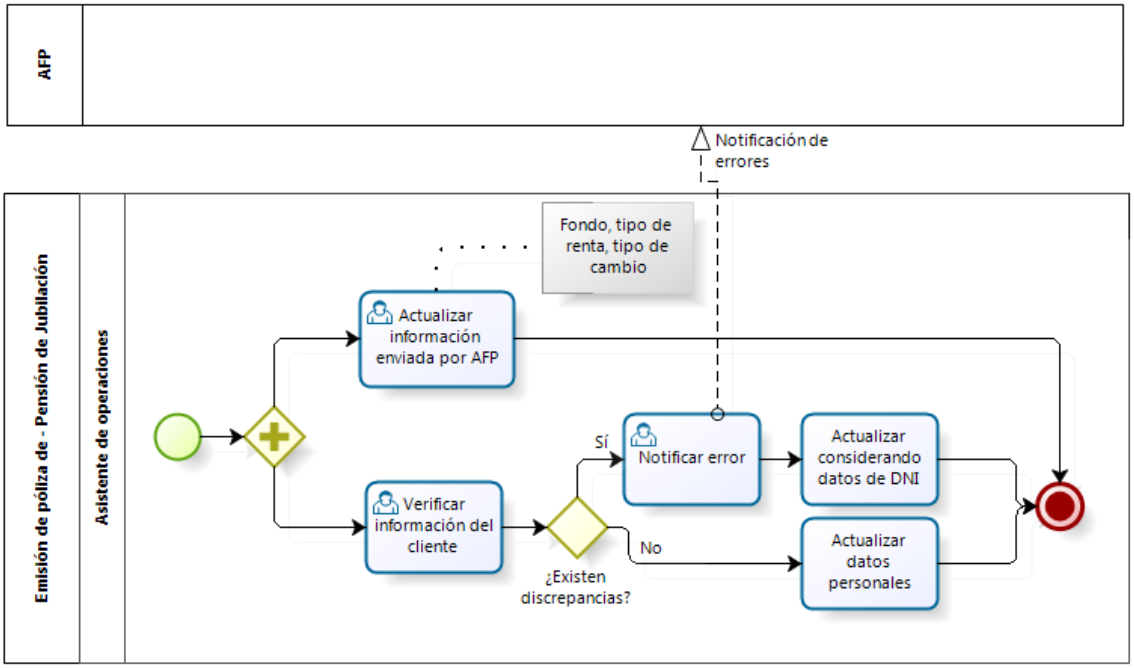
Modelado 3: Pensión de Jubilación - Emisión de la póliza y endoso



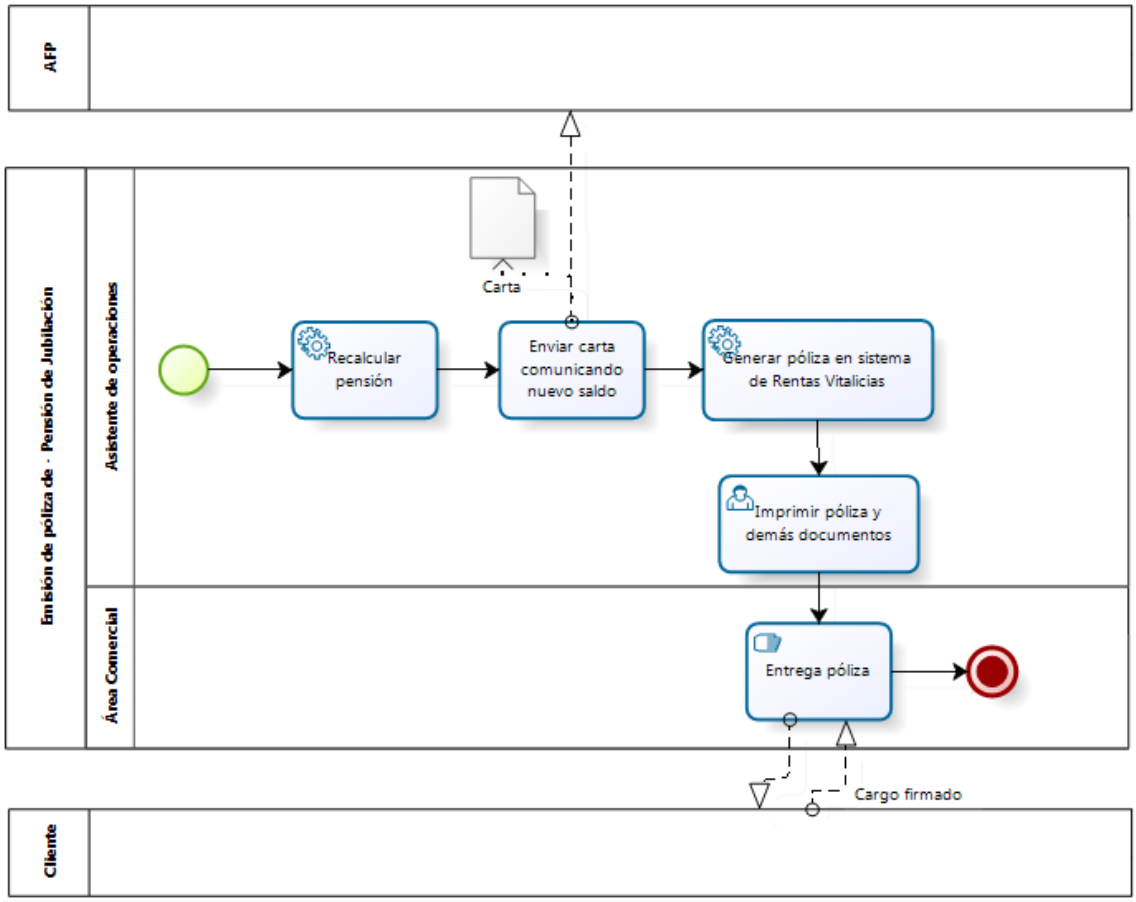
Ingresar datos



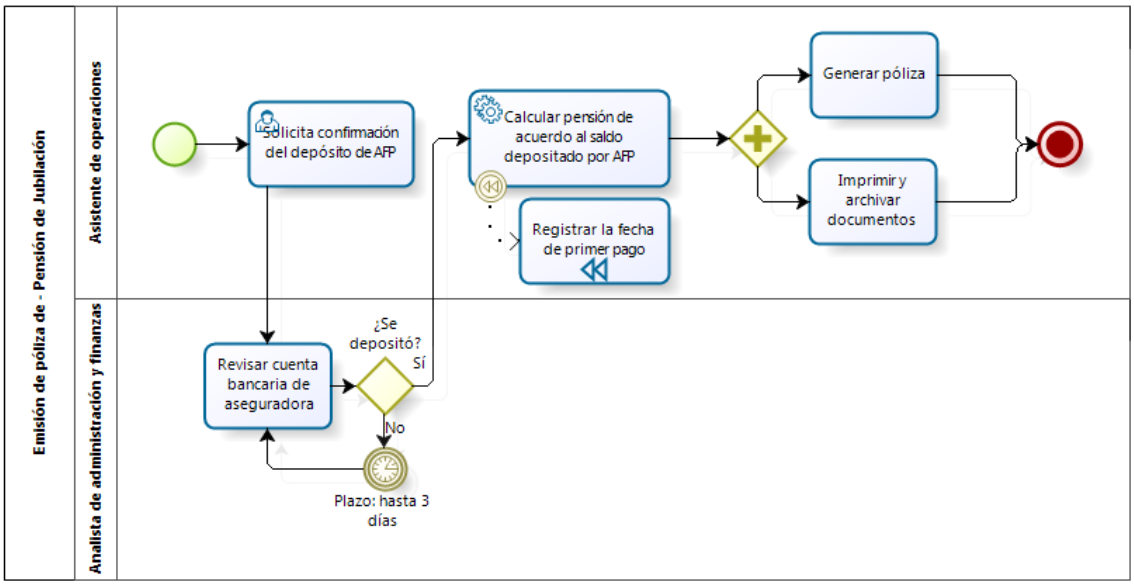
Actualizar información



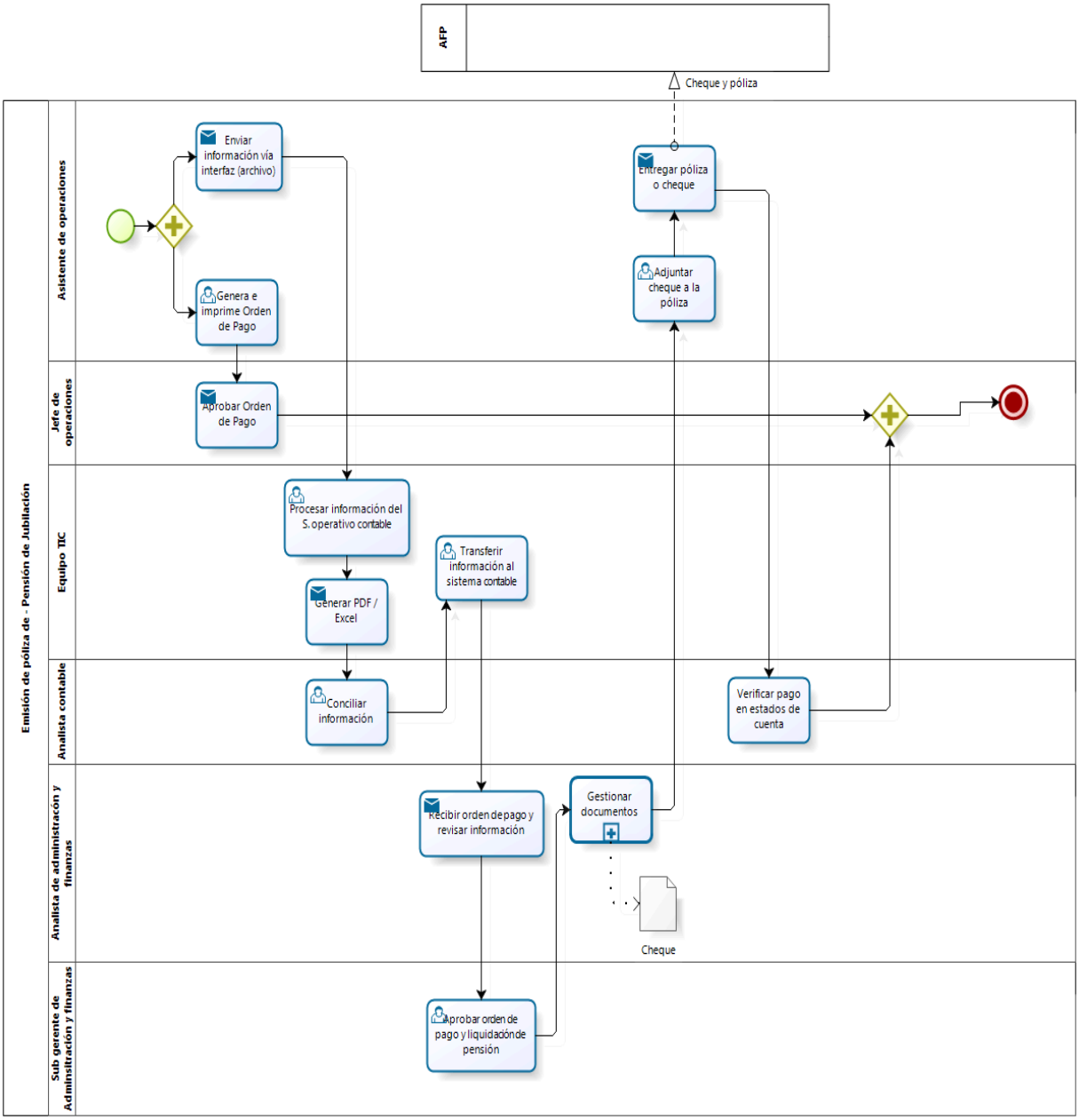
Generar póliza de renta diferida



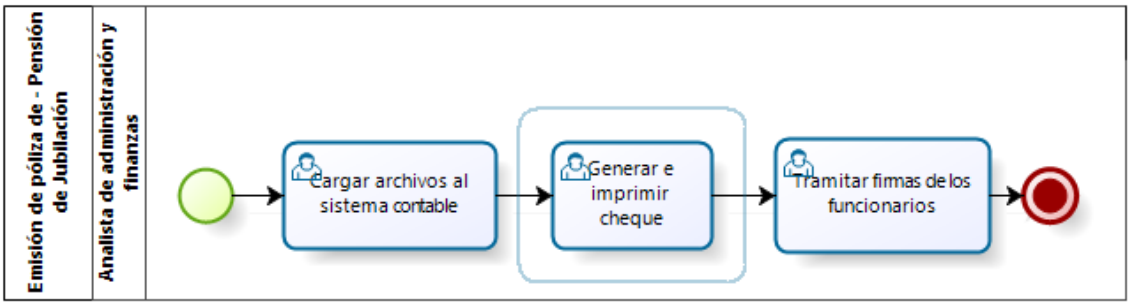
Generar póliza de renta inmediata



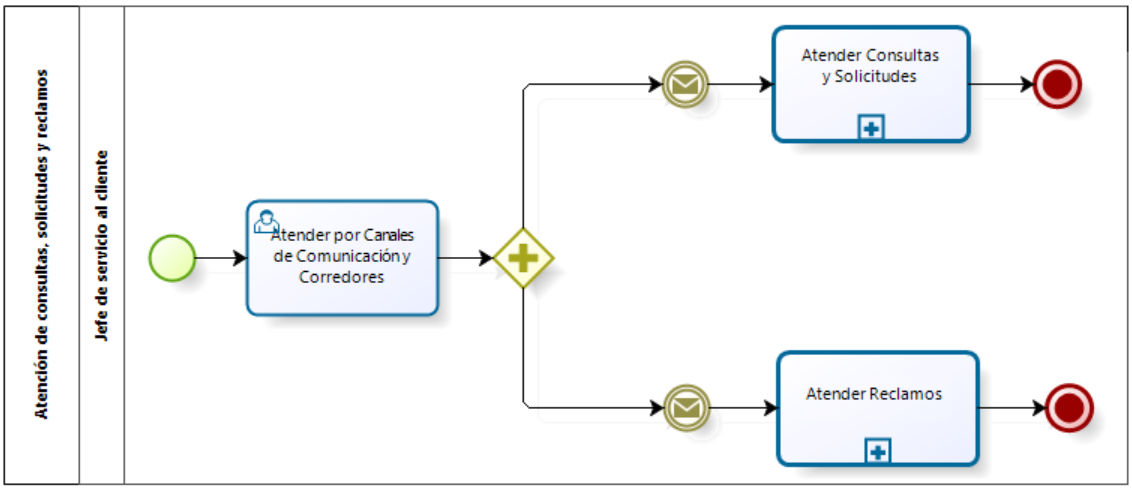
Generar primer pago



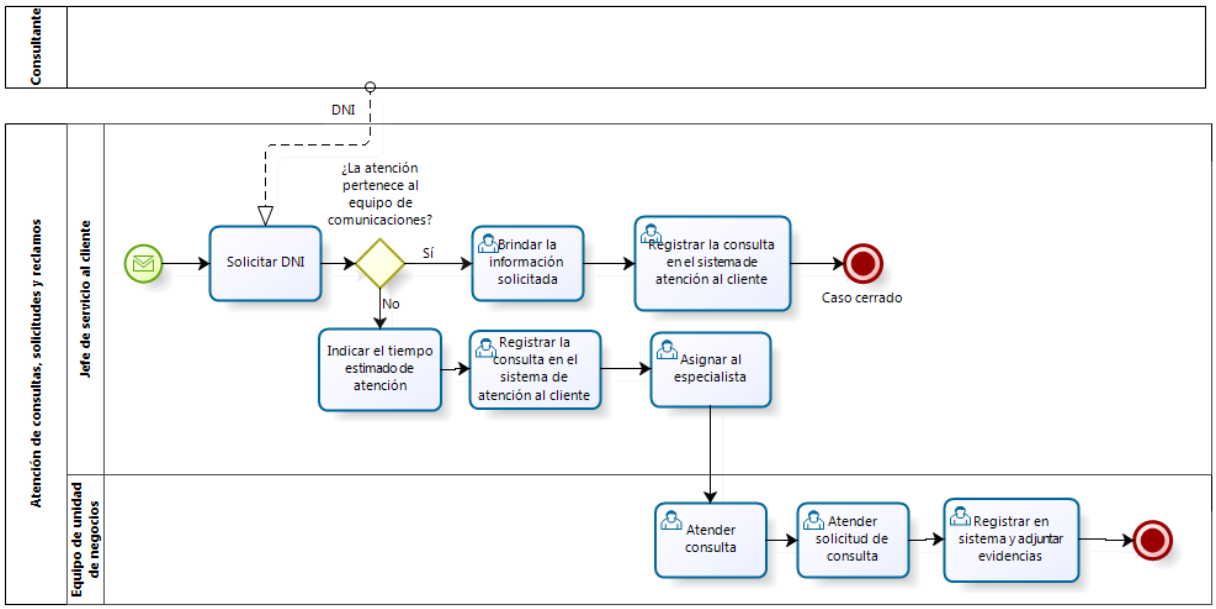
Gestionar documentos



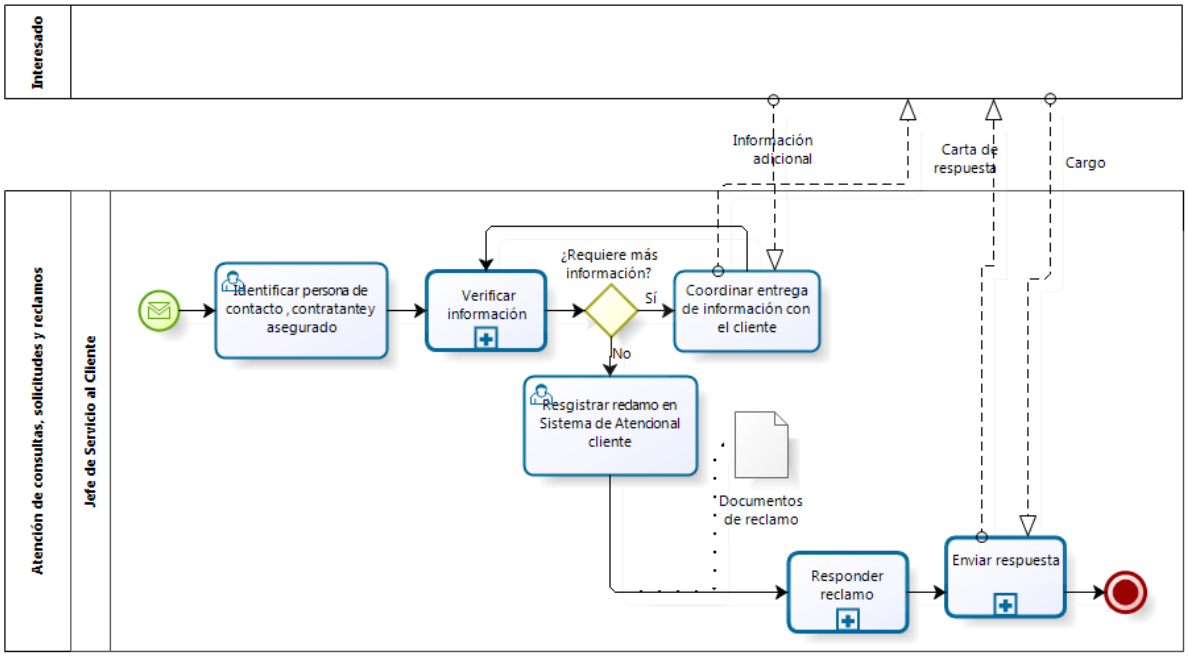
Modelado 4: Gestión de servicio al cliente



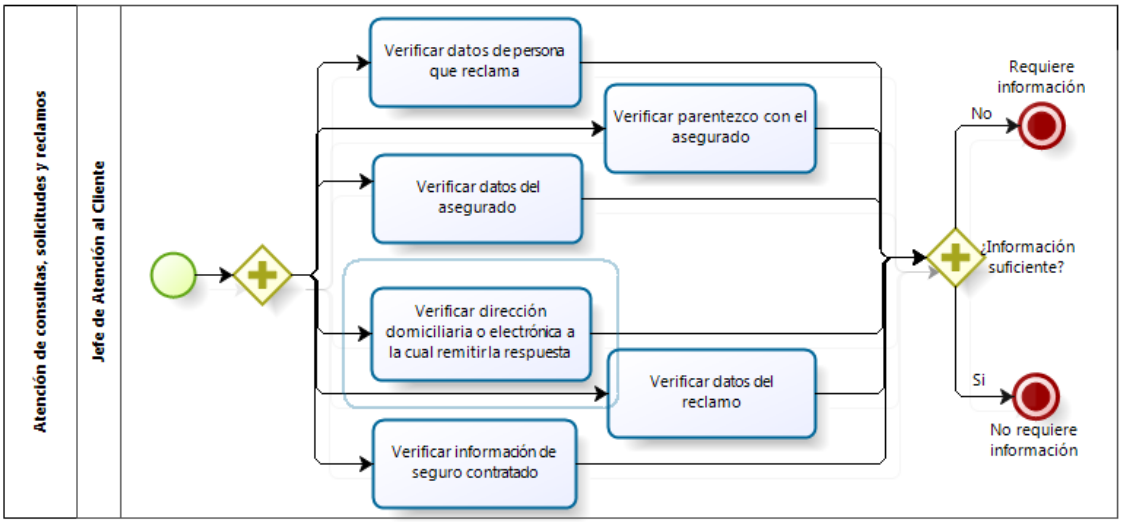
Atender consultas y solicitudes



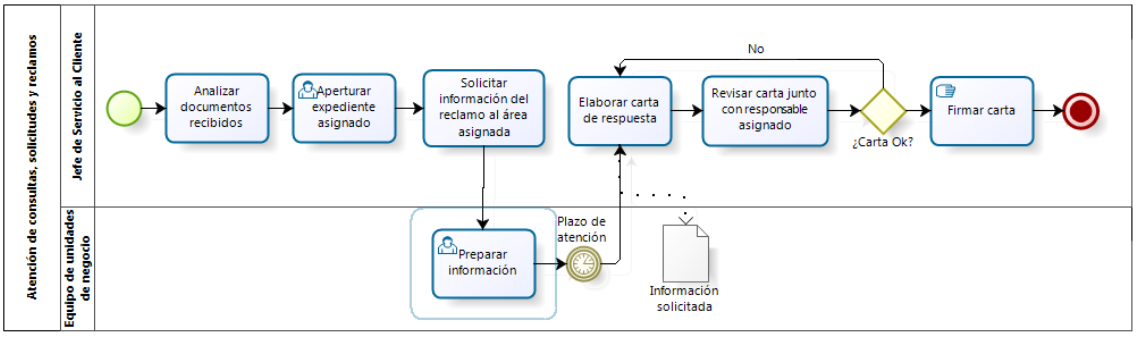
Atender reclamos



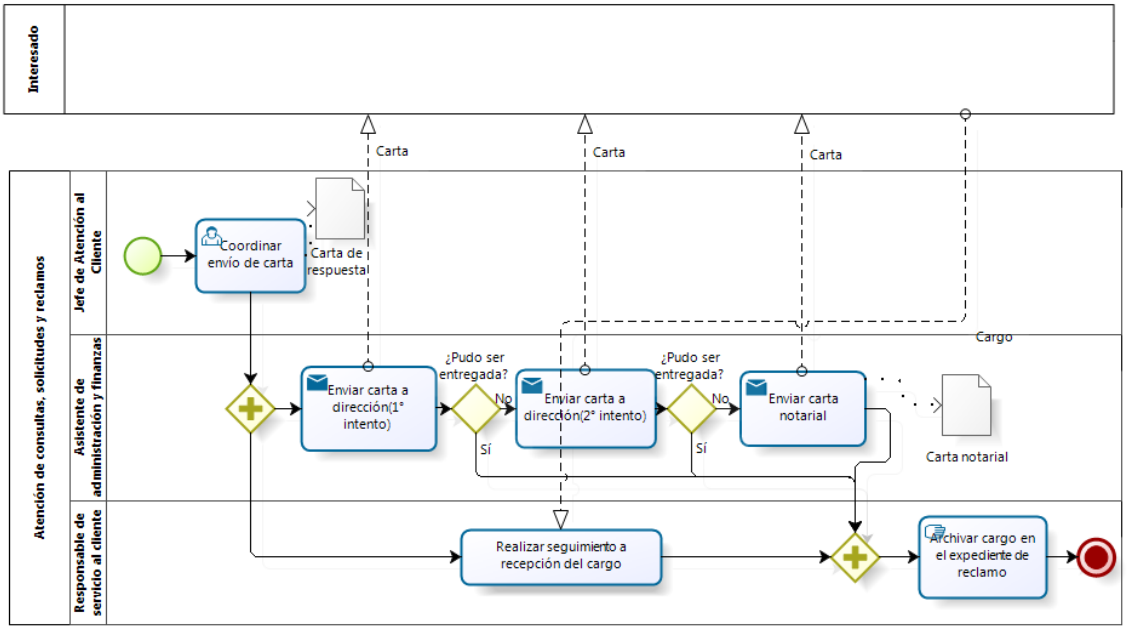
Verificar información



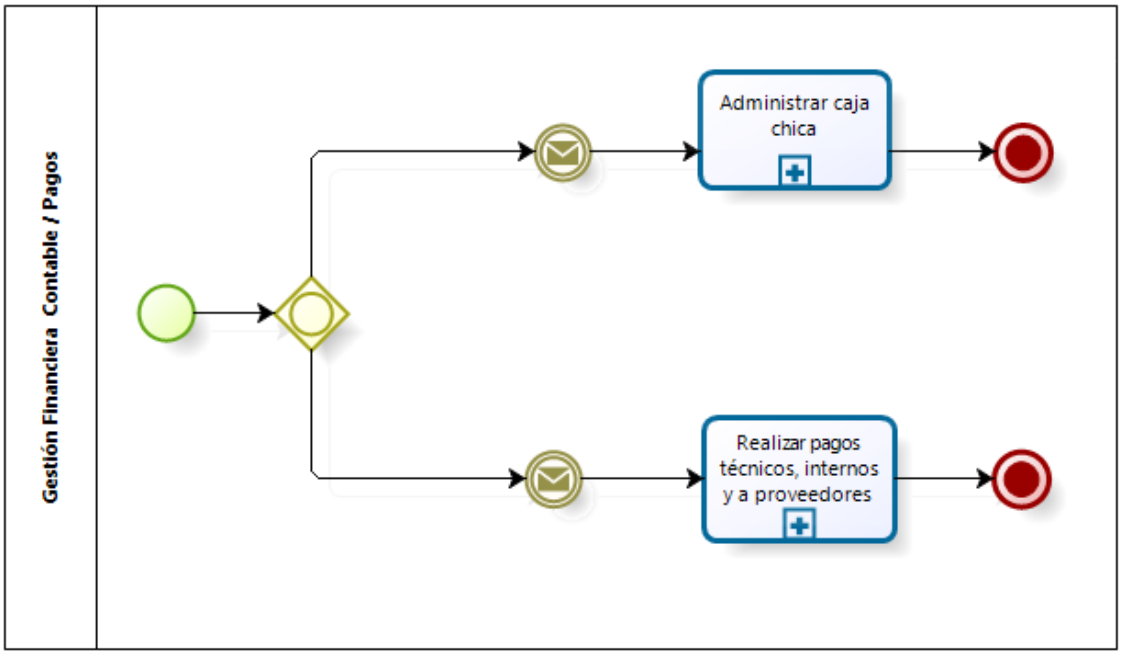
Responder reclamo



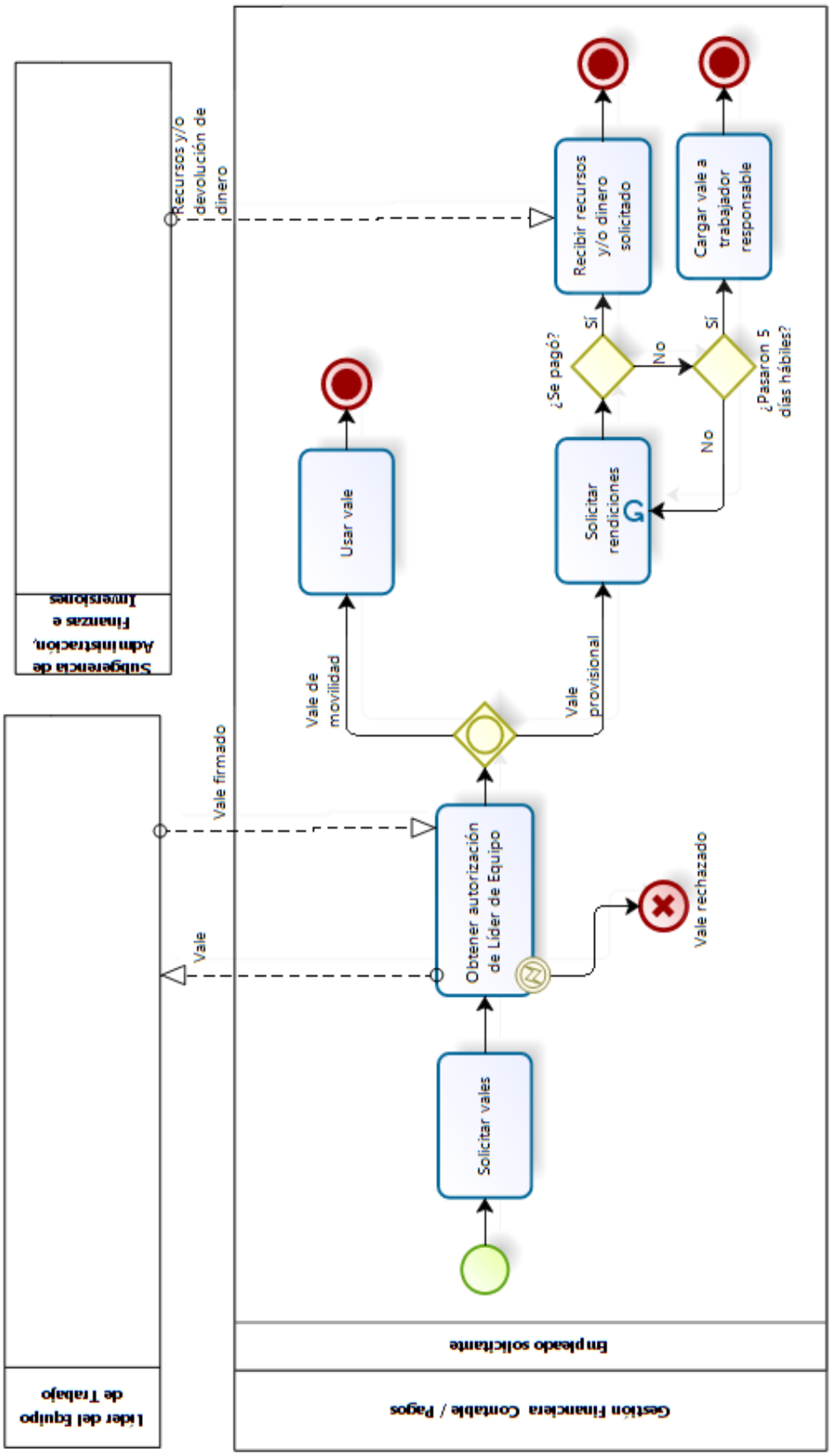
Enviar respuesta



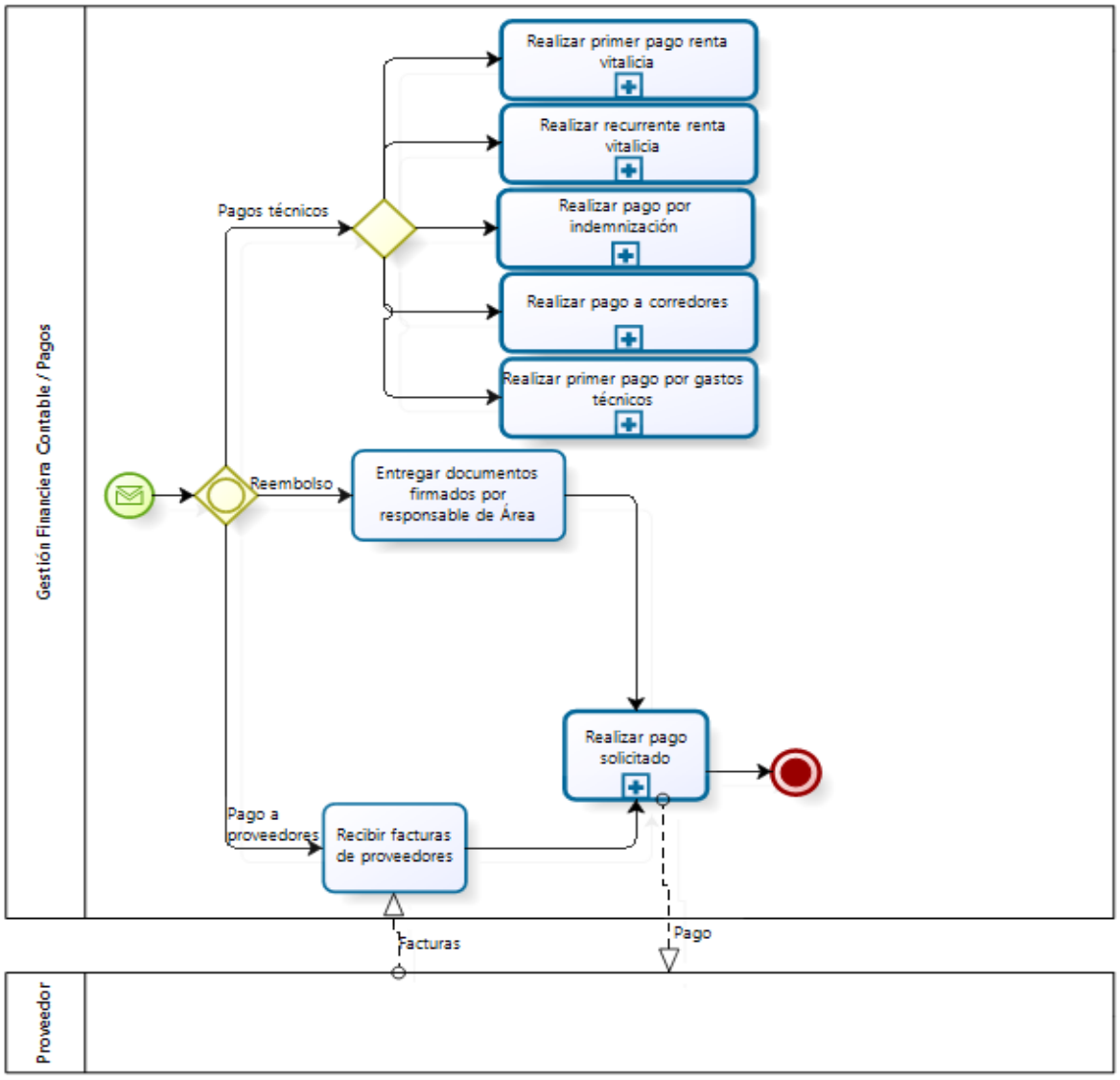
Modelado 5: Gestión de pagos



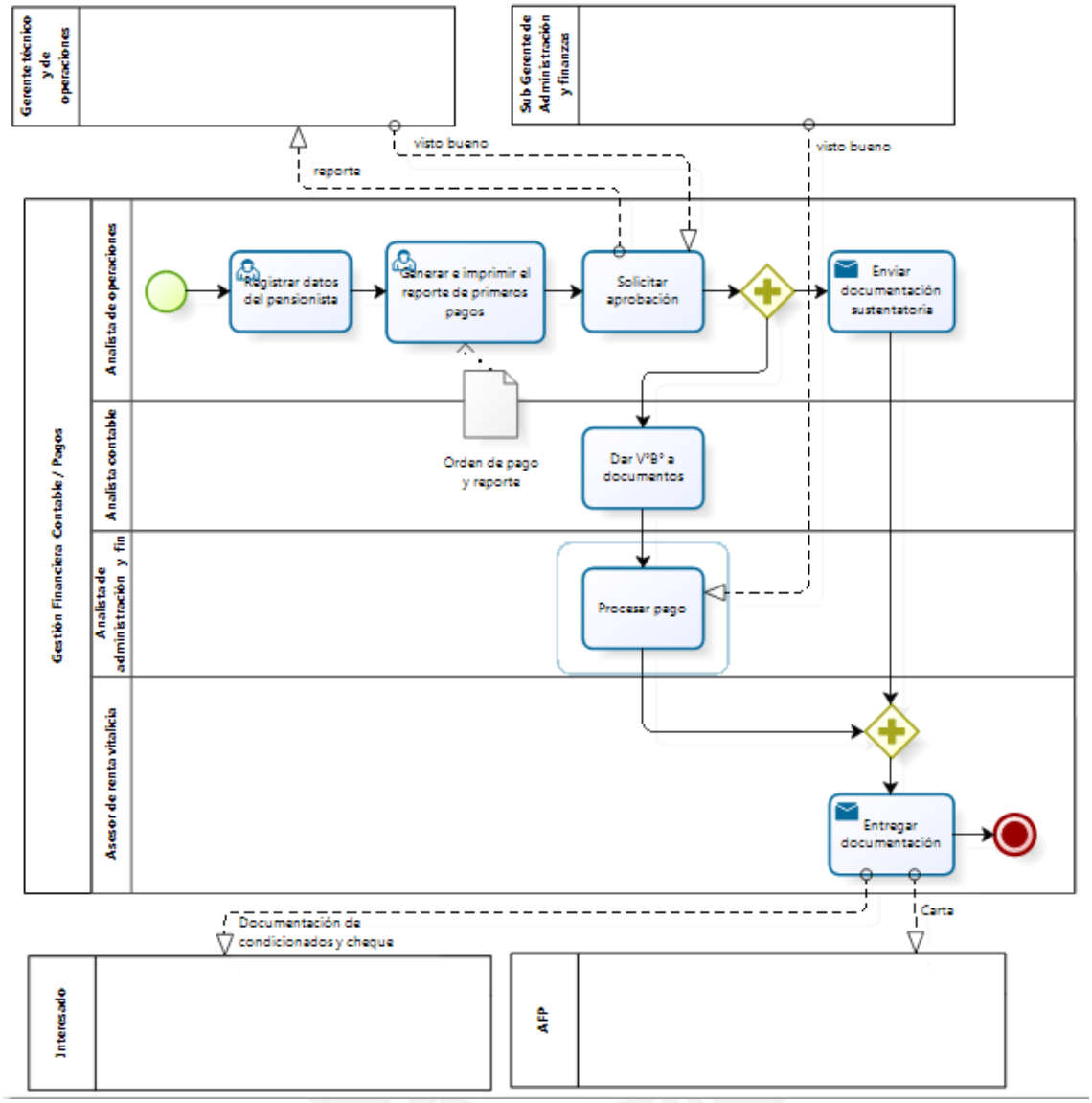
Administrar caja chica



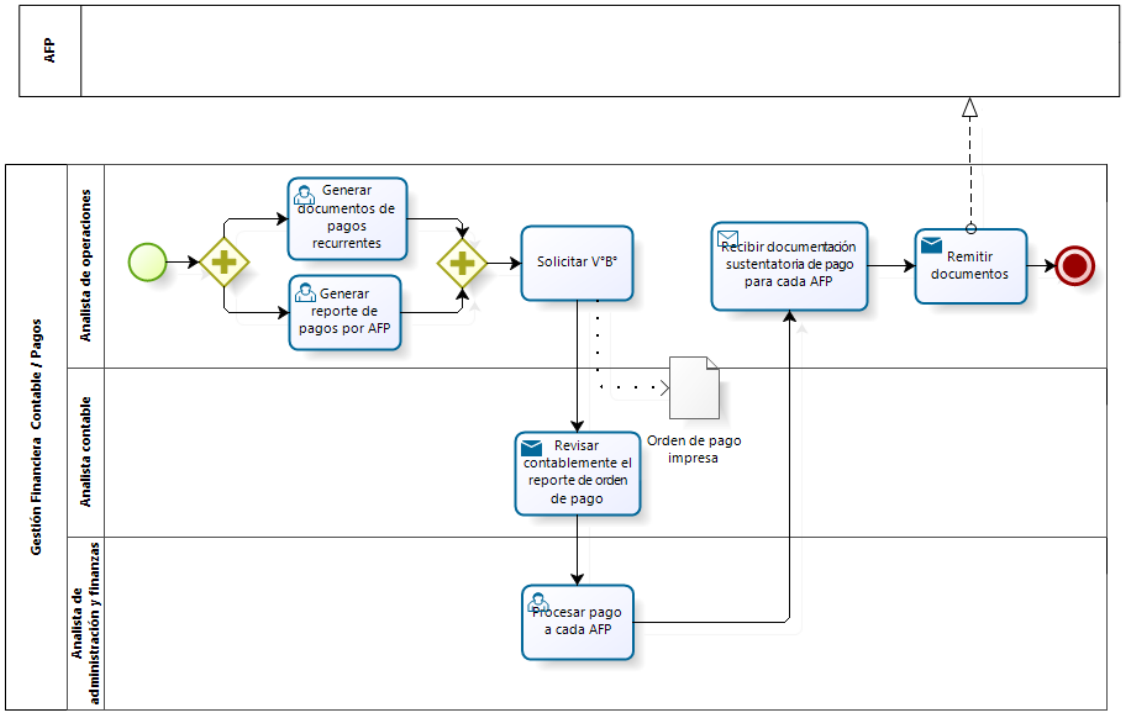
Realizar pagos técnicos internos y a proveedores



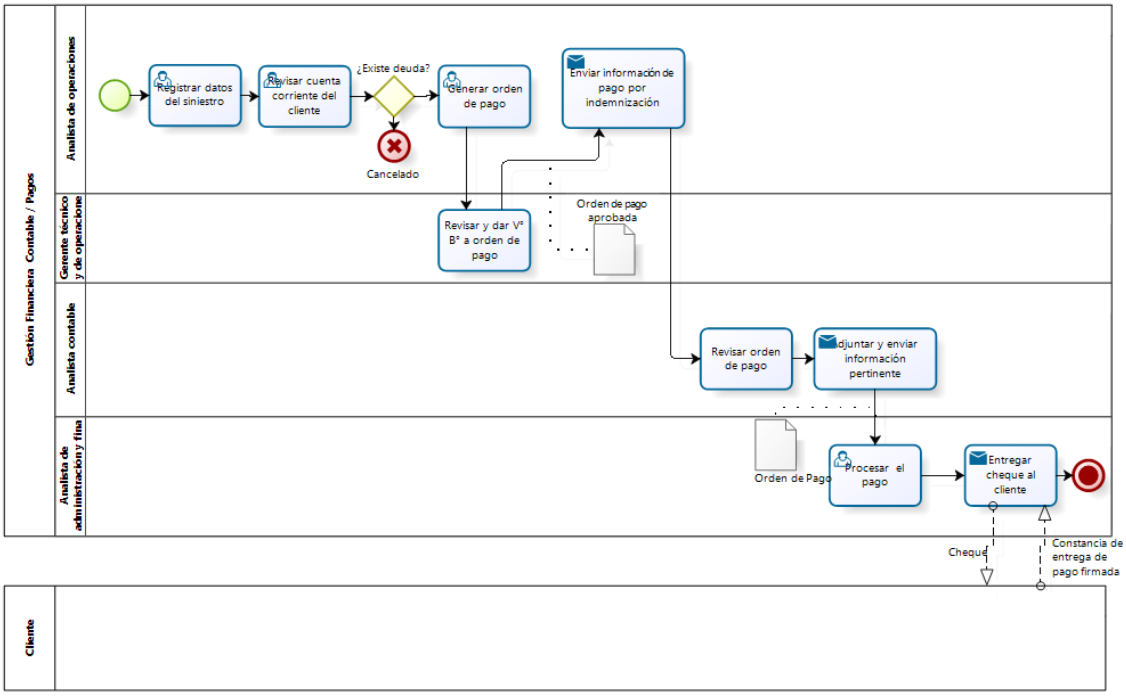
Realizar primer pago renta vitalicia



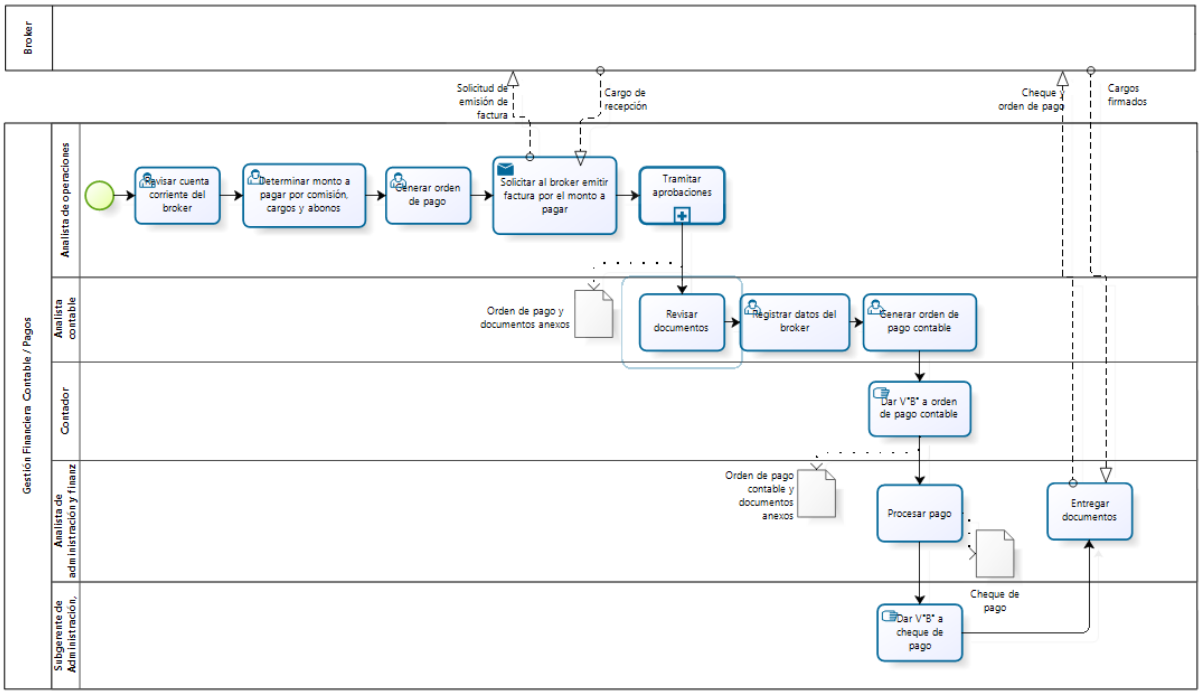
Realizar pago recurrente renta vitalicia



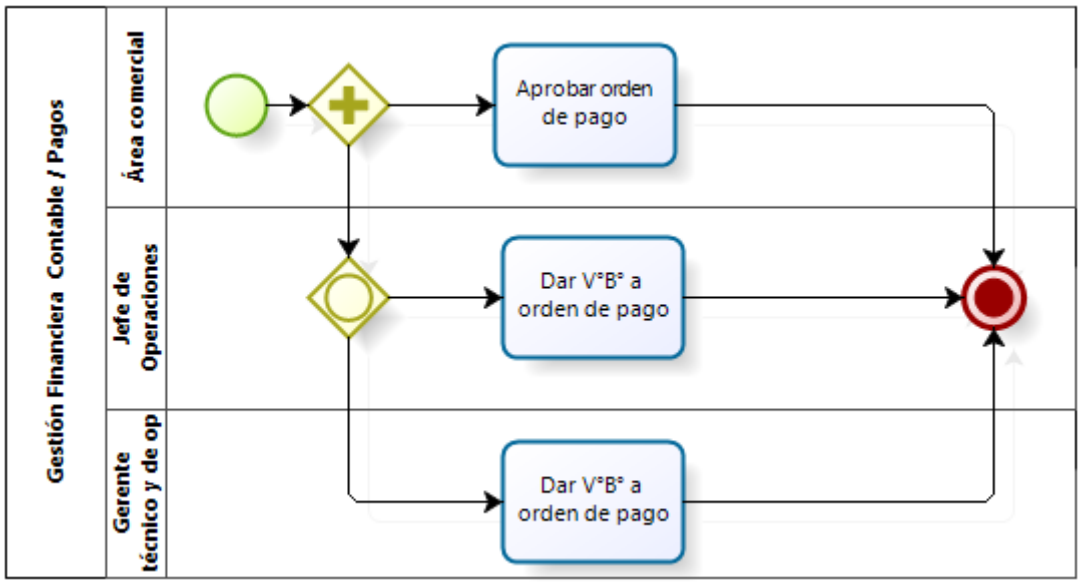
Realizar pago por indemnización



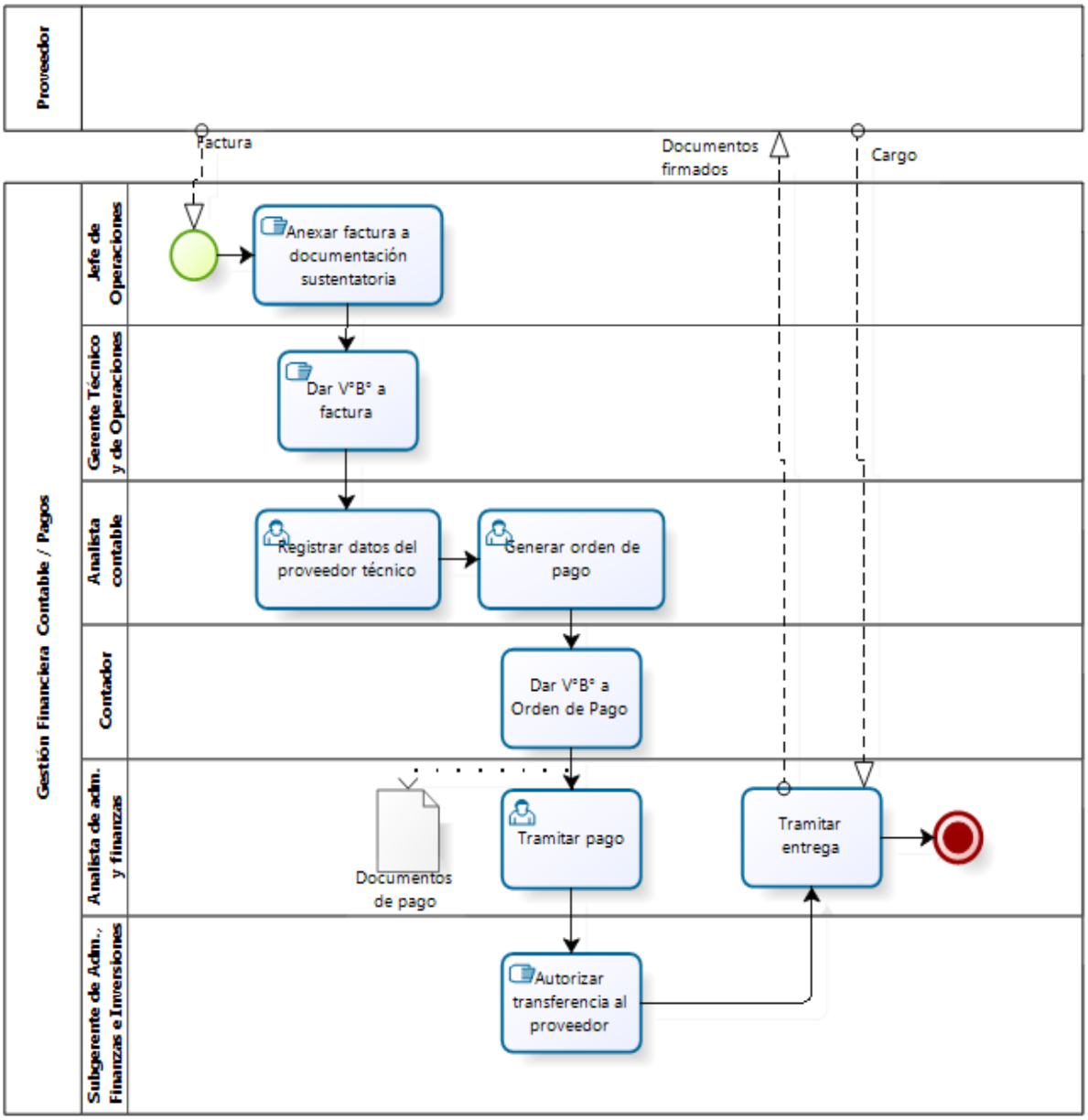
Realizar pago a corredores



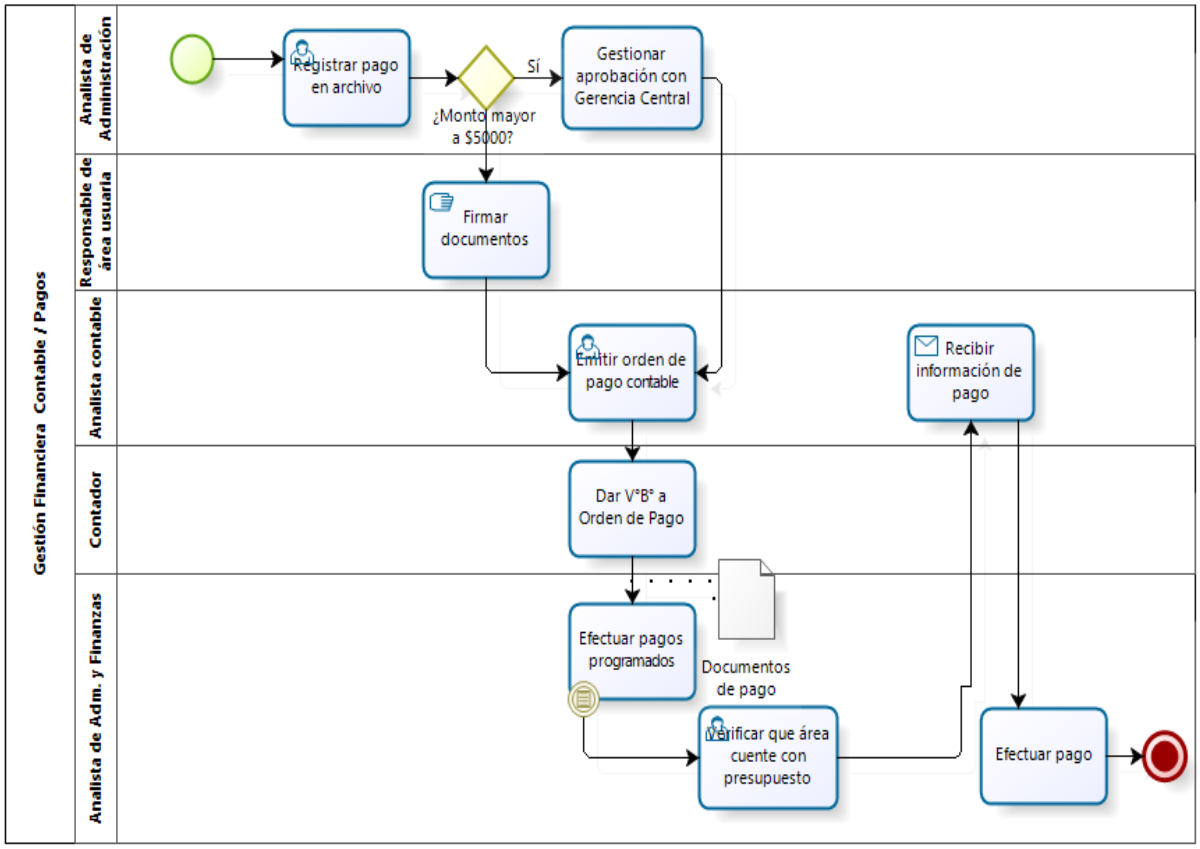
Tramitar aprobaciones



Realizar primer pago por gastos técnicos



Realizar pago solicitado



15. Anexo 15: Estrategias de Continuidad por tipo de Recurso

Personal

Estrategia	Tipo	Responsable
Identificación de roles críticos y alternos		
1. Identificar personal necesario para la recuperación de los procesos críticos del negocio, determinando la cantidad mínima de personas para la continuidad de los servicios.	**Estratégico**	Cada Área del Negocio
2. Identificar el perfil para cada tipo de rol, especificando los conocimientos mínimos que debe tener así como también las habilidades técnicas y personales necesarias. Esto permitirá una adecuada selección de personal alterno.	**Estratégico**	Cada Área del Negocio
3. Documentar detalladamente y mantener actualizada todas las actividades de los roles críticos a modo de manual de usuario para asegurar el correcto cumplimiento de las tareas.	**Estratégico**	Cada Área del Negocio
4. Identificar al personal alterno conveniente para asegurar la continuidad de las operaciones de la empresa en caso el personal primario no esté disponible a causa de un desastre. Se debe considerar más de un alterno que cuente con el perfil necesario para cumplir las funciones del personal primario. Además se debe considerar el trabajar desde casa en caso no se pueda contar con algún ambiente de trabajo.	**Estratégico**	Cada Área del Negocio
5. Designar a un responsable del DRP calificado con los conocimientos y habilidades adecuados para poder dirigir y llevar a cabo dicho plan. Esta persona debe tener una dedicación exclusiva a ello y se le deberá brindar todos los recursos humanos, tecnológicos y logísticos necesarios.	**Estratégico**	Gerencia de Tecnología de Información
Capacitación de personal y Simulacros		

Estrategia	Tipo	Responsable
6. Definir un programa anual de capacitaciones sobre la Gestión de Riesgos, Seguridad, Gestión de Continuidad de Negocio y temas afines en la empresa que implique la participación de toda la empresa, desde la Alta Dirección hasta el personal operativo y administrativo con el objetivo de formar conciencia sobre el tema.	**Estratégico**	Gerencia de Riesgos
7. Incluir dentro del programa anual de capacitaciones algunas especializadas sobre los Planes de Continuidad de Negocios y Seguridad de la información tanto a personal primario como alterno con el fin de reducir brechas de conocimiento entre estos.	**Estratégico**	Cada Área del Negocio
8. Incluir dentro del programa anual de capacitaciones algunas especializadas para el Equipo TIC, las cuales abarquen temas técnicos y de procesos específicos así como la recuperación de los mismos, alineados al DRP.	**Estratégico**	Equipo TIC
9. Incluir dentro del programa anual de capacitaciones algunas especializadas en seguridad para el trabajo para el manejo de emergencias, buscando la participación de los bomberos, defensa civil, entre otros.	**Estratégico**	Área de RRHH
10. Realizar talleres para el manejo de situaciones de crisis con personal de la Alta Dirección, especialmente con aquellos que participen directamente en el plan de gestión de crisis, de modo que se pueda simular escenarios, realizar toma de decisiones de acuerdo al plan y finalmente realizar una evaluación para recolectar lecciones aprendidas.	**Estratégico**	Gerencia de Riesgos
11. Realizar talleres sobre el manejo de situaciones de crisis para del personal operativo y administrativo para asegurar una respuesta adecuada durante un desastre.	**Estratégico**	Gerencia de Riesgos

Estrategia	Tipo	Responsable
Comunicaciones en la organización		
12. Definir una estructura de comunicación en toda la organización, para que, dependiendo del tipo de evento se comunique a las personas adecuadas garantizando una comunicación efectiva.	**Estratégico**	Gerencia de Riesgos
13. Definir niveles de comunicación dependiendo del tipo de evento que ocurra en la organización, manejando básicamente dos niveles: ➢ Nivel operativo: Para incidentes referentes a fallas técnicas u operativas que puedan ser manejadas por personal del Equipo TIC o administrativo, según sea el caso. Este tipo de incidentes no generan impacto reputacional ni financiero. ➢ Nivel táctico – estratégico: Incidentes escalados a la Alta Dirección porque aún no han podido ser resueltos y podrían generar un alto impacto reputacional o financiero, implicando la publicación de la noticia en medios de comunicación y sociales.	**Estratégico**	Gerencia de Riesgos
14. Identificar los canales de comunicación adecuados entre los miembros responsables de la gestión de crisis y recuperación de los mismos. Estos pueden incluir mensajes masivos, creación de listas de distribución de correo, uso de distintos dispositivos de comunicación entre otros.	**Estratégico**	Gerencia de Riesgos
15. Difundir y actualizar constantemente una agenda que contenga los datos de personas a contactar en caso de una emergencia o crisis en la empresa. La información mostrada incluye: ➢ Nombre completo ➢ Cargo ➢ Tipo de rol (titular o alterno) ➢ Anexo	**Estratégico**	Gerencia de RRHH

Estrategia	Tipo	Responsable
➢ Celular de la empresa		
16. Definir los recursos adecuados para la adecuada comunicación entre los miembros de la organización dependiendo del rol que desempeñen. Los recursos a utilizar pueden ir desde teléfonos (anexos), celulares, smartphones o hasta celulares satelitales para miembros de la Alta Dirección.	**Operativo**	Gerencia de Riesgos
Políticas		
17. Definir políticas para la asignación de vacaciones del personal titular y alterno, de modo que siempre se cuente con por lo menos uno de ellos.	**Estratégico**	Área de RRHH
18. Implementar políticas que consideren la disposición de efectivos y recursos (víveres o vales de compra) para poder brindar ayuda humanitaria al personal afectado por un desastre	**Estratégico**	Área de RRHH
19. Establecer comités periódicos de riesgo operacional y continuidad de negocios, definiendo el objetivo, los temas a tratar y los participantes convocados.	**Estratégico**	Gerencia de Riesgos
20. Definir políticas para determinar las diferentes formas de trabajar en caso de la ocurrencia de un desastre, de modo que considere la probabilidad de no contar con un ambiente adecuado para el desempeño de sus labores.	**Operativo**	Área de RRHH
21. Definir políticas de atención en caso de crisis, de modo que se determine qué servicios se atenderán en caso de la ocurrencia de un desastre y su comunicación oportuna a los clientes.	**Operativo**	Todas
22. Establecer indicadores de continuidad del Negocio que midan el desempeño del personal al personal que participa en las actividades de	**Operativo**	Gerencia de Riesgos

Estrategia	Tipo	Responsable
recuperación y además evalúe la efectividad de los controles aplicados en las situaciones.		
Brigadas de emergencia		
23. Difundir y mantener actualizado un lista de los números de contacto de entidades de apoyo externas como lo son: ➢ Bomberos ➢ Policía Nacional (comisarías cercanas) ➢ Clínicas/hospitales ➢ Defensa civil ➢ Serenazgo	**Operativo**	Área de RRHH
24. Difundir y mantener un listado de brigadistas actualizado y organizado por funciones para Evacuación, Seguridad, Incendio y Primeros Auxilios.	**Operativo**	Área de RRHH
Responsabilidad social		
25. Realizar un plan de asistencia humanitaria que incluya los siguientes aspectos: a. Definir un equipo responsable de tomar y ejecutar las decisiones de asistencia humanitaria que apliquen según el escenario establecido. b. Considerar como beneficiarios a todos los empleados de la empresa (estén o no en las instalaciones de la empresa al momento del desastre) así como familiares directos. c. Definir un paquete básico para la asistencia a empleados compuesto principalmente por: Alimentos no perecibles, abrigos y medicinas básicas de primeros auxilios. d. Considerar dentro del presupuesto anual un porcentaje del mismo para asistencia humanitaria en caso de crisis.	**Operativo**	Área de RRHH
26. Definir líderes de responsabilidad social (independiente a los brigadistas del apoyo interno)	**Operativo**	Área de RRHH

Estrategia	Tipo	Responsable
cuyo objetivo sea gestionar las actividades orientadas a velar por el bienestar de los familiares de personal y de la comunidad en general.		

Infraestructura

Estrategia	Tipo	Responsable
Espacio Físico		
1. Definir las características que debe cumplir un sitio alterno de negocio y de TI	**Táctico**	Operaciones
2. Seleccionar los sitios alternos para los procesos críticos de Negocio y TI.	**Táctico**	Gerencia de Finanzas
3. Definir los recursos mínimos que necesitan adquirirse y cuáles requieren ser trasladados a los sitios alternos.	**Táctico**	Operaciones
Priorización de aplicaciones/servidores		
4. Anualmente, revisar el estado de los servidores, considerando su capacidad, antigüedad y utilidad para determinar si es necesario adquirir nuevos servidores o redistribuir la carga de los mismos.	**Táctico**	Equipo TIC
5. Definir procedimientos para la adquisición e integración de nuevas aplicaciones o sistemas al ambiente de producción y al DRP. Estos procedimientos deberán incluir la realización del análisis completo para definir el RPO y RPO correspondiente.	**Táctico**	Equipo TIC
6. Realizar y mantener actualizado un inventario de aplicaciones y servidores con el fin de facilitar el mantenimiento y revisión de los mismos.	**Táctico**	Equipo TIC
Asegurar enlaces de comunicación:		
7. Asegurar en el Sitio Alterno una salida a Internet (mínimo 24 Mb) que cubra los requerimientos de las aplicaciones dentro de las primeras horas	**Táctico**	Equipo TIC

Tecnología

Estrategia	Tipo	Responsable
Equipos de cómputo / equipos de comunicaciones		
1. Elaborar un inventario de aplicaciones y sistemas, considerando la siguiente información: ➢ Área responsable ➢ Nombre de aplicación o sistema ➢ Procesos, productos o servicios que soporta ➢ Infraestructura mínima ➢ Usuarios ➢ Administrador de sistema ➢ Vigencia ➢ Proveedor ➢ Versión ➢ Fecha de último mantenimiento	**Operativo**	Equipo TIC
2. Elaborar una lista de requerimientos de equipos de cómputo (cantidad, tipo y características técnicas) y de oficina que estarán ubicados en el sitio alterno	**Operativo**	Equipo TIC
3. Dependiendo del tipo de Sitio Alterno, distribuir los recursos según las necesidades, determinando qué equipos estarán en el sitio Alterno permanentemente y cuáles tendrán que ser trasladados después de ocurrido el desastre	**Operativo**	Equipo TIC
4. Considerar como alternativa el uso de switches inalámbricos para lograr acelerar la disponibilidad de la red. Esto es importante para lograr que las computadoras portátiles se conecten de manera rápida, en caso el Sitio Alterno requiera habilitarse para más personal.	**Operativo**	Equipo TIC
Pruebas y simulacros		
5. Realizar pruebas periódicas a los equipos de comunicación en caso de crisis, como lo son lo	**Estratégico**	Equipo TIC

Estrategia	Tipo	Responsable
los teléfonos en sitios alternos, radios y celulares satelitales, con el fin de asegurar su correcto funcionamiento cuando sea oportuno.		
6. Realizar simulacros de ejecución de operaciones en contingencia desde el sitio alterno, midiendo los tiempos para compararlos con los indicadores BIA e identificar oportunidades de mejora.	**Estratégico**	Equipo TIC
Insumos y suministros (Compras)		
7. Definir un inventario de las necesidades mínimas que requiere cada Sitio Alterno de Operación considerando una cantidad promedio de horas de interrupción.	**Operativo**	Administración
8. Establecer un listado de proveedores titulares hasta 2 alternos de insumos y suministros.	**Operativo**	Administración
Políticas		
9. Definir políticas para alinear el proceso de inventariado y actualización de datos de equipos de cómputo con los objetivos del SGCN.	**Operativo**	Administración

Información

Estrategia	Tipo	Responsable
Política para la gestión de registros vitales		
1. Definir políticas de gestión de seguridad de información tomando en cuenta el rol crítico que tiene el proveedor de custodia de documentos físicos, de modo que se cumplan con las normas internas y regulaciones nacionales.	**Estratégico**	Área de Riesgos
2. Definir, como parte de la política institucional de seguridad de la información, requerimientos mínimos a cumplir por los proveedores de custodia de documentos físicos y digitales.	**Estratégico**	Área de Riesgos

Estrategia	Tipo	Responsable
3. Definir procedimientos para el traslado de la información en caso de la ocurrencia de una crisis, estableciendo acuerdos con el proveedor.	**Estratégico**	Equipo TIC
Gestión de la información		
6. Elaborar y mantener actualizado un inventario consolidado por área de la información física o digital que se maneja por proceso, tomando en cuenta la criticidad y el riesgo que implica la custodia de los mismos.	**Estratégico**	Cada Área de Negocio
7. Identificar al custodio responsable de los registros vitales tomando como referencia la información relevada en el BIA.	**Operativo**	Cada Área de Negocio
8. Usando el inventario de documentos físicos y digitales, evaluar las diferentes medidas de seguridad que se deben tomar para cada documento.	**Operativo**	Área de Riesgos
Accesos y roles		
9. Identificar al personal afín que puede servir de apoyo en caso de contingencia.	**Operativo**	Cada Área de Negocio
10. Asignar a un custodio de la información, que asegure su integridad y confidencialidad.	**Operativo**	Cada Área de Negocio
11. Crear roles adicionales para que personal afín pueda tener acceso a la red solo en caso de contingencia.	**Operativo**	Área de Riesgo
12. Coordinar con el personal de control de accesos y elaborar un procedimiento, para que se puedan habilitar accesos/roles especiales en caso contingencia para el personal de apoyo.	**Operativo**	Seguridad de la Información
Capacitación		
13. Difundir la política de manejo de información crítica	**Estratégico**	Seguridad de la Información

Proveedores

Estrategia	Tipo	Responsable

Estrategia	Tipo	Responsable
Proceso de contratación		
1. Definir estándares mínimos de cumplimiento, con el fin de contratar servicios de alta calidad acorde a las necesidades de la empresa.	**Estratégico**	Área de compras
Acuerdos de servicio y/o cláusulas en los contratos		
2. Incorporar en los contratos, acuerdos de prioridad que permitan formalizar el compromiso de los proveedores para realizar una primera evaluación de los daños y determinar la posibilidad de continuar las operaciones en la instalación afectada.	**Operativo**	Seguridad de la Información
3. Identificar proveedores para la reconstrucción/reparación de las instalaciones y establecer contratos que contengan acuerdos de nivel de servicio requerido.	**Operativo**	Administración
4. Incorporar en los contratos, una descripción completa de los requerimientos mínimos necesarios para el adecuado almacenamiento y traslado de los documentos en sus instalaciones.	**Operativo**	Administración
Políticas		
5. Actualizar anualmente la política de proveedores existente para contar con un contrato base que considere la inclusión de la cláusula de Riesgo Operacional, estableciendo los requisitos mínimos con los que debe cumplir un proveedor y contemple la auditoría de los esquemas de continuidad de negocios de los proveedores críticos.	**Operativo**	Área Legal
6. Establecer visitas periódicas a las instalaciones de los proveedores para poder censar/revisar los esquemas de continuidad ofrecidos por ellos	**Operativo**	Gerencia de Administración
Pruebas a proveedores		

Estrategia	Tipo	Responsable
7. Definir un Plan Anual de Pruebas de los servicios y/o aplicaciones relacionados a los procesos que están dentro del alcance del BIA que involucre a los principales proveedores, definiendo pruebas y ejercicios que evalúen diferentes escenarios y niveles de estrés.	**Operativo**	Área de Operaciones / Equipo TIC
8. Establecer comités con los principales proveedores con el fin de mostrar los resultados de sus pruebas, mostrando los gaps entre el servicio real y el esperado para plantear estrategias de mejora.	**Estratégico**	Área de Riesgos

16. Anexo 16: Matriz de riesgos por proceso

Suscripción, emisión y registro de información

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-01	Estructura del edificio dañado.	Sismo	Eventos Externos	Se diagnostica que los ambientes de la empresa no pueden ser usados para las operaciones después del sismo.	Falta de espacio para retomar las operaciones.	Imposibilidad de retomar las operaciones en un tiempo prudente dentro de un ambiente seguro para el personal	C-01	Establecimiento de Plan de Continuidad de Operaciones, aplicando para este caso el Plan de Gestión de Crisis y Plan de Emergencia.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Centro de negocios alternos implementados.	Riesgos / Continuidad	Preventivo	Buena	Continua				
							C-03	Contratación de Póliza de Seguros para Activos.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
R-02	Reacción de las personas frente a un evento natural en el edificio	Sismo / Incendio	Personas	Salida abrupta y desordenada de personas durante la evacuación.	Falta de entrenamiento, señalización y procedimientos en caso de sismos.	Personas heridas y/o desaparecidas durante evacuación.	C-01	Establecimiento de Plan de Emergencia.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	1	6	Moderado
							C-02	Señalización de ambientes, ubicando salidas de escape y alarmas en caso de emergencia	Seguridad	Disuasivo	Buena	Continua				
							C-03	Programación de capacitación de simulacros y seguridad en el trabajo.	Seguridad	Preventivo	Buena	Trimestral				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-03	Funcionamiento de servidor principal (ubicado en el 3er piso de edificio)	Sismo	Tecnología	Daños o golpes en el hardware, producidos durante el sismo.	Ausencia o inadecuado soporte físico de los servidores para evitar que sufran golpes	Inoperatividad del servidor y posible pérdida de datos.	C-01	Establecimiento de Plan de Continuidad de Operaciones, aplicando para este caso el Plan de Recuperación de Servicios de Tecnología de Información.	Riesgos / Continuidad	Preventivo	Buena	Continua	4	1	5	Moderado
							C-02	Implementación de servidor alterno y políticas de respaldo.	Equipo TIC	Preventivo	Buena	Continua				
							C-03	Contratación de Póliza de Seguros para Activos.	Riesgos / Continuidad	Preventivo	Buena	Continua				
R-04	Funcionamiento de servidor alterno.	Sismo	Tecnología	Dificultades o imposibilidad de uso de servidor alterno en caso se requiera su uso.	Error en el almacenamiento de información o dificultades para levantar el servicio desde el servidor.	Imposibilidad de retomar las operaciones dentro del tiempo planificado	C-01	Planificación y ejecución de pruebas de servidor alterno.	Equipo TIC	Preventivo	Buena	Trimestral	5	1	6	Moderado
							C-02	Establecimiento de un programa de mantenimiento de servidores.	Equipo TIC	Preventivo	Buena	Trimestral				
R-05	Infraestructura de centro de datos dañada.	Sismo / Incendio	Tecnología	Error en el funcionamiento, almacenamiento de datos proceso de respaldo.	Destrucción y/o deterioro de los equipos localizados en el lugar.	Posible pérdida de datos o hasta obsolescencia de los equipos	C-01	Proceso de respaldo constante en el servidor alterno	Equipo TIC	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Establecimiento de medidas de seguridad física en el centro de datos como por ejemplo:	Equipo TIC	Preventivo	Buena	Continua				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
								Detector de humo, sistemas de detección de incendios y refuerzos estructurales.								
							C-03	Mantenimiento y monitoreo periódico del estado del centro de datos, estableciendo estándares de condiciones mínimas y óptimas.	Equipo TIC	Preventivo	Buena	Bimestral				
							C-04	Intervención del equipo de recuperación autorizado, de modo que estén capacitados para tomar las medidas adecuadas con los equipos después de un desastre	Equipo TIC	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-06	Ingreso no autorizado a instalaciones de la empresa	Sismo / Saqueo	Eventos Externos	Robo de activos que se encuentran en el edificio de la empresa	Instalaciones vulnerables después del sismo, debido al pánico colectivo y las evacuaciones.	Pérdida o robo de activos de información críticos para la empresa.	C-01	Una vez comprobada la evacuación de los miembros de la organización y realizar las verificaciones convenientes, proceder al cierre de todas las posibles entradas a las instalaciones.	Equipo TIC	Preventivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Elaborar y mantener un inventario de activos de información para llevar un control de los activos que posee la empresa.	Riesgos / Continuidad	Preventivo	Excelente	Continua				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-03	Después del sismo y la evacuación, realizar la verificación de activos de información en base al último inventario elaborado para identificar qué activos faltan y cuál es su impacto en la operación de los procesos.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-07	Ingreso a centro de datos vulnerable	Sismo / Saqueo	Eventos Externos	Ingresos no autorizados al centro de datos.	Posibles fallas en los controles de entrada al edificio y al centro de datos después del sismo, ya que todos han evacuado.	Pérdida de información y robo de equipos.	C-01	Implementación de controles biométricos en la entrada del centro de datos, restringiendo el acceso de personas no autorizadas.	Equipo TIC	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Después del sismo y la evacuación, realizar la verificación de activos del centro de datos (cantidad de discos, servidores, cables, routers y otros) en base al último inventario elaborado para identificar las faltas, calcular el impacto en la operación y realizar la recuperación correspondiente	Equipo TIC	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-08	Disponibilidad de flujo eléctrico	Sismo	Tecnología	Pérdida de fluido eléctrico general (en todo Lima).	Fallas en la infraestructura del proveedor de luz.	Incapacidad para reiniciar operaciones y comunicaciones en centro alterno y/o	C-01	Uso de dispositivos de energía ininterrumpida UPS.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
						edificio principal	C-02	Instalación de grupos electrógenos.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
							C-03	Establecimiento de cronograma de mantenimiento y pruebas de grupo electrógeno y UPS, para asegurar su correcto funcionamiento.	Seguridad	Preventivo	Buena	Bimestral				
R-09	Disponibilidad de servicios telefónicos.	Sismo	Tecnología	Pérdida de servicio telefónico general.	Fallas en la infraestructura del proveedor de telefonía.	Incapacidad de comunicación entre coordinadores principales de gestión de crisis. Incapacidad de comunicación en la realización de operaciones de procesos de negocio.	C-01	Aplicación del plan de crisis, indicando que, frente a pérdida de telefonía se recomienda el uso del servicio de internet como forma alterna de comunicación.	Riesgos / Continuidad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Adquisición y uso de celulares satelitales para los coordinadores principales, de modo que las principales	Equipo TIC	Preventivo	Buena	Continua				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
								comunicaciones no se vean interrumpidas.								
R-10	Documentos físicos críticos para los procesos negocio.	Sismo / Incendio	Procesos	Exposición de documentos físico críticos durante la ocurrencia del sismo (y posible incendio).	Inadecuada protección de documentos críticos.	Pérdida o deterioro de documentos físicos necesarios para continuar con las operaciones de los procesos críticos de negocio.	C-01	Contratación de servicio de custodia de documentos con un proveedor.	Equipo TIC	Preventivo	Regular	Continua	5	2	7	Alto
							C-02	Digitalización de documentos críticos, almacenados en servidores (con el respaldo correspondiente).	Equipo TIC	Preventivo	Buena	Continua				
R-10	Disponibilidad de servicio de custodia de documentos físicos.	Sismo / Incendio	Procesos	Falla en servicio del proveedor de custodia.	Error en procedimientos o ambientes de custodia durante sismo.	Pérdida o deterioro de documentos físicos usados como evidencia o resultado de procesos.	C-01	Establecimiento de SLA con el proveedor, incluyendo revisiones periódicas para asegurar su disponibilidad	Equipo TIC	Preventivo	Buena	Semestral	2	1	3	Bajo
R-11	Tercerización de servicios de TI	Sismo	Procesos	Dificultades en la administración del centro de cómputo principal	Personal disponible insuficiente para la revisión y recuperación de equipos después de desastre.	Posible diagnóstico inadecuado de equipos y dificultades en la recuperación de servicios.	C-01	Establecimiento de SLA con el proveedor, estableciendo términos de servicio en días estándar y requerimientos específicos en caso de crisis.	Equipo TIC	Preventivo	Buena	Continua	3	1	4	Moderado

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-12	Personal de operaciones	Sismo / Incendio	Procesos	Personal crítico para los procesos (como lo son los analistas de operaciones) con dificultades de acción en caso de desastre.	Falta de capacitaciones y simulacros de ejecución de planes de acción en caso de desastres.	Lentitud de procesos y sobrecarga de trabajo, creando un cuello de bottella en el proceso.	C-01	Programación de capacitaciones y simulacros.	Seguridad	Preventivo	Buena	Bimestral	4	3	7	Alto
							C-02	Establecimiento de políticas de servicio, que establezcan qué servicios estarán disponibles en caso de crisis o desastre, tomando en cuenta los más críticos para el negocio.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
R-13	Jefes y/o Gerentes autorizadores	Sismo	Personas	Necesidad de tener conformidad de documentos (como órdenes de pago y liquidaciones de siniestros) para continuar con el proceso.	Ausencia por convalecencia o fallecimiento de jefe y/o gerente.}	Interrupción del proceso y acumulación de documentos (como órdenes de pago y liquidación de siniestros)	C-01	Establecimiento de hasta 2 personas alternas que tengan la potestad de firmar documentos en representación de los jefes y/o gerentes.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	2	7	Alto

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-15	Entrega de documentos enviados al cliente y/o interesado por Courier	Sismo	Procesos	Dificultad o hasta imposibilidad de traslado de documentos al cliente.	Fallas en el servicio del proveedor o dificultad de acceso a algunos lugares que pudieron ser muy afectados del sismo.	Demora en la entrega de documentos, pudiendo incumplir plazos acordados.	C-01	Establecimiento de proveedores alternos, definiendo el alcance por ubicación y distribuyendo el trabajo.	Riesgos / Continuidad	Preventivo	Buena	Continua	3	2	5	Moderado
R-16	Sistema de atención de consultas	Sismo	Tecnología	Caída o lentitud extrema del sistema de atención de consultas.	Falla en infraestructura del centro de datos.	Gran cantidad de reportes de quedas de clientes, quienes necesitan con urgencia el servicio de consultas y reclamos.	C-01	Establecimiento de procesos alternos de registro, atención y cierre de consultas o reclamos que no hagan uso del sistema, permitiendo almacenar los registros en archivos digitales o formularios físicos para que, una vez restaurado el sistema, se guarden correctamente.	Equipo TIC	Correctivo	Excelente	Continua	5	4	9	Extremo
R-17	Tareas asignadas al personal	Sismo	Procesos	Ausencia o escasez de personal para realizar las tareas administrativas y	Muerte u hospitalización de personal producto del sismo o aumento de carga laboral.	Cuellos de botella o falta de recursos humanos que realice las actividades necesarias.	C-01	Asignación de personas alternas para los roles más críticos en la ejecución de los procesos.	Riesgos / Continuidad	Preventivo	Buena	Anual	5	4	9	Extremo

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
				operativas de cada uno de los procesos.			C-02	Capacitaciones a personas alternas, de modo que estén actualizadas e informadas de los posibles cambios a lo largo del tiempo.	Riesgos / Continuidad	Preventivo	Buena	Semestral				
							C-03	Realizar una adecuada gestión del conocimiento, elaborando un manual detallado y actualizado de las tareas y funciones de cada rol.	Riesgos / Continuidad	Preventivo	Buena	Continua				
							C-04	Establecimiento de contrato con proveedor de recursos humanos, quien será el encargado de abastecer de personal "alterno" competente para los procesos afectados.	Riesgos / Continuidad	Preventivo	Buena	Anual				
R-20	Cableado y conexiones eléctricas.	Sismo	Tecnología	Corto circuito en conexiones de las oficinas de la empresa.	Movimiento propio del sismo y fallas eléctricas en las instalaciones	Personas heridas cercanas al perímetro heridas. Incendios y deterioro o maltrato de equipos, documentación	C-01	Establecimiento de procedimientos que permitan apagar el fluido eléctrico a partir de un grado determinado de sismo.	Seguridad	Preventivo	Regular	Continua	4	2	6	Moderado

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
						y otros activos de la empresa.										

Atención de solicitudes de Cobertura

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-01	Estructura del edificio dañando.	Sismo	Eventos Externos	Se diagnostica que los ambientes de la empresa no pueden ser usados para las operaciones después del sismo.	Falta de espacio para retomar las operaciones.	Imposibilidad de retomar las operaciones en un tiempo prudente dentro de un ambiente seguro para el personal	C-01	Establecimiento de Plan de Continuidad de Operaciones, aplicando para este caso el Plan de Gestión de Crisis y Plan de Emergencia.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Centro de negocios alternos implementados.	Riesgos / Continuidad	Preventivo	Buena	Continua				
							C-03	Contratación de Póliza de Seguros para Activos.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
R-02	Reacción de las personas frente a un evento natural en el edificio	Sismo / Incendio	Personas	Salida abrupta y desordenada de personas durante la evacuación.	Falta de entrenamiento, señalización y procedimientos en caso de sismos.	Personas heridas y/o desaparecidas durante evacuación.	C-01	Establecimiento de Plan de Emergencia.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	1	6	Moderado
							C-02	Señalización de ambientes, ubicando salidas de escape y alarmas en caso de emergencia	Seguridad	Disuasivo	Buena	Continua				
							C-03	Programación de capacitación de simulacros y seguridad en el trabajo.	Seguridad	Preventivo	Buena	Trimestral				
R-03	Funcionamiento de servidor principal (ubicado en el 3er piso de edificio)	Sismo	Tecnología	Daños o golpes en el hardware, producidos durante el sismo.	Ausencia o inadecuado soporte físico de los servidores para evitar que sufran golpes	Inoperatividad del servidor y posible pérdida de datos.	C-01	Establecimiento de Plan de Continuidad de Operaciones, aplicando para este caso el Plan de Recuperación de Servicios de Tecnología de Información.	Riesgos / Continuidad	Preventivo	Buena	Continua	4	1	5	Moderado

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-02	Implementación de servidor alterno y políticas de respaldo	Equipo TIC	Preventivo	Buena	Continua				
							C-03	Contratación de Póliza de Seguros para Activos.	Riesgos / Continuidad	Preventivo	Buena	Continua				
R-04	Funcionamiento de servidor alterno.	Sismo	Tecnología	Dificultades o imposibilidad de uso de servidor alterno en caso se queriera su uso.	Error en el almacenamiento de información o dificultades para levantar el servicio desde el servidor.	Imposibilidad de retomar las operaciones dentro del tiempo planificado	C-01	Planificación y ejecución de pruebas de servidor alterno.	Equipo TIC	Preventivo	Buena	Trimestral	5	1	6	Moderado
							C-02	Establecimiento de un programa de mantenimiento de servidores.	Equipo TIC	Preventivo	Buena	Trimestral				
R-05	Infraestructura de centro de datos dañada.	Sismo / Incendio	Tecnología	Error en el funcionamiento, almacenamiento de datos proceso de respaldo.	Destrucción y/o deterioro de los equipos localizados en el lugar.	Posible pérdida de datos o hasta obsolescencia de los equipos	C-01	Proceso de respaldo constante en el servidor alterno	Equipo TIC	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Establecimiento de medidas de seguridad física en el centro de datos como por ejemplo: Detector de humo, sistemas de detección de incendios y refuerzos estructurales.	Equipo TIC	Preventivo	Buena	Continua				
							C-03	Mantenimiento y monitoreo periódico del estado del centro de datos, estableciendo	Equipo TIC	Preventivo	Buena	Bimestral				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
								estándares de condiciones mínimas y óptimas.								
							C-04	Intervención del equipo de recuperación autorizado, de modo que estén capacitados para tomar las medidas adecuadas con los equipos después de un desastre	Equipo TIC	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-06	Ingreso no autorizado a instalaciones de la empresa	Sismo / Saqueo	Eventos Externos	Robo de activos que se encuentran en el edificio de la empresa	Instalaciones vulnerables después del sismo, debido al pánico colectivo y las evacuaciones.	Pérdida o robo de activos de información críticos para la empresa.	C-01	Una vez comprobada la evacuación de los miembros de la organización y realizar las verificaciones convenientes, proceder al cierre de todas las posibles entradas a las instalaciones.	Equipo TIC	Preventivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Elaborar y mantener un inventario de activos de información para llevar un control de los activos que posee la empresa.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
							C-03	Después del sismo y la evacuación, realizar la verificación de activos de información en base al último inventario elaborado para identificar qué activos faltan y cuál es su impacto en la operación de los procesos.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-07	Ingreso a centro de datos vulnerable	Sismo / Saqueo	Eventos Externos	Ingresos no autorizados al centro de datos.	Posibles fallas en los controles de entrada al edificio y al centro de datos después del sismo, ya que todos han evacuado.	Pérdida de información y robo de equipos.	C-01	Implementación de controles biométricos en la entrada del centro de datos, restringiendo el acceso de personas no autorizadas.	Equipo TIC	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Después del sismo y la evacuación, realizar la verificación de activos del centro de datos (cantidad de discos, servidores, cables, routers y otros) en base al último inventario elaborado para identificar las faltas, calcular el impacto en la operación y realizar la recuperación correspondiente	Equipo TIC	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-08	Disponibilidad de flujo eléctrico	Sismo	Tecnología	Pérdida de fluido eléctrico general (en todo Lima).	Fallas en la infraestructura del proveedor de luz.	Incapacidad para reiniciar operaciones y comunicaciones en centro alterno y/o edificio principal	C-01	Uso de dispositivos de energía ininterrumpida UPS.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Instalación de grupos electrógenos.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-03	Establecimiento de cronograma de mantenimiento y pruebas de grupo electrógeno y UPS, para asegurar su correcto funcionamiento.	Seguridad	Preventivo	Buena	Bimestral				
R-09	Disponibilidad de servicios telefónicos.	Sismo	Tecnología	Pérdida de servicio telefónico general.	Fallas en la infraestructura del proveedor de telefonía.	Incapacidad de comunicación entre coordinadores principales de gestión de crisis. Incapacidad de comunicación en la realización de operaciones de procesos de negocio.	C-01	Aplicación del plan de crisis, indicando que, frente a pérdida de telefonía se recomienda el uso del servicio de internet como forma alterna de comunicación.	Riesgos / Continuidad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Adquisición y uso de celulares satelitales para los coordinadores principales, de modo que las principales comunicaciones no se vean interrumpidas.	Equipo TIC	Preventivo	Buena	Continua				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-10	Documentos físicos críticos para los procesos negocio.	Sismo / Incendio	Procesos	Exposición de documentos físico críticos durante la ocurrencia del sismo (y posible incendio).	Inadecuada protección de documentos críticos.	Pérdida o deterioro de documentos físicos necesarios para continuar con las operaciones de los procesos críticos de negocio.	C-01	Contratación de servicio de custodia de documentos con un proveedor.	Equipo TIC	Preventivo	Regular	Continua	5	2	7	Alto
							C-02	Digitalización de documentos críticos, almacenados en servidores (con el respaldo correspondiente).	Equipo TIC	Preventivo	Buena	Continua				
R-10	Disponibilidad de servicio de custodia de documentos físicos.	Sismo / Incendio	Procesos	Falla en servicio del proveedor de custodia.	Error en procedimientos o ambientes de custodia durante sismo.	Pérdida o deterioro de documentos físicos usados como evidencia o resultado de procesos.	C-01	Establecimiento de SLA con el proveedor, incluyendo revisiones periódicas para asegurar su disponibilidad	Equipo TIC	Preventivo	Buena	Semestral	2	1	3	Bajo
R-11	Tercerización de servicios de TI	Sismo	Procesos	Dificultades en la administración del centro de cómputo principal	Personal disponible insuficiente para la revisión y recuperación de equipos después de desastre.	Posible diagnóstico inadecuado de equipos y dificultades en la recuperación de servicios.	C-01	Establecimiento de SLA con el proveedor, estableciendo términos de servicio en días estándar y requerimientos específicos en caso de crisis.	Equipo TIC	Preventivo	Buena	Continua	3	1	4	Moderado
R-12	Personal de operaciones	Sismo /	Procesos	Personal crítico para	Falta de capacitaciones	Lentitud de procesos y	C-01	Programación de capacitaciones y simulacros.	Seguridad	Preventivo	Buena	Bimestral	4	3	7	Alto

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
		Incendio		los procesos (como lo son los analistas de operaciones) con dificultades de acción en caso de desastre.	y simulacros de ejecución de planes de acción en caso de desastres.	sobrecarga de trabajo, creando un cuello de botella en el proceso.	C-02	Establecimiento de políticas de servicio, que establezcan qué servicios estarán disponibles en caso de crisis o desastre, tomando en cuenta los más críticos para el negocio.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
R-13	Jefes y/o Gerentes autorizadores	Sismo	Personas	Necesidad de tener conformidad de documentos (como órdenes de pago y liquidaciones de siniestros) para continuar con el proceso.	Ausencia por convalecencia o fallecimiento de jefe y/o gerente.}	Interrupción del proceso y acumulación de documentos (como órdenes de pago y liquidación de siniestros)	C-01	Establecimiento de hasta 2 personas alternas que tengan la potestad de firmar documentos en representación de los jefes y/o gerentes.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	2	7	Alto

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-14	Entrega de documentos enviados al cliente y/o interesado por Courier	Sismo	Procesos	Dificultad o hasta imposibilidad de traslado de documentos al cliente.	Fallas en el servicio del proveedor o dificultad de acceso a algunos lugares que pudieron ser muy afectados del sismo.	Demora en la entrega de documentos, pudiendo incumplir plazos acordados.	C-01	Establecimiento de proveedores alternos, definiendo el alcance por ubicación y distribuyendo el trabajo.	Riesgos / Continuidad	Preventivo	Buena	Continua	3	2	5	Moderado
R-15	Tareas asignadas al personal	Sismo	Procesos	Ausencia o escacez de personal para realizar las tareas administrativas y operativas de cada uno de los procesos.	Muerte u hospitalización de personal producto del sismo o aumento de carga laboral.	Cuellos de botella o falta de recursos humanos que realice las actividades necesarias.	C-01	Asignación de personas alternas para los roles más críticos en la ejecución de los procesos.	Riesgos / Continuidad	Preventivo	Buena	Anual	5	4	9	Extremo
							C-02	Capacitaciones a personas alternas, de modo que estén actualizadas e informadas de los posibles cambios a lo largo del tiempo.	Riesgos / Continuidad	Preventivo	Buena	Semestral				
							C-03	Realizar una adecuada gestión del conocimiento, elaborando un manual detallado y actualizado de las tareas y funciones de cada rol.	Riesgos / Continuidad	Preventivo	Buena	Continua				

Riesgo del Proceso							Controles					Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-04	Establecimiento de contrato con proveedor de recursos humanos, quien será el encargado de abastecer de personal "alterno" competente para los procesos afectados.	Riesgos / Continuidad	Preventivo	Buena	Anual				
R-16	Cableado y conexiones eléctricas.	Sismo	Tecnología	Corto circuito en conexiones de las oficinas de la empresa.	Movimiento propio del sismo y fallas eléctricas en las instalaciones	Personas heridas cercanas al perímetro heridas. Incendios y deterioro o maltrato de equipos, documentación y otros activos de la empresa.	C-01	Establecimiento de procedimientos que permitan apagar el fluido eléctrico a partir de un grado determinado de sismo.	Seguridad	Preventivo	Regular	Continua	4	2	6	Moderado

Emisión de la póliza y endoso

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-01	Estructura del edificio dañado.	Sismo	Eventos Externos	Se diagnostica que los ambientes de la empresa no pueden ser usados para las operaciones después del sismo.	Falta de espacio para retomar las operaciones.	Imposibilidad de retomar las operaciones en un tiempo prudente dentro de un ambiente seguro para el personal	C-01	Establecimiento de Plan de Continuidad de Operaciones, aplicando para este caso el Plan de Gestión de Crisis y Plan de Emergencia.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Centro de negocios alternos implementados.	Riesgos / Continuidad	Preventivo	Buena	Continua				
							C-03	Contratación de Póliza de Seguros para Activos.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
R-02	Reacción de las personas frente a un evento natural en el edificio	Sismo / Incendio	Personas	Salida abrupta y desordenada de personas durante la evacuación.	Falta de entrenamiento, señalización y procedimientos en caso de sismos.	Personas heridas y/o desaparecidas durante evacuación.	C-01	Establecimiento de Plan de Emergencia.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	1	6	Moderado
							C-02	Señalización de ambientes, ubicando salidas de escape y alarmas en caso de emergencia	Seguridad	Disuasivo	Buena	Continua				
							C-03	Programación de capacitación de simulacros y seguridad en el trabajo.	Seguridad	Preventivo	Buena	Trimestral				
R-03	Funcionamiento de servidor principal (ubicado en el 3er piso de edificio)	Sismo	Tecnología	Daños o golpes en el hardware, producidos durante el sismo.	Ausencia o inadecuado soporte físico de los servidores para evitar que sufran golpes	Inoperatividad del servidor y posible pérdida de datos.	C-01	Establecimiento de Plan de Continuidad de Operaciones, aplicando para este caso el Plan de Recuperación de Servicios de Tecnología de Información.	Riesgos / Continuidad	Preventivo	Buena	Continua	4	1	5	Moderado

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-02	Implementación de servidor alterno y políticas de respaldo	Equipo TIC	Preventivo	Buena	Continua				
							C-03	Contratación de Póliza de Seguros para Activos.	Riesgos / Continuidad	Preventivo	Buena	Continua				
R-04	Funcionamiento de servidor alterno.	Sismo	Tecnología	Dificultades o imposibilidad de uso de servidor alterno en caso se quiera su uso.	Error en el almacenamiento de información o dificultades para levantar el servicio desde el servidor.	Imposibilidad de retomar las operaciones dentro del tiempo planificado	C-01	Planificación y ejecución de pruebas de servidor alterno.	Equipo TIC	Preventivo	Buena	Trimestral	5	1	6	Moderado
							C-02	Establecimiento de un programa de mantenimiento de servidores.	Equipo TIC	Preventivo	Buena	Trimestral				
R-05	Infraestructura de centro de datos dañada.	Sismo / Incendio	Tecnología	Error en el funcionamiento, almacenamiento de datos proceso de respaldo.	Destrucción y/o deterioro de los equipos localizados en el lugar.	Posible pérdida de datos o hasta obsolescencia de los equipos	C-01	Proceso de respaldo constante en el servidor alterno	Equipo TIC	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Establecimiento de medidas de seguridad física en el centro de datos como por ejemplo: Detector de humo, sistemas de detección de incendios y refuerzos estructurales.	Equipo TIC	Preventivo	Buena	Continua				
							C-03	Mantenimiento y monitoreo periódico del estado del centro de datos, estableciendo	Equipo TIC	Preventivo	Buena	Bimestral				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
								estándares de condiciones mínimas y óptimas.								
							C-04	Intervención del equipo de recuperación autorizado, de modo que estén capacitados para tomar las medidas adecuadas con los equipos después de un desastre	Equipo TIC	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-06	Ingreso no autorizado a instalaciones de la empresa	Sismo / Saqueo	Eventos Externos	Robo de activos que se encuentran en el edificio de la empresa	Instalaciones vulnerables después del sismo, debido al pánico colectivo y las evacuaciones.	Pérdida o robo de activos de información críticos para la empresa.	C-01	Una vez comprobada la evacuación de los miembros de la organización y realizar las verificaciones convenientes, proceder al cierre de todas las posibles entradas a las instalaciones.	Equipo TIC	Preventivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Elaborar y mantener un inventario de activos de información para llevar un control de los activos que posee la empresa.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
							C-03	Después del sismo y la evacuación, realizar la verificación de activos de información en base al último inventario elaborado para identificar qué activos faltan y cuál es su impacto en la operación de los procesos.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-07	Ingreso a centro de datos vulnerable	Sismo / Saqueo	Eventos Externos	Ingresos no autorizados al centro de datos.	Posibles fallas en los controles de entrada al edificio y al centro de datos después del sismo, ya que todos han evacuado.	Pérdida de información y robo de equipos.	C-01	Implementación de controles biométricos en la entrada del centro de datos, restringiendo el acceso de personas no autorizadas.	Equipo TIC	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Después del sismo y la evacuación, realizar la verificación de activos del centro de datos (cantidad de discos, servidores, cables, routers y otros) en base al último inventario elaborado para identificar las faltas, calcular el impacto en la operación y realizar la recuperación correspondiente	Equipo TIC	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-08	Disponibilidad de flujo eléctrico	Sismo	Tecnología	Pérdida de fluido eléctrico general (en todo Lima).	Fallas en la infraestructura del proveedor de luz.	Incapacidad para reiniciar operaciones y comunicaciones en centro alterno y/o edificio principal	C-01	Uso de dispositivos de energía ininterrumpida UPS.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Instalación de grupos electrógenos.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-03	Establecimiento de cronograma de mantenimiento y pruebas de grupo electrógeno y UPS, para asegurar su correcto funcionamiento.	Seguridad	Preventivo	Buena	Bimestral				
R-09	Disponibilidad de servicios telefónicos.	Sismo	Tecnología	Pérdida de servicio telefónico general.	Fallas en la infraestructura del proveedor de telefonía.	Incapacidad de comunicación entre coordinadores principales de gestión de crisis. Incapacidad de comunicación en la realización de operaciones de procesos de negocio.	C-01	Aplicación del plan de crisis, indicando que, frente a pérdida de telefonía se recomienda el uso del servicio de internet como forma alterna de comunicación.	Riesgos / Continuidad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Adquisición y uso de celulares satelitales para los coordinadores principales, de modo que las principales comunicaciones no se vean interrumpidas.	Equipo TIC	Preventivo	Buena	Continua				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-10	Documentos físicos críticos para los procesos negocio.	Sismo / Incendio	Procesos	Exposición de documentos físico críticos durante la ocurrencia del sismo (y posible incendio).	Inadecuada protección de documentos críticos.	Pérdida o deterioro de documentos físicos necesarios para continuar con las operaciones de los procesos críticos de negocio.	C-01	Contratación de servicio de custodia de documentos con un proveedor.	Equipo TIC	Preventivo	Regular	Continua	5	2	7	Alto
							C-02	Digitalización de documentos críticos, almacenados en servidores (con el respaldo correspondiente).	Equipo TIC	Preventivo	Buena	Continua				
R-11	Disponibilidad de servicio de custodia de documentos físicos.	Sismo / Incendio	Procesos	Falla en servicio del proveedor de custodia.	Error en procedimientos o ambientes de custodia durante sismo.	Pérdida o deterioro de documentos físicos usados como evidencia o resultado de procesos.	C-01	Establecimiento de SLA con el proveedor, incluyendo revisiones periódicas para asegurar su disponibilidad	Equipo TIC	Preventivo	Buena	Semestral	2	1	3	Bajo
R-12	Tercerización de servicios de TI	Sismo	Procesos	Dificultades en la administración del centro de cómputo principal	Personal disponible insuficiente para la revisión y recuperación de equipos después de desastre.	Posible diagnóstico inadecuado de equipos y dificultades en la recuperación de servicios.	C-01	Establecimiento de SLA con el proveedor, estableciendo términos de servicio en días estándar y requerimientos específicos en caso de crisis.	Equipo TIC	Preventivo	Buena	Continua	3	1	4	Moderado
R-13	Personal de operaciones	Sismo /	Procesos	Personal crítico para	Falta de capacitaciones	Lentitud de procesos y	C-01	Programación de capacitaciones y simulacros.	Seguridad	Preventivo	Buena	Bimestral	4	3	7	Alto

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
		Incendio		los procesos (como lo son los analistas de operaciones) con dificultades de acción en caso de desastre.	y simulacros de ejecución de planes de acción en caso de desastres.	sobrecarga de trabajo, creando un cuello de botella en el proceso.	C-02	Establecimiento de políticas de servicio, que establezcan qué servicios estarán disponibles en caso de crisis o desastre, tomando en cuenta los más críticos para el negocio.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
R-14	Jefes y/o Gerentes autorizadores	Sismo	Personas	Necesidad de tener conformidad de documentos (como órdenes de pago y liquidaciones de siniestros) para continuar con el proceso.	Ausencia por convalecencia o fallecimiento de jefe y/o gerente.}	Interrupción del proceso y acumulación de documentos (como órdenes de pago y liquidación de siniestros)	C-01	Establecimiento de hasta 2 personas alternas que tengan la potestad de firmar documentos en representación de los jefes y/o gerentes.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	2	7	Alto

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-15	Entrega de documentos enviados al cliente y/o interesado por courier	Sismo	Procesos	Dificultad o hasta imposibilidad de traslado de documentos al cliente.	Fallas en el servicio del proveedor o dificultad de acceso a algunos lugares que pudieron ser muy afectados del sismo.	Demora en la entrega de documentos, pudiendo incumplir plazos acordados.	C-01	Establecimiento de proveedores alternos, definiendo el alcance por ubicación y distribuyendo el trabajo.	Riesgos / Continuidad	Preventivo	Buena	Continua	3	2	5	Moderado
R-16	Aplicativo MELER	Sismo	Tecnología	Indisponibilidad del aplicativo web para realizar consultas.	Error en infraestructura o servicio ofrecido por la SUNAT.	Imposibilidad de determinar las cotizaciones ganadas, interrumpiendo el proceso.	C-01	Definir diferentes canales de comunicación (cartas, mail, radio, carteles, entre otros) para explicar el motivo de la indisponibilidad del proceso.	Comunicaciones	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	2	2	4	Moderado
R-17	Tareas asignadas al personal	Sismo	Procesos	Ausencia o escacez de personal para realizar las tareas administrativas y	Muerte u hospitalización de personal producto del sismo o aumento de carga laboral.	Cuellos de botella o falta de recursos humanos que realice las actividades necesarias.	C-01	Asignación de personas alternas para los roles más críticos en la ejecución de los procesos.	Riesgos / Continuidad	Preventivo	Buena	Anual	5	4	9	Extremo

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
				operativas de cada uno de los procesos.			C-02	Capacitaciones a personas alternas, de modo que estén actualizadas e informadas de los posibles cambios a lo largo del tiempo.	Riesgos / Continuidad	Preventivo	Buena	Semestral				
							C-03	Realizar una adecuada gestión del conocimiento, elaborando un manual detallado y actualizado de las tareas y funciones de cada rol.	Riesgos / Continuidad	Preventivo	Buena	Continua				
							C-04	Establecimiento de contrato con proveedor de recursos humanos, quien será el encargado de abastecer de personal "alterno" competente para los procesos afectados.	Riesgos / Continuidad	Preventivo	Buena	Anual				
R-18	Cableado y conexiones eléctricas.	Sismo	Tecnología	Corto circuito en conexiones de las oficinas de la empresa.	Movimiento propio del sismo y fallas eléctricas en las instalaciones	Personas heridas cercanas al perímetro heridas. Incendios y deterioro o maltrato de equipos, documentación y otros activos de la empresa.	C-01	Establecimiento de procedimientos que permitan apagar el fluido eléctrico a partir de un grado determinado de sismo.	Seguridad	Preventivo	Regular	Continua	4	2	6	Moderado

Gestión de servicio al cliente

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-01	Estructura del edificio dañada.	Sismo	Eventos Externos	Se diagnostica que los ambientes de la empresa no pueden ser usados para las operaciones después del sismo.	Falta de espacio para retomar las operaciones.	Imposibilidad de retomar las operaciones en un tiempo prudente dentro de un ambiente seguro para el personal	C-01	Establecimiento de Plan de Continuidad de Operaciones, aplicando para este caso el Plan de Gestión de Crisis y Plan de Emergencia.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Centro de negocios alternos implementados.	Riesgos / Continuidad	Preventivo	Buena	Continua				
							C-03	Contratación de Póliza de Seguros para Activos.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
R-02	Reacción de las personas frente a un evento natural en el edificio	Sismo / Incendio	Personas	Salida abrupta y desordenada de personas durante la evacuación.	Falta de entrenamiento, señalización y procedimientos en caso de sismos.	Personas heridas y/o desaparecidas durante evacuación.	C-01	Establecimiento de Plan de Emergencia.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	1	6	Moderado
							C-02	Señalización de ambientes, ubicando salidas de escape y alarmas en caso de emergencia	Seguridad	Disuasivo	Buena	Continua				
							C-03	Programación de capacitación de simulacros y seguridad en el trabajo.	Seguridad	Preventivo	Buena	Trimestral				
R-03	Funcionamiento de servidor principal (ubicado en el 3er piso de edificio)	Sismo	Tecnología	Daños o golpes en el hardware, producidos durante el sismo.	Ausencia o inadecuado soporte físico de los servidores para evitar que sufran golpes	Inoperatividad del servidor y posible pérdida de datos.	C-01	Establecimiento de Plan de Continuidad de Operaciones, aplicando para este caso el Plan de Recuperación de Servicios de Tecnología de Información.	Riesgos / Continuidad	Preventivo	Buena	Continua	4	1	5	Moderado

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-02	Implementación de servidor alterno y políticas de respaldo	Equipo TIC	Preventivo	Buena	Continua				
							C-03	Contratación de Póliza de Seguros para Activos.	Riesgos / Continuidad	Preventivo	Buena	Continua				
R-04	Funcionamiento de servidor alterno.	Sismo	Tecnología	Dificultades o imposibilidad de uso de servidor alterno en caso se quiera su uso.	Error en el almacenamiento de información o dificultades para levantar el servicio desde el servidor.	Imposibilidad de retomar las operaciones dentro del tiempo planificado	C-01	Planificación y ejecución de pruebas de servidor alterno.	Equipo TIC	Preventivo	Buena	Trimestral	5	1	6	Moderado
							C-02	Establecimiento de un programa de mantenimiento de servidores.	Equipo TIC	Preventivo	Buena	Trimestral				
R-05	Infraestructura de centro de datos dañada.	Sismo / Incendio	Tecnología	Error en el funcionamiento, almacenamiento de datos proceso de respaldo.	Destrucción y/o deterioro de los equipos localizados en el lugar.	Posible pérdida de datos o hasta obsolescencia de los equipos	C-01	Proceso de respaldo constante en el servidor alterno	Equipo TIC	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Establecimiento de medidas de seguridad física en el centro de datos como por ejemplo: Detector de humo, sistemas de detección de incendios y refuerzos estructurales.	Equipo TIC	Preventivo	Buena	Continua				
							C-03	Mantenimiento y monitoreo periódico del estado del centro de datos, estableciendo	Equipo TIC	Preventivo	Buena	Bimestral				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
								estándares de condiciones mínimas y óptimas.								
							C-04	Intervención del equipo de recuperación autorizado, de modo que estén capacitados para tomar las medidas adecuadas con los equipos después de un desastre	Equipo TIC	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-06	Ingreso no autorizado a instalaciones de la empresa	Sismo / Saqueo	Eventos Externos	Robo de activos que se encuentran en el edificio de la empresa	Instalaciones vulnerables después del sismo, debido al pánico colectivo y las evacuaciones.	Pérdida o robo de activos de información críticos para la empresa.	C-01	Una vez comprobada la evacuación de los miembros de la organización y realizar las verificaciones convenientes, proceder al cierre de todas las posibles entradas a las instalaciones.	Equipo TIC	Preventivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Elaborar y mantener un inventario de activos de información para llevar un control de los activos que posee la empresa.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
							C-03	Después del sismo y la evacuación, realizar la verificación de activos de información en base al último inventario elaborado para identificar qué activos faltan y cuál es su impacto en la operación de los procesos.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-07	Ingreso a centro de datos vulnerable	Sismo / Saqueo	Eventos Externos	Ingresos no autorizados al centro de datos.	Posibles fallas en los controles de entrada al edificio y al centro de datos después del sismo, ya que todos han evacuado.	Pérdida de información y robo de equipos.	C-01	Implementación de controles biométricos en la entrada del centro de datos, restringiendo el acceso de personas no autorizadas.	Equipo TIC	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Después del sismo y la evacuación, realizar la verificación de activos del centro de datos (cantidad de discos, servidores, cables, routers y otros) en base al último inventario elaborado para identificar las faltas, calcular el impacto en la operación y realizar la recuperación correspondiente	Equipo TIC	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-08	Disponibilidad de flujo eléctrico	Sismo	Tecnología	Pérdida de fluido eléctrico general (en todo Lima).	Fallas en la infraestructura del proveedor de luz.	Incapacidad para reiniciar operaciones y comunicaciones en centro alterno y/o edificio principal	C-01	Uso de dispositivos de energía ininterrumpida UPS.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Instalación de grupos electrógenos.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-03	Establecimiento de cronograma de mantenimiento y pruebas de grupo electrógeno y UPS, para asegurar su correcto funcionamiento.	Seguridad	Preventivo	Buena	Bimestral				
R-09	Disponibilidad de servicios telefónicos.	Sismo	Tecnología	Pérdida de servicio telefónico general.	Fallas en la infraestructura del proveedor de telefonía.	Incapacidad de comunicación entre coordinadores principales de gestión de crisis. Incapacidad de comunicación en la realización de operaciones de procesos de negocio.	C-01	Aplicación del plan de crisis, indicando que, frente a pérdida de telefonía se recomienda el uso del servicio de internet como forma alterna de comunicación.	Riesgos / Continuidad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Adquisición y uso de celulares satelitales para los coordinadores principales, de modo que las principales comunicaciones no se vean interrumpidas.	Equipo TIC	Preventivo	Buena	Continua				
R-12	Congestión de líneas telefónicas	Sismo	Tecnología	Posible caída de líneas telefónicas de atención	Gran incremento de llamadas telefónicas por	Indisponibilidad del servicio de atención al cliente.	C-01	Implementación de línea alterna de llamadas para disminuir el tráfico de llamadas.	Riesgos / Continuidad	Correctivo	Buena	No aplica (el control se aplica cuando el	5	4	9	Extremo

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
				de servicio al cliente para consultas y reclamos.	parte de los clientes.							evento ocurre)				
							C-02	Apertura de canales de comunicación secundarios: - Buzón de consultas (vía mail) - Módulos ambulatorios de consultas y reclamos ubicados estratégicamente.	Riesgos / Continuidad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-15	Entrega de documentos enviados al cliente y/o interesado por courier	Sismo	Procesos	Dificultad o hasta imposibilidad de traslado de documentos al cliente.	Fallas en el servicio del proveedor o dificultad de acceso a algunos lugares que pudieron ser muy afectados del sismo.	Demora en la entrega de documentos, pudiendo incumplir plazos acordados.	C-01	Establecimiento de proveedores alternos, definiendo el alcance por ubicación y distribuyendo el trabajo.	Riesgos / Continuidad	Preventivo	Buena	Continua	3	2	5	Moderado
R-16	Personal de atención de consultas	Sismo	Personas	Ausencia o escacez de personal adecuado y disponible para atender las consultas que servicio al cliente derive según el caso.	Sobrecarga de trabajo en momento de crisis.	Lentitud o hasta interrupción de servicio al cliente	C-01	Elaborar un manual de "Preguntas frecuentes" para los servicios disponibles, de modo que sirva de guía a las asesoras de servicio al cliente y se disminuyan las solicitudes que requieran ser derivadas.	Atención al cliente	Preventivo	Buena	Continua	5	2	7	Alto

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-18	Sistema de atención de consultas	Sismo	Tecnología	Caída o lentitud extrema del sistema de atención de consultas.	Falla en infraestructura del centro de datos.	Gran cantidad de reportes de quedas de clientes, quienes necesitan con urgencia el servicio de consultas y reclamos.	C-01	Establecimiento de procesos alternos de registro, atención y cierre de consultas o reclamos que no hagan uso del sistema, permitiendo almacenar los registros en archivos digitales o formularios físicos para que, una vez restaurado el sistema, se guarden correctamente.	Equipo TIC	Correctivo	Excelente	Continua	5	4	9	Extremo
R-19	Tareas asignadas al personal	Sismo	Procesos	Ausencia o escasez de personal para realizar las tareas administrativas y operativas de cada uno de los procesos.	Muerte u hospitalización de personal producto del sismo o aumento de carga laboral.	Cuellos de botella o falta de recursos humanos que realice las actividades necesarias.	C-01	Asignación de personas alternas para los roles más críticos en la ejecución de los procesos.	Riesgos / Continuidad	Preventivo	Buena	Anual	5	4	9	Extremo
							C-02	Capacitaciones a personas alternas, de modo que estén actualizadas e informadas de los posibles cambios a lo largo del tiempo.	Riesgos / Continuidad	Preventivo	Buena	Semestral				
							C-03	Realizar una adecuada gestión del conocimiento, elaborando un manual detallado y actualizado de las tareas y funciones de cada rol.	Riesgos / Continuidad	Preventivo	Buena	Continua				

Riesgo del Proceso							Controles					Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-04	Establecimiento de contrato con proveedor de recursos humanos, quien será el encargado de abastecer de personal "alterno" competente para los procesos afectados.	Riesgos / Continuidad	Preventivo	Buena	Anual				
R-20	Cableado y conexiones eléctricas.	Sismo	Tecnología	Corto circuito en conexiones de las oficinas de la empresa.	Movimiento propio del sismo y fallas eléctricas en las instalaciones	Personas heridas cercanas al perímetro heridas. Incendios y deterioro o maltrato de equipos, documentación y otros activos de la empresa.	C-01	Establecimiento de procedimientos que permitan apagar el fluido eléctrico a partir de un grado determinado de sismo.	Seguridad	Preventivo	Regular	Continua	4	2	6	Moderado

Gestión de Pagos

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-01	Estructura del edificio dañada.	Sismo	Eventos Externos	Se diagnostica que los ambientes de la empresa no pueden ser usados para las operaciones después del sismo.	Falta de espacio para retomar las operaciones.	Imposibilidad de retomar las operaciones en un tiempo prudente dentro de un ambiente seguro para el personal	C-01	Establecimiento de Plan de Continuidad de Operaciones, aplicando para este caso el Plan de Gestión de Crisis y Plan de Emergencia.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Centro de negocios alternos implementados.	Riesgos / Continuidad	Preventivo	Buena	Continua				
							C-03	Contratación de Póliza de Seguros para Activos.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
R-02	Reacción de las personas frente a un evento natural en el edificio	Sismo / Incendio	Personas	Salida abrupta y desordenada de personas durante la evacuación.	Falta de entrenamiento, señalización y procedimientos en caso de sismos.	Personas heridas y/o desaparecidas durante evacuación.	C-01	Establecimiento de Plan de Emergencia.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	1	6	Moderado
							C-02	Señalización de ambientes, ubicando salidas de escape y alarmas en caso de emergencia	Seguridad	Disuasivo	Buena	Continua				
							C-03	Programación de capacitación de simulacros y seguridad en el trabajo.	Seguridad	Preventivo	Buena	Trimestral				
R-03	Funcionamiento de servidor principal (ubicado en el 3er piso de edificio)	Sismo	Tecnología	Daños o golpes en el hardware, producidos durante el sismo.	Ausencia o inadecuado soporte físico de los servidores para evitar que sufran golpes	Inoperatividad del servidor y posible pérdida de datos.	C-01	Establecimiento de Plan de Continuidad de Operaciones, aplicando para este caso el Plan de Recuperación de Servicios de Tecnología de Información.	Riesgos / Continuidad	Preventivo	Buena	Continua	4	1	5	Moderado

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-02	Implementación de servidor alterno y políticas de respaldo	Equipo TIC	Preventivo	Buena	Continua				
							C-03	Contratación de Póliza de Seguros para Activos.	Riesgos / Continuidad	Preventivo	Buena	Continua				
R-04	Funcionamiento de servidor alterno.	Sismo	Tecnología	Dificultades o imposibilidad de uso de servidor alterno en caso se quiera su uso.	Error en el almacenamiento de información o dificultades para levantar el servicio desde el servidor.	Imposibilidad de retomar las operaciones dentro del tiempo planificado	C-01	Planificación y ejecución de pruebas de servidor alterno.	Equipo TIC	Preventivo	Buena	Trimestral	5	1	6	Moderado
							C-02	Establecimiento de un programa de mantenimiento de servidores.	Equipo TIC	Preventivo	Buena	Trimestral				
R-05	Infraestructura de centro de datos dañada.	Sismo / Incendio	Tecnología	Error en el funcionamiento, almacenamiento de datos proceso de respaldo.	Destrucción y/o deterioro de los equipos localizados en el lugar.	Posible pérdida de datos o hasta obsolescencia de los equipos	C-01	Proceso de respaldo constante en el servidor alterno	Equipo TIC	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Establecimiento de medidas de seguridad física en el centro de datos como por ejemplo: Detector de humo, sistemas de detección de incendios y refuerzos estructurales.	Equipo TIC	Preventivo	Buena	Continua				
							C-03	Mantenimiento y monitoreo periódico del estado del centro de datos, estableciendo	Equipo TIC	Preventivo	Buena	Bimestral				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
								estándares de condiciones mínimas y óptimas.								
							C-04	Intervención del equipo de recuperación autorizado, de modo que estén capacitados para tomar las medidas adecuadas con los equipos después de un desastre	Equipo TIC	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-06	Ingreso no autorizado a instalaciones de la empresa	Sismo / Saqueo	Eventos Externos	Robo de activos que se encuentran en el edificio de la empresa	Instalaciones vulnerables después del sismo, debido al pánico colectivo y las evacuaciones.	Pérdida o robo de activos de información críticos para la empresa.	C-01	Una vez comprobada la evacuación de los miembros de la organización y realizar las verificaciones convenientes, proceder al cierre de todas las posibles entradas a las instalaciones.	Equipo TIC	Preventivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Elaborar y mantener un inventario de activos de información para llevar un control de los activos que posee la empresa.	Riesgos / Continuidad	Preventivo	Excelente	Continua				
							C-03	Después del sismo y la evacuación, realizar la verificación de activos de información en base al último inventario elaborado para identificar qué activos faltan y cuál es su impacto en la operación de los procesos.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
R-07	Ingreso a centro de datos vulnerable	Sismo / Saqueo	Eventos Externos	Ingresos no autorizados al centro de datos.	Posibles fallas en los controles de entrada al edificio y al centro de datos después del sismo, ya que todos han evacuado.	Pérdida de información y robo de equipos.	C-01	Implementación de controles biométricos en la entrada del centro de datos, restringiendo el acceso de personas no autorizadas.	Equipo TIC	Preventivo	Buena	Continua	5	2	7	Alto
							C-02	Después del sismo y la evacuación, realizar la verificación de activos del centro de datos (cantidad de discos, servidores, cables, routers y otros) en base al último inventario elaborado para identificar las faltas, calcular el impacto en la operación y realizar la recuperación correspondiente	Equipo TIC	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				
R-08	Disponibilidad de flujo eléctrico	Sismo	Tecnología	Pérdida de fluido eléctrico general (en todo Lima).	Fallas en la infraestructura del proveedor de luz.	Incapacidad para reiniciar operaciones y comunicaciones en centro alterno y/o edificio principal	C-01	Uso de dispositivos de energía ininterrumpida UPS.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Instalación de grupos electrógenos.	Seguridad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)				

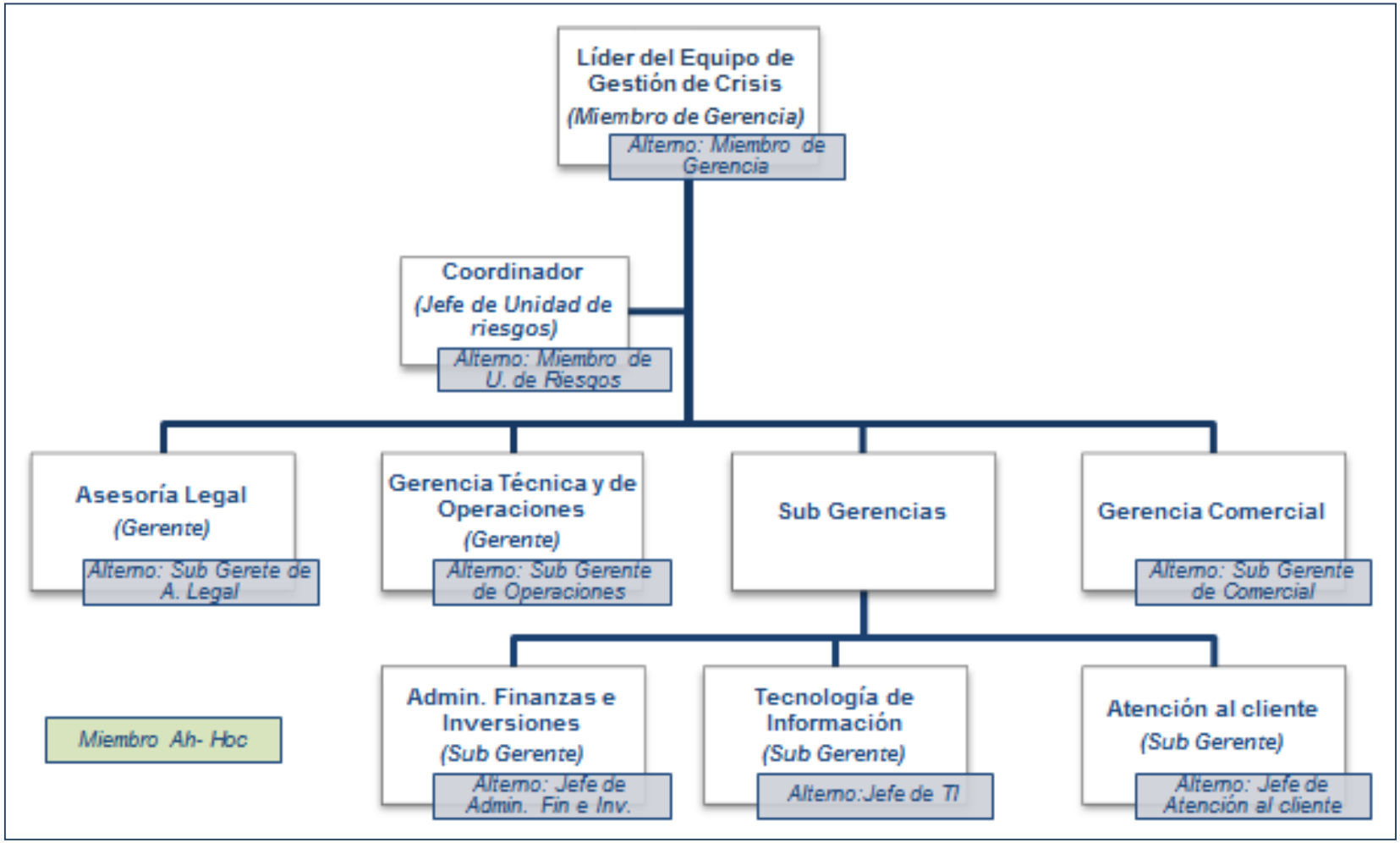
Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-03	Establecimiento de cronograma de mantenimiento y pruebas de grupo electrógeno y UPS, para asegurar su correcto funcionamiento.	Seguridad	Preventivo	Buena	Bimestral				
R-09	Disponibilidad de servicios telefónicos.	Sismo	Tecnología	Pérdida de servicio telefónico general.	Fallas en la infraestructura del proveedor de telefonía.	Incapacidad de comunicación entre coordinadores principales de gestión de crisis. Incapacidad de comunicación en la realización de operaciones de procesos de negocio.	C-01	Aplicación del plan de crisis, indicando que, frente a pérdida de telefonía se recomienda el uso del servicio de internet como forma alterna de comunicación.	Riesgos / Continuidad	Correctivo	Buena	No aplica (el control se aplica cuando el evento ocurre)	4	1	5	Moderado
							C-02	Adquisición y uso de celulares satelitales para los coordinadores principales, de modo que las principales comunicaciones no se vean interrumpidas.	Equipo TIC	Preventivo	Buena	Continua				
R-13	Personal de operaciones	Sismo / Incendio	Procesos	Personal crítico para los procesos (como lo son	Falta de capacitaciones y simulacros de ejecución de	Lentitud de procesos y sobrecarga de trabajo,	C-01	Programación de capacitaciones y simulacros.	Seguridad	Preventivo	Buena	Bimestral	4	3	7	Alto
							C-02	Establecimiento de políticas de servicio, que establezcan qué	Riesgos / Continuidad	Preventivo	Excelente	Continua				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
				los analistas de operaciones) con dificultades de acción en caso de desastre.	planes de acción en caso de desastres.	creando un cuello de botella en el proceso.		servicios estarán disponibles en caso de crisis o desastre, tomando en cuenta los más críticos para el negocio.								
R-14	Jefes y/o Gerentes autorizadores	Sismo	Personas	Necesidad de tener conformidad de documentos (como órdenes de pago y liquidaciones de siniestros) para continuar con el proceso.	Ausencia por convalecencia o fallecimiento de jefe y/o gerente.}	Interrupción del proceso y acumulación de documentos (como órdenes de pago y liquidación de siniestros)	C-01	Establecimiento de hasta 2 personas alternas que tengan la potestad de firmar documentos en representación de los jefes y/o gerentes.	Riesgos / Continuidad	Preventivo	Buena	Continua	5	2	7	Alto
R-15	Entrega de documentos enviados al cliente y/o interesado por courier	Sismo	Procesos	Dificultad o hasta imposibilidad de traslado de documentos al cliente.	Fallas en el servicio del proveedor o dificultad de acceso a algunos lugares que pudieron ser muy	Demora en la entrega de documentos, pudiendo incumplir plazos acordados.	C-01	Establecimiento de proveedores alternos, definiendo el alcance por ubicación y distribuyendo el trabajo.	Riesgos / Continuidad	Preventivo	Buena	Continua	3	2	5	Moderado

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
					afectados del sismo.											
R-19	Tareas asignadas al personal	Sismo	Procesos	Ausencia o escasez de personal para realizar las tareas administrativas y operativas de cada uno de los procesos.	Muerte u hospitalización de personal producto del sismo o aumento de carga laboral.	Cuellos de botella o falta de recursos humanos que realice las actividades necesarias.	C-01	Asignación de personas alternas para los roles más críticos en la ejecución de los procesos.	Riesgos / Continuidad	Preventivo	Buena	Anual	5	4	9	Extremo
							C-02	Capacitaciones a personas alternas, de modo que estén actualizadas e informadas de los posibles cambios a lo largo del tiempo.	Riesgos / Continuidad	Preventivo	Buena	Semestral				
							C-03	Realizar una adecuada gestión del conocimiento, elaborando un manual detallado y actualizado de las tareas y funciones de cada rol.	Riesgos / Continuidad	Preventivo	Buena	Continua				

Riesgo del Proceso							Controles						Evaluación de riesgos controlados			
Id	Origen	Escenario	Factor de riesgo	Evento	Causa	Consecuencia	Id	Descripción	Responsable	Tipo de control	Efectividad del Control	Frecuencia	Impacto	Probabilidad	Nivel de riesgo	Criticidad
							C-04	Establecimiento de contrato con proveedor de recursos humanos, quien será el encargado de abastecer de personal "alterno" competente para los procesos afectados.	Riesgos / Continuidad	Preventivo	Buena	Anual				
R-20	Cableado y conexiones eléctricas.	Sismo	Tecnología	Corto circuito en conexiones de las oficinas de la empresa.	Movimiento propio del sismo y fallas eléctricas en las instalaciones	Personas heridas cercanas al perímetro heridas. Incendios y deterioro o maltrato de equipos, documentación y otros activos de la empresa.	C-01	Establecimiento de procedimientos que permitan apagar el fluido eléctrico a partir de un grado determinado de sismo.	Seguridad	Preventivo	Regular	Continua	4	2	6	Moderado

17. Anexo 17: Estructura del Equipo de Gestión de Crisis



18. Anexo 18: Informe de evento

<NOMBRE DEL EVENTO > - INFORME DE EVENTO	
Fecha de actualización: __ / __ / ____	
Fecha Inicio: __ / __ / ____ **Hora Inicio: __ / __ / ____** **Producto o Servicio Impactado:** **Dueño del Producto o Servicio:** **Incidente reportado por:**	**Asistentes:**
DESCRIPCIÓN / ESTADO DEL EVENTO	
(Indicar todos los datos conocidos del estado del evento especificando la fuente de la misma)	
RESUMEN DE LAS ACTIVIDADES DE RESPUESTA EJECUTADAS	
Resumen de acciones ejecutadas hasta el momento	
Acciones ejecutadas por Equipo de Gestión de Incidentes de TI (Si aplica): **Acciones ejecutadas por Equipo de Respuesta ante Emergencias (Si aplica):** **Acciones ejecutadas por el dueño del proceso/producto/servicio (Si aplica):** **Acciones ejecutadas por equipos especializados (Si aplica):**	
Acciones planificadas de respuesta	
(Describir la respuesta estratégica elaborada por el equipo)	

19. Anexo 19: Guía de Análisis

<NOMBRE DEL EVENTO > - GUÍA DE ANÁLISIS
Última actualización: __ / __ / ____
Registrado por:
IMPACTO HUMANO (Muertes, lesiones, etc.)
Incluir información sobre: ✓ *El estado de salud de las personas heridas.* ✓ *Relación de fallecidos y la situación de su familia.* ✓ *Desaparecidos*
IMPACTO EN LA REPUTACIÓN
Proporcionar información la reputación respecto a: ✓ *Clientes* ✓ *Imagen Corporativa* ✓ *Organizaciones Reguladoras* ✓ *Empleados* ✓ *Proveedores* ✓ *Accionistas*
IMPACTO EN LAS OPERACIONES
Definir el impacto que el evento puede ocasionar en: ✓ *Operaciones del proceso* ✓ *Operaciones de TI* ✓ *Pérdida de información*
IMPACTO FINANCIERO
Proporcionar información sobre los posibles costos y pérdidas en: ✓ *Acciones de Respuesta* ✓ *Pérdida de ingresos* ✓ *Costos de remuneraciones* ✓ *Pago de multas y sanciones*
IMPACTO LEGAL

Especificar si el impacto legal puede incluir:

- ✓ *Acciones legales contra la empresa*
- ✓ *Demandas de clientes*
- ✓ *Cierre temporal de la empresa*
- ✓ *Cierre definitivo o pérdida de permiso de funcionamiento.*

INFRAESTRUCTURA

Incluir detalles sobre las cuestiones relacionadas a:

- ✓ *Seguridad física (estado del edificio de la empresa)*
- ✓ *Seguridad de información*

COMENTARIOS

Explicar, en caso existan, situaciones particulares que ocurran durante el desarrollo del evento y que deban tomarse en cuenta en el análisis.

20. Anexo 20: Funciones y Responsabilidades del Equipo de Respuesta a Emergencias

Rol	Responsabilidades
Coordinador General De Emergencia (CGE)	– Dirigir el **Comité de Emergencia** (CE) y del manejo de las situaciones de emergencia. – Apoyar y participar directamente con el **Comité de Crisis** a fin de controlar los imprevistos. – Asegurar los recursos necesarios para la atención de emergencias. – Coordinar el despliegue de las actividades según correspondan con el **Coordinador de Seguridad y Salud Ocupacional** (SSO) y el **Coordinador de Evaluación y Control de Daños** (CECD).
Coordinador de Seguridad y Salud Ocupacional (SSO)	– Gestionar las revisiones y asesorías de especialistas. – Capacitar a los coordinadores y líderes brigadistas. – Definir los tiempos de evacuación adecuados. – Gestionar la estrategia en caso de emergencia con los brigadistas de primeros auxilios, lucha contra incendio y evacuación.
Coordinador de Brigada de Evacuación (CBE)	– Gestionar sus requerimientos preventivos para las evacuaciones. – Programar y dirigir los simulacros de evacuación para todo el personal, incluyendo terceros, según el programa de simulacros establecido. – Determinar, difundir y comunicar las rutas de evacuación y las zonas seguras en caso de sismos, así como las zonas de reunión externas. – Medir los tiempos de evacuación y sugerir las acciones correctivas o de mejora al **Coordinador de Seguridad y Salud Ocupacional** (SSO). – Dirigir las acciones de rescate y búsqueda de personas en la zona afectada, en coordinación con el **SSO.**

Rol	Responsabilidades
Coordinador de Brigada Contra Incendios (CBCI)	– Gestionar los requerimientos preventivos para la lucha contra incendios. – Programar y dirigir los simulacros contra incendio para todo el personal, incluyendo terceros, según el programa anual de simulacros establecido. – Realizar mantenimiento preventivo, correctivo e inspecciones de los equipos e infraestructura de lucha contra incendios. – Dirigir el control o amago de incendio con los miembros de su brigada. – En coordinación con el **SSO**, es responsable de dirigir las acciones de evacuación parcial o total de las instalaciones afectadas por incendios. – Responsable de coordinar el despliegue de las actividades de los brigadistas miembros del equipo.
Coordinador de Brigada de Primeros Auxilios (CBPA)	– Definir el requerimiento para la atención de primeros auxilios. – Coordinar con el **Coordinador de Brigada Contra Incendios** (CBCI) y el **Coordinador de Brigada de Evacuación** (CBE) las acciones pertinentes para la ubicación y traslado de víctimas. – Implementar un área de atención exclusiva de primeros auxilios para todo el personal afectado. – Coordinar el despliegue de las actividades de los brigadistas de su equipo.
Coordinador de Evaluación y Control de Daños (CECD)	– Informar oportunamente al **Coordinador General de Emergencias** (CGE) sobre el estado real de los daños. – Asegurar el cumplimiento de las Inspecciones Técnicas anuales de Seguridad a cargo del Instituto Nacional de Defensa Civil. – Mantener la vigencia y coherencia de los procedimientos de evaluación y control de daños de la infraestructura física.

Rol	Responsabilidades
Coordinador de Mantenimiento (CM)	– Proponer el Programa de Mantenimiento preventivo, correctivo e inspección de los componentes de seguridad y protección ante emergencias. – Participar en las acciones de control, seguridad y rehabilitación de las instalaciones – Participar en la evaluación de daños de la infraestructura afectada conjuntamente con el **Coordinador de Evaluación y Control de Daños** (CECD). – Participar en la reparación y/o reconstrucción de la infraestructura afectada. – Apoyar al CECD en el abastecimiento de materiales en general, repuestos o insumos, equipos, así como de recursos de prevención y protección para las actividades de respuesta y control que eventualmente serán requeridos en la emergencias. – Gestionar el proceso de compras de recursos según lo requerido en la emergencia

21. Anexo 21: Roles y responsabilidades por tipo de escenario

N°	Descripción de la tarea	Rol				Amenaza	
		R2	R3 R4 R5	R6	R7	Sismo	Incendio
1.	**Respecto a los recursos:** – Coordinar con las gerencias respectivas a fin de obtener el equipamiento y recursos necesarios para la atención de la emergencia, antes, durante y después de la ocurrencia de la misma. – Habilitar el equipamiento y recursos en el edificio.	X		X		⊙	⊙
2.	**Respecto a la difusión y entrenamiento:** – Coordinar y gestionar un programa anual de capacitación y entrenamiento – Coordinar y gestionar un programa anual de ejercicios y simulacros de evacuación – Coordinar la participación de las instituciones de emergencia como son Bomberos, Defensa Civil y Policía Nacional.	X		X		⊙	⊙
3.	**Respecto a la difusión y entrenamiento:** – Promover la participación de la alta dirección en las iniciativas de la respuesta a emergencias. – Verificar el cumplimiento y la difusión del Plan entre el personal y los proveedores según corresponda. – Validar la difusión de las zonas seguras y rutas de evacuación de cada sede.	X		X		⊙	⊙
4.	**Respecto a la difusión y entrenamiento:** – Realizar ejercicios y simulacros para el buen entendimiento y correcta aplicación del plan. Considerar diferentes escenarios con grados de estrés cada vez más complejos. – Realizar el cálculo de los tiempos de evacuación, en base al aforo de cada instalación.		X		X	⊙	⊙

N°	Descripción de la tarea	Rol				Amenaza	
		R2	R3 R4 R5	R6	R7	Sismo	Incendio
	– Realizar capacitaciones al personal sobre el uso del equipamiento y recursos adquiridos – Identificar oportunidades de mejora en los ejercicios y simulacros o, en emergencias reales. – Identificar y validar las zonas seguras y rutas de evacuación de cada local. – Identificar oportunidades de mejora producto de la ejecución del simulacro de evacuación mediante talleres de lecciones aprendidas con los brigadistas.						
5.	**Respecto a la Infraestructura Física:** – Coordinar que se realice una evaluación anual de la infraestructura física del edificio. – Coordinar la oportuna señalización de las rutas de evacuación interna y externa. – Coordinar que las áreas de reunión externas al edificio se encuentren debidamente señalizadas. – Coordinar que las rutas de evacuación del edificio se encuentren libres de obstáculos y sean las apropiadas para facilitar la evacuación del personal. – Coordinar que el plano o croquis de evacuación sea el último plano revisado. – Coordinar que el plano o croquis de evacuación se ubique en un lugar visible para todos los trabajadores y visitantes de cada local.	X		X		⊙	⊙
6.	**Respecto al mantenimiento y actualización del plan:** – Verificar que el plan sea revisado, actualizado y extraordinariamente cuando se produzcan	X		X		⊙	⊙

N°	Descripción de la tarea	Rol				Amenaza	
		R2	R3 R4 R5	R6	R7	Sismo	Incendio
	cambios importantes en la organización o en sus instalaciones.						
7.	**Respecto a la disponibilidad del personal:** - Validar que primario y alterno del mismo rol no estén ausentes en periodos similares. - Validar que la información de contacto del personal requerido está actualizada	X	X	X	X	⊙	⊙
8.	**Respecto a externos:** - Validar números de teléfonos de la Compañía de Bomberos, Defensa Civil, Policía Nacional, Centros de Salud y todos los órganos de Apoyo definidos.	X				⊙	⊙
9.	**Respecto a los riesgos asociados:** - Coordinar la realización de la evaluación de riesgos (IPER) que permita la identificación de mejora de controles existentes contra Terremoto, Incendio u otro tipo de amenaza latente en la zona.	X				⊙	⊙
10	**Respecto a los elementos de seguridad física:** - Validar la existencia, buen estado y funcionamiento de los elementos de seguridad del edificio y/o gestionar la compra de los mismos (Ejemplo: Luces de emergencia, extintores, Detectores de humo, etc.)			X		⊙	⊙
11	**Respecto a los elementos de seguridad ocupacional:** - Validar la existencia, buen estado y funcionamiento del kit de primeros auxilios, así como gestionar la compra de los mismos (Ejemplo: linterna, silbato, paleta, mascarillas)	X				⊙	⊙

N°	Descripción de la tarea	Rol				Amenaza	
		R2	R3 R4 R5	R6	R7	Sismo	Incendio
12	**Respecto de los sistemas de alarma:** – Definir la necesidad del uso de alarmas para evacuación como alarma sonora, visual, uso de silbatos, entre otros. – Coordinar que la alarma se encuentre conectada con el proveedor. – Validar la existencia, buen estado y correcto funcionamiento de los sistemas de alarma.			X		⊙	⊙
13	**Respecto de los sistemas de alarma:** – Definir los instructivos o procedimientos de activación y de responsabilidades, en correspondencia a los posibles eventos según la evaluación de riesgos.	X		X		⊙	⊙
14	**Respecto de los sistemas de alarma:** – Validar que los instructivos de activación de alarmas los conozca todo el personal idóneo, según corresponda al tipo de evento, edificio y local. – Validar que los instructivos de activación de alarmas sean los últimos instructivos aprobados.	X				⊙	⊙
15	**Respecto a los elementos de Rescate y Primeros Auxilios:** – Evaluar la necesidad de contar con camillas, férulas, silla de ruedas	X	X			⊙	⊙
16	**Respecto a los elementos de Rescate y Primeros Auxilios:** – Evaluar un procedimiento de evacuación del personal afectado a áreas especializadas como son Clínicas, Centros Médicos entre otros.	X				⊙	⊙

N°	Descripción de la tarea	Rol				Amenaza	
		R2	R3 R4 R5	R6	R7	Sismo	Incendio
17	**Respecto a los elementos de Rescate y Primeros Auxilios:** – Validar que el centro de salud, tópico cuente con los implementos necesarios contra intoxicaciones. En caso de no contar con la implementación necesaria gestionar su adquisición inmediata.	X				⊙	⊙
18	**Respecto a reportes:** – Generar y enviar reportes e indicadores al Gestor de Continuidad (Capacitaciones realizadas, Cantidad de simulacros, edificios involucrados, personal participantes, proveedores, visitante y otros)	X		X		⊙	⊙

22. Anexo 22: Directorio de Servicios de Emergencia

No.	Empresa	Teléfonos
1	**COMPAÑÍA DE BOMBEROS**	
	Central de Emergencias	116
2	**POLICÍA NACIONAL DE PERÚ**	
	Central de Emergencias	105
	Comisaria de Surquillo	445-9083
	UDEX (Unidad de Desactivación de Explosivos)	433-3333
		433-5991
3	**DEFENSA CIVIL**	
	Central de Emergencias	115
4	**SERENAZGO**	
	Central de Atención Surquillo	241-0413
5	**HOSPITAL**	
	Clínica San Pablo	610-3333
	Hospital Dos de Mayo (Emergencia)	328-1424
	Hospital Arzobispo Loayza (Emergencia)	330-0241
6	**CLÍNICA MAS CERCANA**	
	Clínica Internacional	433-4306
	Clínica Ricardo Palma	224-2224
7	**AMBULANCIAS**	
	Alerta Medica	225-4040
	Cruz Roja	265-8783
	Cruz Verde	372-6025
8	**CENTRO DE MONITOREO DE LA EMPRESA**	
		418-1938
9	**CENTRAL DE MANTENIMIENTO DE LA EMRPESA**	
		418-1826

23. Anexo 23: Estrategias de Recuperación de TI

Escenario: Sismo (con posible ocurrencia de incendio)	
Componente	**Descripción de la Estrategia**
Infraestructura (Instalaciones)	**Situación actual:** ✓ La empresa cuenta con un centro alterno de operaciones en el Callao, el cual es un ambiente que cumple con las características mínimas para poder ser ambientado en caso de la ocurrencia de un desastre.
	Estrategia propuesta: ✓ Subcontratar el servicio de habilitación de centro alterno de operaciones con un proveedor que, como mínimo, cumpla los siguientes requerimientos: o Ofrecer centros alternos de operaciones en zonas seguras, es decir, en distritos que no tengan un alto índice de riesgo en caso de sismos. o Permitir realizar pruebas periódicas de activación del centro alterno desde la activación, operación y desactivación del mismo. o Ofrecer ambientes en condiciones adecuadas, de modo que permitan cumplir con el RTO de la empresa permitiéndole alcanzar los principales objetivos de recuperación. o Permitir la instalación de tantos puestos de trabajo como sea necesario para poder continuar con las operaciones vitales y poder cumplir con las obligaciones solicitadas por los principales interesados. ✓ Como segunda alternativa se plantea habilitar como centro alterno de operaciones alguna oficina o sede en provincia que sea lo suficientemente amplia y cuente con la infraestructura adecuada para satisfacer los requerimientos de operación en contingencia.
Infraestructura de TI (servidores)	**Situación actual:** ✓ El servicio de respaldo es brindado por un proveedor.

Escenario: Sismo (con posible ocurrencia de incendio)	
Componente	**Descripción de la Estrategia**
	✓ La frecuencia de respaldo de los servidores diaria o de acuerdo a la cantidad de transacciones que se realicen. ✓ Se cuenta con un centro de datos alterno.
	Estrategia propuesta: ✓ Ajustar las políticas de respaldo con el proveedor, con el fin de poder cumplir el RPO definido para los procesos críticos de continuidad ya que, actualmente estos valores son iguales poniendo a la empresa en una situación límite con grandes probabilidades de no cumplir los objetivos de recuperación.
Infraestructura de Comunicaciones (enlaces)	**Situación actual:** ✓ Enlaces de comunicación que soportan el acceso de usuarios autorizados a través de internet desde el centro alterno de operaciones al centro de datos alterno desde un punto de acceso a través de internet.
	Estrategia propuesta: ✓ Implementar un enlace de comunicación dedicado entre el centro alterno de operaciones y de datos con el objetivo de asegurar un mejor tiempo de recuperación y el acceso adecuado de los usuarios a la red.
Medios de Transporte	**Situación actual:** ✓ Los medios de transporte en caso de activación del centro alterno de operaciones no están contemplados.
	Estrategia propuesta: ✓ Considerando la ubicación y los posibles obstáculos de acceso que se puedan generar después de ocurrido el sismo (como cierre de calles u obstaculización de pistas), se pueden plantear diferentes alternativas como: ○ Transporte de buses particulares para la empresa. ○ Entrega de “vales por concepto de transporte” que cubran un porcentaje del gasto de transporte extra que genere la nueva ubicación.

Escenario: Sismo (con posible ocurrencia de incendio)	
Componente	**Descripción de la Estrategia**
Personal Alterno	**Situación actual:** ✓ La empresa no cuenta con personal alterno.
	Estrategia propuesta: ✓ Designar personal titular y alterno considerando los siguientes aspectos: o Deberán vivir como mínimo en diferentes zonas o distritos de Lima. o No deberán realizar las mismas actividades en un mismo instante de tiempo para no generar cuellos de botella y retrasos. ✓ En caso el titular y el alterno se encuentren ausentes, se deberá contactar al proveedor de RRHH, con quien previamente se establecieron acuerdos para poder cumplir con los requerimientos de continuidad. Dicho agente deberá proporcionar al personal pertinente de acuerdo al perfil solicitado. ✓ El personal alterno deberá contar con un manual de funciones detallando las principales tareas y responsabilidades que deberá cumplir, disminuyendo las dependencias a una sola persona. ✓ En caso el centro alterno esté ubicado en un sede fuera de la ciudad de Lima, se seleccionará como personal alterno a empleados que laboran en dicha sede, siendo capacitados según los procedimientos establecidos y proporcionándoles las guías o manuales necesarios. De este modo, la recepción de solicitudes se atenderá en Lima pero el proceso y las validaciones serán derivados fuera de la ciudad.
Medios de comunicación	**Situación actual:** ✓ Cuentan con correo electrónico y chat interno. ✓ Algunas personas cuentan con Blackberry RPM (con correo interno sincronizado).
	Estrategia propuesta:

Escenario: Sismo (con posible ocurrencia de incendio)	
Componente	**Descripción de la Estrategia**
	✓ Mantener el uso de teléfonos móviles como Blackberry para asegurar el acceso al correo electrónico interno. ✓ Asignar teléfonos satelitales al personal clave en el proceso de recuperación (como por ejemplo, miembros del Equipo de Gestión de Crisis) con el fin de no interrumpir las comunicaciones de coordinación.
Soporte a Usuarios / Mesa de Ayuda	**Situación actual:** ✓ El soporte a usuarios es responsabilidad directa del área de TI a través del correo interno.
	Estrategia propuesta: ✓ Asegurar la presencia de personal titular o alterno de TI necesario para colaborar con los requerimientos técnicos y de sistemas que se requieran durante el proceso de recuperación y operación en contingencia.
Información (física o digital)	**Situación actual:** ✓ Información física: o La información original necesaria para realizar las operaciones críticas se encuentra almacenada con un proveedor. o Las copias se encuentran bajo custodia del personal respectivo dependiendo de la operación. o El proveedor brindará la información requerida según solicitud de la empresa. ✓ Información digital: o Los documentos físicos que son digitalizados son enviados vía correo electrónico. Por ende, los documentos sólo son guardados en el servidor de correo ocasionando que, para la recuperación, el usuario tenga que hacer una búsqueda manual en su correo, lo cual pone en riesgo la probabilidad de cumplimiento del RPO del proceso, producto o servicio.
	Estrategia propuesta: ✓ Información física:

Escenario: Sismo (con posible ocurrencia de incendio)	
Componente	**Descripción de la Estrategia**
	Mantener la estrategia de tercerización tomando en cuenta las consideraciones del siguiente punto (Servicios de Proveedores) ✓ Información Digital: o Asignar un servidor específico para el almacenamiento de los principales documentos manejados por los procesos críticos, de modo que se prescinda de la búsqueda manual de documentos digitales en el correo electrónico por el usuario en caso de la ocurrencia de una crisis. o Coordinar con el proveedor de TI para asegurar el correcto respaldo y contingencia del servidor en mención.
Servicios de Proveedores	**Situación actual:** ✓ Se cuenta con los siguientes servicios asignados a proveedores: o Servicio de respaldo y contingencia de TI. o Custodia de documentos físicos. o Servicios básicos (luz, agua, teléfono, internet) o Servicios de Courier. ✓ Se cuenta con acuerdos establecidos, pero no con SLA definidos y conocidos por los principales interesados. ✓ No existe un procedimiento o medidas establecidas para asegurar que los proveedores cumplen con los objetivos estratégicos que requiere la organización, poniendo en riesgo la completa satisfacción de sus necesidades.
	Estrategia propuesta: ✓ Establecer como mínimo los siguientes procedimientos: o Verificar que la priorización del proveedor respecto a la empresa permite el cumplimiento del RPO. o Verificar que el proveedor cumpla con un SGCN que asegure la integridad, confidencialidad y disponibilidad de la información en custodia. o Al manejar información sensible de los clientes se debe verificar que el proveedor cumpla con las directrices

Escenario: Sismo (con posible ocurrencia de incendio)	
Componente	**Descripción de la Estrategia**
	pertinentes conforme a la Ley de Protección de Datos Personales (Ley N° 29733). ✓ Para el caso específico del proveedor de centro de datos alterno, se debe verificar que este cumpla con las características de infraestructura adecuadas, haciendo revisiones periódicas.

24. Anexo 24: Habilidades del Equipo de Recuperación Principal de TI

Rol	Función	Habilidad
Líder de Recuperación	1. Establecer protocolo para activar sitio Alterno. 2. Comunicar los acuerdos al Equipo de Gestión de Crisis. 3. Gestionar la disponibilidad de los sistemas en producción y contingencia de sistemas 4. Gestionar la seguridad Informática de la compañía. 5. Gestionar proyectos de compra, migración y mejora de la performance de la infraestructura de tecnologías de la información. 6. Identifica soluciones que permitan la mejora continua y la optimización de recursos. 7. Conocer de la arquitectura de los sistemas de la compañía.	• Liderazgo • Comunicación a todo nivel • Seguridad, confianza para manejar incidentes • Motivador e integrador de equipos de trabajo • Manejo de recursos humanos bajo presión.
Coordinador de Infraestructura de Locales	1. Gestión de Infraestructura y Servicios de TI. 2. Implementación y mantenimiento de planes y políticas de la seguridad física. 3. Supervisión de las instalaciones y condiciones físicas de los activos de TI de la organización. 4. Administración del inventario de activos de sistemas. 5. Mantener actualizado y seguro la configuración del centro alterno. 6. Evaluar el daño en la plataforma tecnológica básica de la empresa coordinar y dirigir las acciones necesarias para su recuperación en el Sitio alterno y su restauración a condiciones normales. 7. Instalar el hardware y software base, así como configurar las últimas versiones de los sistemas operativos, en los ambientes del Sitio alterno.	Tener conocimientos de: • Soluciones de almacenamiento • Gestión de incidentes de TI. • Documentación y control de cambios. • Infraestructura de negocios. • Hardware y software de servidores

Rol	Función	Habilidad
Coordinador de Redes y BD	1. Implementar los sistemas de comunicaciones. 2. Ejecutar el plan de continuidad de equipos de comunicaciones. 3. Monitorear los servicios de red. 4. Administrar redes y comunicaciones 5. Evaluar el daño en las redes de comunicación de datos y coordinar las estrategias de recuperación con los proveedores de servicios. 6. Mantener actualizado el diagrama actual de conexiones de dispositivos, el diagrama alterno y el inventario de equipos de telecomunicaciones a ser usado en caso de desastre. 7. Mantener, recuperar y/o restaurar los enlaces de red y comunicaciones entre las oficinas centrales de RENIEC y el Sitio alterno. 8. Diseño e implementación de redes de datos. 9. Monitoreo y mejoras del rendimiento de las redes de datos. 10. Monitoreo y mejoras del rendimiento de las bases de datos. 11. Gestión de proyectos de migración de bases de datos. 12. Diseño de políticas de la seguridad e integridad de las bases de datos 13. Diseño, implementación y supervisión de los procesos de respaldo de información. 14. Levantar los servicios de Base de Datos, con la data restaurada, válida, íntegra, probada y disponible para los usuarios, en el sitio alterno. 15. Informar a los usuarios acerca de la cantidad de información que se ha perdido como consecuencia del desastre y que será necesario recuperar.	• Capacidad de Trabajo en equipo. • Capacidad de trabajo bajo presión. • Administración de redes y comunicaciones. • Hardware y software de servidores • Virtualización de servidores • Monitoreo de servicios de red • Vocación de Servicio. • Iniciativa. • Orden. • Capacidad de Trabajo en equipo. • Capacidad de trabajo bajo presión.

Rol	Función	Habilidad
	16. Velar por el funcionamiento adecuado de las Bases de Datos.	
Coordinador de Información y Registros	1. Asegurar que toda la documentación relacionada a estándares, operaciones y registros se encuentren custodiados en condiciones adecuadas en la empresa con el proveedor. 2. Apoyo en la documentación de las políticas de seguridad y procedimientos del área. 3. Supervisar el cumplimiento de los controles que permitan asegurar la integridad, confidencialidad y disponibilidad de la información durante la situación de emergencia y recuperación. 4. Realizar coordinaciones con el proveedor de seguridad de información, de modo que ponga a disposición la información requerida de manera oportuna. 5. Realizar la revisión de la información una vez pasado el desastre, para eliminar la posibilidad de desfases o daños a los registros.	• Vocación de Servicio. • Iniciativa. • Orden. • Capacidad de Trabajo en equipo. • Capacidad de trabajo bajo presión.
Coordinador de Personal Operativo	1. Conocer el requerimiento de personal de cada proceso. 2. Mantener actualizada la agenda de contacto del personal operativo titular y alterno. 3. Gestionar el traslado del personal. 4. Identificar las principales necesidades del personal para permitir un adecuado desempeño durante la atención en contingencia. 5. En caso de desastre, contactar a cada personal operativo necesario para su traslado al centro alterno de operaciones. 6. Asignar y distribuir las responsabilidades entre el personal antes y durante la operación en contingencia.	• Vocación de Servicio. • Iniciativa. • Orden. • Capacidad de Trabajo en equipo. • Capacidad de trabajo bajo presión.

Rol	Función	Habilidad
Coordinador de Aplicaciones	1. Apoyar en la instalación de sistemas y aplicaciones del centro alterno de operaciones. 2. Asistir a los usuarios en la atención de incidentes de TI. 3. Monitorear el desarrollo de las operaciones en contingencia. 4. Informar al Coordinador de Recuperación de TI las principales incidencias. 5. Participar en la elaboración de diagnósticos de estado para ser informados al Equipo de Gestión de Crisis. 6. Aprobar, con el Coordinador de Redes y BD, la puesta en marcha del centro alterno de operaciones. 7. Asistir a los usuarios en la reinstalación de los sistemas y aplicativos en el edificio de la empresa una vez superado el desastre. 8. Brindar apoyo y soporte al Coordinador de Redes y BD en la ejecución de algunas tareas, según lo requiera.	9. Capacidad de Trabajo en equipo. 10. Capacidad de trabajo bajo presión. 11. Administración de redes y comunicaciones. 12. Dominio de los sistemas y aplicaciones. 13. Capacidad de búsqueda de soluciones

25. Anexo 25: Actividades de Prevención para la Recuperación de TI

N°	Descripción de la tarea	Frecuencia	CTI	CIL	CRB	CIR	CPO	CAP
Revisiones al centro de cómputo alterno								
1.	✓ Realizar visitas o auditorías al centro de cómputo alterno y validar la existencia y funcionamiento de: ○ Servidores y sus componentes. ○ Registros vitales (cintas de respaldo, script de configuración, contraseñas no personales, etc.) ○ Condiciones de infraestructura adecuadas ✓ Efectuar revisiones anuales de los SLA y cumplimiento de los mismos, para que según sea el caso, estos puedan ajustarse a las necesidades del negocio.	Anual	⊙		X			⊙
Revisiones al centro alterno de operaciones								
2.	✓ Realizar visitas o auditorías al centro alterno de operaciones y validar la existencia o disponibilidad de: ○ Señalización o instrumentos básicos de seguridad (extintores, luces de emergencia, botiquín). ○ Aforo soportado por el centro alterno. ○ Equipos de operación (laptop, terminales, consolas, etc.)	Semestral	⊙	X				

N°	Descripción de la tarea	Frecuencia	CTI	CIL	CRB	CIR	CPO	CAP
	○ Instalaciones básicas (luz, agua, teléfono)							
Preparación y actualización de información necesaria:								
3.	✓ Definir y coordinar procedimientos con el proveedor de custodia de documentos físicos para el traslado y disposición de la información según los requerimientos de la empresa.	Anual	⊙			X		
	✓ Realizar pruebas periódicas de traslado y disposición de la información desde la sede principal del proveedor hasta el centro alterno de operaciones.	Semestral	⊙			X		
Disponibilidad del personal:								
4.	✓ Validar la viabilidad del plan respecto a la vigencia del personal existente.	Trimestral		⊙			X	
5.	✓ Realizar coordinaciones con Recursos Humanos de modos que, el personal de operaciones titular y alterno no se encuentre ausente o de vacaciones en los mismos periodos.	Trimestral		⊙			X	
Respecto al esquema interno de notificación:								
6.	✓ Efectuar pruebas de comunicación entre el personal a fin de:	Trimestral	⊙	X	X	X	X	X

N°	Descripción de la tarea	Frecuencia	CTI	CIL	CRB	CIR	CPO	CAP
	○ Validar la vigencia de la información de contacto registrada en el plan. ○ Evaluar la efectividad de los recursos asignados para las comunicaciones (correos, celulares y teléfonos satelitales en caso aplique).							
Proveedores:								
7.	✓ Validar funcionamiento de los números de teléfono de los proveedores externos clave necesarios para la recuperación de TI.	Trimestral	⊙		X			X
Evaluación de indicadores:								
8.	✓ Realizar seguimiento a los indicadores de continuidad de áreas u oficinas en base a: ○ La ejecución de pruebas periódicas. ○ Resultados de crisis o incidentes anteriores.	Semestral	⊙	X	X	X	X	X

26. Anexo 26: Guía para la Elaboración y Ejecución de Pruebas

A continuación se muestra el diseño de las diferentes pruebas mencionadas en el plan:

Tabletop

Objetivos de la Prueba

Los objetivos del ejercicio son los siguientes:

- Demostrar la viabilidad del plan de continuidad de negocios utilizando escenarios bien definidos con interrupciones relevantes que puedan generar discrepancias o inconsistencias.
- Recolectar las anotaciones hechas por los participantes, incluyendo puntos y áreas de mejora en determinados planes.
- Educar a los responsables del funcionamiento del plan.

Alcance

El presente ejercicio involucra principalmente a todos los miembros del Equipo de Gestión de Crisis. Cabe mencionar que, la asistencia a esta reunión involucra tanto a los miembros titulares como alternos de cada equipo, siendo obligatorio la asistencia de por lo menos uno de ellos.

Determinación de escenarios

El equipo de gestión de continuidad de negocios debe seleccionar uno o más escenarios de interrupción durante la ejecución del ejercicio. Estos escenarios deben ser creados utilizando determinados criterios como:

- Las oportunidades que ofrece el escenario para activar o poner en práctica múltiples planes de continuidad, propiciando la interacción entre ellos.
- El manejo de la situación debe implicar una coordinación y comunicación significativa.
- El escenario puede ser severo y hasta asumir la ocurrencia de eventos improbables que hagan la situación más extrema, pero no puede sobrepasar los límites de lo real.

Acorde a esto, se determina el escenario base a partir del cual se desarrollarán las pruebas:

Resumen del escenario General	
Evento	Sismo de 7 grados de magnitud en la escala de Richter.
Epicentro	Lima o alrededores
Duración	1 minuto

Figura 2. Escenario base de prueba

Planificación de actividades

Se deben identificar los diferentes tipos de recursos necesarios para la correcta ejecución del ejercicio. Las principales actividades de coordinación que se deben realizar son:

- Acordar un horario disponible para la ejecución del ejercicio dependiendo de la disponibilidad de los involucrados
- Contratación o capacitación de un miembro del equipo de Continuidad de Negocio para cumplir el rol de moderador durante la ejecución del ejercicio.
- Dependiendo de la mecánica a usar, gestionar el abastecimiento de recursos logísticos que faciliten el desarrollo de la prueba como por ejemplo: Reserva de ambiente disponible para la reunión, útiles de escritorio, proyector, entre otros.

Elaboración del "Guión" de la Prueba

A continuación, se presenta el desarrollo completo de los escenarios a ser planteado en la prueba:

PARTE I: Escenario Inicial	
Descripción	El día lunes a las 4:00am se registró un terremoto de 7 grados de magnitud en la escala de Richter con epicentro en Lima o alrededores y duración de 1 minuto.
Hora (ficticia) de reunión	Lunes a las 10:00am aproximadamente.
Detalle de sucesos	**4:00am – 7:00am:** El Equipo de Manejo de Emergencias realiza la evaluación de daños, determinando que el edificio principal de operaciones ha sido gravemente dañado y el 90% de los

PARTE I: Escenario Inicial	
	equipos no estarán disponibles requiriendo mantenimiento urgente. El Equipo de Recuperación de TI determina que las transacciones que se ejecutaban, fueron dañadas y se ha perdido un porcentaje de información. **7:00am – 8:00am:** Las operaciones de la empresa se detuvieron por completo y no podrán realizar la apertura en plataforma. **8:00am – 9:00am:** Los medios de comunicación televisivos reportan serios daños en el distrito donde está ubicado el edificio principal de la empresa. Además se registran saqueos en los alrededores corriendo el riesgo de que las instalaciones de la empresa sean afectadas. Por otro lado, se reciben reportes de que un 80% del personal operativo crítico para la ejecución de los principales procesos no está disponible debido a sufrieron daños físicos durante el terremoto y se encuentran siendo atendidos.

Figura 3. Escenario inicial de crisis

PARTE II: Primeras complicaciones	
Descripción	En el transcurso del día, los clientes se van a acercando a las instalaciones de la empresa y al ver que no hay atención, se van registrando las primeras quejas.
Hora (ficticia) de reunión	Lunes a las 4:00pm aproximadamente.
Detalle de sucesos	**9:00am – 3:00pm:** Se registran quejas de clientes, que requieren atención inmediata.

PARTE II: Primeras complicaciones	
	Se reporta que hay dificultades para la activación del centro alterno de operaciones debido a inconvenientes con el proveedor y el traslado de las personas. **3:00pm – 4:00pm:** Se registran las primeras noticias referente a las empresas que han dejado de funcionar como consecuencia del terremoto, dentro de ellas se menciona a la empresa aseguradora, creando incertidumbre en sus clientes y mayor cantidad de llamadas en al centro de atención de consultas y reclamos. Se requiere elaborar un comunicado y elaborar estrategias para mitigar el impacto reputacional. Por otro lado, el Equipo de Manejo de Emergencias informa que se han registrado las primeras muertes de empleados como consecuencia del terremoto, está a la espera de indicaciones para iniciar con las actividades de apoyo humanitario.

Figura 4. Escenario alterno

PARTE II: Situación controlada	
Descripción	Luego de ejecutadas las actividades de recuperación de los procesos, se logra una mayor estabilidad de en las operaciones en contingencia obteniendo un mejor flujo de atención al cliente.
Hora (ficticia) de reunión	Lunes a las 10:00pm aproximadamente.
Detalle de sucesos	**4:00pm – 6:00pm:** Se logra restablecer los servicios de TI, permitiendo iniciar la atención al cliente presentándose algunos inconvenientes de servicio que logran ser manejados.

PARTE II: Situación controlada	
	Sin embargo, la capacidad de atención sigue siendo insuficiente respecto al volumen de solicitudes que se registran. **6:00pm – 10:00pm:** El Equipo de Recuperación de TI informa que los servicios se encuentran estables y están a la espera de indicaciones para coordinar el periodo recomendado de atención en contingencia.

Figura 5. Escenario final

Ejecución del Ejercicio

Para el desarrollo de la prueba, se plantea la siguiente estructura:

Agenda de Reunión		
Etapa	**Descripción**	**Preguntas del moderador**
1. Introducción	✓ Presentación de moderador ✓ Presentación de objetivos. ✓ Descripción de dinámica.	• ¿Se encuentran todas las personas convocadas? • ¿Se ha entendido la mecánica de trabajo? • ¿Todos han leído el plan de continuidad de negocios de la empresa? • ¿Comprenden su rol en la gestión de la continuidad?
2. Presentación de escenario	✓ Presentación del escenario. ✓ Descripción de los hechos por periodo de tiempo.	• ¿Han comprendido el escenario de interrupción? • ¿Existen algunas consideraciones o asunciones que quisieran acordar como equipo antes de iniciar?
3. Simulación	✓ Evaluación del impacto. ✓ Revisión de los planes de continuidad.	• ¿Quién toma la decisión de activar el plan de continuidad?

Agenda de Reunión		
Etapa	**Descripción**	**Preguntas del moderador**
	✓ Definición de estrategias	• ¿Conocen el orden de las actividades? • ¿Cuál es el tiempo permitido para esta actividad? • ¿Qué barreras encuentran? • ¿Qué planes deben activarse? • ¿Cuál es la estrategia de tratamiento? • ¿A quién es necesario convocar? • ¿Necesitan que algún otro detalle esté incluido en el plan? • ¿Encuentran algún vacío en los procedimientos? • ¿Cuál puede ser el impacto en el negocio? • ¿Las operaciones ya se han normalizado? • ¿Qué podemos y qué no podemos hacer? • ¿La alternativa o estrategia seleccionada cuenta con personal adecuado y capacitado? • ¿Cuáles son los requerimientos para regresar a la operación normal?

Agenda de Reunión		
Etapa	**Descripción**	**Preguntas del moderador**
4. Revisión	✓ El equipo de continuidad toma nota de las decisiones tomadas. ✓ Se evalúa el conocimiento y compromiso que cada uno tiene respecto a su rol dentro del Equipo de Gestión de Crisis. ✓ Comentarios iniciales sobre apreciaciones generales por parte del especialista en continuidad.	• El moderador no realiza preguntas en este punto.
5. Variación	✓ En caso exista otro escenario programado, volver al **punto 2** (en el diseño, se proponen 3 posibles escenarios, ver **Figuras 2, 3** y **4**).	• El moderador no realiza preguntas en este punto.
6. Evaluación y Cierre	✓ Repartir pequeñas encuestas a los miembros del Equipo de Gestión de Crisis para obtener una retroalimentación e identificar oportunidades de mejora en futuras pruebas (Ver figura 10).	• El moderador no realiza preguntas en este punto.

Figura 6. Estructura del ejercicio

Evaluación de Resultados

Durante el desarrollo de la prueba, los especialistas en continuidad de negocios tomarán nota de las diferentes decisiones tomadas a lo largo del ejercicio, esto con el objetivo de que, posteriormente, se pueda realizar un análisis para obtener un diagnóstico que permita identificar el nivel de madurez del Comité de Gestión de Crisis.

Para la evaluación se considerarán las siguientes preguntas:

N°	Pregunta
1	¿La estrategia planteada está acorde a los lineamientos del SGCN?
2	¿El tiempo requerido para tomar la decisión fue el adecuado?
3	¿Los asistentes conocían el rol que tenían que asumir?
4	¿La estrategia planteada era viable en función a los recursos y condiciones del escenario?
5	¿El nivel de comunicación entre los asistentes propiciaba un acuerdo común?
6	¿Las decisiones tomadas hubieran permitido proteger la reputación y garantizar la continuidad de operaciones de la empresa?

Figura 7. Preguntas del cuestionario de evaluación

Para cada pregunta se plantean las siguientes alternativas:

Alternativa	Puntaje	Descripción
a)	5	Satisfactorio
b)	4	Muy bueno
c)	3	Bueno
d)	2	Regular
e)	1	Malo

Figura 8. Puntajes por alternativa

Luego, se obtiene la calificación por escenario de acuerdo a la siguiente matriz:

	Puntaje por pregunta						Nota (Suma)
Escenario N°	P1	P2	P3	P4	P5	P6	
1							
2							
3							
…							
n							
						Promedio	Resultado

Figura 9. Matriz de calificación

Finalmente, se obtiene el resultado usando el promedio ponderado de las notas. De acuerdo a ello se establecen los siguientes rangos:

Rango	Calificación	Diagnóstico
[0 - 15[	Malo	No se evidencia un conocimiento mínimo de la estructura y contenido de los planes. Es necesario realizar capacitaciones individuales y personales.
[15 - 20[	Regular	Hay un conocimiento básico de la estructura y contenido de los planes, sin embargo las estrategias planteadas pueden no ser muy eficientes.
[20 -25[	Bueno	El Equipo de Gestión de Crisis conoce los procedimientos de acción, sin embargo, es recomendable ajustar algunos aspectos como el tiempo de respuesta, eficiencia de estrategias o nivel de comunicación.
[25 – 30]	Satisfactorio	El Equipo de Gestión de Crisis posee un alto nivel de conocimiento respecto a los planes planteando estrategias adecuadas que permiten asegurar la continuidad de las operaciones y el bienestar de los empleados.

Figura 10. Diagnóstico según el resultado obtenido

Identificación de oportunidades de mejora

Para la identificación de las oportunidades de mejora, se realizarán encuestas a los miembros del Equipo de Gestión de Crisis al final de la ejecución del ejercicio (Ver Figura 10).

Identificación de Oportunidades de Mejora
1. ¿Cuál es su opinión respecto a los escenarios presentados?
2. ¿Cómo se sintió durante la ejecución del ejercicio? ¿Cómo calificaría su participación y desenvolvimiento dentro del equipo?
3. ¿Qué otros escenarios considera que son importantes para próximas pruebas?

Identificación de Oportunidades de Mejora
4. Mencione alguna sugerencia, comentario u observación que haya identificado para poder mejorar futuras pruebas.

Figura 11. Encuesta para la identificación de oportunidades de mejora

Actualizaciones y ajustes en los planes de continuidad.

Los planes de continuidad podrían sufrir cambios o actualizaciones en caso se identifique alguna de las siguientes situaciones:

- ✓ La cantidad de personas que conforman el equipo excede o es muy escasa para las necesidades de la empresa.
- ✓ No se logra cumplir los plazos o tiempos determinados para la toma de decisiones.
- ✓ Los integrantes del Equipo de Gestión de Crisis manifiestan que el plan es difícil de entender.
- ✓ Los procedimientos descritos en el plan entorpecen y enredan a los asistentes.

Pruebas de Escritorio Operativas

|

Objetivos de la Prueba

Los objetivos del ejercicio son los siguientes:

- Demostrar la viabilidad del Plan de Recuperación ante Desastres utilizando escenarios con interrupciones de servicio relevantes.
- Recolectar las anotaciones hechas por los participantes, incluyendo preguntas sobre la satisfacción de los recursos asignados.
- Educar y ejercitar a los encargados de ejecutar el plan.
- Reconocer el Centro Alterno de Operaciones y los recursos para la recuperación asociados.
- Crear conciencia sobre importancia de los recursos logísticos, de operación y otros necesarios para la operación de los servicios en caso de desastre.

Alcance

El presente ejercicio involucra principalmente a todos los miembros del Equipo de Recuperación ante Desastres. Cabe mencionar que, la asistencia a la prueba es obligatoria para poder evaluar el desempeño de cada uno y la interacción del equipo.

Determinación de escenarios

El equipo de gestión de continuidad de negocios debe seleccionar un escenario de interrupción para aplicarlo durante la ejecución del ejercicio. Este debe ser creado utilizando determinados criterios como:

- Las oportunidades que ofrece el escenario para activar o poner en práctica el plan de recuperación ante desastres.
- El manejo de la situación debe implicar una coordinación y comunicación significativa.
- El escenario puede implicar la restauración de los servicios en el edificio principal o hasta la necesidad activar el centro alterno de datos y operaciones.

Acorde a esto, se determina el escenario base a partir del cual se desarrollarán las pruebas:

Resumen del escenario General	
Evento	Sismo de 7 grados de magnitud en la escala de Richter.
Epicentro	Lima o alrededores
Duración	1 minuto

Figura 12. Escenario base de prueba

Planificación de actividades

Se deben identificar los diferentes tipos de recursos necesarios para la correcta ejecución del ejercicio. Las principales actividades de coordinación que se deben realizar son:

- Acordar un horario adecuado para las pruebas, de modo que no perjudique la ejecución normal de las operaciones. Se recomienda hacerlo en horas de l madrugada o un domingo.

- Dependiendo de la mecánica a usar, gestionar el abastecimiento de recursos logísticos que faciliten el desarrollo de la prueba.
- Disponer de copias del Plan de Continuidad de Negocios y del Plan de Recuperación ante desastres para repartirlo a cada asistente.

Elaboración del "Guion" de la Prueba

El escenario presentado a continuación:

PARTE I: Escenario Inicial	
Descripción	El día lunes a las 4:00am se registró un terremoto de 7 grados de magnitud en la escala de Richter con epicentro en Lima o alrededores y duración de 1 minuto.
Detalle de sucesos	**4:00am – 7:00am:** El Equipo de Manejo de Emergencias realiza la evaluación de daños, determinando que el edificio principal de operaciones ha sido gravemente dañado y el 90% de los equipos no estarán disponibles requiriendo mantenimiento urgente. Se determina que las transacciones que se ejecutaban, fueron dañadas y se ha perdido un porcentaje de información. **7:00am – 8:00am:** Las operaciones de la empresa se detuvieron por completo y no podrán realizar la apertura en plataforma. **8:00am – 9:00am:** Los medios de comunicación televisivos reportan serios daños en el distrito donde está ubicado el edificio principal de la empresa. Además se registran saqueos en los alrededores corriendo el riesgo de que las instalaciones de la empresa sean afectadas.

Figura 13. Escenario de prueba

Ejecución del Ejercicio

Para el desarrollo de la prueba, se plantea la siguiente estructura:

Agenda	
Etapa	**Descripción**
1. Introducción	✓ Presentación de objetivos. ✓ Descripción de dinámica. ✓ Breve estructura del plan.
2. Presentación de escenario	✓ Presentación del escenario. ✓ Descripción de los hechos por periodo de tiempo. ✓ Determinación de premisas necesarias.
3. Simulación	✓ Ejecución del plan (incluye activación centro de operaciones alternos con conexión desde el centro de datos alterno).
4. Revisión	✓ El equipo de continuidad toma nota de las acciones realizadas. ✓ Se va controlando el tiempo transcurrido para saber si se va alcanzando los indicadores de continuidad. ✓ Comentarios iniciales sobre apreciaciones generales por parte del especialista en continuidad.
5. Evaluación y Cierre	✓ Repartir pequeñas encuestas a los miembros del Equipo de Recuperación ante Desastres para obtener una retroalimentación e identificar oportunidades de mejora en futuras pruebas (Ver figura 18).

Figura 14. Estructura de prueba

Evaluación de Resultados

Durante el desarrollo de la prueba, los especialistas en continuidad de negocios tomarán nota de las dudas o incidentes que ocurran a lo largo del ejercicio, esto con el objetivo de que, posteriormente, se pueda realizar un análisis para obtener un diagnóstico que permita identificar el nivel efectividad del plan.

Para la evaluación se considerarán las siguientes preguntas:

N°	Pregunta
1	¿Las actividades descritas están acorde a las necesidades de recuperación?
2	¿Cómo calificaría la estructura y la distribución de tareas en el equipo?
3	¿Cuál es el nivel de conocimiento del rol que desempeña cada uno?
4	¿Los recursos asignados fueron suficientes?

N°	Pregunta
5	¿Se cumplieron los indicadores de continuidad?
6	¿Cómo calificaría el desempeño de los proveedores en el desarrollo delas pruebas?

Figura 15. Preguntas del cuestionario de evaluación

Para cada pregunta se plantean las siguientes alternativas:

Alternativa	Puntaje	Descripción
a)	5	Satisfactorio
b)	4	Muy bueno
c)	3	Bueno
d)	2	Regular
e)	1	Malo

Figura 16. Puntajes por alternativa

Luego, se obtiene la calificación por escenario de acuerdo a la siguiente matriz:

	Puntaje por pregunta						
Escenario N°	P1	P2	P3	P4	P5	P6	Resultado
1							

Figura 17. Matriz de calificación

Finalmente, se obtiene el resultado usando el promedio ponderado de las notas. De acuerdo a ello se establecen los siguientes rangos:

Rango	Calificación	Diagnóstico
[0 - 15[	Malo	No se evidencia un conocimiento mínimo de la estructura y contenido del. Es necesario realizar capacitaciones.
[15 - 20[	Regular	Hay un conocimiento básico de la estructura y contenido del plan, sin embargo no se logra cumplir con los indicadores de continuidad.
[20 -25[	Bueno	El Equipo de Recuperación de Desastres conoce los procedimientos de acción, sin embargo, es recomendable ajustar algunos aspectos como el tiempo de recuperación, eficiencia de estrategias o nivel de comunicación.

Rango	Calificación	Diagnóstico
[25 – 30]	Satisfactorio	El Equipo de Recuperación de Desastres posee un alto nivel de conocimiento respecto a los planes planteando soluciones adecuadas que permiten asegurar la continuidad de las operaciones y el bienestar de los empleados.

Figura 18. Diagnóstico según el resultado obtenido

Identificación de oportunidades de mejora

Para la identificación de las oportunidades de mejora, se realizarán encuestas a los miembros del Equipo de Manejo de Crisis al final de la ejecución del ejercicio (Ver Figura 10).

Identificación de Oportunidades de Mejora
1. ¿Cuál es su opinión respecto al escenario presentado?
2. ¿Cómo se sintió durante la ejecución del ejercicio? ¿Cómo calificaría su participación y desenvolvimiento dentro del equipo?
3. ¿Qué otros escenarios considera que son importantes para próximas pruebas?
4. ¿Considera que los recursos de TI utilizados en el ejercicio fueron suficientes para lograr una recuperación satisfactoria?
5. Mencione alguna sugerencia, comentario u observación que haya identificado para poder mejorar futuras pruebas.

Figura 19. Encuesta para la identificación de oportunidades de mejora

Actualizaciones y ajustes en los planes de continuidad

EL DRP y los planes relacionados continuidad podrían sufrir cambios o actualizaciones en caso se identifique alguna de las siguientes situaciones:

- ✓ La cantidad de personas que conforman el equipo excede o es muy escasa para las necesidades de la empresa.
- ✓ No se logra cumplir los plazos o tiempos determinados para la toma de decisiones.
- ✓ Los asistentes manifiestan que el plan es difícil de entender y es engorroso.
- ✓ Los procedimientos descritos en el plan entorpecen y enredan a los asistentes.
- ✓ No se cumplen los indicadores de continuidad.