



**DISEÑAMOS
SOLUCIONES,
CONSTRUIMOS
COFIANZA.**



PLAN DE CONTINUIDAD DE NEGOCIO - PCN

Actualización:
06/2025
Bogotá, Colombia



Colombia – Perú – Estados Unidos – España



www.yeapdata.com

Carrera 19B #84-17
Piso 4 – Torre OVER III
Bogotá D.C, Colombia
+57(601)7430077
info@yeapdata.com



SC - 20018374



SI - 2001640

Documento de uso interno
pág. 1

TABLA DE CONTENIDO

1	OBJETIVO	7
1.1	OBJETIVOS ESPECÍFICOS	7
2	ALCANCE	7
3	TERMINOS Y DEFINICIONES	8
4	SUPUESTOS DEL PLAN DE CONTINUIDAD DE NEGOCIO	9
5	GOBIERNO DE CONTINUIDAD DEL NEGOCIO	10
5.1	POLÍTICA DE CONTINUIDAD DEL NEGOCIO	10
5.2	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10
5.2.1	Gestión de la Continuidad del Negocio	10
5.2.2	Entendimiento de la organización	10
5.2.3	Determinar la estrategia de continuidad de la operación	11
5.2.4	Desarrollo e implementación de planes de continuidad de operación	11
5.2.5	Ejercicios y pruebas, mantenimiento y revisión de la gestión de continuidad	11
5.2.6	Incorporación dentro de la cultura organizacional de la gestión de continuidad	11
5.3	ROLES Y RESPONSABILIDADES	12
5.3.1	Nivel estratégico	12
5.3.2	Nivel táctico	14
5.3.3	Nivel operativo	15
5.3.4	Proveedores	16
5.4	COMUNICACIONES	16
6	CONTEXTO ORGANIZACIONAL DE YEAPDATA	17
6.1	ESCENARIOS DE DESASTRE ASOCIADOS AL PLAN DE CONTINUIDAD	19
6.2	PERSONAL CRÍTICO	22
6.3	PROVEEDORES CRÍTICOS	23
7	GESTIÓN DE INCIDENTES DE INTERRUPCIÓN	25
7.1	FASE 1 - RESPUESTA	26
7.2	FASE 2 - ACTIVACIÓN Y RECUPERACIÓN	26
7.2.1	Prioridad de recuperación según criticidad del proceso	28
7.2.2	Recursos mínimos en la recuperación	28
7.3	FASE 3 - CONTINGENCIA	30
7.4	FASE 4 - RETORNO A LA OPERACIÓN NORMAL	31
7.5	FLUJO Y ACTIVIDADES DE LA GESTIÓN DE INCIDENTES DE INTERRUPCIÓN	31
7.6	FLUJOS DE APOYO	39
7.6.1	Evaluación de la situación actual	39
7.6.2	Activación del nivel estratégico	40
7.6.3	Coordinación de colaboradores	42
7.6.4	Contrataciones de recursos de emergencia	44
7.6.5	Supervisión y reporte	45
7.6.6	Restauración de locación	47

8	CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	50
9	MANTENIMIENTO Y ACTUALIZACIÓN DEL PCN	55
9.1	FACTORES DE ACTUALIZACIÓN	56
10	PLAN DE PRUEBAS	56
10.1	PREPARACIÓN	56
10.2	EJECUCIÓN	56
10.3	ACTIVIDADES POST PRUEBA	57
10.4	EVALUACIÓN DE RESULTADOS	57
10.5	APLICACIÓN DE MEJORAS	57
11	INFORME DE ANÁLISIS DE IMPACTO AL NEGOCIO – BIA	57
11.1	CRITERIOS PARA BIA	58
11.1.1	<i>Criterios para la evaluación de los diferentes tipos de impactos</i>	58
11.2	RESULTADOS BIA POR PROCESO	59
11.2.1	<i>Gestión Estratégica</i>	60
11.2.2	<i>Alianzas</i>	60
11.2.3	<i>Talento Humano</i>	60
11.2.4	<i>Sistema Integrado de Gestión</i>	61
11.2.5	<i>Comercial</i>	61
11.2.6	<i>Implementación</i>	62
11.2.7	<i>Gestión Operación Cliente</i>	62
11.2.8	<i>SOC</i>	63
11.2.9	<i>Procurement</i>	63
11.2.10	<i>Financiera</i>	64
11.2.11	<i>Tecnologías de la información</i>	64
11.3	INFORMACIÓN Y ACTIVOS ASOCIADOS CRÍTICOS	65
11.4	AFECTACIÓN DE LA INTERRUPCIÓN A SUS PARTES INTERESADAS	69
11.4.1	<i>Impacto a las partes interesadas internas</i>	70
11.4.2	<i>Impacto a las partes interesadas externas</i>	70
12	REFERENCIAS	71
13	ANEXOS	71
14	APROBACIÓN	72
15	CONTROL DE CAMBIOS	72

LISTA DE ILUSTRACIONES

	Pág.
<i>Ilustración 1. Mapa de procesos Yeapdata</i>	<i>7</i>
<i>Ilustración 2. Nivel estratégico PCN</i>	<i>12</i>
<i>Ilustración 3. Nivel táctico PCN</i>	<i>14</i>
<i>Ilustración 4. Flujo de comunicación para el árbol de llamadas</i>	<i>17</i>
<i>Ilustración 5. Flujo general de la gestión de incidentes de interrupción</i>	<i>31</i>
<i>Ilustración 6. Flujo evaluación de la situación actual.....</i>	<i>39</i>
<i>Ilustración 7. Flujo activación del nivel estratégico.....</i>	<i>40</i>
<i>Ilustración 8. Flujo coordinación de colaboradores.....</i>	<i>42</i>
<i>Ilustración 9. Flujo contratación de recursos de emergencia.....</i>	<i>44</i>
<i>Ilustración 10. Flujo supervisión y reporte</i>	<i>45</i>
<i>Ilustración 11. Flujo restauración de locación.....</i>	<i>47</i>
<i>Ilustración 12. Flujo retorno a la operación normal.....</i>	<i>49</i>

LISTA DE TABLAS

	Pág.
Tabla 1. Responsabilidades del nivel estratégico	13
Tabla 2. Responsabilidades del nivel táctico	15
Tabla 3. Responsabilidades del nivel operativo	16
Tabla 4. RTO-MTD y prioridad de recuperación de los servicios	19
Tabla 5. Escenarios de riesgos asociados a la continuidad de Yeapdata	22
Tabla 6. Listado de personal crítico	23
Tabla 7. Listado de proveedores críticos	25
Tabla 8. Criterios para evaluar los proveedores	25
Tabla 9. Estrategias de continuidad según escenario de desastre	28
Tabla 10. Prioridad y orden de recuperación de los procesos	28
Tabla 11. Listado de recursos de contingencia para los procesos	30
Tabla 12. Detalle de las actividades gestión de incidentes de interrupción	38
Tabla 13. Detalle de las actividades evaluación de la situación actual	40
Tabla 14. Detalle de las actividades activación del nivel estratégico	42
Tabla 15. Detalle de las actividades coordinación de colaboradores	44
Tabla 16. Detalle de las actividades contratación de recursos emergencia	45
Tabla 17. Detalle de las actividades supervisión y reporte	46
Tabla 18. Detalle de las actividades restauración de locación	48
Tabla 19. Detalle de las actividades retorno a la operación normal	50
Tabla 20. Continuidad de la seguridad de la información	51
Tabla 21. Requisitos de seguridad de la información a dar continuidad	55
Tabla 22. Tipos de impactos analizados	58
Tabla 23. Criterios de evaluación de los impactos	59
Tabla 24. BIA Gestión Estratégica	60
Tabla 25. BIA Alianzas	60
Tabla 26. BIA Talento Humano	61
Tabla 27. BIA Sistema Integrado de Gestión	61
Tabla 28. BIA Comercial	62
Tabla 29. BIA Implementación	62
Tabla 30. BIA Gestión Operación Cliente	63
Tabla 31. BIA SOC	63
Tabla 32. BIA Procurement	64
Tabla 33. BIA Financiera	64
Tabla 34. BIA Tecnologías de la Información	65
Tabla 35. RTO-RPO-MTD Activos de información	68
Tabla 36. Criterios para evaluar las partes interesadas	69
Tabla 37. Resultados evaluación partes interesadas internas	70
Tabla 38. Resultados evaluación partes interesadas externas	71

INTRODUCCIÓN

En la gestión de continuidad en Yeapdata busca identificar amenazas potenciales y estimar sus impactos para planificar las acciones necesarias que garanticen la continuidad de la prestación de los servicios en los niveles predefinidos como aceptables, desde el momento en que se presente el desastre hasta el restablecimiento a la normalidad de los procesos de la compañía.

Con la planeación de la continuidad se fortalece el gobierno y estructura de gestión de riesgos, ofreciendo seguridad a las partes interesadas internas y externas frente a imprevistos, buscando garantizar un adecuado nivel de estabilidad organizacional durante la respuesta a un evento de interrupción, la recuperación de las operaciones o procesos críticos y la reanudación de la operación normal. Asimismo, se busca:

- Proteger la integridad de los colaboradores de Yeapdata durante el desastre.
- Preparar a la compañía en las acciones necesarias para mantener la disponibilidad de los servicios críticos ante la ocurrencia de interrupciones significativas.
- Minimizar el impacto de los efectos de las interrupciones que afecten la operación
- Asegurar una oportuna restauración de las operaciones afectadas por la interrupción.
- Cumplir con los requisitos contractuales y contemplados en la normativa vigente.
- Agilizar la toma de decisiones durante una situación de desastre.
- Identificar los proyectos de mejora que se requieran implementar hacia la continuidad del negocio.

1 OBJETIVO

Establecer las medidas o acciones a seguir en caso de un desastre no planificado que afecte la normal operación de Yeapdata, detallando las actividades de respuesta según el escenario de desastre identificado y así mitigar los impactos o los efectos en los objetivos de la compañía y en la continuidad a la prestación de los servicios críticos.

1.1 OBJETIVOS ESPECÍFICOS

- Minimizar el tiempo de respuesta y recuperación ante una interrupción total de los procesos de Yeapdata.
- Establecer el gobierno, roles y responsabilidades para la gestión de la continuidad de negocio.
- Contar con un documento guía que permita orientar sobre la forma en que los equipos de trabajo responderán a las interrupciones, según los escenarios planteados y reanudarán las actividades dentro del alcance del PCN.
- Definir los criterios para la activación de los planes de respuesta frente a la declaración de un incidente de interrupción.
- Proponer criterios para evaluación de daños y toma de decisiones por parte de los equipos involucrados.

2 ALCANCE

El alcance de este plan es recuperar la operación de los procesos de Yeapdata (según el mapa de procesos), que han sido definidos como críticos con prioridad 1 durante el Análisis de Impacto del Negocio (BIA), y que pueden llegar a afectar las operaciones de Yeapdata en un escenario de interrupción.

Este alcance estará sujeto a las actualizaciones requeridas por la Alta Gerencia y por las actividades de la compañía.



Ilustración 1. Mapa de procesos Yeapdata

Adicionalmente, este PCN se define para las sedes:

- Sede YEC: Avenida el Dorado, No. 96J – 66, Oficina 302, Edificio Optimus Complejo Empresarial y Hotelero, Bogotá D.C.
- Sede Salitre: Carrera 46 No. 22b-20, Edificio Salitre Office P.H, Bogotá D.C.
- Sede Principal: Carrera 19B No. 84 – 17, Oficina 403-404, Torre Over 3, Bogotá D.C.
- Sede Sudameris: Carrera 11 # 94A - 03, Bogotá piso 5, Bogotá D.C.
- Sede CEDI: Carrera 48 # 145-18, Bogotá D.C.

3 TERMINOS Y DEFINICIONES

Aceptación del riesgo: Decisión informada de asumir un determinado riesgo. La aceptación del riesgo puede producirse sin tratamiento del riesgo o durante el proceso de tratamiento del riesgo. Los riesgos aceptados están sujetos a seguimiento y revisión (ISO/IEC 27000, 2018).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, servicios, aplicaciones, personas...) que tenga valor para la organización (ISO/IEC 27000, 2018).

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de este.

Análisis de Impacto al Negocio: Proceso de análisis del impacto a lo largo del tiempo de una interrupción en la organización. El resultado es una declaración y justificación de los requisitos de continuidad del negocio (ISO/IEC 22301, 2019).

Disponibilidad: Propiedad de ser accesible y utilizable a petición de una entidad autorizada (ISO/IEC 27000, 2018).

Evaluación del riesgo: Proceso global de identificación de riesgos, análisis de riesgos y evaluación de riesgos (ISO/IEC 27000, 2018).

Escenario de desastre: Conjunto predefinido de condiciones que describen una interrupción de los procesos del negocio de una organización para diseñar los planes y definir quién administraría la respuesta.

Evento de seguridad de la información: La ocurrencia o cambio de un estado del activo de información que indica un posible incumplimiento de las políticas de seguridad de la información o controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

Impacto: Resultado de una interrupción que afecta a los objetivos (ISO/IEC 22301, 2019).

Integridad: Propiedad de exactitud y completitud de la información (ISO/IEC 27000, 2018).

Interrupción: Incidente, previsto o imprevisto, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de una organización.

Parte interesada: Persona u organización que puede afectar, ser afectada o percibirse afectada por una decisión o actividad (ISO/IEC 22301, 2019).

Plan de Recuperación de Desastres (DRP): Conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los servicios informáticos.

Plan de continuidad del negocio: Información documentada que guía a una organización para responder a una interrupción y reanudar, recuperar y restaurar la entrega de productos y servicios de acuerdo con sus objetivos de continuidad de negocio (ISO/IEC 22301, 2019).

Proceso: Conjunto de actividades interrelacionadas o que interactúan entre sí y que transforman insumos en productos (ISO/IEC 22301, 2019).

Producto y servicio: Salida o resultado proporcionado por una organización a las partes interesadas.

Riesgo: Efecto de la incertidumbre sobre los objetivos (ISO/IEC 27000, 2018).

RPO (Recovery Point Objective): Punto de Recuperación Objetivo. Punto en el cual la información usada por una actividad debe ser restaurada para permitir la reanudación de la operación.

RTO (Recovery Time Objective): Tiempo de Recuperación Objetivo. Periodo de tiempo después de un incidente en el que el producto o servicio debe ser reanudado, o la actividad debe reanudarse o los recursos deben ser recuperados.

MTD (Maximum Tolerable Downtime): es el tiempo máximo que una empresa podría aguantar sin actividad antes de sufrir consecuencias irreversibles, como pérdida relevante de clientes y daño total a la reputación.

Seguridad de la información: Preservación de confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27000, 2018).

4 SUPUESTOS DEL PLAN DE CONTINUIDAD DE NEGOCIO

El Plan de Continuidad de Negocio (PCN) definido se construyó bajo los siguientes supuestos:

- Se cuenta con disponibilidad de las personas clave (o en su defecto de los sucesores) para activar el plan de continuidad del negocio.
- Se cuenta con las copias de respaldo actualizadas de la información del Plan de Continuidad de Negocio (PCN), Plan de Recuperación de Desastres (DRP) y Matrices de Contacto de cada uno de ellos.
- La documentación de procesos y procedimientos está actualizada, es vigente y está disponible con acceso para los involucrados en los planes.
- Los grupos de trabajo integrantes de los equipos de recuperación de procesos y tecnologías han sido capacitados y entrenados oportunamente.
- Las estrategias de recuperación y recursos tales como equipos adicionales o infraestructura, se han probado previamente y están disponibles para implementarse durante una interrupción.
- Las partes interesadas externas como proveedores, aliados y otros, son razonablemente cooperativos.
- Se cuenta con la asistencia de los miembros convocados o de sus sucesores, sin que, por esto, se vean afectados los tiempos de respuesta, ni se generen retrasos en las actividades de tratamiento.
- Yeapdata cuenta con planes de emergencias para la protección de la vida y la seguridad de todos los colaboradores según las respectivas sedes.
- Que el Plan de Recuperación de Desastres (DRP) esté implementado y probado.
- Que los Planes de Emergencia estén implementados y probados.
- Se incluyen como supuestos del componente tecnológico los desarrollados dentro del Plan de Recuperación ante Desastres (DRP).

Nota: Dado que la intención de este plan no es recrear en detalle los procesos y operaciones existentes de cada uno de los procesos, este no debe entenderse como un única o fuente definitiva para el curso de acción. Los colaboradores responsables de la recuperación pueden ajustar o cambiar el plan propio de su proceso e identificar otras actividades, para responder y recuperar las operaciones en situaciones específicas que no estén detalladas en este documento.

5 GOBIERNO DE CONTINUIDAD DEL NEGOCIO

5.1 POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Yeapdata en coherencia con su misión, visión, valores y filosofía, y compromiso con las partes interesadas, gestiona, mantiene y mejora la continuidad operativa de sus servicios y soluciones, mediante la identificación de estrategias e implementación de planes y controles que permitan salvaguardar la seguridad de la información, cumplir con los requisitos legales y contractuales vigentes y aplicables y mitigar los impactos de diferente naturaleza asociados a la interrupción de su operación.

En ese sentido, realiza de manera periódica actividades que aseguren la continuidad operativa y que a su vez mitigan y reducen los impactos negativos generados por los desastres producidos.

Para el aseguramiento de las actividades que contribuye a la continuidad del negocio, el Chief Operation Officer del Negocio es responsable del cumplimiento de las responsabilidades descritas en el siguiente numeral.

5.2 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

5.2.1 Gestión de la Continuidad del Negocio

- La alta dirección de Yeapdata se compromete con la gestión de la continuidad del negocio a través de la definición de una estructura organizacional adecuada para controlar y gestionar los eventos asociados a la interrupción del servicio, en busca de dar una respuesta adecuada que minimice los impactos.
- La alta dirección de Yeapdata entregará a sus colaboradores la política de continuidad del negocio (contenida en el presente documento) la cual brinda los lineamientos necesarios para llevar a cabo la implementación, gestión y mejoramiento del programa de continuidad del negocio que soportará la operación de la compañía.
- La alta dirección de Yeapdata buscará preservar la disponibilidad de los servicios, las relaciones a largo plazo con sus partes interesadas y la protección de su entorno a través de la planeación, implementación, prueba y mejora del Plan de Continuidad de Negocio (PCN).
- Todos los temas en materia de gestión de continuidad del negocio que se presenten dentro de la compañía serán de conocimiento y aprobación por parte del nivel estratégico o quien haga sus veces.
- La alta dirección de Yeapdata y sus equipos de trabajo deberán contar con roles y responsabilidades identificados que apoyan la correcta aplicación de la gestión de la continuidad de operaciones y tecnologías.
- Como política fundamental de la gestión de la continuidad de negocio, la seguridad y salud de los colaboradores prevalecerá en caso de que se presente un evento disruptivo.

5.2.2 Entendimiento de la organización

Los integrantes de los procesos identificados como críticos y sus equipos de trabajo:

- Deberán identificar los cambios en los procesos o servicios que soportan la operación de Yeapdata que pudieran generar vulnerabilidades o representar amenazas, que materialicen riesgos asociados a la interrupción.
- Deberán analizar los impactos asociados a la materialización de riesgos que interrumpan la normal operación de Yeapdata.
- Deberán revisar los tiempos de recuperación (RPO, RTO y MTD) de sus procesos a intervalos planificados o cuando se presenten cambios significativos en los procesos o en los servicios prestados.

5.2.3 Determinar la estrategia de continuidad de la operación

La alta dirección del Yeapdata con el apoyo de sus colaboradores deberá identificar las estrategias de continuidad de operación que propendan por:

- Contar con una o varias alternativas de operación para los procesos identificados como críticos ante escenario de falla total de la sede principal de la Entidad.
- Contar con un datacenter alternativo para los servicios de tecnología que soportan los procesos identificados como críticos.
- Contar con estrategias de gestión o planes de sucesión que permitan que el conocimiento de los colaboradores sea compartido a sus pares y dependientes en caso de que los responsables principales no puedan estar disponibles, y el fortalecimiento de la integración de profesionales que puedan colaborar en las actividades de recuperación de la compañía.
- Definir la sede adecuada para llevar a cabo la gestión de la crisis durante la interrupción de las operaciones de la compañía.
- Tomar las medidas de control en la gestión de continuidad de los servicios que proveen los proveedores a los procesos identificados como críticos.

5.2.4 Desarrollo e implementación de planes de continuidad de operación

- La alta dirección de Yeapdata debe contar con una estructura que apoye la respuesta a los incidentes asociados a la interrupción de las operaciones.
- La alta dirección de Yeapdata con el apoyo de sus colaboradores debe diseñar, implementar y mejorar el plan de continuidad de negocio (PCN), plan de recuperación de desastres (DRP) y el plan de manejo de crisis.
- La alta dirección de Yeapdata deberá integrar la gestión de la continuidad del negocio con otros sistemas de gestión (Calidad, Medio Ambiente, Seguridad de la Información) y con los planes de emergencias y seguridad física.
- La alta dirección de Yeapdata entregará y divulgará a sus colaboradores los roles y responsabilidades asociados a cada uno de los planes identificados e implementados en el cumplimiento de la estrategia de continuidad de negocio.

5.2.5 Ejercicios y pruebas, mantenimiento y revisión de la gestión de continuidad

- La alta dirección de Yeapdata con el apoyo de sus colaboradores llevará a cabo de manera periódica la realización de pruebas, mantenimiento y revisión sobre el plan de continuidad de negocio (PCN) y plan de recuperación ante desastres (DRP).
- La alta dirección de Yeapdata se encuentra comprometida con el mejoramiento continuo de la gestión de continuidad de negocio a través de la realización de revisiones gerenciales y de revisiones internas que generen acciones correctivas y de mejora.

5.2.6 Incorporación dentro de la cultura organizacional de la gestión de continuidad

- La alta dirección de Yeapdata se encuentra comprometida con el fortalecimiento de las competencias de sus colaboradores para llevar a cabo una adecuada, sistemática y homologada gestión de la continuidad del negocio.

5.3 ROLES Y RESPONSABILIDADES

El gobierno de continuidad de negocio está conformado por las posiciones de liderazgo más altas de la compañía y los procesos/servicios críticos que se han identificado en el BIA.
Este numeral busca definir el esquema de responsabilidades de todas las personas que dentro de sus funciones tienen las de aportar y/o recuperar, reanudar y restaurar los procesos críticos de manera oportuna, ordenada y eficiente.

Para esto, se define tres niveles que estarán a cargo de la gestión, recuperación y reanudación ante un evento de la continuidad del negocio. Estos son: nivel estratégico, nivel táctico y nivel operativo.

Nota: Dependiendo del tipo de desastre materializado las personas que participen en alguno de estos niveles pueden variar ligeramente.

5.3.1 Nivel estratégico

Sus principales funciones son la toma de decisiones frente a los aspectos críticos a nivel operativo, tecnológico, jurídico, de servicio, regulatorio, de imagen, reputación o financieros durante la ocurrencia de un desastre. El nivel estratégico está compuesto por todos los Chief de los distintos procesos que se ven afectadas ante la ocurrencia de la contingencia. Los miembros son los siguientes:

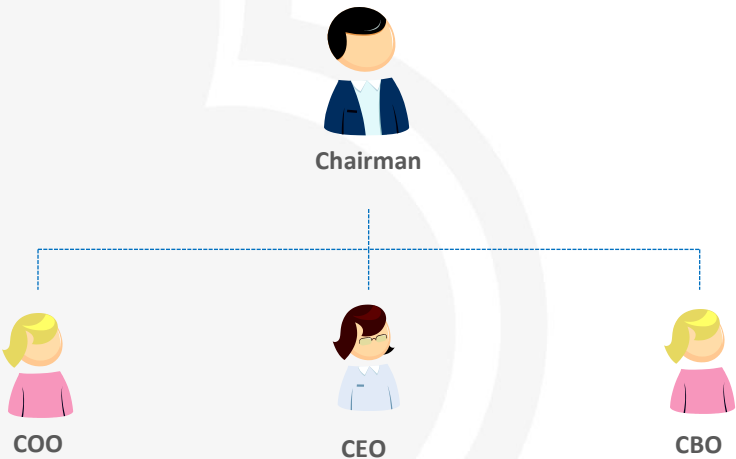


Ilustración 2. Nivel estratégico PCN

ETAPA	RESPONSABILIDADES
Antes del Incidente	Aprobar los procesos críticos y sus tiempos de recuperación.
	Aprobar y proveer recursos para implementar, mantener y mejorar continuamente el Plan de Continuidad de Negocio.
	Participar y promover activamente en la planeación y ejecución de pruebas.

ETAPA	RESPONSABILIDADES
	Revisar el Plan de Continuidad de Negocio (PCN) para asegurar su conformidad y efectividad.
	Promover la ejecución de revisiones al Plan de Continuidad del Negocio (PCN).
	Contribuir con la sensibilización de los colaboradores de forma tal, que apoye el compromiso con la gestión de la continuidad dentro de la compañía.
	Hacer un seguimiento periódico a los resultados de los ejercicios de pruebas y auditorías del plan.
<i>Durante el Incidente</i>	Reunirse, evaluar el incidente presentado y tomar la decisión de activar el Plan de Continuidad del Negocio (PCN).
	Realizar seguimiento a la recuperación de los procesos críticos de Yeapdata.
	Evaluar los posibles impactos e informar la situación a la Comercial quienes se encargarán de validar la necesidad de activar los procedimientos de comunicación.
	Suministrar al Chief Operation Officer la información técnica sobre la causa del incidente presentado (aplica si la causa de la interrupción se presentó en el proceso que reporta) y sobre el desempeño del proceso de recuperación para el desarrollo del informe del incidente.
	Velar por la recuperación de los recursos principales (Personas, Infraestructura Física, Tecnología y Proveedores) según aplique.
	Tomar todas las decisiones de alto nivel en la gestión del incidente de interrupción hasta el retorno a la operación normal.
<i>Después del incidente</i>	Evaluar el resultado de la recuperación y reanudación de los procesos críticos y emitir sus recomendaciones para el mejoramiento continuo del Plan de Continuidad del Negocio (PCN).
	Aprobar y fomentar el desarrollo de las acciones de mejoramiento del Plan de Continuidad del Negocio (PCN).

Tabla 1. Responsabilidades del nivel estratégico

5.3.2 Nivel táctico

Este nivel es el encargado de guiar las actividades de recuperación y realizar definiciones tácticas que apoyen el desarrollo de las actividades definidas para el nivel operativo, así como, administrar y dar soporte a la gestión y mejora de la continuidad de negocio. El nivel táctico está compuesto por:

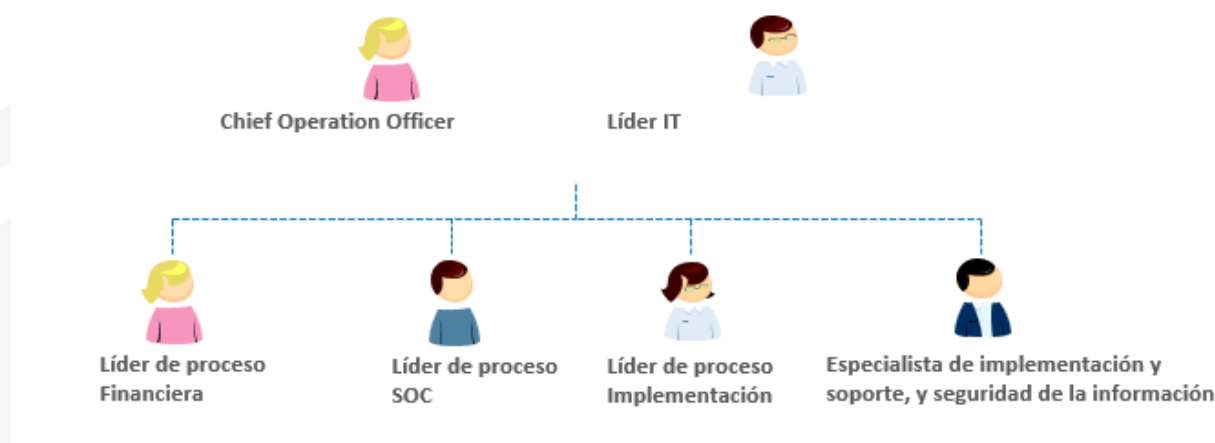


Ilustración 3. Nivel táctico PCN

Nota: El detalle de los procesos según su grupo de prioridad se encuentra en el numeral 7.2.1 Prioridad de recuperación según criticidad del proceso.

Las responsabilidades del Chief Operations Officer se enmarcan en coordinar y enlazar los diferentes equipos, procesos, etapas y actividades implícitas en el Plan de Continuidad de Negocio (PCN) y Plan de Recuperación de Desastres (DRP). Por lo tanto, deben conocer y administrar la metodología, estructura y procedimientos de la continuidad definidos en Yeapdata. Sus responsabilidades son:

ETAPA	RESPONSABILIDADES
Antes del Incidente	Asegurar la implementación, mantenimiento y mejora de:
	✓ El análisis de los riesgos de interrupción (RIA)
	✓ El análisis de impacto al negocio (BIA).
	✓ Las estrategias de continuidad de negocio.
	✓ El plan o planes de continuidad de negocio (PCN)
	Programar y realizar sesiones de sensibilización y capacitación en continuidad de negocio.
	Realizar la planeación de pruebas y coordinar su ejecución.
	Programar y conducir auditorías al Plan de Continuidad del Negocio (PCN).
	Promover y programar la realización de las revisiones al Plan de Continuidad del Negocio (PCN).
	Asegurar que las acciones de mejoramiento del Plan de Continuidad del Negocio (PCN) sean implementadas.

ETAPA	RESPONSABILIDADES
Durante el Incidente	• Suministrar al Chief Operations Officer la información técnica sobre la causa del incidente presentado (aplica si la causa de la interrupción se presentó en el proceso que reporta) y sobre el desempeño del proceso de recuperación para el desarrollo $\delta\epsilon\lambda\ \iota\upsilon\phi\omicron\rho\mu\epsilon\ \delta\epsilon\lambda\ \iota\upsilon\chi\iota\delta\epsilon\nu\tau\epsilon$.
	• Analizar la información de contexto del incidente y transmitirla al nivel estratégico, asegurando su veracidad.
	• Identificar los procedimientos existentes y aplicables para la atención del incidente de interrupción y coordinar con el líder del proceso la ejecución de las actividades de recuperación correspondientes.
	• Establecer comunicación permanente con los demás niveles de la estructura, involucrados en el proceso de recuperación para asegurar el flujo oportuno de la información.
	• Consolidar y suministrar la información necesaria para apoyar las decisiones y acciones que deben ser tomadas por el nivel estratégico.
Después del Incidente	• Desarrollar el informe del incidente, definiendo las acciones a tomar para mejorar el desempeño del Plan de Continuidad del Negocio (PCN) y las acciones correctivas necesarias para asegurar que la causa que originó el incidente no se vuelva a presentar.
	• Asegurar que las acciones de mejoramiento del Plan de Continuidad del Negocio (PCN) sean implementadas.

Tabla 2. Responsabilidades del nivel táctico

5.3.3 Nivel operativo

Encargado de la ejecución de las actividades de recuperación y retorno a normalidad de los procesos críticos de la compañía. Son responsables principalmente de la ejecución de las tareas operativas requeridas antes, durante y después de un evento disruptivo. La información de los participantes se puede encontrar en el análisis de impacto al negocio (BIA).

ETAPA	RESPONSABILIDADES
Antes del Incidente	• Conocer y entender el Plan de Continuidad del Negocio (PCN).
	• Asistir a las sesiones de divulgación, sensibilización y capacitación del Plan de Continuidad del Negocio (PCN).
	• Participar activamente en la ejecución de pruebas o simulacros.
	• Asistir como participantes cuando sea convocado a las revisiones del Plan de Continuidad del Negocio (PCN).
	• Coordinar con el Líder de Continuidad, las actualizaciones necesarias al plan y los procedimientos, teniendo en cuenta la identificación de cambios / oportunidades de mejora, relacionados con los procesos críticos y la tecnología que los soporta.
Durante el Incidente	• Atender las indicaciones una vez sea activado el plan para desplegar las estrategias a que haya lugar de acuerdo con el incidente enfrentado, en conformidad con las indicaciones del Líder de Continuidad.

ETAPA	RESPONSABILIDADES
	Validar que los requerimientos mínimos de recuperación estén disponibles y funcionen adecuadamente en las estrategias alternas de trabajo.
	Ejecutar el procedimiento de recuperación del proceso y/o de la plataforma de tecnología afectada.
	Suministrar información al Chief Operations Officersobre la recuperación del proceso.
	Realizar actividades de monitoreo sobre la operación del proceso o la plataforma tecnológica en contingencia.
Después del Incidente	Suministrar al rChief Operations Officerla información técnica sobre la causa del incidente presentado (aplica si la causa de la interrupción se presentó en el proceso que reporta) y sobre el desempeño del proceso de recuperación para el desarrollo del informe del incidente.
	Validar el desempeño de la operación del proceso cuando sea recuperado.
	Proponer acciones correctivas para mejorar el desempeño del Plan de Continuidad del Negocio (PCN) y para asegurar que la causa que originó el incidente no se vuelva a presentar.

Tabla 3. Responsabilidades del nivel operativo

5.3.4 Proveedores

Los proveedores actuales o los que se incorporen a Yeapdata y que soporten funciones críticas, deben asegurar la implementación de la política de continuidad del negocio durante la ejecución de los contratos, a efectos de garantizar que sus servicios no se verán interrumpidos ante desastres o que paralicen la normal operación de la compañía:

- Garantizar la protección de datos e información.
- Realizar periódicamente pruebas de seguridad a la infraestructura utilizada para la prestación de los servicios a Yeapdata.
- En el caso que aplique, corregir las vulnerabilidades técnicas identificadas en las pruebas de seguridad.
- Establecer y ejecutar planes de contingencia cuando ocurran eventos de fuerza mayor o caso fortuito que afecten la prestación de los servicios.
- Colaborar con Yeapdata y sus demás proveedores para la configuración, operación y la resolución de fallas e interrupciones.
- Buscar la causa raíz de las fallas que afectan la prestación de sus servicios y proporcionar una solución a ellas en el tiempo establecido.
- Cumplir los protocolos de entrega y finalización de los servicios/productos definidos.
- Garantizar el mantenimiento de la infraestructura y los cambios de sus componentes para garantizar la prestación de los servicios.
- Responder a los reclamos, consultas y solicitudes de Yeapdata.
- Suministrar las garantías de cumplimiento establecidas dentro de los acuerdos contractuales.

5.4 COMUNICACIONES

En este numeral se establece el esquema de comunicación durante la contingencia y recuperación de la operación.

Para notificar la activación del Plan de Continuidad de Negocio (PCN) y el estado de la implementación de este, se define el “Anexo 1. Matriz de contactos del PCN”, el cual relaciona los contactos con los que se desarrolla el árbol de comunicaciones y el plan de sucesión. Lo anterior, con el objetivo de mantener todos los contactos centralizados, actualizados y disponibles en el caso en que se presente la interrupción.

El árbol de llamadas opera a través de un flujo de comunicación en el que un responsable despliega las comunicaciones hacia abajo a un número limitado de participantes, y así mismo contar con un punto de reporte único de contacto hacia arriba. En la siguiente ilustración, se observa una secuencia de comunicación del nivel estratégico al nivel táctico y de este hacia el nivel operativo. De igual forma, existe un flujo de comunicación entre el nivel operativo y nivel táctico, quien a su vez se comunica con el nivel estratégico de continuidad. Este flujo se presenta a continuación:

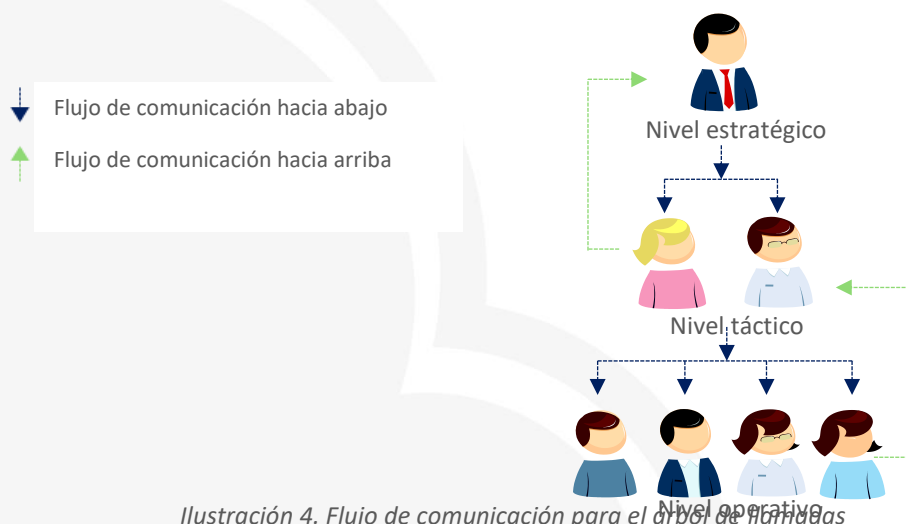


Ilustración 4. Flujo de comunicación para el árbol de llamadas

El plan de sucesión que implementa Yeapdata permite que cada uno de los responsables de la continuidad del negocio cuente con un sucesor que apoye las actividades de continuidad en caso de que el responsable principal no se encuentre disponible durante la interrupción. La información de los sucesores de cada responsable se consigna de igual forma dentro del “Anexo No. 1 - Yeapdata - Lista de contactos del árbol de llamadas PCN”.

6 CONTEXTO ORGANIZACIONAL DE YEAPDATA

Dentro de los aspectos del contexto de Yeapdata analizados por su relevancia para lograr el propósito de la compañía y que podrían llegar afectar su capacidad para lograr los resultados previstos se encuentran:

- **MISIÓN:** Somos una empresa de tecnología que integra recursos profesionales altamente capacitados y comprometidos con brindar un servicio excepcional, a través de modelos de servicios y operación innovadores. Ofrecemos soluciones en tecnologías de la información y telecomunicaciones adaptables a un mundo de constante evolución y que cumplen con los más altos estándares de calidad y seguridad
- **VISIÓN:** “Seremos una corporación global referente, que transforma con soluciones disruptivas y de alto impacto la forma de llevar la tecnología a las empresas”.

- **OBJETIVOS ESTRATÉGICOS:** Los objetivos estratégicos de Yeapdata se encuentran definidos en el documento EST-A1-01 PLANTEAMIENTO ESTRATEGICO YEAPDATA.
- **PARTES INTERESADAS:** Las partes interesadas identificadas para la continuidad del negocio de Yeapdata son:
 - Accionistas.
 - Colaboradores.
 - Proveedores.
 - Clientes.
 - Aliados
 - Entes de control
 - Entidades de emergencia
 - Comités internos
 - Alta dirección
 - Entes certificadores
- **SERVICIOS Y SOLUCIONES:** Los servicios y soluciones de Yeapdata contemplados en el alcance del plan de continuidad del negocio son:
 - Servicios gestionados: Cocreación y desarrollo de un modelo operativo IT inteligente y adaptativo a la necesidad de tu negocio y los recursos del ecosistema digital con capacidades de automatización, proactividad y analítica, orientados a la experiencia de usuario y continuidad de tus servicios a través de KPIs que permitan aumentar la eficiencia de personas, procesos y herramientas.
 - Infraestructura: Soluciones de redes de datos empresariales para cualquier industria o negocio, incluyendo LAN, WLAN, NAC, SDLAN, SDWAN, Data Center, IPv6 y Assessment de Red. Provee soluciones de infraestructura eléctrica y aire acondicionado para Data Center, y servicios de cableado estructurado. Cuenta con implementación, administración y soporte especializado en todas estas soluciones.
 - Colaboración: Construcción de soluciones empresariales de Comunicaciones Unificadas y Colaboración en la nube (UC & UCaaS), para cualquier industria o vertical de negocio. Desarrollo de tecnología aplicada a Centros de Contacto Omnicanal y Customer Experience (CX). También provee soluciones de aulas y espacios inteligentes para suplir necesidades audiovisuales, de conectividad, control y automatización de salas.

Al determinar el RTO y MTD de los servicios críticos se obtiene su prioridad de recuperación:

PRODUCTO	RTO	MTD	PRIORIDAD DE RECUPERACIÓN
LAN (Local Area Network)	1 hora	1,5 horas	1
Internet	1 hora	1,5 horas	2
WLAN (Wireless Local Area Network)	2 horas	4 horas	3
NAC (Network Access Control)	2 horas	4 horas	4
SDLAN (Software Defined Local Area Network)	2 horas	4 horas	5
SDWAN (Software Defined World Area Network)	2 horas	4 horas	6
Data Center	2 horas	4 horas	7
Backup	2 horas	4 horas	8
Mesa de Servicios	1 hora	2 horas	9
UCC (Comunicaciones Unificadas y Colaboración)	2 horas	4 horas	10
UCaaS (Comunicaciones Unificadas as a Service)	2 horas	4 horas	11
Contact Center (CC) Omnicanal	2 horas	4 horas	12
CCaaS (Contact Center as a Service)	2 horas	4 horas	13
Monitoreo	2 horas	4 horas	14

Tabla 4. RTO-MTD y prioridad de recuperación de los servicios

6.1 ESCENARIOS DE DESASTRE ASOCIADOS AL PLAN DE CONTINUIDAD

A continuación, se presentan los escenarios de desastre identificados por parte de los conocedores de los procesos de Yeapdata:

ID	ESCENARIOS	CAUSAS POTENCIALES	CONSECUENCIAS INMEDIATAS
1	Posible afectación o pérdida de la disponibilidad de la información procesada o almacenada en los servicios entregados por los proveedores (Microsoft, Conectividad, Mantenimiento, Energía y otros)	- Dependencia de proveedores críticos sin suplente o plan de acción - Falla o interrupciones de los servicios suministrados por el proveedor de servicios en la cadena de suministro - Falla o interrupciones de los servicios suministrados por el proveedor de servicios en la cadena de suministro - Ausencia de un proceso para el seguimiento a los productos/servicios TIC - Ausencia de requisitos de seguridad de la información y de	- Interrupción de las operaciones de los procesos de la compañía - Deterioro de la reputación organizacional, buen nombre e imagen de la compañía - Afectación de la calidad de los servicios prestados Yeapdata - Incurrir en costos económicos - Retrasos en la entrega de servicios a los clientes

ID	ESCENARIOS	CAUSAS POTENCIALES	CONSECUENCIAS INMEDIATAS
		continuidad del negocio con los proveedores	
2	Posible generación de afectación o imposibilidad de acceso o uso de las instalaciones físicas de la compañía y a los datacenter que soportan las operaciones de los procesos de Yeapdata	• Daño total o parcial de la infraestructura por eventos físicos, desastres naturales o ambientales: Incendios, inundaciones, sismos, terremotos, vandalismo, inundaciones por fuga de agua, daños sanitarios o granizadas • Bloqueo del acceso por ocurrencia de fenómenos políticos o sociales como protestas, disturbios, conflictos, manifestaciones, cambios políticos y legales, medidas de seguridad, huelgas, paros laborales • Restricción de la movilidad por estados de excepción/emergencia en el país • Actos malintencionados • Medidas para ahorro recursos (racionamiento agua)	• Interrupción y deterioro de las operaciones de los procesos de la compañía • Afectación de la calidad de los servicios prestados por Yeapdata a sus clientes • La compañía queda sin sitio donde operar total o parcialmente • Retrasos en la entrega de servicios a los clientes • Colaboradores en presencialidad se quedan sin sitio de trabajo, sin embargo, el impacto se reduce al existir otras sedes y ser viable el teletrabajo para la mayoría de los procesos • Incumplimiento de requisitos legales, contractuales y acuerdos de nivel de servicio
3	Posible afectación o indisponibilidad del personal considerado como crítico por su conocimiento o experiencia en la administración de los servicios TI	• Ocurrencia de emergencias que afectan la salud pública • Incapacidad del personal crítico para llegar al lugar de trabajo • Personal sin el conocimiento requerido para atender la operación	• Disminución de la capacidad de Yeapdata para operar de manera normal • Incurrir en costos económicos por reprocesos o ajustes a los procesos actuales • Pérdida de conocimiento y experiencia • Retrasos en la entrega de servicios a los clientes • Interrupción y deterioro de las operaciones de los procesos de la compañía • Afectación de la calidad de los servicios prestados Yeapdata • Incumplimiento de requisitos

ID	ESCENARIOS	CAUSAS POTENCIALES	CONSECUENCIAS INMEDIATAS
			legales, contractuales y acuerdos de nivel de servicio Afectación de la reputación, imagen y buen nombre
4	Posible afectación de la disponibilidad de la información procesada o almacenada en la infraestructura tecnológica física de propiedad o administrada por YeapData	- Daños físicos o fallas en el hardware del datacenter principal - Eventos físicos, desastres naturales o ambientales: Incendios, inundaciones, sismos, terremotos, vandalismo, inundaciones por fuga de agua o granizadas - Actos malintencionados (sabotaje, vandalismo) - Actos accidentales (omisión, error) - Fallas en los enlaces de comunicaciones - Daño total o parcial en la infraestructura física del datacenter - Fallas técnicas o daños en la red eléctrica del proveedor de energía - Fallas en condiciones ambientales de los centros de cómputo - Errores en la renovación del licenciamiento o suscripciones	- Incumplimiento de requisitos legales, contractuales y acuerdos de nivel de servicios - Interrupción o retraso de las operaciones de los procesos de la compañía - Atraso de operaciones que no tienen respaldo tecnológico en el Datacenter alterno - Afectación de la reputación, imagen y buen nombre de Yeapdata - Afectación de la calidad de los servicios prestados Yeapdata
5	Posible afectación de la confidencialidad, integridad y disponibilidad de los sistemas de información y servicios TI debido a un ataque informático	- Actos malintencionados (sabotaje, vandalismo) - Ataques maliciosos a los sistemas de información y servicios tecnológicos (Código malicioso, denegación de servicio, hacking, ingeniería social)	- Incumplimiento de requisitos legales, contractuales y acuerdos de nivel de servicios - Interrupción o retraso de las operaciones de los procesos de la compañía - Atraso de operaciones que no tienen respaldo tecnológico en el Datacenter alterno - Afectación de la reputación, imagen y buen nombre de Yeapdata

ID	ESCENARIOS	CAUSAS POTENCIALES	CONSECUENCIAS INMEDIATAS
			Afectación de la calidad de los servicios prestados Yeapdata

Tabla 5. Escenarios de riesgos asociados a la continuidad de Yeapdata

Es de aclarar que los escenarios de falla pueden presentarse de manera tal que se combinen, por ejemplo: las instalaciones físicas y a las personas pueden verse afectadas ante un escenario de terrorismo.

En lo referente al escenario “Indisponibilidad de las tecnologías de la información y comunicación”, se tiene un documento específico de acción a través del Plan de Recuperación ante Desastres (DRP), el cual es complementario al presente plan.

Por otro lado, en lo correspondiente a los escenarios “Indisponibilidad de acceso a las instalaciones físicas de la compañía” e “Indisponibilidad del personal crítico para la compañía” se tiene un documento específico de acción a través del Plan de Emergencias, el cual es complementario al presente plan y varía según la sede de Yeapdata (Calle 85, Salitre, YEC, Sudameris y CEDI).

6.2 PERSONAL CRÍTICO

El personal considerado necesario para la recuperación de los procesos críticos ante un escenario catastrófico en Yeapdata es:

PROCESO	PERSONAL CRÍTICO	PERSONAL SUPLENTE
Gestión Estratégica	CEO	COO
Alianzas	Coordinador de Alianzas	Vacante
Talento Humano	Líder de Talento Humano	Profesional de compliance
Talento Humano	Profesional de compliance	Líder de Talento humano
Sistema Integrado de Gestión	Líder SIG	Especialista de implementación, soporte y seguridad de la información
Sistema Integrado de Gestión	Líder SIG	Profesional SIG
Sistema Integrado de Gestión	Especialista de implementación, soporte y seguridad de la información	Vacante
Comercial	Desarrollador de negocios	Líder administrativo de ventas
Comercial	Líder administrativo de ventas	Desarrollador de negocios
Comercial	Arquitecto de soluciones	Desarrollador de negocios

PROCESO	PERSONAL CRÍTICO	PERSONAL SUPLENTE
Implementación	Líder PMO	Gerente de proyectos
Implementación	Gerente de proyectos	Ingeniero de proyectos
Implementación	Especialista de implementación y soporte	Ingeniero de implementación y soporte
Gestión Operación Cliente	COO	Gerente operaciones cliente
SOC	Especialista de implementación y soporte	Especialista de implementación, soporte y seguridad de la información
Procurement	Líder de costos y adquisiciones	Profesional de compras
Procurement	Coordinador Logístico	Delivery
Gestión Administrativa y Financiera	CBO	Líder de planeación financiera y tesorería
Gestión Administrativa y Financiera	Contador	Auxiliar contable
Tecnologías de la Información	Profesional IT	Líder IT
Tecnologías de la Información	Líder IT	Profesional IT
Tecnologías de la Información	Especialista de implementación y soporte	Vacante

Tabla 6. Listado de personal crítico

En el “Anexo No. 1 - Yeapdata - Lista de contactos del árbol de llamadas PCN” se complementa la información de contacto del personal crítico.

6.3 PROVEEDORES CRÍTICOS

Entre los proveedores con su criticidad para los procesos de Yeapdata se encuentran:

PROCESO	PROVEEDOR/ALIADO	CRITICIDAD
TALENTO HUMANO	BIENESTAR PRIMERO BIP SAS	Baja
TALENTO HUMANO	LABORATORIO CLINICO COLMEDICOS IPS SAS	Baja
TALENTO HUMANO	PAUL MULLER CONSULTORES SAS	Baja
TALENTO HUMANO	PEOPLE GROWTH S.A.S.	Baja
TALENTO HUMANO	PROASISTEMAS S.A.	Alta
TALENTO HUMANO	ZADA SALUD OCUPACIONAL SAS	Baja
TALENTO HUMANO	MANPOWER PROFESSIONAL LTDA - Experis	Baja
TALENTO HUMANO	MEDISANITAS SAS COMPAÑÍA DE MEDICINA PREPAGADA	Baja
TALENTO HUMANO	GRUPO RECORDAR	Baja
SOC	LUMU TECHNOLOGIES S.A.S. - NDR	Alta
SOC	Kaspersky	Alta

PROCESO	PROVEEDOR/ALIADO	CRITICIDAD
SOC	SIEM - CrowdStrike	Alta
SISTEMA INTEGRADO DE GESTIÓN	ICONTEC	Media
SISTEMA INTEGRADO DE GESTIÓN	KAWAK COL SAS	Media
SISTEMA INTEGRADO DE GESTIÓN	PBT CONSULTING SAS	Baja
GESTION OPERACIÓN CLIENTE	ASISTEL SOLUCIONES TELEINFORMATICAS	Baja
GESTION OPERACIÓN CLIENTE	FAEDCA SAS	Baja
GESTION OPERACIÓN CLIENTE	REDELECTRON - D&S SAS	Baja
GESTION OPERACIÓN CLIENTE	INGECALL SAS	Baja
GESTION OPERACIÓN CLIENTE	CINATEL SAS	Baja
GESTIÓN ADMINISTRATIVA Y FINANCIERA	GRUPO D&P S.A.S	Media
GESTIÓN ADMINISTRATIVA Y FINANCIERA	ACEVEDO ABOGADOS CONSULTORES SAS	Media
GESTIÓN ADMINISTRATIVA Y FINANCIERA	MEDINA ABOGADOS S.A.S.	Media
GESTIÓN ADMINISTRATIVA Y FINANCIERA	GESTION Y DESARROLLO PROFESIONAL SAS (Gedespro)	Media
GAF	JOHN JAIRO LOPOEZ	Baja
GESTIÓN ADMINISTRATIVA Y FINANCIERA	PETI SOLUCIONES PRODUCTIVAS S.A.S.	Alta
GESTIÓN ADMINISTRATIVA Y FINANCIERA	YEAPP SAS	Alta
GESTIÓN ADMINISTRATIVA Y FINANCIERA	PROASISTEMAS S.A.	Alta
COMERCIAL	Ariba (ETB)	Alta
COMERCIAL	GEPsmart (Telefónica)	Media
ALIANZAS	IMPRESISTEM Distribuciones - Huawei	Baja
ALIANZAS	AVAYA COMMUNICATION DE COLOMBIA	Media
ALIANZAS	LUMU TECHNOLOGIES S.A.S. - NDR	Media
ALIANZAS	INGRAM MICRO S.A.S.	Baja
TECNOLOGÍAS DE LA INFORMACIÓN	CRISTIHAN DIAZ CARRILLO	Baja
IMPLEMENTACIÓN	ASISTEL SOLUCIONES TELEINFORMÁTICAS	Media
IMPLEMENTACIÓN	FAEDCA SAS	Media
IMPLEMENTACIÓN	REDELECTRON - D&S SAS	Media
IMPLEMENTACIÓN	INGECALL SAS	Media
IMPLEMENTACIÓN	CINATEL SAS	Media
IMPLEMENTACIÓN	ECOMIL SAS	Media
IMPLEMENTACIÓN	MATIZZO	Media

PROCESO	PROVEEDOR/ALIADO	CRITICIDAD
COMERCIAL	SECOP	Media
COMERCIAL	Cámara de Comercio de Bogotá	Baja
ALIANZAS	NEXSYS DE COLOMBIA SAS	Baja
ALIANZAS	TD SYNnex LTDA	Baja
ALIANZAS	MICROSYSLABS SAS	Alta
TECNOLOGÍAS DE LA INFORMACIÓN	ETB S.A. E.S.P.	Alta
TECNOLOGÍAS DE LA INFORMACIÓN	Telefónica S.A.	Alta
TECNOLOGÍAS DE LA INFORMACIÓN	Tigo S.A.	Alta
TECNOLOGÍAS DE LA INFORMACIÓN	Claro	Alta
TECNOLOGÍAS DE LA INFORMACIÓN	Microsoft	Alta
TECNOLOGÍAS DE LA INFORMACIÓN	Asistel – Soluciones Teleinformáticas Ltda.	Media
TECNOLOGÍAS DE LA INFORMACIÓN	TD SYNnex	Media
TECNOLOGÍAS DE LA INFORMACIÓN	GoDaddy	Alta
TECNOLOGÍAS DE LA INFORMACIÓN	Fortinet	Alta
TECNOLOGÍAS DE LA INFORMACIÓN	Kaspersky	Alta
TECNOLOGÍAS DE LA INFORMACIÓN	Infocomunicaciones	Media

Tabla 7. Listado de proveedores críticos

La criticidad de los anteriores proveedores fue evaluada de acuerdo con los siguientes criterios:

DESCRIPCIÓN	CRITICIDAD
Dependencia del proveedor para la operación del proceso mayor al 60%	Alta
Dependencia del proveedor para la operación del proceso entre el 31% y 60%	Media
Dependencia del proveedor para la operación del proceso menor al 30%	Baja

Tabla 8. Criterios para evaluar los proveedores

Este numeral es complementado con el “Anexo No. 2 - Yeapdata - Evaluación de criticidad de proveedores”, el cual describe la información de contacto del proveedor, su proceso propietario y la evaluación de todos los proveedores identificados para los procesos.

7 GESTIÓN DE INCIDENTES DE INTERRUPCIÓN

El objetivo de la gestión de incidentes de continuidad del negocio es responder y recuperar oportunamente dentro de los tiempos definidos por el proceso (RTO), ante eventos que puedan afectar la continuidad de los procesos críticos, y en general la operación en contingencia hasta el retorno a los niveles normales de la operación, con el fin

de mantener al máximo la disponibilidad de los procesos y por ende la prestación de los servicios de Yeapdata a las partes interesadas. Para describir la gestión de incidentes de interrupción se establecen las siguientes cuatro fases:

7.1 FASE 1 - RESPUESTA

Esta fase considera todas aquellas actividades que requieren ser ejecutadas para dar una respuesta inicial al incidente disruptivo. Tiene como objetivo velar por la integridad del recurso afectado (Personas, procesos, infraestructura física, tecnología y proveedores) y realizar el escalamiento inicial para permitir una toma de decisiones oportuna. Para el caso de las personas, dentro de esta fase se puede llegar a considerar la ejecución de las actividades relacionadas como parte de la gestión y manejo de emergencias (Plan de emergencias).

7.2 FASE 2 - ACTIVACIÓN Y RECUPERACIÓN

Dentro de esta fase se consideran las actividades necesarias para desplegar la estrategia de acuerdo con los escenarios de desastre materializados. Tiene como objetivo recuperar los procesos críticos de operación (definidos previamente en el BIA) para la prestación de servicios en niveles aceptables. Para el inicio de la fase de recuperación se requiere la declaración de activación del plan de continuidad por parte del equipo/rol responsable, o la activación de los planes de contingencia diseñados por Yeapdata para recuperar recursos específicos ante fallas puntuales.

Teniendo en cuenta la lista de los procesos críticos identificados durante la fase de análisis de impacto del negocio (BIA), a continuación, se presentan las estrategias de continuidad del negocio en relación con los procesos necesarios para cada una:

ESCENARIO	ESTRATEGIA	DESCRIPCIÓN	PROCESOS AL QUE APLICA
Posible afectación o pérdida de la disponibilidad de la información procesada o almacenada en los servicios entregados por los proveedores (Microsoft, Conectividad, Mantenimiento, Energía y otros)	Requerir continuidad de negocio/DRP en los contratos con proveedores	Exigir a los proveedores contar con un plan de continuidad de negocio o esquemas redundantes que deben implementarse durante la ejecución del contrato	Todos los procesos con proveedores de criticidad "Alta" y "Media"
	Contratar proveedores sustitutos	Contratar proveedores en modalidad de contingencia para que inicien la operación en caso de que el proveedor actual/principal no esté disponible	
	Activación de contingencias locales	Aplicar procedimiento de activación de contingencia automática o manual según plataforma y proceso	
	Teletrabajo/Trabajo remoto	En la modalidad de trabajo remoto las personas desarrollarán sus actividades desde casa, con solo disponer de un equipo de cómputo con el software y conectividad a	Todos los procesos

ESCENARIO	ESTRATEGIA	DESCRIPCIÓN	PROCESOS AL QUE APLICA
		internet para ingresar a las herramientas colaborativas	
	Traslado a otra sede /centro alternativo de operaciones	Esta estrategia implica el traslado del personal crítico a cualquiera de las otras tres sedes disponibles de Yeapdata	Todos los procesos
Posible generación de afectación o imposibilidad de acceso o uso de las instalaciones físicas de la compañía y a los datacenter que soportan las operaciones de los procesos de Yeapdata	Teletrabajo/Trabajo remoto	En la modalidad de trabajo remoto las personas desarrollarán sus actividades desde casa, con solo disponer de un equipo de cómputo con el software y conectividad a internet para ingresar a las herramientas colaborativas	Todos los procesos
	Traslado a otra sede /centro alternativo de operaciones	Esta estrategia implica el traslado del personal crítico a cualquiera de las otras tres sedes disponibles de Yeapdata	Todos los procesos
Posible afectación o indisponibilidad del personal considerado como crítico por su conocimiento o experiencia en la administración de los servicios TI	Desarrollar el plan de sucesión para el personal considerado como crítico	El sucesor de una persona crítica para el proceso inicia la ejecución de las actividades en el momento en que se genera la interrupción por causa de la ausencia del responsable principal. Ver Tabla 6. Listado de personal crítico	Todos los procesos
	Capacitar al personal	Evaluar el conocimiento actual del personal frente a los procedimientos operativos desarrollados en los procesos, con base en los resultados, planear y ejecutar la capacitación	Todos los procesos
Posible afectación de la disponibilidad de la información procesada o almacenada en la infraestructura tecnológica física de propiedad o administrada por YeapData	Uso de datacenter alternativo disponible en otra sede	Si los servicios TI del datacenter principal fallan, entonces se recuperan los servicios redundantes disponible en el datacenter alternativo	Todos los procesos
	Uso de servicios TI en nube	Si datacenter principal se encuentra indisponible, entonces los servicios se recuperan en infraestructura de la nube	Todos los procesos

Tabla 9. Estrategias de continuidad según escenario de desastre

7.2.1 Prioridad de recuperación según criticidad del proceso

A continuación, se presenta el listado de todos los procesos de Yeapdata organizados por orden de recuperación:

PROCESO	ORDEN DE RECUPERACIÓN POR PROCESO
Tecnologías de la Información	1
Gestión Operación Cliente	2
SOC	3
Financiera	4
Talento Humano	5
Sistema Integrado de Gestión	6
Procurement	7
Comercial	8
Gestión Estratégica	9
Implementación	10
Alianzas	11

Tabla 10. Prioridad y orden de recuperación de los procesos

7.2.2 Recursos mínimos en la recuperación

De igual forma, la fase de activación y recuperación contempla la implementación de recursos mínimos durante la interrupción. A continuación, se relacionan los recursos mínimos identificados como necesarios en la fase de recuperación para cada uno de los procesos:

PROCESO	RECURSOS MÍNIMOS
Gestión Estratégica	• Personal identificado como crítico
	• Internet
	• SIM Card
	• Microsoft 364
	• Computadores
	• ODOO
Alianzas	• Personal identificado como crítico
	• Internet
	• SIM Card
	• Microsoft 364
	• Computadores
	• ODOO
Talento Humano	• Personal identificado como crítico

PROCESO	RECURSOS MÍNIMOS
	• Internet
	• SIM Card
	• Microsoft 365
	• Helisa
	• Carpetas laborales
	• Computadores
Sistema Integrado de Gestión	• Personal identificado como crítico
	• Internet
	• SIM Card
	• Kawak
	• Microsoft 365
	• Computadores
	• Aranda
Comercial	• Personal identificado como crítico
	• Internet
	• SIM Card
	• Microsoft 365
	• Computadores
	• ODOO
Implementación	• Personal identificado como crítico
	• Internet
	• SIM Card
	• Microsoft 365
	• Computadores
Gestión Operación Cliente	• Personal identificado como crítico
	• Internet
	• SIM Card
	• Microsoft 365
	• Computadores
	• Aranda
	• Wolkvox
	• Herramientas físicas de trabajo: diademas
SOC	• Personal identificado como crítico
	• Internet
	• SIM Card
	• Computadores
	• Microsoft 365
	• SIEM

PROCESO	RECURSOS MÍNIMOS
	• NDR
	• XDR
	• OpenVas
	• EDR
	• Aranda
	• Video wall
Procurement	• Personal identificado como crítico
	• Internet
	• SIM Card
	• Microsoft 365
	• ODOO
	• Computadores
Financiera	• Personal identificado como crítico
	• Internet
	• SIM Card
	• Microsoft 365
	• Computadores
	• ODOO
	• Helisa
	• Tokens digitales y físicos
Tecnologías de la Información	• Personal identificado como crítico
	• Internet
	• SIM Card
	• Microsoft 365
	• Computadores
	• Monitores auxiliares
	• VPN

Tabla 11. Listado de recursos de contingencia para los procesos

7.3 FASE 3 - CONTINGENCIA

Dentro de esta fase se consideran las actividades necesarias para asegurar el alcance de los niveles de operación en contingencia definidos para los procesos críticos. Tiene como objetivo ofrecer los niveles mínimos de servicio por parte de los procesos dentro del alcance establecido. Esta fase es equivalente al periodo de operación en contingencia, es decir, mientras los planes de continuidad de operaciones o plan de recuperación ante desastres se encuentren activos.

7.4 FASE 4 - RETORNO A LA OPERACIÓN NORMAL

Esta fase contempla la realización de las actividades de restauración y retorno necesarias para restablecer los niveles normales de operación de los procesos críticos de negocio, es decir retorno a la operación normal. Para el desarrollo de la fase se requiere que el recurso afectado por el incidente se encuentre en la misma, o mejores condiciones operativas que antes del desastre que generó su indisponibilidad.

7.5 FLUJO Y ACTIVIDADES DE LA GESTIÓN DE INCIDENTES DE INTERRUPCIÓN

A continuación, se presenta el diagrama de flujo que reúne las actividades correspondientes a las cuatro fases: respuesta, activación y recuperación, contingencia y retorno a la operación normal y su relación con los equipos involucrados (estratégico, táctico y operativo), adicionalmente a ello se identifican aquellas actividades que tienen un diagrama de flujo o actividades que apoyan su ejecución.

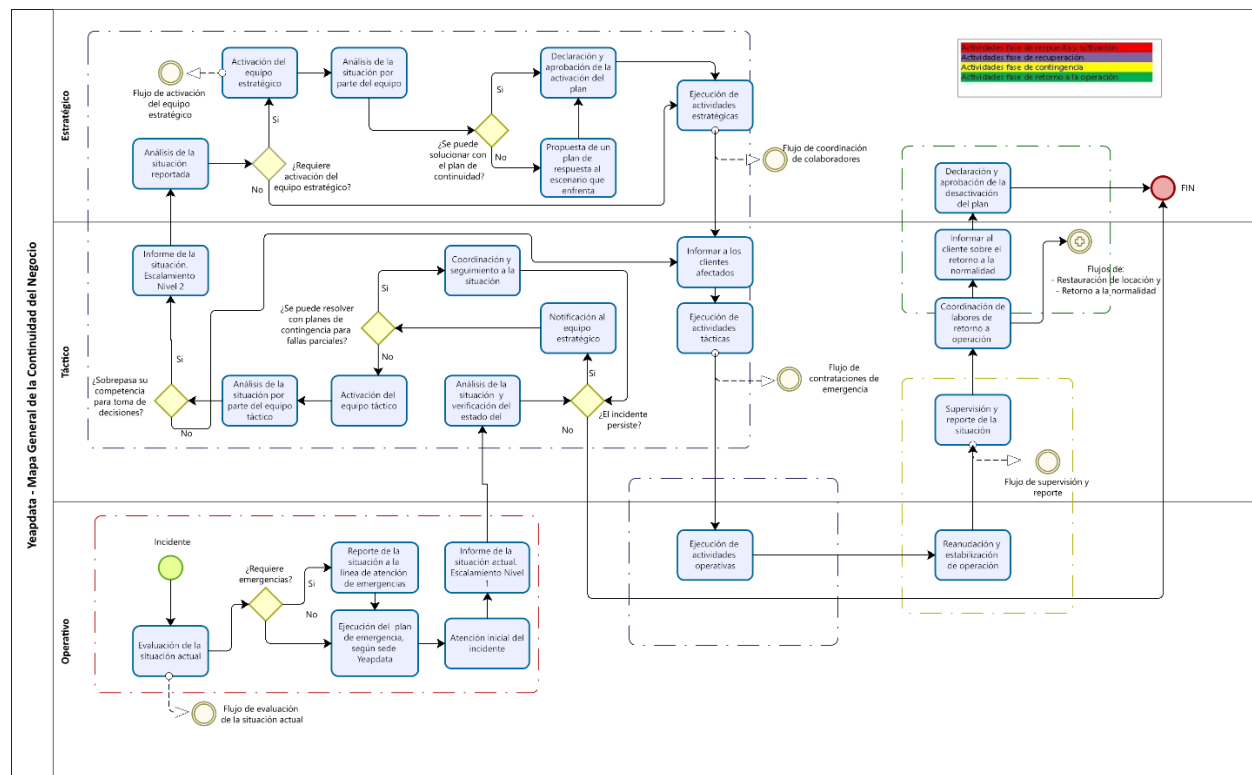


Ilustración 5. Flujo general de la gestión de incidentes de interrupción

A continuación, se describen las actividades mencionadas dentro del flujograma:

ID	FASE	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Respuesta	Incidente (Dirigirse al ID 2)	Todo inicia con la materialización o amenaza de materialización de un incidente de interrupción que potencialmente requiera la activación del PCN.	Operativo
2	Respuesta	Evaluación de la situación actual (Dirigirse al ID 3)	Consiste en la evaluación detallada de los daños o condición en la se encuentra Yeapdata. A partir de esto, tomar las decisiones pertinentes para salvaguardar la vida de las personas y la consecuente continuidad de las operaciones. La ejecución de esta actividad se apoya con el flujo de “Evaluación de la situación actual” y el “Anexo No. 3 – Yeapdata - Formato de evaluación de daños”.	Operativo
3	Respuesta	¿Requiere atención de emergencia?	Toma de decisión. Se plantea la necesidad de desplegar el plan de emergencias de Yeapdata, esto resulta clave en la toma de decisiones toda vez que puede implicar activar el plan de emergencias por ejemplo para movilizar / evacuar las personas (colaboradores, terceros, visitantes, entre otros). La vida e integridad de las personas es prioritaria a la continuidad de operaciones.	Operativo
4	Respuesta	SI (Dirigirse al ID 6)	Toma de decisión.	Operativo
5	Respuesta	NO (Dirigirse al ID 8)	Toma de decisión.	Operativo
6	Respuesta	Reporte de la situación a la línea de atención de emergencias (Dirigirse al ID 7)	Emitir comunicación a la(s) líneas de atención de emergencias propias o de autoridades locales para efectos de reportar el evento que está sucediendo y en caso de requerirse pedir la asistencia respectiva.	Operativo
7	Respuesta	Ejecución del plan de emergencias (Dirigirse al ID 8)	Esta actividad básicamente referencia todas las actividades de planes de emergencias con los que cuenta Yeapdata, por ejemplo: ante escenarios como sismos, incendios, amenazas terroristas, asonadas, entre otros.	Operativo
8	Respuesta	Atención inicial del incidente (Dirigirse al ID 9)	Una vez se tengan las condiciones de seguridad y salud en el trabajo, se procede con actividades propias de la atención del incidente, por ejemplo: convocatoria de los equipos de respuesta y recuperación, involucramiento de terceros o especialistas en caso de ser requerido, entre otras.	Operativo

ID	FASE	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
9	Respuesta	Informe de la situación actual a las partes interesadas. Escalamiento Nivel 1 (Dirigirse al ID 10)	Desde la perspectiva de líderes e integrantes de procesos afectados por la interrupción se realiza la consolidación de daños, de posibles medidas de contingencia y en general toda la información que sirva de apoyo para la toma de decisiones de los equipos tácticos y estratégicos. Se informará a los clientes afectados por el incidente, si aplica. El escalamiento deberá realizarse con base en los contactos del "Anexo No. 1 - Yeapdata - Lista de contactos del árbol de llamadas PCN" proporcionando toda la información relevante de la situación.	Operativo
10	Activación y recuperación	Análisis de la situación y verificación del estado del incidente (Dirigirse al ID 11)	Con la información procedente de los análisis anteriores de líderes de procesos, emergencias, salud, seguridad, TI o cualquier otro involucrado con el incidente, se debe verificar el impacto del incidente y analizar posibles acciones de escalamiento al nivel estratégico en caso de persistencia en la interrupción.	Táctico
11	Activación y recuperación	¿El incidente persiste?	Toma de decisión. Aquí se plantea la necesidad de analizar si el incidente generará una interrupción prolongada en el tiempo (superior al RTO establecido para los procesos de negocio).	Táctico
12	Activación y recuperación	SI (Dirigirse al ID 14)	Toma de decisión	Táctico
13	Activación y recuperación	NO (Dirigirse al ID 45)	Toma de decisión	Táctico
14	Activación y recuperación	Notificación al equipo estratégico	Con la información recopilada y últimas actualizaciones del estado del incidente, se debe notificar de formar prioritaria (de inmediato) al equipo estratégico respecto de la condición afrontada.	Táctico
15	Activación y recuperación	¿Se puede resolver con planes de contingencia para fallas parciales?	Toma de decisión. Este condicional lo deben evaluar los líderes de procesos involucrados junto con el Chief Operation Officer para determinar si ante el incidente presentado se puede dar alguna solución mediante planes de contingencia o planes por fallas parciales.	Táctico
16	Activación y recuperación	SI (Dirigirse al ID 18)	Toma de decisión	Táctico
17	Activación y recuperación	NO (Dirigirse al ID 19)	Toma de decisión	Táctico

ID	FASE	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
18	Activación y recuperación	Coordinación y seguimiento a la solución de la falla parcial (Dirigirse al ID 11)	Ejecución de otras actividades de planes de contingencia o planes ante fallas parciales que se desplegarán para recuperar las operaciones. Durante el periodo de tiempo en paralelo de deben llevar a cabo acciones de seguimiento a la recuperación y notificación al equipo estratégico de los avances y finalización de la contingencia.	Táctico
19	Activación y recuperación	Activación del equipo táctico (Dirigirse al ID 20)	Si se ha llegado a este punto está claro que no se ha podido dar solución al incidente con procedimientos o planes de contingencia parciales preestablecidos, por lo tanto, los líderes de continuidad deben reunirse junto con otros líderes de procesos según corresponda con la naturaleza del incidente enfrentado para analizar escenarios y proponer alternativas de atención.	Táctico
20	Activación y recuperación	Análisis de la situación por parte del equipo táctico (Dirigirse al ID 21)	Con la información obtenida hasta este punto del tiempo, el equipo reunido analiza si hay medidas de emergencia adicionales a tomar, por ejemplo: contrataciones de emergencia, movilización de recursos internos, solicitudes adicionales a proveedores, apalancamiento en servicios prestados por aliados, etc. Así mismo, cuando se realice este análisis, el equipo debe plantearse como mínimo los siguientes aspectos: · El cumplimiento de los objetivos de recuperación (RTO y RPO) · Los beneficios, ventajas y desventajas de las medidas de emergencia · Los riesgos que se enfrentarán por cada acción propuesta y los riesgos de no actuación · Plantearse si activando los planes de continuidad (PCN, DRP) se obtendrían mejores resultados en lugar de persistir en otras alternativas · La potestad o niveles de autoridad necesarios para desplegar recursos · La coordinación de acción con otros equipos al interior de Yeapdata para desplegar cualquier actividad	Táctico
21	Activación y recuperación	¿Sobrepasa su competencia para la toma de decisiones?	Toma de decisión. El equipo táctico evalúa si las decisiones requeridas están dentro de sus competencias o se requiere escalamiento para la toma de decisiones.	Táctico
22	Activación y recuperación	SI (Dirigirse al ID 24)	Toma de decisión	Táctico
23	Activación y recuperación	NO (Dirigirse al ID 36)	Toma de decisión	Táctico

ID	FASE	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
24	Activación y recuperación	Informe de la situación. Escalamiento Nivel 2	El Chief Operation Officer de las operaciones completa/documenta el informe del incidente y la gestión realizada con base en los resultados de las actividades anteriores y todas aquellas adicionales establecidas como producto de la gestión adelantada. El escalamiento se realiza con base en "Anexo No. 1 - Yeapdata - Lista de contactos del árbol de llamadas PCN" proporcionando toda la información relevante de la situación.	Táctico
25	Activación y recuperación	Análisis de la situación reportada (Dirigirse al ID 26)	Con base en la información reportada por el Chief Operation Officer se analiza la necesidad de convocar en pleno al equipo estratégico.	Estratégico
26	Activación y recuperación	¿Requiere activación del equipo estratégico?	Toma de decisión. Para la toma de decisión de activación de PCN o DRP ante desastres se requerirá quorum y previo a ello se plantea la necesidad de activar el equipo estratégico en pleno.	Estratégico
27	Activación y recuperación	SI (Dirigirse al ID 29)	Toma de decisión	Estratégico
28	Activación y recuperación	NO (Dirigirse al ID 35)	Toma de decisión	Estratégico
29	Activación y recuperación	Activación del equipo estratégico (Dirigirse al ID 30)	La activación del equipo estratégico se coordina por uno de sus integrantes y opcionalmente con la asistencia del Chief Operation Officer. Nota: La ejecución de esta actividad se apoya con el flujo: "Activación del equipo estratégico".	Estratégico
30	Desarrollar el plan de sucesión para el personal considerado como crítico	Análisis de la situación por parte del equipo (Dirigirse al ID 31)	Con base en la información de las etapas anteriores: evaluación de daños, despliegue de planes de contingencia o de fallas parciales, potenciales impactos a los grupos de interés, actividades de emergencia planteadas previamente, cumplimiento de objetivos de recuperación, operatividad de estrategias, entre otras; el equipo estratégico dicta disposiciones y toma decisiones en pro de recuperar las funciones primordiales de los procesos críticos que se hayan visto afectadas.	Estratégico
31	Activación y recuperación	¿Se puede solucionar con el plan de continuidad?	Toma de decisión. El equipo estratégico toma la decisión de activación del Plan (PCN o DRP) siempre y cuando existan posibilidades reales de superar la crisis a partir de la aplicación de los planes, sino se requerirá estudiar nuevas alternativas de solución.	Estratégico
32	Activación y recuperación	SI (Dirigirse al ID 34)	Toma de decisión	Estratégico
33	Activación y recuperación	NO (Dirigirse al ID 44)	Toma de decisión	Estratégico

ID	FASE	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
34	Activación y recuperación	Declaración y aprobación de la activación del plan (Dirigirse al ID 35)	Esta aprobación de declaración de la “crisis” y respectiva activación del plan (PCN o DRP) es exclusiva del nivel estratégico y es producto del análisis previo con la revisión de todas las demás alternativas de solución posibles.	Estratégico
35	Activación y recuperación	Ejecución de actividades estratégicas (Dirigirse al ID 36)	Dependiendo de la naturaleza y complejidad del incidente el nivel estratégico lleva a cabo las actividades y responsabilidades propias de la gestión durante el incidente, entre otras: dar lineamientos de actuación, tomar decisiones del alto nivel con implicaciones para toda la compañía, facilitar los recursos necesarios para la recuperación, coordinar actuación con otras partes interesadas, monitorear el progreso durante la contingencia. Nota: La ejecución de esta actividad se apoya con el flujo: “Coordinación de colaboradores”.	Estratégico
36	Activación y recuperación	Informar a los clientes afectados	Informar a los clientes afectados sobre la activación del plan de continuidad, si aplica.	Táctico
37	Activación y recuperación	Ejecución de actividades tácticas (Dirigirse al ID 38)	Esta actividad reúne las responsabilidades propias del equipo táctico respecto de la actuación durante un incidente (ver numeral de responsabilidades), entre otras: hacer análisis de información, coordinación con líderes de procesos, comunicación permanente con los demás integrantes de equipos de continuidad, consolidar y suministrar información para la toma de decisiones. Verificar el cumplimiento de los objetivos de recuperación establecidos por Yeapdata mediante el seguimiento y apoyo constante en el desarrollo de las actividades. Nota: La ejecución de esta actividad se apoya con el flujo: “Contrataciones de emergencia”.	Táctico

ID	FASE	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
38	Activación y recuperación	Ejecución de actividades Operativas (Dirigirse al ID 39)	Trata de las actividades que los líderes de procesos y sus equipos despliegan para recuperar las actividades críticas de la operación, entre otras se pueden tener las actividades/responsabilidades de: Atender las indicaciones una vez sea activado del plan para desplegar las estrategias a que haya lugar de acuerdo con el incidente enfrentado, en conformidad con las indicaciones del nivel estratégico. Validar que los requerimientos mínimos de recuperación estén disponibles y funcionen adecuadamente en las estrategias alternas de trabajo. Ejecutar el procedimiento de recuperación del proceso y/o de la plataforma de Tecnología afectada, según corresponda. Suministrar información al Chief Operation Officer de las operaciones sobre la recuperación del proceso. Realizar actividades de monitoreo sobre la operación del proceso o la plataforma tecnológica en contingencia.	Operativo
39	Contingencia	Reanudación y estabilización de operación (Dirigirse al ID 40)	Una vez activado el plan (PCN o DRP) se operará en “ambiente de contingencia” mientras se logran las condiciones adecuadas para retorno a la normalidad. Durante este periodo de tiempo la operación debe ser estabilizada y supervisada para garantizar unos mínimos de nivel de servicio a pesar de ser un ambiente parcial o contingente.	Operativo
40	Contingencia	Supervisión y reporte de la situación (Dirigirse al ID 41)	Todo el tiempo que se mantenga un ambiente de operación “en contingencia” corresponderá supervisión permanente y reporte de la situación y avance al nivel estratégico y partes interesadas claves del progreso en la recuperación y retorno a la normalidad. Se debe informar a los clientes afectados, si aplica. Nota: La ejecución de esta actividad se apoya con el flujo: “Supervisión y reporte”.	Táctico

ID	FASE	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
41	Retorno a la operación	Coordinación de labores de retorno a operación normal (Dirigirse al ID 42)	Conforme pase el tiempo de operación en contingencia, se adelantarán con algún tiempo de sincronismo las actividades tendientes al retorno a la operación normal (la misma condición de operación anterior a la materialización del incidente), el periodo de duración y el detalle de las actividades dependerán de la severidad y naturaleza del incidente enfrentado. Por ejemplo, no son iguales los tiempos y actividades a realizarse ante los escenarios 1) amenaza de atentado terrorista, que tomaría unos pocos días para volver a la sede normal de trabajo; que 2) un atentado terrorista, que podría tomar varias semanas o inclusive meses para reconstruir la sede y volver a la condición inicial; en ambos casos las actividades serían muy diferentes. Nota: La ejecución de esta actividad se apoya con los flujos: Restauración de locación. Retorno a la operación normal.	Táctico
42	Retorno a la operación	Informar al cliente sobre el retorno a la normalidad (Dirigirse al ID 43)	Se informará a los clientes afectados, que el servicio ya fue recuperado en el ambiente de productivo, si aplica.	Táctico
43	Retorno a la operación	Declaración y aprobación de la desactivación del plan (Dirigirse al ID 45)	Así como el nivel estratégico fue responsable por la activación del plan, también es responsable por declarar el fin de la “crisis” y aprobar la desactivación del PCN, cumpliendo con los criterios pertinentes de una desactivación y retorno a la normalidad segura, estable y duradera.	Estratégico
44	Activación y recuperación	Propuesta de un plan de respuesta al escenario que enfrenta Yeapdata (Dirigirse al ID 34)	En caso de que después de los análisis de alternativas de solución para afrontar la crisis, ventajas/desventajas de activar el plan de continuidad, se determine que se requieren planes (PCN, DRP) diferentes a los previamente establecidos, el nivel estratégico da lineamientos de actuación y facilita los recursos que permitan desplegar rápidamente nuevos procedimientos de actuación que regirán el actuar en los equipos tácticos y operativos.	Estratégico
45	Retorno a la operación	FIN	Con el retorno a la normalidad producto de la ejecución del PCN o planes de contingencia ante fallas parciales se finaliza el ciclo de gestión del incidente.	Estratégico

Tabla 12. Detalle de las actividades gestión de incidentes de interrupción

7.6 FLUJOS DE APOYO

7.6.1 Evaluación de la situación actual

El siguiente flujograma plantea las actividades para llevar a cabo la evaluación de la situación actual en la fase de respuesta:

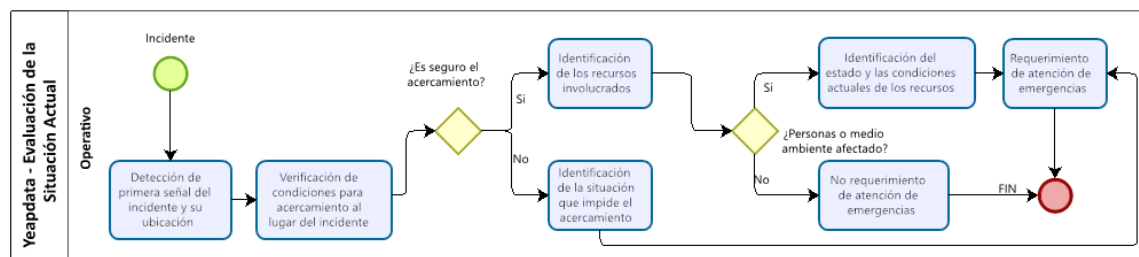


Ilustración 6. Flujo evaluación de la situación actual

A continuación, se describen las actividades mencionadas dentro del flujograma:

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Incidente (Dirigirse al ID 2)	Se genera un incidente disruptivo.	Operativo
2	Detección de la primera señal del incidente y su ubicación (Dirigirse al ID 3)	A través de observación directa, alarmas tempranas o el uso de controles preventivos y/o detectivos con los que cuente Yeapdata se obtiene señales de alertamiento ante la materialización de incidentes.	Operativo
3	Verificación de condiciones para acercamiento al lugar del incidente (Dirigirse al ID 4)	En caso de tratarse de afectaciones a la infraestructura física (ej., edificaciones, datacenter, ascensores, transformadores, etc.) se aplican los protocolos de seguridad en el trabajo antes de cualquier intervención.	Operativo
4	¿Es seguro el acercamiento?	Toma de decisión.	Operativo
5	SI (Dirigirse al ID 7)	Toma de decisión.	Operativo
6	NO (Dirigirse al ID 13)	Toma de decisión.	Operativo
7	Identificación de los recursos involucrados (Dirigirse al ID 8)	Determinar el inventario de recursos/activos que se encuentran comprometidos por el incidente o potencial incidente.	Operativo
8	¿Personas o medio ambiente afectados?	Toma de decisión.	Operativo
9	SI (Dirigirse al ID 11)	Toma de decisión.	Operativo
10	NO (Dirigirse al ID 14)	Toma de decisión.	Operativo
11	Identificación del estado y las condiciones actuales del recurso (Dirigirse al ID 12)	Determinar el inventario de daños actuales y potenciales daños siguientes junto con los recursos involucrados, cuanto mayor detalle se tenga mejor será la toma de decisiones posterior.	Operativo

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
12	Requerimiento de atención de emergencias (Dirigirse al ID 15)	De acuerdo con la situación enfrentada se determinar la activación de planes de emergencia para priorizar la vida y salud de las personas, todo dependerá de la naturaleza y magnitud del evento. Esta actividad debe realizarse por los brigadistas, autoridades o personal idóneo para la determinación de la situación y la toma de decisiones.	Operativo
13	Identificación de la situación que impide el acercamiento seguro (Dirigirse al ID 12)	Guardando las medidas de precaución respectivas en conformidad con los protocolos de seguridad se identifica y decide si es viable la utilización del lugar de trabajo. La actividad debe ser realizada por profesionales pertinentes e idóneos para esta función.	Operativo
14	No requerimiento de atención de emergencias (Dirigirse al ID 15)	Al no reportarse afectación/daños a la salud o ambiente se podrá continuar con las actividades de gestión de incidentes.	Operativo
15	FIN	Si no hay afectación (ID 14) o se supera la emergencia salvaguardando la salud de las personas se podrá continuar con actividades para la recuperación de procesos.	Operativo

Tabla 13. Detalle de las actividades evaluación de la situación actual

7.6.2 Activación del nivel estratégico

El siguiente flujograma plantea las actividades para llevar a cabo la activación del equipo estratégico en la fase de activación y recuperación:

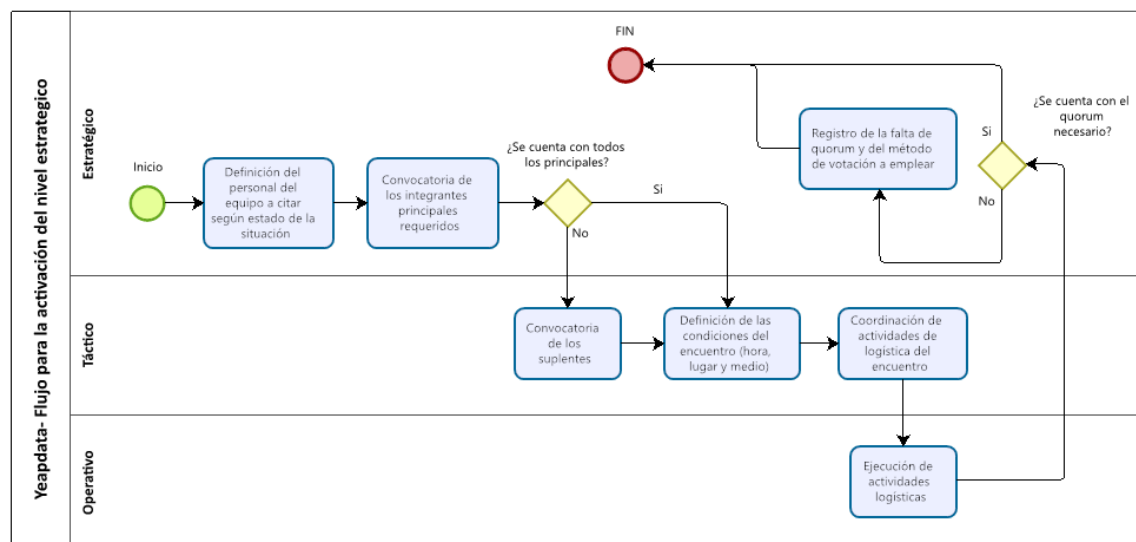


Ilustración 7. Flujo activación del nivel estratégico

A continuación, se describen las actividades mencionadas dentro del flujograma:

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Inicio (Dirigirse al ID 2)	Ante el incidente presentado el nivel estratégico está activo para tomar decisiones y/o movilizar recursos según sea necesario. Una de las decisiones más claves consiste en si activar o no el plan de continuidad (PCN y/o DRP).	Estratégico
2	Definición del personal del equipo a citar según estado de la situación (Dirigirse al ID 3)	Dependiendo del escenario enfrentado el nivel estratégico podrá definir líderes de procesos o nuevos participantes de apoyo en los niveles táctico y operativo.	Estratégico
3	Convocatoria de los integrantes principales requeridos (Dirigirse al ID 4)	Dependiendo del escenario enfrentado el nivel estratégico convoca a los líderes de procesos o nuevos participantes de apoyo en los niveles táctico y operativo para desplegar preparativos con miras a la activación del plan.	Estratégico
4	¿Se cuenta con todos los principales?	Toma de decisión	Estratégico
5	SI (Dirigirse al ID 7)	Toma de decisión	Estratégico
6	NO (Dirigirse al ID 10)	Toma de decisión	Estratégico
7	Definición de las condiciones del encuentro (hora, lugar y medio) (Dirigirse al ID 8)	Esta actividad establece el “encuentro” (lugar, hora y medio) para movilizar recursos necesarios en la activación del plan.	Táctico
8	Coordinación de actividades de logística del encuentro (Dirigirse al ID 9)	Según la naturaleza del evento enfrentado se prepara la logística previa a la movilización de recursos. Por ejemplo, no es igual el alistamiento ante una amenaza terrorista que obliga evacuación a una situación de afectación de los servicios tecnológicos que soportan los procesos, en cada caso la coordinación tendrá sus variantes respectivas.	Táctico
9	Ejecución de actividades logísticas (Dirigirse al ID 11)	Esta actividad consiste en confirmar que se cuentan con los recursos mínimos de recuperación para responder inmediatamente se apruebe la activación del Plan. Dependiendo de la naturaleza del incidente los recursos mínimos podrán cambiar, ejemplos de estos son: personal, puestos de trabajo, equipos de cómputo, acceso a los servicios y aplicaciones de TI, disponibilidad de los servicios de proveedores, entre otros.	Operativo
10	Convocatoria de los suplentes (Dirigirse al ID 7)	En caso de no contar directamente con los líderes de procesos, se podrá convocar a los suplentes que cumplan las funciones del principal o titular.	Táctico
11	¿Se cuenta con el quórum necesario?	Toma de decisión	Estratégico

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
12	SI (Dirigirse al ID 15)	Toma de decisión	Estratégico
13	NO (Dirigirse al ID 14)	Toma de decisión	Estratégico
14	Registro de la falta de quórum y del método de votación a emplear (Dirigirse al ID 15)	En caso dado que no se cuente con el quórum suficiente para la toma de decisión unánime del nivel estratégico, respecto de la activación del Plan, y sea inminente la necesidad y pertinencia de la activación del Plan, se plantea un nuevo quorum estimado en los participantes presentes al momento de tomar la decisión. Esta actividad y las decisiones que se deriven deben ser documentadas.	Estratégico
15	FIN	El resultado esperado de este flujo es contar con la preparación del nivel estratégico para iniciar la toma de decisión de activar el plan.	Estratégico

Tabla 14. Detalle de las actividades activación del nivel estratégico

7.6.3 Coordinación de colaboradores

El siguiente flujograma plantea las actividades para llevar a cabo la coordinación del personal de Yeapdata que ejecutará la recuperación durante la fase de activación y recuperación:

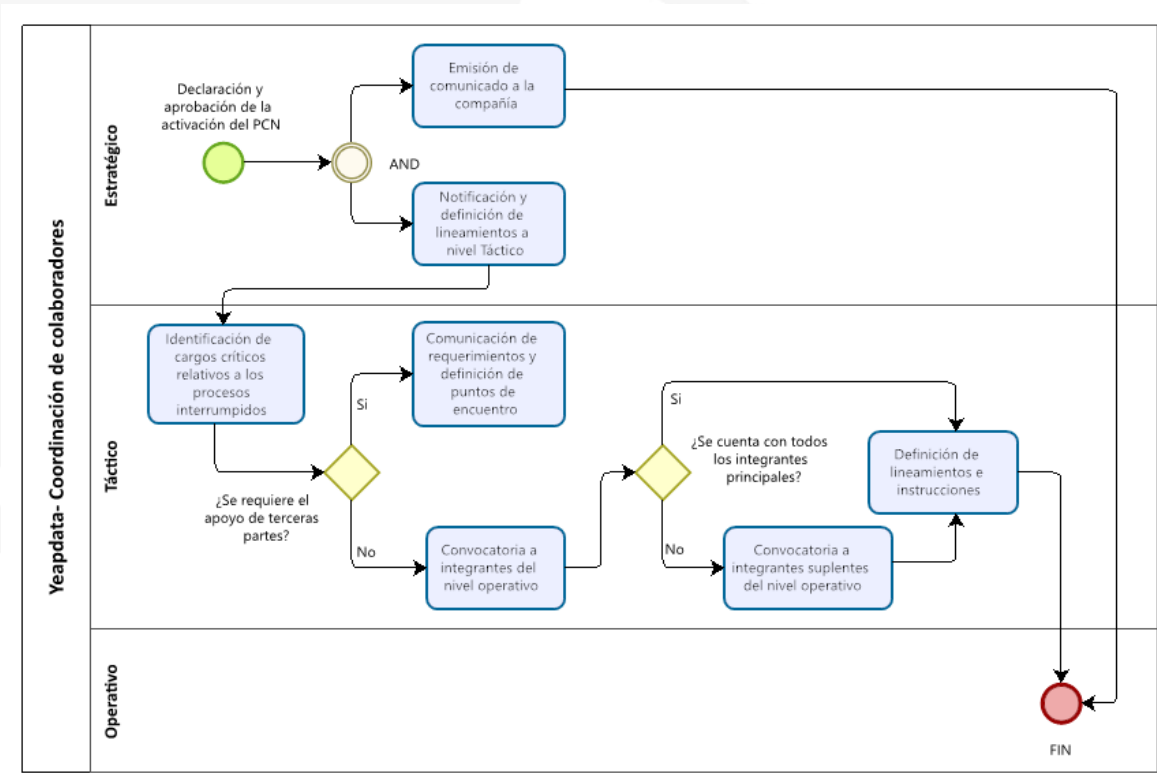


Ilustración 8. Flujo coordinación de colaboradores

A continuación, se describen las actividades mencionadas dentro del flujograma:

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Declaración y aprobación de la activación del plan (Dirigirse al ID 2 y 3)	A partir de la declaración de activación del Plan se convoca los colaboradores directamente necesarios para la recuperación inicial.	Estratégico
2	Emisión de comunicado de la Entidad	La activación del PCN viene acompañada de un comunicado inicialmente interno para los colaboradores. Las comunicaciones deben ser manejadas en conformidad con las políticas y procedimientos de comunicaciones de Yeapdata. El presente plan cuenta con el “Anexo No. 4 - Yeapdata - Guiones de comunicación sugeridos” como apoyo a la definición de las comunicaciones a emitir.	Estratégico
3	Notificación y definición de lineamientos a nivel táctico (Dirigirse al ID 4)	Al mismo tiempo de la comunicación general, se dan los lineamientos de actuación a los líderes del nivel táctico para el despliegue y operación en contingencia.	Estratégico
4	Identificación de cargos críticos relativos a los procesos interrumpidos (Dirigirse al ID 5)	Además de los líderes de procesos críticos se debe vincular a los colaboradores requeridos para recuperación de la operación, esta actividad se realiza en cooperación entre líderes de procesos y líderes de continuidad.	Táctico
5	¿Se requiere el apoyo de terceras partes?	Toma de decisión	Táctico
6	SI (Dirigirse al ID 8)	Toma de decisión	Táctico
7	NO (Dirigirse al ID 9)	Toma de decisión	Táctico
8	Comunicación de requerimientos y definición de puntos de encuentro (Dirigirse al ID 9)	Algunas de las actividades de la operación son realizadas por contratistas, en este entendido se ha planteado esta actividad para rescatar que puede llegar a ser necesario convocar a estos integrantes para la recuperación.	Táctico
9	Convocatoria a integrantes del nivel operativo (Dirigirse al ID 10)	Los colaboradores de los procesos definidos como críticos serán convocados para participar en la recuperación, esto puede implicar movilización a sede alterna, teletrabajo, trabajo remoto, cambio de roles por contingencia o cualquier otra alternativa de continuidad de acuerdo con el incidente enfrentado.	Táctico
10	¿Se cuenta con todos los integrantes principales?	Toma de decisión	Táctico
11	SI (Dirigirse al ID 13)	Toma de decisión	Táctico
12	NO (Dirigirse al ID 14)	Toma de decisión	Táctico
13	Definición de lineamientos e instrucciones (Dirigirse al ID 15)	De acuerdo con el incidente enfrentado se darán las instrucciones de primera movilización para la recuperación.	Táctico
14	Convocatoria a integrantes suplentes del nivel operativo (Dirigirse al ID 13)	En caso de no contar directamente con los colaboradores que normalmente operan el proceso, se podrá convocar a los colaboradores (sucesores) que cumplan las funciones del principal. En este punto también debe considerarse las	Táctico

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
		actividades desempeñadas por otro personal y que resultan vitales en la recuperación.	
15	FIN	Se han desplegado las comunicaciones y convocatoria de los colaboradores y otro personal para la movilización hacia la recuperación y continuidad de la operación.	Táctico

Tabla 15. Detalle de las actividades coordinación de colaboradores

7.6.4 Contrataciones de recursos de emergencia

El siguiente flujograma plantea las actividades para llevar a cabo la contratación de recursos de manera emergente durante la fase de activación y recuperación:

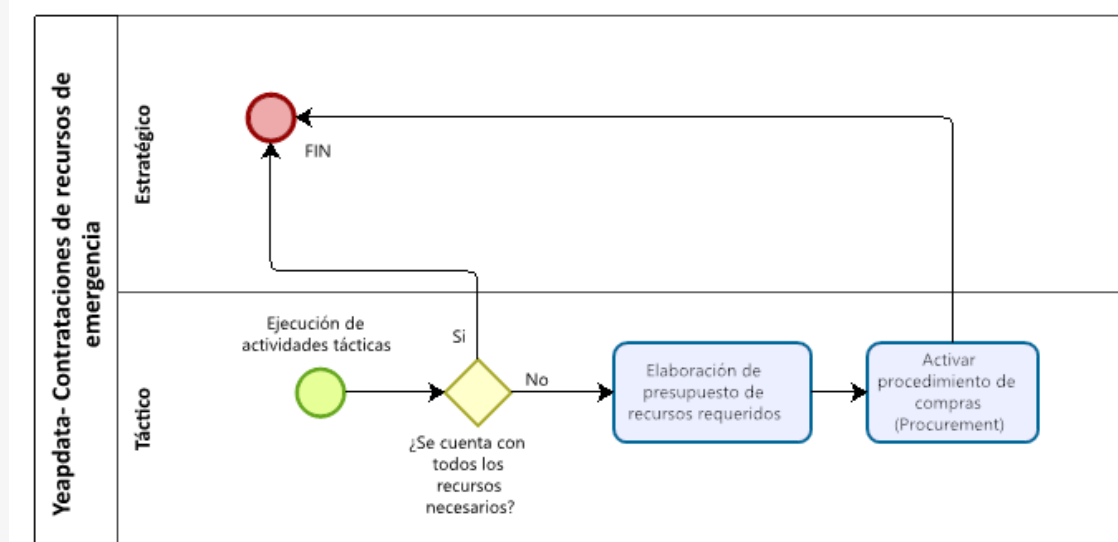


Ilustración 9. Flujo contratación de recursos de emergencia

A continuación, se describen las actividades mencionadas dentro del flujograma:

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Ejecución de actividades tácticas (Dirigirse al ID 2)	Dentro de las posibles actividades que se requieren en una contingencia están las contrataciones o compras de emergencia, en este entendido se deben respetar las políticas y procedimientos de compra de Yeapdata, sin perder de vista que se trataría de un escenario de urgencia manifiesta y que se requerirá un manejo excepcional para minimizar los tiempos de interrupción de la operación de la compañía.	Táctico
2	¿Se cuenta con todos los recursos necesarios?	Toma de decisión	Táctico
3	SI (Dirigirse al ID 5)	Toma de decisión	Táctico

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
4	NO (Dirigirse al ID 6)	Toma de decisión	Táctico
5	Elaboración de presupuesto de recursos requeridos (Dirigirse al ID 6)	El equipo táctico lidera la actividad de consolidación de requerimientos junto con el apoyo de líderes de procesos y Procurement.	Táctico
6	Activar procedimiento de compras	Se deberán surtir los procedimientos de compras y logística, así como los controles que puedan ser aplicables para la autorización de pagos.	Táctico
7	FIN	Se ha logrado gestionar la compra o contratación de emergencia o sencillamente se cuenta con todos los recursos sin necesidad de nuevas contrataciones.	Estratégico

Tabla 16. Detalle de las actividades contratación de recursos emergencia

7.6.5 Supervisión y reporte

El siguiente flujograma plantea las actividades para llevar a cabo la supervisión y reporte durante la fase de contingencia:

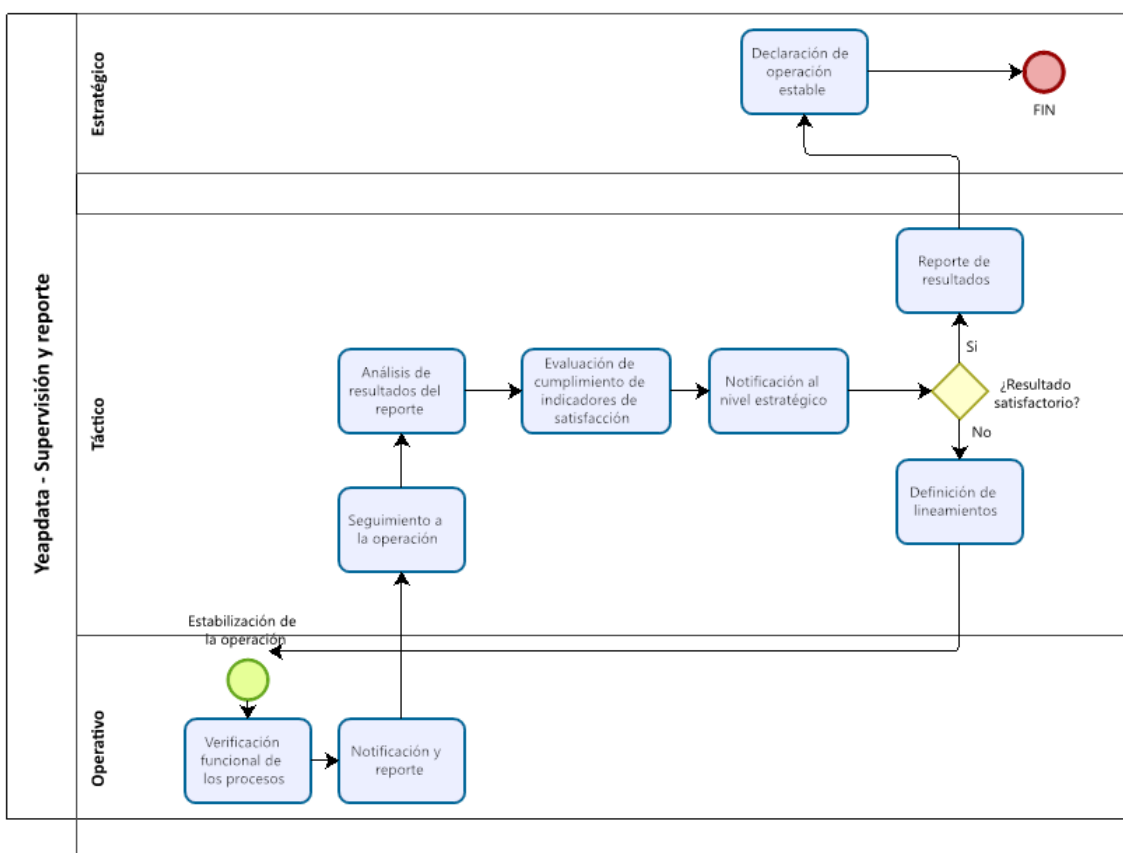


Ilustración 10. Flujo supervisión y reporte

A continuación, se describen las actividades mencionadas dentro del flujograma:

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Estabilización de la operación (Dirigirse al ID 2)	Una vez se ha desplegado el PCN y se han iniciado las actividades de movilización de recursos para la recuperación de procesos, la operación en el nuevo ambiente de “contingencia” debe ser supervisada de cerca y los reportes respectivos enviados al equipo táctico y operativo.	Operativo
2	Verificación funcional de los procesos (Dirigirse al ID 3)	Los líderes de procesos involucrados en la recuperación y operación en contingencia realizan la verificación funcional en las nuevas condiciones de trabajo, bien sea por cualquier de las estrategias de continuidad que se haya desplegado, por ejemplo, en utilización de centros de trabajo alterno, teletrabajo, aplicaciones de respaldo por el DRP, proveedores adicionales o sustitutos, entre otros.	Operativo
3	Notificación y reporte (Dirigirse al ID 3)	Diariamente se deben enviar notificaciones y reporte del estado de la operación en el ambiente de contingencia.	Operativo
4	Seguimiento de la operación (Dirigirse al ID 5)	Corresponderá a los líderes de continuidad dar seguimiento a la operación en contingencia para gestionar novedades de parte de los equipos operativos o requerimientos de otras partes interesadas.	Táctico
5	Análisis de resultados del reporte (Dirigirse al ID 6)	Los líderes de continuidad analizan los resultados de la operación para asegurar el cumplimiento de los objetivos de recuperación (RTO y RPO) y en caso de novedades, impedimentos o dificultades gestionar su pronta resolución.	Táctico
6	Evaluación de cumplimiento de indicadores de satisfacción (Dirigirse al ID 7)	Los principales indicadores de satisfacción apuntan al cumplimiento de los objetivos de recuperación RTO y RPO que se han definido para los procesos críticos junto con las aplicaciones y servicios de TI que soportan su operación.	Táctico
7	Notificación al nivel estratégico (Dirigirse al ID 8)	El nivel estratégico debe recibir las notificaciones periódicas (diaria como mínimo) respecto del avance de la operación en contingencia.	Táctico
8	¿Resultado satisfactorio?	Toma de decisión	Táctico
9	SI (Dirigirse al ID 10)	Toma de decisión	Táctico
10	NO (Dirigirse al ID 12)	Toma de decisión	Táctico
11	Declaración de operación estable (Dirigirse al ID 13)	Si se cumplen los objetivos de recuperación, la estrategia funciona y se entregan los niveles mínimos de servicio se puede dar la declaración de una operación de continuidad estable.	Estratégico
12	Definición de lineamientos (Dirigirse al ID 1)	Se requiere más información o ajuste en las maneras de operar en la nueva condición de continuidad toda vez que aún no se logra estabilizar por completo la operación en las nuevas condiciones.	Táctico
13	FIN	Llegado a este punto significa que la operación en modo “contingencia” está funcionando, es decir se ha logrado la recuperación de procesos y la operación se encuentra de manera razonable estabilizada	Estratégico

Tabla 17. Detalle de las actividades supervisión y reporte

7.6.6 Restauración de locación

El siguiente flujograma plantea las actividades para llevar a cabo la restauración de las instalaciones físicas que se reconstruyan durante la etapa de retorno a la operación:

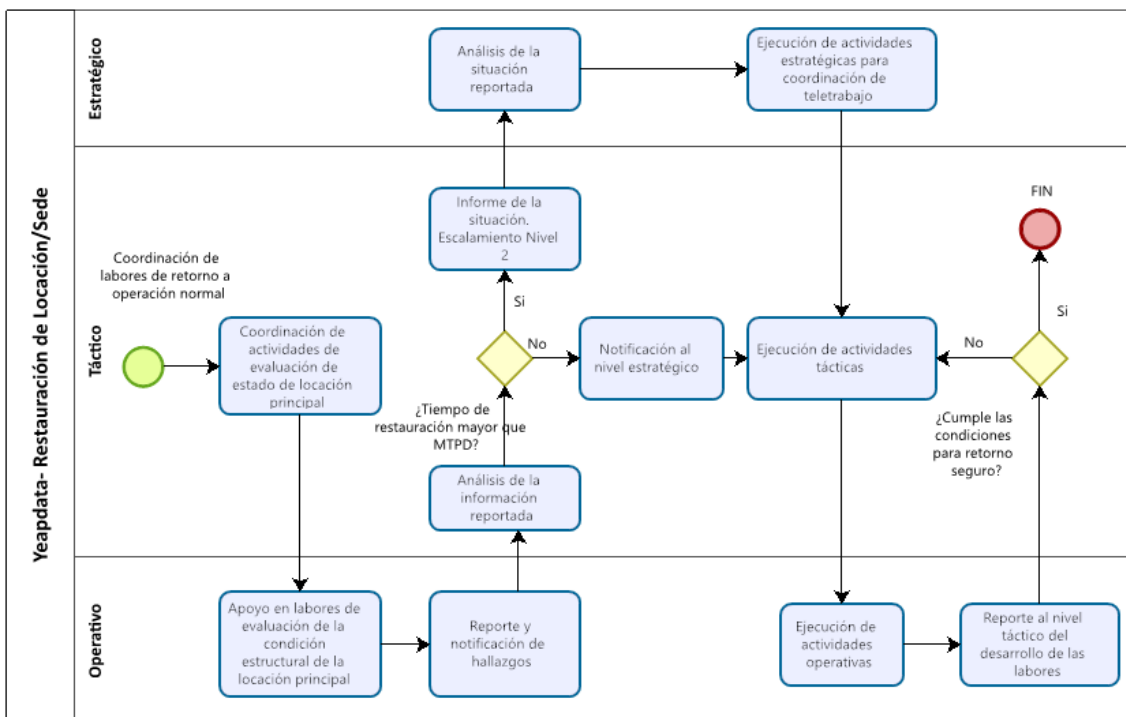


Ilustración 11. Flujo restauración de locación

A continuación, se describen las actividades mencionadas dentro del flujograma:

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Coordinación de labores de retorno a la operación normal (Dirigirse al ID 2)	Además de planear y trabajar para la recuperación en sede operaciones alterna, también se requiere evaluar la posibilidad de retorno a la condición normal de operación.	Táctico
2	Coordinación de actividades de evaluación de estado de locación principal (Dirigirse al ID 3)	Se debe vincular a especialistas internos y externos en caso de ser necesario, por ejemplo, de autoridades en gestión de riesgos de desastres o especialistas de aseguradoras.	Táctico
3	Apoyo en labores de peritaje de la condición estructural de la locación principal (Dirigirse al ID 4)	Se toma como referencia las listas de chequeo de evaluación de daños (Anexo No. 3 - Yeapdata - Formato de evaluación de daños) y todos los artefactos que los especialistas provean para esta actividad.	Operativo
4	Reporte y notificación de hallazgos (Dirigirse al ID 5)	Resultado del peritaje debe ser reportado a los niveles táctico y estratégico.	Operativo

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
5	Análisis de la información reportada (Dirigirse al ID 6)	Con la información recibida se debe analizar y determinar la viabilidad de utilización en el inmediato plazo del lugar de trabajo en condición normal.	Táctico
6	¿Tiempo de restauración mayor que MTPD?	Toma de decisión	Táctico
7	SI (Dirigirse al ID 9)	Toma de decisión	Táctico
8	NO (Dirigirse al ID 12)	Toma de decisión	Táctico
9	Informe de la situación. Escalamiento Nivel 2 (Dirigirse al ID 10)	Llegar a esta actividad significa que la sede principal de trabajo no estará disponible en el corto plazo y que el retorno a operación normal tomará varios días, por tanto, se seguirá las actividades de las etapas de recuperación y estabilización de la operación.	Táctico
10	Análisis de la situación reportada (Dirigirse al ID 11)	Se toman decisiones para activar las estrategias ante ausencia de la sede principal de trabajo entre otras para la movilización de recursos en caso de ser necesario.	Estratégico
11	Ejecución de actividades estratégicas para coordinación de teletrabajo (Dirigirse al ID 13)	En caso dado que la mejor alternativa ante la ausencia de la sede principal de trabajo sea teletrabajo o trabajo remoto, se debe iniciar el despliegue de recursos y controles de seguridad de la información para esta actividad.	Estratégico
12	Notificación al equipo estratégico (Dirigirse al ID 13)	La notificación indica que las condiciones de la instalación permitirán retornar a la sede principal antes que se venzan los tiempos límite de MTPD, no se cumplirán probablemente los RTO, pero se podrá recuperar en un tiempo máximo tolerable.	Táctico
13	Ejecución de actividades tácticas (Dirigirse al ID 14)	Actividades propias de seguimiento, coordinación, monitoreo propias de las responsabilidades del nivel táctico.	Táctico
14	Ejecución de actividades operativas (Dirigirse al ID 15)	Actividades propias de ejecución, coordinación, reporte propias de las responsabilidades del nivel operativo.	Operativo
15	Reporte al equipo táctico del desarrollo de las labores (Dirigirse al ID 16)	Actividades propias de ejecución, coordinación, reporte propias de las responsabilidades del nivel operativo.	Operativo
16	¿Cumple las condiciones para retorno seguro?	Toma de decisión	Táctico
17	SI (Dirigirse al ID 19)	Toma de decisión	Táctico
18	NO (Dirigirse al ID 13)	Toma de decisión	Táctico
19	FIN	Llegar a este punto significa que se tiene la posibilidad de retorno a la sede de trabajo principal de manera segura.	Táctico

Tabla 18. Detalle de las actividades restauración de locación

7.6.5. Retorno a la operación normal

El siguiente flujograma plantea las actividades para llevar a cabo el retorno a la operación normal:

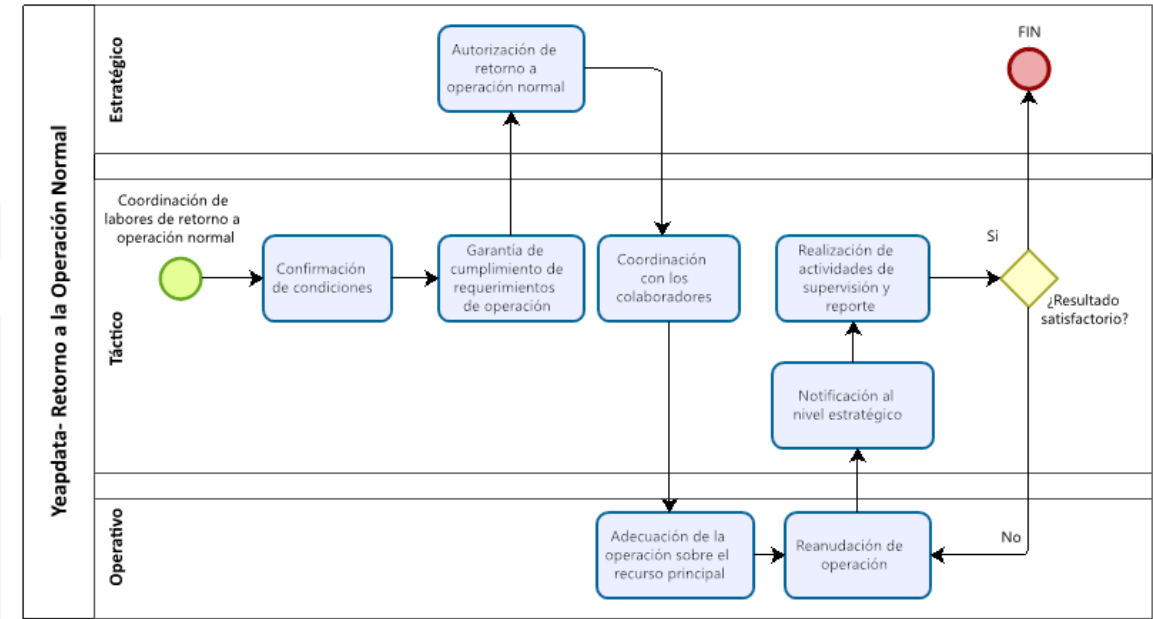


Ilustración 12. Flujo retorno a la operación normal

A continuación, se describen las actividades mencionadas dentro del flujograma:

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Coordinación de labores de retorno a la operación normal (Dirigirse al ID 2)	Corresponde a todas las actividades propias para el alistamiento del retorno a la operación normal. Se tiene como supuesto que Yeapdata ha desarrollado todos aquellos trabajos de obras civiles, infraestructura, eléctricas, de redes de datos, servicios públicos, etc., que son necesarias para una restauración adecuada de la sede de trabajo principal.	Táctico
2	Confirmación de condiciones (Dirigirse al ID 3)	Actividad que debe realizarse por especialistas internos o colaboradores calificados para tal fin, puede ser de la compañía aseguradora o autoridad en materia de gestión de riesgos de desastres.	Táctico
3	Garantía de cumplimiento de requerimientos de operación (Dirigirse al ID 4)	Se espera obtener visto bueno de garantía de parte de autoridad externa según pueda aplicar, puede ser de la compañía aseguradora o autoridad en materia de gestión de riesgos de desastres.	Táctico
4	Autorización de retorno a la operación normal (Dirigirse al ID 5)	Así como es responsabilidad exclusiva del nivel estratégico aprobar la activación del PCN, también será su responsabilidad dar la autorización para el retorno a operación normal.	Estratégico
5	Coordinación con los empleados (Dirigirse al ID 6)	Igualmente se requiere la coordinación con los colaboradores para el retorno organizado y seguro a las instalaciones de Yeapdata.	Táctico

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
6	Adecuación de la operación sobre el recurso principal (Dirigirse al ID 7)	Una vez se avanza en el retorno a operación normal es posible que se requieran adecuaciones de la operatividad pues quizás las condiciones hayan cambiado respecto a distribución de espacios, por ejemplo.	Operativo
7	Reanudación de operación (Dirigirse al ID 8)	Se hace referencia con esta actividad a todas aquellas tareas que se deben llevar a cabo para la reanudación de la operación en la sede principal de trabajo de la Entidad.	Operativo
8	Notificación al equipo estratégico (Dirigirse al ID 9)	De manera permanente al igual que en etapas anteriores se debe notificar al Comité de Continuidad el progreso en las actividades de retorno a la operación normal.	Táctico
9	Realización de actividades de supervisión y reporte (Dirigirse al ID 10)	De manera permanente al igual que en etapas anteriores se debe notificar al Comité de Continuidad el progreso en las actividades de retorno a la operación normal. La supervisión es una tarea permanente en la etapa de retorno a la normalidad.	Táctico
10	¿Resultado satisfactorio?	Toma de decisión	Táctico
11	SI (Dirigirse al ID 13)	Toma de decisión	Estratégico
12	NO (Dirigirse al ID 7)	Toma de decisión	Táctico
13	FIN	Llegar a este punto significa que se ha podido retornar a la operación normal luego de haber activado el PCN y trabajado en ambiente de contingencia	Estratégico

Tabla 19. Detalle de las actividades retorno a la operación normal

8 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

La continuidad de la seguridad de la información implica mantener la operación de Yeapdata garantizando la confidencialidad, integridad y disponibilidad de la información y de los activos durante la contingencia.

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1	Establecer los requisitos de seguridad de la información a mantener durante la interrupción	Los requisitos de seguridad de la información a mantenerse durante la interrupción dependen del escenario de desastre materializado y la estrategia de recuperación, para lo cual, en la <i>Tabla 21. Requisitos de seguridad de la información a dar continuidad</i> se describen.	Líder DRP Líder PCN Especialista de implementación y soporte, y seguridad de la información
2	Implementar acciones para mantener la seguridad de la información	Ejecutar las actividades que permitirán la continuidad de la Seguridad de la Información. Entre ellas pueden estar: · Preparar las TIC para la continuidad del negocio. · Mantener los procedimientos operativos documentados. · Mantener planes de respuesta a incidentes. · Establecer procesos para dar seguimiento a las redes, los sistemas, aplicaciones.	Líder DRP Especialista de implementación y soporte, y seguridad de la información

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
		· Definición de personal para la respuesta ante un escenario, actividades y tiempos de recuperación.	
3	Verificar y evaluar de la continuidad de la seguridad de la información	Se verifica la continuidad de la seguridad de la información durante los ejercicios de pruebas establecidos, y de acuerdo con los resultados obtenidos pasa a la actividad 4.	Líder DRP Líder PCN Especialista de implementación y soporte, y seguridad de la información
4	Mejorar la continuidad de la seguridad de la información	Durante esta actividad se implementan las mejoras evidenciadas en los resultados de las pruebas al PCN, DRP y a la continuidad de la Seguridad de la Información.	Líder DRP Líder PCN Especialista de implementación y soporte, y seguridad de la información

Tabla 20. Continuidad de la seguridad de la información

A continuación, se identifican los requisitos generales de seguridad de la información que deben ser tenidos en cuenta en la ejecución de cada una de las estrategias de recuperación, para los escenarios de desastre para la compañía:

ESCENARIO	ESTRATEGIA	REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN
Indisponibilidad de servicios/productos de proveedores	Requerir continuidad de negocio/DRP en los contratos con proveedores	- Abordar la seguridad de la información dentro de los acuerdos con los proveedores que se requieran contratar. - Establecer acuerdos de confidencialidad y transferencia de información. - Gestionar la seguridad de la información en la cadena de suministro de TIC. - Realizar seguimiento, revisión y gestión del cambio de los servicios de los proveedores. - Proporcionar medios para la transferencia segura de información. - Compartir las políticas de seguridad de la información. - Informar el proceso para la notificación de eventos y debilidades en seguridad de la información.
	Contratar proveedores sustitutos	Cumplimiento de la política de seguridad de proveedores
Indisponibilidad del servicio de suministro de energía	Traslado a otra sede /centro alternativo de operaciones / Contingencia de suministro eléctrico temporal	- Gestión de autorizaciones para el retiro de activos de información de las instalaciones de Yeapdata. - Cumplimiento de las medidas establecidas en la política para teletrabajo. - Disponibilidad de medios seguros para la transferencia de la información. - Disponibilidad de medios para el reporte de eventos y debilidades de seguridad de la información. - Mantener la disponibilidad de las instalaciones de procesamiento de información alterna que soportan los procesos críticos. - Uso de dispositivos corporativos para realizar las labores en contingencia. - Mantener las políticas de seguridad en los equipos perimetrales de seguridad. - Configuración de las VPN del personal requerido. - Aplicar las políticas de contraseñas seguras. - Gestionar la capacidad de los recursos tecnológicos.

ESCENARIO	ESTRATEGIA	REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN
		- Ejecución de las copias de seguridad de la información. - Controles de acceso físico para la entrada a las oficinas o sede alterna de Yeapdata.
Indisponibilidad de acceso a las instalaciones físicas de la compañía	Teletrabajo/Trabajo remoto	- Aplicar las políticas de contraseñas seguras. - Mantener las políticas de seguridad en los equipos perimetrales de seguridad. - Mantener la disponibilidad de las instalaciones de procesamiento de información alterna que soportan los procesos críticos. - El acceso a los activos de información durante el teletrabajo debe cumplir con las políticas de seguridad de la información. - Cumplimiento de las medidas establecidas en la política para teletrabajo. - Cumplimiento de las medidas establecidas en la política de escritorio limpio y fondo de pantalla. - La conexión a los activos de información solo se debe permitir desde los dispositivos asignados por Yeapdata. - Para la revisión y soporte del equipo se deberá contactar al área de TI quienes son los únicos autorizados a intervenir dichos dispositivos. - En caso de retiro del colaborador es obligación de este devolver todos los dispositivos en la sede donde fueron entregados.
Indisponibilidad del personal crítico para la compañía	Desarrollar el plan de sucesión para el personal considerado como crítico	- Desarrollo de estudio de seguridad para las nuevas contrataciones. - Incorporación de cláusulas de confidencialidad y reserva de la información, propiedad intelectual y autorización de tratamiento de datos personales - Configuración de las VPN del personal requerido. - Habilitación de controles de acceso físico y lógico, por ejemplo: VPN, entrada a oficinas y zonas seguras, activos de información críticos. - Conocimiento, aceptación y cumplimiento de políticas de seguridad de la información por parte del personal alterno.
	Capacitar al personal	Desarrollo de estrategias de capacitación y concientización en seguridad de la información, sobre controles, políticas, procedimientos y

ESCENARIO	ESTRATEGIA	REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN
		demás lineamientos en seguridad de la información.
Indisponibilidad de las tecnologías de la información y comunicación	Uso de datacenter alternativo disponible en otra sede	- Disponibilidad de medios seguros para la transferencia de la información. - Disponibilidad de medios para el reporte de eventos y debilidades de seguridad de la información. - Mantener los procesos para la gestión de incidentes de seguridad de la información - Mantener la disponibilidad de las instalaciones de procesamiento de información alternas que soportan los procesos del alcance. - Mantener las políticas de seguridad en los equipos perimetrales de seguridad. - Validar y/o configurar las VPN del personal requerido para las comunicaciones o conectividad con la infraestructura alterna. - Asegurar la aplicación de las políticas de contraseñas seguras. - Monitorear la capacidad de los recursos tecnológicos. - Ejecutar las copias de seguridad de la información. - Contingencia de las bases de datos, aplicaciones, sistemas de información, archivos, servicios TI críticos o mínimos para la operación - Separación de las redes de forma virtual. - Disponibilidad del personal administrador de infraestructura TI. - Mantener el cifrado de la información en tránsito y reposo. - Mantener los procesos y controles de ingreso seguro. - Mantener la verificación del cumplimiento de los requisitos de seguridad de la información - Privacidad y protección de los datos personales. - Mantener establecido el contacto con las autoridades y grupos de interés especial. - Manejar los activos de información de acuerdo con las políticas de la compañía. - Mantener el proceso de registro y cancelación de usuarios.

ESCENARIO	ESTRATEGIA	REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN
		• Dar uso adecuado a la información de autenticación secreta.
		• Mantener los procedimientos de operación definidos (gestión de cambios, gestión de capacidad, borrado seguro, separación de ambientes, desarrollo de software).
		• Mantener la configuración de los accesos y privilegios a los activos de información
		• Mantener la protección contra códigos maliciosos.
		• Mantener el registro y monitoreo acerca de las actividades usuarios, fallas, amenazas y eventos de seguridad de la información.
	Uso de servicios TI en nube	• Mantener la gestión de las vulnerabilidades técnicas de los sistemas.
		• Dar cumplimiento a los requisitos legales y contractuales pertinentes a la seguridad de la información

Tabla 21. Requisitos de seguridad de la información a dar continuidad

Nota: Los requisitos de continuidad de la seguridad de la información establecidos e implementados deben ser verificados o integrados con las pruebas del Plan de Recuperación de Desastres y Plan de Continuidad del Negocio de Yeapdata.

9 MANTENIMIENTO Y ACTUALIZACIÓN DEL PCN

Es necesario que el plan de continuidad se mantenga actualizado y de ser necesario mejorar cada vez que se requiera o ante cambios significativos en políticas, personas, procesos, tecnología o servicios; siendo necesario que en esta revisión participen los procesos involucrados.

El nivel operativo debe coordinar con el Líder de Continuidad, las actualizaciones necesarias al plan y los procedimientos, teniendo en cuenta la identificación de cambios o las oportunidades de mejora, relacionados con los procesos críticos y la tecnología que los soporta.

Componentes del plan de continuidad a actualizar:

- El análisis de impacto a la operación debe actualizarse cada vez que sea necesario, teniendo en cuenta los cambios y necesidades de la operación de Yeapdata.
- Cada vez que se requiera se realizará monitoreo a los escenarios de riesgos de continuidad.
- La estrategia general de respuesta a la contingencia será probada según la planeación.
- La estrategia general se revisará cada vez que el nivel estratégico y táctico lo considere, o como resultado del análisis de riesgos de gestión de seguridad de la información.

9.1 FACTORES DE ACTUALIZACIÓN

Pueden ocurrir ciertos sucesos no programados al interior de Yeapdata o fuera de ésta, que afectan el PCN. A continuación, se relaciona una lista de los que pueden generar una revisión al PCN:

- Requerimientos legales aplicables a la compañía.
- Nuevos productos críticos dentro del proceso Comercial.
- Nueva adquisición de plataforma y servicios tecnológicos.
- Cambio de un proveedor crítico.
- Cambio de sedes.
- Cambios en el personal o rotación de este.
- Tercerización de funciones.
- Resultados de las pruebas del PCN y DRP.
- Cambios en el Sistema de Gestión de Calidad y Procesos.

10 PLAN DE PRUEBAS

Objetivo: Verificar la efectividad de los planes diseñados y medir la capacidad de respuesta de Yeapdata ante un escenario de riesgo predefinido.

Alcance: Todos los procesos

Responsable: Nivel estratégico, táctico y operativo.

El plan de pruebas consta de cinco etapas: preparación, ejecución, actividades post prueba, evaluación y mejoramiento.

10.1 PREPARACIÓN

Se debe de realizar todas las actividades necesarias para armar el escenario de la prueba. En esta primera fase, se realiza la coordinación con los principales responsables de los procesos para que comuniquen a sus equipos sobre la fecha de inicio, la duración y las actividades que se realizarán durante la prueba. También, se debe comunicar, transmitir y entregar los documentos de los planes para que tengan conocimientos de estos.

10.2 EJECUCIÓN

En esta fase, se realizan las pruebas reales a los planes. Según el escenario seleccionado, se prueba las cargas de datos, llamadas por teléfono, traslado de personal, restauraciones de copias de seguridad, llamadas con proveedores, entre otros. El equipo designado realiza un examen del personal involucrado mientras se realizan las tareas. Ello indica el nivel de preparación de Yeapdata para responder ante un desastre.

Esta labor debe realizarse anualmente, ya que con el paso del tiempo las estrategias planteadas dejan de ser efectivas a lo cual se suman nuevos riesgos. Los tipos de pruebas que se pueden realizar son las de escritorio, para comprobar la efectividad de los flujos de trabajo definidos, las pruebas orientadas a la tecnología, para comprobar si la infraestructura TI de respaldo funciona correctamente en el momento de simular un escenario de contingencia y las pruebas orientadas a servicios, para verificar el nivel de capacidad de los procesos.

10.3 ACTIVIDADES POST PRUEBA

Esta fase consiste en dejar los servicios, entornos de prueba, sitios principales y alternos en las mismas condiciones previas a la prueba, es decir, devolver todos los recursos a su ubicación correcta. Además, evaluar el plan realizado e implementar las mejoras observadas.

10.4 EVALUACIÓN DE RESULTADOS

En esta fase, se realiza la recopilación de los resultados obtenidos pasos a paso para evaluar la efectividad que tuvo el plan durante la ejecución de la prueba. Todo esto será detallado dentro de un informe de resultados de la implementación por cada uno de los planes. De acuerdo con este informe, se podrán tomar acciones de mejora para los procedimientos de cada uno de los planes de continuidad del negocio.

10.5 APLICACIÓN DE MEJORAS

En esta última fase, se modifica el contenido de los planes para mejorar la efectividad de estos para la próxima prueba, incluso para el desastre.

11 INFORME DE ANÁLISIS DE IMPACTO AL NEGOCIO – BIA

Este proceso busca analizar los impactos del negocio para determinar las prioridades y requisitos de continuidad del negocio. Por lo cual este BIA busca:

- Definir los tipos de impacto y los criterios relevantes para el contexto de Yeapdata;
- Identificar las actividades que apoyan la provisión de productos y servicios;
- Utilizar los tipos y criterios de impacto para evaluar los impactos a lo largo del tiempo que resultan de la interrupción de estas actividades;
- Identificar el marco de tiempo dentro del cual los impactos de no reanudar las actividades serían inaceptables para Yeapdata;
- Establecer marcos de tiempo priorizados para reanudar las actividades interrumpidas a una capacidad mínima aceptable especificada;
- Utilizar este análisis para identificar actividades priorizadas;
- Determinar qué recursos son necesarios para apoyar actividades priorizadas;
- Determinar las dependencias, incluidos los socios y proveedores, y las interdependencias de las actividades priorizadas.

El análisis de impacto al negocio se focalizó en la operación de los 11 procesos de Yeapdata, con la participación de las siguientes personas:

- Gabriel Quiñones Lara (Cuyo rol actualmente está vacante) por el proceso Gestión Estratégica.
- William David Blanco Lizarazo por el proceso Alianzas.
- Andrea Ximena Rodríguez Rodríguez por el proceso Talento Humano.
- Daniela Artunduaga Arboleda y Johan Camilo Palacio Álvarez por el proceso Sistema Integrado de Gestión
- Fausto Camilo Vanegas por el proceso Comercial.
- Ana Elisa Quintero Cetina por el proceso Implementación.
- Jennifer Astrid Caicedo por el proceso Gestión Operación Cliente.
- David Sierra y Johan Camilo Palacio Álvarez por el proceso SOC.

- Paula Andrea Aguilar Cabezas (Cuyo rol está cubierto actualmente por Oscar Contreras) por el proceso Procurement.
- Lucía Segura por el proceso Financiera.
- Jonathan Esteban Cogua Leal por el proceso Tecnologías de la Información.

11.1 CRITERIOS PARA BIA

Los tipos de impactos analizados son:

ID	Tipo de impacto	Descripción
1	Impacto Operación	Determina cómo la interrupción del proceso impacta la operación general de Yeapdata.
2	Impacto Reputación / Imagen	Determina cómo la interrupción del proceso afecta la imagen, la marca, el buen nombre y la reputación de Yeapdata ante las partes interesadas.
3	Impacto Bienestar	Determina cómo la interrupción del proceso afecta el bienestar de las partes interesadas (productividad, estrés laboral, presión, crecimiento, sobrecarga mental, laboral y emocional).
4	Impacto Financiero	Determina cómo la interrupción del proceso puede generar pérdidas cuantificables en dinero, lo cual impacta las finanzas de Yeapdata.
5	Impacto Seguridad de la Información	Determina cómo la interrupción del proceso impacta la confidencialidad, integridad y disponibilidad de la información de Yeapdata.
6	Impacto Servicio al cliente	Determina cómo la interrupción del proceso afecta la prestación del servicio a los clientes, la calidad, la entrega oportuna y su satisfacción
7	Impacto Legal / Normativo	Determina cómo la interrupción del proceso genera incumplimientos de los requisitos legales y normativos vigentes y aplicables para Yeapdata.

Tabla 22. Tipos de impactos analizados

11.1.1 Criterios para la evaluación de los diferentes tipos de impactos

Cada tipo de impacto relacionado en la tabla anterior es evaluado teniendo en cuenta los siguientes criterios:

TIPO DE IMPACTO	CRITERIOS				
	5. Muy Alto	4. Alto	3. Medio	2. Bajo	1. Insignificante
IMPACTO OPERACIÓN	Afecta más del 50% de la operación.	Afecta del 31% al 50% de la operación.	Afecta del 16% al 30% de la operación.	Afecta del 6% al 15% de la operación.	Afectación menor al 6% de la operación.

TIPO DE IMPACTO	CRITERIOS				
	5. Muy Alto	4. Alto	3. Medio	2. Bajo	1. Insignificante
IMPACTO REPUTACIÓN / IMAGEN	Afectación significativa de la reputación de Yeapdata.	Afectación importante de la reputación de Yeapdata.	Afectación parcial de la reputación de Yeapdata.	Afectación moderada de la reputación de Yeapdata.	Afectación menor a moderada en la reputación de Yeapdata.
IMPACTO BIENESTAR	Afectación significativa del bienestar de las personas de Yeapdata.	Afectación importante al bienestar de las personas de Yeapdata.	Afectación parcial del bienestar de las personas de Yeapdata.	Afectación moderada del bienestar de las personas de Yeapdata.	Afectación menor a moderada del bienestar de las personas de Yeapdata.
IMPACTO FINANCIERO	Afecta más del 50% de la operación financiera de Yeapdata.	Afecta del 31% al 50% de la operación financiera de Yeapdata.	Afecta del 16% al 30% de la operación financiera de Yeapdata.	Afecta del 6% al 15% de la operación financiera de Yeapdata.	Afectación menor al 6% de la operación financiera de Yeapdata.
IMPACTO SEGURIDAD DE LA INFORMACIÓN	Afectación significativa de la CID de Yeapdata.	Afectación importante de la CID de Yeapdata.	Afectación parcial de la CID de Yeapdata.	Afectación moderada de la CID de Yeapdata.	Afectación menor a moderada de la CID de Yeapdata.
IMPACTO SERVICIO AL CLIENTE	Afecta la operación de más del 50% de los clientes	Afecta la operación del 31% al 50% de los clientes	Afecta la operación del 16% al 30% de los clientes	Afecta la operación del 6% al 15% de los clientes	Afectación menor al 6% de los clientes.
IMPACTO LEGAL / NORMATIVO	Afecta más del 50% de los aspectos legales o normativos.	Afecta del 31% al 50% de los aspectos legales o normativos.	Afecta del 16% al 30% de los aspectos legales o normativos.	Afecta del 6% al 15% de los aspectos legales o normativos.	Afectación menor al 6% de los aspectos legales o normativos.

Tabla 23. Criterios de evaluación de los impactos

11.2 RESULTADOS BIA POR PROCESO

El resultado del análisis de impacto a la operación por proceso es el siguiente. Los rangos de tiempo se establecieron con base en el conocimiento y experiencia de los participantes del BIA, a la capacidad de recuperación y al tiempo estimado para recuperar la operación:

11.2.1 Gestión Estratégica

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 8 horas	8 - 18 horas	18 - 46 horas	Mayor a 46 horas
Impacto Operación	2. Bajo	2. Bajo	2. Bajo	2. Bajo
Impacto Reputación / Imagen	1. Insignificante	1. Insignificante	2. Bajo	2. Bajo
Impacto Bienestar	1. Insignificante	1. Insignificante	2. Bajo	2. Bajo
Impacto Financiero	1. Insignificante	2. Bajo	2. Bajo	2. Bajo
Impacto Seguridad Información	2. Bajo	2. Bajo	2. Bajo	2. Bajo
Impacto Servicio al Cliente	2. Bajo	2. Bajo	2. Bajo	2. Bajo
Impacto Legal / Normativo	2. Bajo	2. Bajo	2. Bajo	2. Bajo

Tabla 24. BIA Gestión Estratégica

11.2.2 Alianzas

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 40 horas	40 - 80 horas	80 - 160 horas	Mayor a 160 horas
Impacto Operación	2. Bajo	2. Bajo	3. Medio	3. Medio
Impacto Reputación / Imagen	2. Bajo	2. Bajo	2. Bajo	2. Bajo
Impacto Bienestar	1. Insignificante	1. Insignificante	1. Insignificante	1. Insignificante
Impacto Financiero	2. Bajo	2. Bajo	2. Bajo	2. Bajo
Impacto Seguridad Información	1. Insignificante	1. Insignificante	2. Bajo	2. Bajo
Impacto Servicio al Cliente	1. Insignificante	1. Insignificante	2. Bajo	2. Bajo
Impacto Legal / Normativo	1. Insignificante	1. Insignificante	2. Bajo	2. Bajo

Tabla 25. BIA Alianzas

11.2.3 Talento Humano

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	1 - 2 horas	2 - 8 horas	8 - 40 horas	Mayor a 40 horas
Impacto Operación	2. Bajo	3. Medio	4. Alto	5. Muy Alto
Impacto Reputación / Imagen	2. Bajo	2. Bajo	4. Alto	5. Muy Alto

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	1 - 2 horas	2 - 8 horas	8 - 40 horas	Mayor a 40 horas
Impacto Bienestar	2. Bajo	3. Medio	4. Alto	5. Muy Alto
Impacto Financiero	1. Insignificante	1. Insignificante	4. Alto	5. Muy Alto
Impacto Seguridad Información	2. Bajo	3. Medio	4. Alto	4. Alto
Impacto Servicio al Cliente	2. Bajo	2. Bajo	3. Medio	4. Alto
Impacto Legal / Normativo	3. Medio	3. Medio	4. Alto	5. Muy Alto

Tabla 26. BIA Talento Humano

11.2.4 Sistema Integrado de Gestión

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 4 horas	4- 8 horas	8 - 40 horas	Mayor a 40 horas
Impacto Operación	2. Bajo	3. Medio	4. Alto	4. Alto
Impacto Reputación / Imagen	1. Insignificante	2. Bajo	3. Medio	4. Alto
Impacto Bienestar	1. Insignificante	2. Bajo	3. Medio	4. Alto
Impacto Financiero	1. Insignificante	2. Bajo	3. Medio	4. Alto
Impacto Seguridad Información	2. Bajo	3. Medio	4. Alto	4. Alto
Impacto Servicio al Cliente	1. Insignificante	2. Bajo	3. Medio	4. Alto
Impacto Legal / Normativo	1. Insignificante	2. Bajo	3. Medio	4. Alto

Tabla 27. BIA Sistema Integrado de Gestión

11.2.5 Comercial

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 1 hora	1 - 8 horas	8 - 40 horas	Mayor a 40 horas
Impacto Operación	1. Insignificante	3. Medio	4. Alto	5. Muy Alto
Impacto Reputación / Imagen	2. Bajo	3. Medio	5. Muy Alto	5. Muy Alto
Impacto Bienestar	1. Insignificante	1. Insignificante	2. Bajo	3. Medio

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 1 hora	1 - 8 horas	8 - 40 horas	Mayor a 40 horas
Impacto Financiero	2. Bajo	3. Medio	5. Muy Alto	5. Muy Alto
Impacto Seguridad Información	1. Insignificante	2. Bajo	3. Medio	3. Medio
Impacto Servicio al Cliente	1. Insignificante	2. Bajo	3. Medio	4. Alto
Impacto Legal / Normativo	1. Insignificante	2. Bajo	3. Medio	4. Alto

Tabla 28. BIA Comercial

11.2.6 Implementación

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 8 horas	8 - 16 horas	16 - 40 horas	Mayor 40 horas
Impacto Operación	3. Medio	3. Medio	3. Medio	3. Medio
Impacto Reputación / Imagen	3. Medio	3. Medio	4. Alto	4. Alto
Impacto Bienestar	2. Bajo	2. Bajo	3. Medio	4. Alto
Impacto Financiero	2. Bajo	2. Bajo	3. Medio	4. Alto
Impacto Seguridad Información	2. Bajo	2. Bajo	2. Bajo	3. Medio
Impacto Servicio al Cliente	2. Bajo	3. Medio	4. Alto	4. Alto
Impacto Legal / Normativo	2. Bajo	3. Medio	4. Alto	4. Alto

Tabla 29. BIA Implementación

11.2.7 Gestión Operación Cliente

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 4 horas	4 - 8 horas	8 - 24 horas	Mayor a 24 horas
Impacto Operación	4. Alto	5. Muy Alto	5. Muy Alto	5. Muy Alto
Impacto Reputación / Imagen	2. Bajo	2. Bajo	3. Medio	4. Alto
Impacto Bienestar	3. Medio	3. Medio	4. Alto	5. Muy Alto
Impacto Financiero	1. Insignificante	2. Bajo	4. Alto	5. Muy Alto

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 4 horas	4 - 8 horas	8 - 24 horas	Mayor a 24 horas
Impacto Seguridad Información	2. Bajo	3. Medio	4. Alto	5. Muy Alto
Impacto Servicio al Cliente	2. Bajo	3. Medio	4. Alto	5. Muy Alto
Impacto Legal / Normativo	2. Bajo	2. Bajo	3. Medio	4. Alto

Tabla 30. BIA Gestión Operación Cliente

11.2.8 SOC

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 1 hora	1 - 2 horas	2 - 24 horas	Mayor a 24 horas
Impacto Operación	3. Medio	4. Alto	5. Muy Alto	5. Muy Alto
Impacto Reputación / Imagen	2. Bajo	2. Bajo	4. Alto	5. Muy Alto
Impacto Bienestar	2. Bajo	3. Medio	5. Muy Alto	5. Muy Alto
Impacto Financiero	3. Medio	4. Alto	5. Muy Alto	5. Muy Alto
Impacto Seguridad Información	5. Muy Alto	5. Muy Alto	5. Muy Alto	5. Muy Alto
Impacto Servicio al Cliente	3. Medio	4. Alto	5. Muy Alto	5. Muy Alto
Impacto Legal / Normativo	3. Medio	4. Alto	5. Muy Alto	5. Muy Alto

Tabla 31. BIA SOC

11.2.9 Procurement

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 4 horas	4 - 8 horas	8 - 40 horas	Mayor a 40 horas
Impacto Operación	2. Bajo	2. Bajo	4. Alto	4. Alto
Impacto Reputación / Imagen	2. Bajo	2. Bajo	3. Medio	4. Alto
Impacto Bienestar	2. Bajo	3. Medio	3. Medio	3. Medio
Impacto Financiero	2. Bajo	2. Bajo	4. Alto	4. Alto
Impacto Seguridad Información	2. Bajo	2. Bajo	3. Medio	4. Alto

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 4 horas	4 - 8 horas	8 - 40 horas	Mayor a 40 horas
Impacto Servicio al Cliente	2. Bajo	2. Bajo	3. Medio	3. Medio
Impacto Legal / Normativo	2. Bajo	2. Bajo	2. Bajo	3. Medio

Tabla 32. BIA Procurement

11.2.10 Financiera

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	0 - 2 horas	2 - 4 horas	4 - 8 horas	Mayor a 8 horas
Impacto Operación	3. Medio	4. Alto	5. Muy Alto	5. Muy Alto
Impacto Reputación / Imagen	2. Bajo	3. Medio	4. Alto	5. Muy Alto
Impacto Bienestar	2. Bajo	2. Bajo	3. Medio	5. Muy Alto
Impacto Financiero	2. Bajo	2. Bajo	3. Medio	4. Alto
Impacto Seguridad Información	2. Bajo	2. Bajo	3. Medio	4. Alto
Impacto Servicio al Cliente	1. Insignificante	2. Bajo	2. Bajo	3. Medio
Impacto Legal / Normativo	1. Insignificante	2. Bajo	2. Bajo	5. Muy Alto

Tabla 33. BIA Financiera

11.2.11 Tecnologías de la información

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	1 - 2 horas	2 - 5 horas	5 - 8 horas	Mayor a 8 horas
Impacto Operación	4. Alto	4. Alto	5. Muy Alto	5. Muy Alto
Impacto Reputación / Imagen	3. Medio	4. Alto	4. Alto	5. Muy Alto
Impacto Bienestar	2. Bajo	2. Bajo	3. Medio	4. Alto
Impacto Financiero	2. Bajo	3. Medio	3. Medio	5. Muy Alto
Impacto Seguridad Información	4. Alto	5. Muy Alto	5. Muy Alto	5. Muy Alto
Impacto Servicio al Cliente	2. Bajo	3. Medio	4. Alto	5. Muy Alto

TIPO DE IMPACTO	RANGOS DE TIEMPOS			
	1 - 2 horas	2 - 5 horas	5 - 8 horas	Mayor a 8 horas
Impacto Legal / Normativo	2. Bajo	3. Medio	4. Alto	5. Muy Alto

Tabla 34. BIA Tecnologías de la Información

11.3 INFORMACIÓN Y ACTIVOS ASOCIADOS CRÍTICOS

La información y los activos asociados identificados como críticos por parte de los procesos se encuentran a continuación, así como las siguientes variables:

- **Punto objetivo de recuperación – RPO:** Punto en el cual la información usada por una actividad debe ser restaurada.
- **Periodo máximo tolerable de interrupción - MTD:** Tiempo que tomaría para que los efectos adversos que pudiera ocurrir como resultado de no proporcionar un producto y/o servicio o realizando una actividad, para convertirse en inaceptable.
- **Objetivo de tiempo de recuperación-RTO:** Periodo de tiempo después de un incidente en el que un producto y/o servicio debe ser reanudado.

PROCESO	ACTIVIDAD CRÍTICA	ACTIVO ASOCIADO	DESCRIPCIÓN DEL ACTIVO ASOCIADO	RTO ^[4]	RPO ^[5]	MTD ^[6]
Gestión Estratégica	Comunicación	Suite de Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint, Teams, OneDrive, SharePoint, Forms, Power BI	12 h	24 h	18 h
Gestión Estratégica	Consulta	Odoo	ERP	12 h	24 h	18 h
Alianzas	Consulta de información de aliados	Odoo	ERP	40 h	40 h	48 h
Alianzas	Búsqueda de aliados, Registro de oportunidades	Suite de Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint, Teams, OneDrive, SharePoint, Forms, Power BI	16 h	8 h	24 h
Talento Humano	Todos	Suite de Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint, Teams, OneDrive,	2 h	1 h	3 h

PROCESO	ACTIVIDAD CRÍTICA	ACTIVO ASOCIADO	DESCRIPCIÓN DEL ACTIVO ASOCIADO	RTO ^[4]	RPO ^[5]	MTD ^[6]
			SharePoint, Forms, Power BI, Power Apps			
Talento Humano	Gestión de nómina de empleados	Helisa	Software de nómina	2 h	8 h	4 h
Sistema Integrado de Gestión	Gestión documental, indicadores y riesgos	Kawak	Gestión de los sistemas de gestión y seguridad información	24 h	8 h	28 h
Sistema Integrado de Gestión	Gestión de incidentes	Aranda	Herramienta de gestión de servicios	4 h	8 h	6 h
Sistema Integrado de Gestión	Comunicación, Inspecciones de SI	Suite de Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint, Teams, OneDrive, SharePoint, Forms, Power BI	4 h	8 h	6 h
Comercial	Gestión de iniciativas y oportunidades	CRM Odoo	Base de datos de iniciativas y oportunidades	5 h	40 h	8 h
Comercial	Desarrollo de propuestas, Entrega de oportunidades ganadas	Suite de Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint, Teams, OneDrive, SharePoint, Forms, Power BI	5 h	16 h	8 h
Comercial	Gestión de entrega de ofertas, Formalización de contratos	Plataformas de los clientes	Cliente (cargue de ofertas y gestión contrato)	1 h	5 h	2 h
Comercial	Gestión de cotizaciones y descuentos	Plataformas de los aliados	Fabricantes y mayoristas	5 h	40 h	8 h
Implementación	Planeación, control del cronograma y seguimiento	Suite de Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint, Teams, OneDrive, SharePoint, Forms, Power BI	16 h	24 h	40 h
Gestión Operación Cliente	Consultas, Comunicación, Gestión de capacidad, Pruebas a servicios	Suite de Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint, Teams, OneDrive, SharePoint, Forms, Power BI	4 h	8 h	5 h
Gestión Operación Cliente	Gestión de eventos, incidentes y solicitudes	Aranda	Herramienta de gestión de servicios	4 h	8 h	5 h

PROCESO	ACTIVIDAD CRÍTICA	ACTIVO ASOCIADO	DESCRIPCIÓN DEL ACTIVO ASOCIADO	RTO ^[4]	RPO ^[5]	MTD ^[6]
Gestión Operación Cliente	Gestión de incidentes	Wolkvox	Solución de Contact center en la nube	2 h	4 h	3 h
SOC	Monitoreo, Parametrización herramientas SOC, Gestión de eventos e incidentes, Ident. Posibles amenazas	Kaspersky	EDR - EPP	1 h	2 h	2 h
SOC	Monitoreo, Parametrización herramientas SOC, Gestión de eventos e incidentes, Ident. Posibles amenazas	CrowdStrike - SIEM	SIEM	1 h	2 h	1.5 h
SOC	Monitoreo, Parametrización herramientas SOC, Gestión de eventos e incidentes, Ident. Posibles amenazas	Lumify Technologies	NDR	1 h	2 h	1.5 h
SOC	Parametrización herramientas SOC, Ident. Posibles amenazas, Gestión de vulnerabilidades	OpenVas	Open Vulnerability Assessment Scanner	2 h	4 h	4 h
SOC	Gestión de eventos e incidentes, Comunicación	Suite de Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint, Teams, OneDrive, SharePoint, Forms, Power BI	1 h	1 h	3 h
SOC	Gestión de eventos e incidentes	Aranda	Herramienta de gestión de servicios	1 h	2 h	1 h
Procurement	Gestionar pedidos de compra y recepción de equipos	Odoo	ERP - Inventario	8 h	8 h	16 h
Procurement	Gestionar pedidos de compra, recepción de equipos y Atención de clientes internos y externos	Suite de Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint, Teams, OneDrive, SharePoint, Forms, Power BI	4 h	8 h	5 h
Gestión Administrativa y Financiera	Consulta y Comunicación	Suite de Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint,	3 h	8 h	8 h

PROCESO	ACTIVIDAD CRÍTICA	ACTIVO ASOCIADO	DESCRIPCIÓN DEL ACTIVO ASOCIADO	RTO ^[4]	RPO ^[5]	MTD ^[6]
			Teams, OneDrive, SharePoint, Forms, Power BI			
Gestión Administrativa y Financiera	Pagos	Plataformas bancarias	BBVA, Occidente, Banco de Bogotá, Davivienda, Bancolombia, Pichincha, HelmBank	2 h	0 h	2 h
Gestión Administrativa y Financiera	Consultas	Helisa	Software contable	5 h	24 h	8 h
Gestión Administrativa y Financiera	Facturación y Confirmación	Odoo	ERP	2 h	4 h	5 h
Gestión Administrativa y Financiera	Pagos	Tokens digitales y físicos	Método de autenticación	2 h	0 h	2 h
Tecnologías de la información	Gestión Seguridad perimetral	Fortinet	Equipo de seguridad perimetral	1 h	0 h	1 h
Tecnologías de la información	Gestión de solicitudes, eventos e incidentes y Gestión de accesos	Aranda	Herramienta de gestión de requerimientos e incidentes	4 h	2 h	8 h
Tecnologías de la información	Monitoreo de la infraestructura, Gestión de capacidad	Zabbix	Herramienta de monitoreo de infraestructura	4 h	2 h	8 h
Tecnologías de la información	Gestión de solicitudes de cambio, Gestión de accesos	Microsoft 365	Aplicaciones y servicios incluidos: Word, Excel, Outlook, PowerPoint, Teams, OneDrive, SharePoint, Forms, Power BI	2 h	4 h	4 h
Tecnologías de la información	Copias de seguridad	Veeam Backup, NAS	Herramienta que presta el servicio de ejecución de copias de respaldo de servidores.	4 h	4 h	8 h

Tabla 35. RTO-RPO-MTD Activos de información

^[4] H: horas, M: mes, S: semanas, D: días

^[5] H: horas, M: mes, S: semanas, D: días

^[6] H: horas, M: mes, S: semanas, D: días

11.4 AFECTACIÓN DE LA INTERRUPCIÓN A SUS PARTES INTERESADAS

A continuación, se presenta por proceso el grado de afectación a las partes interesadas de Yeapdata, a causa de una interrupción en la operación del proceso.

La criticidad fue evaluada de acuerdo con los siguientes criterios:

DESCRIPCIÓN	CRITICIDAD
Afectación de la operación de la parte interesada mayor al 60%	Alta
Afectación de la operación de la parte interesada entre el 31% y 60%	Media
Afectación de la operación de la parte interesada menor al 31%	Baja

Tabla 36. Criterios para evaluar las partes interesadas

11.4.1 Impacto a las partes interesadas internas

PROCESO ANALIZADO	Accionistas	Colaboradores	Gestión Estratégica	Alianzas	Talento Humano	Sistema Integrado de Gestión	Comercial	Implementación	Gestión Operación Cliente	SOC	Procurement	Gestión Admin. y Financiera	Tecnologías de la información
Gestión Estratégica	Alta	Baja	Alta	Baja	Baja	Baja	Media	Baja	Media	Baja	Media	Baja	Baja
Alianzas	Baja	Baja	Baja	Alta	Baja	Baja	Media	Baja	Baja	Baja	Media	Baja	Baja
Talento Humano	Baja	Alta	Baja	Baja	Alta	Baja	Baja	Alta	Alta	Media	Baja	Media	Baja
Sistema Integrado de Gestión	Baja	Media	Baja	Baja	Baja	Alta	Baja	Media	Media	Media	Baja	Baja	Alta
Comercial	Baja	Baja	Baja	Media	Baja	Baja	Alta	Alta	Media	Media	Baja	Media	Baja
Implementación	Baja	Baja	Baja	Baja	Baja	Baja	Media	Alta	Alta	Alta	Media	Alta	Baja
Gestión Operación Cliente	Baja	Media	Baja	Baja	Media	Baja	Media	Media	Alta	Media	Baja	Media	Media
SOC	Baja	Media	Media	Baja	Media	Alta	Media	Media	Alta	Alta	Media	Media	Alta
Procurement	Baja	Media	Baja	Media	Media	Baja	Alta	Alta	Media	Media	Alta	Alta	Media
Gestión Administrativa y Financiera	Media	Media	Baja	Baja	Baja	Baja	Media	Media	Media	Baja	Alta	Alta	Baja
Tecnologías de la información	Baja	Media	Baja	Baja	Alta	Media	Baja	Baja	Alta	Media	Media	Media	Alta

Tabla 37. Resultados evaluación partes interesadas internas

11.4.2 Impacto a las partes interesadas externas

PROCESO ANALIZADO	Clientes	Aliados	Proveedores	Estado	Ambiente
Gestión Estratégica	Baja	Baja	Baja	Baja	Baja
Alianzas	Baja	Media	Media	Baja	Baja
Talento Humano	Baja	Alta	Baja	Media	Baja

PROCESO ANALIZADO	Cientes	Aliados	Proveedores	Estado	Ambiente
Sistema Integrado de Gestión	Baja	Baja	Baja	Baja	Baja
Comercial	Media	Baja	Baja	Baja	Baja
Implementación	Media	Baja	Baja	Baja	Baja
Gestión Operación Cliente	Alta	Baja	Baja	Baja	Baja
SOC	Media	Baja	Baja	Baja	Baja
Procurement	Media	Alta	Alta	Baja	Baja
Gestión Administrativa y Financiera	Media	Media	Media	Baja	Baja
Tecnologías de la información	Media	Baja	Baja	Baja	Baja

Tabla 38. Resultados evaluación partes interesadas externas

12 REFERENCIAS

International Organization For Standardization. ISO/IEC 22301:2019 Security and resilience — Business continuity management systems — Requirements

Información documentada del SGC y SGSI

13 ANEXOS

Anexo No. 1 - Yeapdata - Lista de contactos del árbol de llamadas PCN.

Anexo No. 2 - Yeapdata - Evaluación de criticidad de proveedores

Anexo No. 3 – Yeapdata - Formato de evaluación de daños.

Anexo No. 4 - Yeapdata - Guiones de comunicación sugeridos.

Anexo No. 5 - Yeapdata - Gestión de Riesgos Continuidad

14 APROBACIÓN

	NOMBRE	CARGO	FECHA
ELABORÓ	PBT Consulting SAS	Consultor	19/06/2025
REVISÓ	Camilo Palacio	Especialista de implementación y soporte, y seguridad de la información	19/06/2025
	Daniela Artunduaga	Líder SIG	
APROBÓ	Jennifer Caicedo	COO	19/06/2025

15 CONTROL DE CAMBIOS

REVISIÓN	DETALLES DE CAMBIOS	FECHA DE ACTUALIZACIÓN
1	Se crea versión 1 del documento con Código PLN-D-03, sin embargo, el documento trae la traza del EST-D7-23 y se realizaron los siguientes cambios: 2. ALCANCE: Se actualizó el Mapa de procesos y se incluyeron las 2 sedes faltantes 3. TÉRMINOS Y DEFINICIONES: se incluyó la definición de MTD (Maximum Tolerable Downtime) 5.3 ROLES Y RESPONSABILIDADES: Se actualizaron las estructuras del Nivel Estratégico PCN y del Nivel Táctico PCN 6. CONTEXTO ORGANIZACIONAL DE YEAPDATA: Se actualizó la Tabla 4. RTO-MTD y prioridad de recuperación de los servicios 6.1 ESCENARIOS DE DESASTRE ASOCIADOS AL PLAN DE CONTINUIDAD: Se actualizó la Tabla 5. Escenarios de riesgos asociados a la continuidad de Yeapdata, alineando los escenarios con los riesgos identificados 6.2 PERSONAL CRÍTICO: Se actualizó la Tabla 6. Listado de personal crítico, de acuerdo con las modificaciones que ha habido en la organización 6.3 PROVEEDORES CRÍTICOS: Se actualizó la Tabla 7. Listado de proveedores críticos, de acuerdo con las modificaciones que ha habido en cada área. 7.2 FASE 2 – ACTIVACIÓN Y RECUPERACIÓN: Se actualizó la Tabla 9. Estrategias de continuidad según escenario de desastre, alineando los escenarios con la Tabla 5. Escenarios de riesgos asociados a la continuidad de Yeapdata	19/06/2025

	7.2.1 Prioridad de recuperación según criticidad del proceso: Se actualizó la Tabla 10. Prioridad y orden de recuperación de los procesos. 7.2.2 Recursos mínimos en la recuperación: Se actualizó la Tabla 11. Listado de recursos de contingencia para los procesos, de acuerdo con la eliminación y adquisición de nuevos recursos para la organización. 7.5 FLUJO Y ACTIVIDADES DE LA GESTIÓN DE INCIDENTES DE INTERRUPCIÓN: Se actualizó la Ilustración 5. Flujo general de la gestión de incidentes de interrupción y la Tabla 12. Detalle de las actividades gestión de incidentes de interrupción, para tener en cuenta en mantener informado al Cliente, en la evolución de la gestión del incidente. 11.2 RESULTADOS BIA POR PROCESO: Se actualizaron cada una de las tablas de los 11 procesos con el líder correspondiente. 11.3 INFORMACIÓN Y ACTIVOS ASOCIADOS CRÍTICOS: Se actualizó la Tabla 35. RTO-RPO-MTD Activos de información, con cada uno de los líderes de los 11 procesos 11.4 AFECTACIÓN DE LA INTERRUPCIÓN A SUS PARTES INTERESADAS: Se actualizaron la Tabla 37. Resultados evaluación partes interesadas internas y la Tabla 38. Resultados evaluación partes interesadas externas, con cada uno de los líderes de los 11 procesos. 13 ANEXOS: Se actualizó EL Anexo No. 1 - Yeapdata - Lista de contactos del árbol de llamadas PCN y el Anexo No. 2 - Yeapdata - Evaluación de criticidad de proveedores, de acuerdo con los cambios en la organización.	
--	--	--