FCEJ | *Tesis*

Diagnóstico de continuidad del negocio en la Agencia para la Reincorporación y Normalización (ARN), sede central, Bogotá

Claudia Patricia Vergara Ruiz

UNIVERSIDAD CENTRAL

Diagnóstico de continuidad del negocio en la Agencia para la Reincorporación y la Normalización (ARN), sede central, Bogotá

Claudia Patricia Vergara Ruiz

UNIVERSIDAD CENTRAL
FACULTAD DE CIENCIAS ADMINISTRATIVAS, ECONÓMICAS Y CONTABLES

Esta es una publicación del Programa de Economía
de la Facultad de Ciencias Empresariales y Jurídicas

Fabio Raúl Trompa
Decano

ISBN (impreso): 978-958-26-0470-7
Primera edición: 2021

Calle 21 n.º 5-84 (4.º piso). Bogotá, D. C., Colombia
PBX: 323 98 68, ext. 1556
editorial@ucentral.edu.co

Catalogación en la Publicación Universidad Central

Vergara Ruiz, Claudia Patricia, autora.
Diagnóstico de continuidad del negocio en la Agencia para la Reincorporación y la Normalización (ARN), sede central, Bogotá / autora Claudia Patricia Vergara Ruiz -- Primera edición -- Bogotá : Universidad Central, 2021.
1 recurso en línea (143 páginas) : ilustraciones.
Incluye referencias bibliográficas.

ISBN: 978-958-26-0470-7 (PDF)

1. Planificación empresarial - Consultores - Normas técnicas 2. Comportamiento organizacional - Consultores - Normas técnicas - Aspectos económicos 3. Administración de riesgos - Consultores - Normas técnicas 4. Planificación estratégica I. Universidad Central (Bogotá, Colombia). Facultad de Ciencias Empresariales y Jurídicas. Programa de Economía.

658.15 – dc23 PTBUC/09-09-2021

Preparación editorial
Coordinación Editorial

Editor:	Héctor Sanabria Rivera
Asistente editorial:	Nicolás Rojas Sierra
Diagramación:	Patricia Salinas Garzón
Corrección de textos:	Pablo Clavijo

Publicado en Colombia • *Published in Colombia*

Contenido

Índice de figuras

Índice de tablas

Lista de abreviaturas

ACR	Agencia Colombiana para la Reintegración
ARN	Agencia para la Reincorporación y la Normalización
BCI	Business Continuity Institute
BCM	*Business continuity methodology*
BCP	*Business continuity plan*
BSC	*Balance score card*
Cobit	*Control objectives for information and related technology*
Conpes	Consejo Nacional de Política Económica y Social
DAFP	Departamento Administrativo de la Función Pública
Dapre	Departamento Administrativo de Presidencia
DDR	Desarme, desmovilización y reintegración
DRII	Disaster Recovery Institute International
DRP	*Disaster recovery plan*
ESAP	Escuela Superior de Administración Pública
GT/PA	Grupo(s) Territorial(es) / Punto(s) de Atención
Icontec	Instituto Colombiano de Normas Técnicas y Certificación
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
MECI	Modelo estándar de control interno
MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones
NFPA	National Fire Protection Association

NTC-GP	Norma Técnica de Calidad para la Gestión Pública
OAP	Oficina Asesora de Planeación
OTI	Oficina de Tecnologías de la Información
PAC	Programa Anual Mensualizado de Caja
PCD	Plan de Conservación Documental
PHVA	Planear-hacer-verificar-actuar
PIC	Plan Institucional de Capacitación
PNRSE	Política Nacional de Reintegración Social y Económica
PPR	Persona(s) en proceso de reintegración
PQR	Preguntas, quejas y reclamos
SGCN	Sistema de gestión de continuidad del negocio
SGSSS	Sistema General de Seguridad Social en Salud
SGSST	Sistema de Gestión de Seguridad y Salud en el Trabajo
Siger	Sistema Integrado de Gestión para la Reintegración
SIIF	Sistema Integrado de Información Financiera
SIR	Sistema de Información para la Reintegración

Resumen

La presente consultoría tuvo como propósito realizar un diagnóstico de continuidad del negocio en la sede central de la Agencia para la Reincorporación y la Normalización (ARN, antes ACR), con tres objetivos en mente: entender la organización a partir de la ISO 22301:2012; identificar y valorar los escenarios de falla y los riesgos de continuidad, y formular recomendaciones. Se definió un diseño cualitativo que implicó la revisión de un gran volumen de documentos institucionales y la aplicación de entrevistas a colaboradores de la entidad. Los resultados evidencian que la Agencia ha avanzado principalmente en establecer acciones de continuidad en materia de sus activos de información; en menor medida lo ha hecho hacia la seguridad de sus colaboradores e instalaciones; y tiene significativas brechas por cerrar en su estrategia global de riesgos cuando se analiza a partir de la continuidad del negocio.

Palabras clave

Continuidad de negocio, escenario de falla, norma ISO 22301:2012, organizaciones, reintegración, riesgo de continuidad, sistema de gestión.

Cómo citar este libro

APA: Vergara, C. P. (2021). *Diagnóstico de continuidad del negocio en la Agencia para la Reincorporación y la Normalización (ARN), sede central, Bogotá.* Ediciones Universidad Central.

MLA: Vergara Ruiz, Claudia Patricia. *Diagnóstico de continuidad del negocio en la Agencia para la Reincorporación y la Normalización (ARN), sede central, Bogotá*. Bogotá: Ediciones Universidad Central, 2021. Impreso.

CHICAGO PARENTÉTICO: Vergara Ruiz, Claudia Patricia. 2021. *Diagnóstico de continuidad del negocio en la Agencia para la Reincorporación y la Normalización (ARN), sede central, Bogotá*. Bogotá: Ediciones Universidad Central.

Introducción

Las organizaciones están constantemente sometidas a variaciones del entorno que pueden poner en riesgo de continuidad —parcial o total— sus operaciones, y de ahí la importancia de gestionar de manera adecuada tales eventualidades. La Agencia para la Reincorporación y la Normalización (ARN, antes ACR) no es ajena a estas variaciones, más cuando pretende garantizar la continuidad en la entrega de servicios y beneficios a los desmovilizados.

La presente consultoría tuvo como fin realizar un diagnóstico de continuidad del negocio en la sede central de la ARN, como insumo para que esta entidad avance y aborde de manera sistemática el tema. Se realizó un diseño cualitativo, en el que el análisis documental y la indagación directa a los colaboradores fueron las herramientas fundamentales para su elaboración.

El informe de consultoría se estructura en cinco capítulos: en el primero se presentan los antecedentes, la problemática, los objetivos, la metodología, la justificación y el marco referencial de la consultoría; en este último se destacan aspectos como la evolución de la continuidad, los referentes conceptuales y los requerimientos de la norma de continuidad. En el segundo capítulo se expone cómo entiende la Agencia la norma ISO 22301:2012 y se destacan las prácticas de *continuidad del negocio* que pudieron identificarse a partir de la estructura y gestión de la entidad.

En el tercer capítulo se abordan los escenarios y riesgos de continuidad identificados y valorados por los colaboradores entrevistados en la sede central, y se ponderan los que adquieren mayor

relevancia para la organización. En el cuarto capítulo se presentan las recomendaciones que surgen del análisis de los temas anteriores, pero también de las propuestas realizadas por los colaboradores. Finalmente, se exponen las conclusiones, donde se destaca que si la Agencia avanza en la implementación de los aspectos de la presente consultoría, comenzaría a recorrer el camino hacia un manejo sistemático e integral en lo que respecta a continuidad del negocio y, a futuro, hacia un sistema de gestión de la continuidad del negocio (SGCN).

Capítulo 1

Sobre la consultoría

1.1 Antecedentes y justificación

La preocupación por la *continuidad del negocio* en la ARN tiene su expresión más visible desde finales de 2015, cuando la entidad proyectó para 2016 la contratación de un experto en la materia, con el fin de avanzar de manera más decidida y sistemática en el asunto. Esta contratación tenía como antecedente la gestión interna que emprende la entidad para el cumplimiento de los requerimientos en relación con la protección y seguridad de la información de la organización. Sin embargo, la contratación no se realizó a pesar de estar proyectada. En ese momento, la Oficina Asesora de Planeación (OAP) y la Oficina de Tecnologías de la Información (OTI) eran las que más impulsaban este tema al interior de la organización.

Para 2017, el tema pasó a estar a cargo de la Secretaría General de la Agencia, que proyectó en ese año la contratación del experto, pero debido a recortes presupuestales tampoco fue posible. En este escenario —en el que la entidad tiene una necesidad identificada, pero no cuenta con los recursos suficientes para contratar un experto— surge la presente consultoría, que se concibe como una oportunidad y una fase preliminar para abordar la continuidad del negocio de una manera más integral.

La realización de la presente consultoría se justificó por varias razones. En primer lugar, era una necesidad identificada por la Agencia; en segundo lugar, permite la entrada de nuevo conocimiento en dos aspectos: por un lado, la entidad no tenía un diag-

nóstico de continuidad, y por el otro, en la literatura es difícil de encontrar este tipo de ejercicios para las entidades públicas, tal como lo afirma Sanguinetti (comunicación personal, marzo de 2016), por lo que, se cree, el presente documento puede servir de insumo para futuros investigadores.

La consultoría tiene relevancia social en caso de que se establezcan prácticas de continuidad en la Agencia a partir del diagnóstico, lo que minimizaría interrupciones en su operación para mantener la oferta de servicios y beneficios, y tendría dos impactos positivos: menores costos administrativos, económicos y políticos para la entidad, y menores costos sociales para los desmovilizados en términos de calidad de vida.

1.2 Planteamiento del problema

Si bien de manera permanente la Agencia implementa acciones para la gestión del proceso de reintegración y estas quizá estén establecidas en los diversos planes de la ARN o en los procesos de su sistema de gestión —en coherencia con las funciones de los grupos que forman la entidad—, la Agencia reconoce que no tiene un conocimiento sistemático e integral de cuáles son las actividades y de qué manera se relacionan con la continuidad del negocio, y, menos aún, cuáles son las brechas que en esta materia tiene para lograr sortear de manera efectiva situaciones de incidentes o accidentes perturbadores que pongan en riesgo la continuidad de sus operaciones.

Esta situación en se relaciona con causas que pueden evidenciarse en afirmaciones de colaboradores:

> Si bien se comienza a observar en algunos de los directivos la importancia de avanzar en este tema, se destaca el desconocimiento técnico y conceptual respecto a continuidad del negocio y de cómo abordarlo de manera sistemática [...] a tal punto que en la entidad no se tiene personal preparado o profesionalizado en la materia. (N. Sarria, comunicación personal, julio de 2016)

Por supuesto, esta afirmación es coherente con los intentos fallidos —por recorte presupuestal— que ha tenido la entidad para contratar un experto en el tema.

El desconocimiento técnico se pudo evidenciar cuando se realizó una exploración inicial entre los colaboradores de la Agencia en relación con escenarios de falla. En esta exploración se observó que no logran identificarlos plenamente (en general, reconocen los que se relacionan con desastres o pérdida de información) y menos aún las acciones que se deben tomar ante los mismos (P. Olaya y B. Bonilla, comunicación personal, julio de 2016). Sin embargo, estos mismos colaboradores coinciden en la importancia de la continuidad del negocio: "No solo se afecta a los clientes de la entidad, sino también a los colaboradores, quienes, ante un escenario de interrupción definitiva del servicio, serán afectados en su vinculación laboral, con alto riesgo de quedar cesantes" (P. Olaya, comunicación personal, julio de 2016).

Otra causa asociada a la anterior es que las directivas casi no destacan la continuidad del negocio como un asunto estratégico y esto puede evidenciarse tanto en el Plan Estratégico 2015-2018, en el que se invisibiliza el tema, como en el Manual del Sistema de Gestión de la Agencia, que no establece una política de continuidad del negocio.

Lo anterior tiene una serie de consecuencias en la gestión institucional de la entidad. Para el caso de la planeación, esta se realiza sin la identificación desde la perspectiva del plan de continuidad del negocio (BCP, por sus sigla en inglés) de los procesos, actividades y servicios críticos, y se desconocen la identificación y análisis de riesgos de interrupción de operaciones, tal como lo establecen los referentes del BCP. Menos aún se identifican los escenarios de falla a los que se expone la Agencia, con lo cual la entidad resulta más reactiva que proactiva en términos de continuidad, un aspecto nada deseable en la gestión de ninguna organización.

De permanecer la situación —no conocer de manera sistemática el estado actual de las prácticas de continuidad, con el fin de abordarlo de manera integral y con suficiencia—, la entidad se mantendrá en situaciones potencialmente peligrosas, como pérdida de confianza en la gestión de la reintegración por las partes interesadas, pérdida de imagen como institución estatal e incluso "podría enfrentar problemas de tipo legal por no cumplir con la

oferta de servicios y beneficios establecidos en la normatividad vigente" (J. Yances, comunicación personal, febrero de 2016).

Con base en todo lo anterior, esta consultoría se planteó como objetivo principal responder a la siguiente pregunta: ¿cuál es el estado actual de las prácticas de continuidad del negocio en la sede central de la ARN? Para este fin, se requirió resolver aspectos de la estructura y la gestión de la Agencia que favorecen la implementación de los requisitos de la ISO 22301:2012, escenarios de falla y riesgos de continuidad a los que está expuesta la entidad, y las recomendaciones que puedan establecerse sobre la materia a la organización.

1.3 Objetivos de la consultoría

1.3.1 Objetivo general

Determinar el estado actual de las prácticas de continuidad del negocio en la sede central de la ARN a partir del estándar establecido por la ISO 22301:2012, *Seguridad de la sociedad. Sistemas de continuidad de negocio. Requisitos*.

1.3.2 Objetivos específicos

a. Entender la organización a partir de su estructura y gestión en relación con los requisitos de la ISO 22301:2012.

b. Determinar y valorar los escenarios de falla y los riesgos de continuidad del negocio para la entidad.

c. Formular recomendaciones orientadas al mejoramiento de las prácticas de continuidad del negocio a partir de la situación actual o del diagnóstico realizado.

1.4 Metodología de la consultoría

Para dar cuenta de los objetivos de la consultoría, se siguieron los lineamientos de estudio de caso y la investigación se asumió como de tipo descriptivo-cualitativo, con lo que se busca "desarrollar una imagen o fiel representación (descripción) del fenóme-

no [...] a partir de sus características" (Clavijo, 2010, p. 151), Esto se hizo partiendo de las subjetividades de los colaboradores de la Agencia y de la revisión e interpretación de fuentes documentales.

La recolección de la información primaria implicó un ejercicio piloto inicial de entrevista, en el que participaron colaboradores de los procesos Direccionamiento estratégico y Gestión de tecnologías de la información, lo que permitió ajustar contenidos de los instrumentos, así como aclarar ciertas preguntas y administrar adecuadamente el tiempo.

Para las entrevistas se utilizaron los formatos: lista de chequeo ISO 22301:2012, matriz de evaluación de escenarios e identificación de riesgos y matriz de valoración de riesgos. Igualmente, se elaboró un formato de consentimiento informado, que permitió darles contexto a los entrevistados acerca del estudio y obtener de ellos su aceptación de participación voluntaria.

Se realizaron 16 entrevistas grupales con un total de 44 colaboradores entrevistados, todos los cuales cumplieron los requisitos de laborar en la sede central y tener como mínimo tres años de vinculación laboral, para asegurar que, en el mayor grado posible, contaran con amplio conocimiento sobre la entidad y que hubiesen pasado por la evolución que ha sufrido la organización en su modelo de gestión y planeación. Se realizó un muestreo por juicio o discrecional; este es un método no probabilístico en el que los sujetos se seleccionan con base en el conocimiento y juicio del investigador (Universo Fórmulas, 2015) y que es coherente con este tipo de estudios. Por tanto, los resultados obtenidos se limitan a este tamaño y tipo de muestreo, reconociendo, en todo caso, que por el tipo de estudio asumido se brinda una comprensión del estado de las prácticas de continuidad del negocio en la entidad.

El tratamiento y análisis de la información primaria implicó el registro de esta en los instrumentos previamente definidos. Seguidamente, se realizó una depuración de esta información cualitativa y se estableció la idea fuerza, o idea central, de las opiniones emitidas respecto a los escenarios de falla y riesgos.

En cuanto a los riesgos, a partir de la información recolectada se construyeron seis categorías: personas, procesos, tecnología, infraestructura física, gerenciales y financieros. En estas categorías están contenidos por afinidad los riesgos identificados por los colaboradores; después, cada riesgo se alinea y se inscribe con la

tipología de riesgo establecida por el DAFP, de modo que facilite —en caso de acogerse las recomendaciones— su incorporación en el tratamiento de riesgos, dado que la entidad sigue esta metodología.

En relación con las recomendaciones, se realizó la recolección en el instrumento diseñado durante la entrevista, luego se sistematizó y, finalmente, se realizó un agrupamiento por afinidad, lo que permitió el establecimiento de recomendaciones globales, acordes con las categorías de riesgos establecidas.

Para el caso de la información secundaria, se revisó un gran volumen de documentos sobre temas como normativa sobre las funciones de grupos, estructura de la entidad, beneficios y servicios de la reintegración, documentos que sustentan la operación de los procesos del sistema de gestión (caracterizaciones, normogramas, manuales, guías, instructivos, procedimientos, formatos, documentos complementarios), informes de gestión y de evaluación institucional, y de planeación estratégica, mapas de riesgo de los procesos, y norma internacional ISO 22301:2012, *Seguridad de la sociedad. Sistema de gestión de la continuidad del negocio. Requisitos*.

Esta revisión se realizó en diálogo con los aspectos y requerimientos de la norma ISO 22301:2012, mediante el establecimiento del nivel de cumplimiento de los requisitos de esta norma en relación con las prácticas de continuidad del negocio que pueden evidenciarse en la entidad. Para corroborar los grados de cumplimiento frente a la norma de continuidad, en algunas ocasiones, se realizaron entrevistas adicionales con personas clave de los procesos, lo que permitió tener mayor validez respecto a ciertas prácticas de continuidad del negocio.

1.5 Marco referencial

El marco referencial expone la evolución que ha tenido el concepto de *continuidad del negocio*. Acto seguido, se expone el marco teórico, en el que se establece una reflexión sobre las metodologías y las posiciones de los principales autores acerca del tema de la continuidad del negocio.

1.5.1 Marco histórico: evolución de la continuidad del negocio

Se puede establecer una cronología en la evolución normativa en relación con la continuidad del negocio:

El lineamiento más antiguo sobre continuidad del negocio fue expedido por la National Fire Protection Association (NFPA 1600) y publicado en 1995. En este documento se establecían criterios para la gestión de desastres, emergencias y programas de continuidad para las organizaciones. En 1997, el Disaster Recovery Institute International (DRII) publicó las prácticas profesionales para la gestión de la continuidad del negocio.

En 2002, el Business Continuity Institute (BCI) publicó lineamientos de buenas prácticas para la continuidad del negocio. En 2003 el BCI publica el lineamiento PAS 56, que establece el proceso, principios y terminología de un sistema de gestión de continuidad del negocio. En este documento, el BCI desarrolla una serie de recomendaciones para buenas prácticas de anticipación a incidentes, y respuestas y técnicas para la evaluación (Servat, 2012).

En 2006 y 2007, la British Standards Institution publicó la norma BS 25999, partes 1 y 2, para establecer la gestión de continuidad de negocio en las organizaciones, y en ella introduce el término *resiliencia*, que se entiende como la capacidad de asumir con flexibilidad situaciones límite y sobreponerse a ellas (Servat, 2012).

En la figura 1 se muestra una evolución de las referencias normativas que han abordado el tema de *continuidad del negocio* hasta la publicación del más reciente estándar ISO 22301 (Servat, 2012).

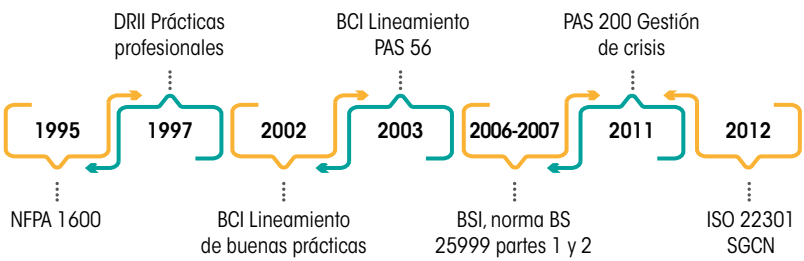

Figura 1. Evolución de los estándares de continuidad del negocio.
Fuente: elaboración propia con base en Servat (2012).

La visión actual acerca de la gestión de continuidad del negocio abarca todas las funciones, recursos y operaciones de la orga-

nización (DiMattia, 2001). El enfoque actual organiza de manera jerárquica, en primer lugar, la continuidad del negocio, seguida del plan de recuperación ante desastres, y considera a la tecnología como elemento de gestión clave para el respaldo y para la recuperación y restauración de datos, aspectos fundamentales para la continuidad del negocio (Barnes, 2001).

1.5.2 Metodologías sobre las prácticas de continuidad del negocio (BCP)

En el mundo, las principales orientaciones metodológicas son establecidas por instituciones y autores en las que no se identifica un único modelo. Entre las más conocidas están:

Disaster Recovery International Institute (DRII)

El DRII es una organización sin ánimo de lucro, líder en la preparación de las organizaciones ante cualquier tipo de desastre, cuya metodología se aborda a partir de la implementación de diez buenas prácticas en continuidad del negocio, que se evalúan a través de una serie de criterios que permiten definir el nivel de implementación y madurez de la organización en la materia: 1) inicio y gestión del programa, 2) evaluación y control de riesgos, 3) análisis de impacto del negocio, 4) estrategias de continuidad del negocio, 5) operaciones y respuesta a la emergencia, 6) planes de continuidad del negocio, 7) programas de entrenamiento y concientización, 8) planes de ejercicios, auditorías y mantenimiento; 9) comunicación en crisis, y 10) coordinación con agencias externas.

Organización Internacional para la Estandarización (ISO)

La ISO es un organismo no gubernamental de alcance mundial, integrado por cuerpos de estandarización de 162 países. Fue el encargado de establecer la ISO 22301:2012, primer estándar internacional para la gestión de la continuidad del negocio, en reemplazo de la norma británica BS 25999 (Organización Internacional de Estandarización, 2012).

La metodología que propone la ISO se desarrolla en cuatro fases: 1) análisis de impacto en el negocio; 2) evaluación de riesgos; 3) estrategia de continuidad de negocio y 4) procedimientos de continuidad de negocio.

Business Continuity Institute (BCI)

Respecto a continuidad del negocio, este instituto es reconocido como la más prestigiosa asociación de profesionales en el mundo y está presente en 89 países. El BCI propone la metodología BCM para la implementación de los planes de continuidad del negocio; esta metodología tiene seis etapas: 1) gerencia del programa BCP; 2) comprensión de la organización; 3) determinación de estrategias; 3) elaboración del plan; 4) pruebas, mantenimiento y actualización del plan, e 5) implementación del plan en la organización (BCI, 2008).

Gaspar (2006), en su *Guía práctica para la elaboración del plan de continuidad del negocio*, recomienda para la implementación del BCP los siguientes pasos: 1) análisis de impacto, 2) determinación de elementos críticos (funciones, aplicaciones y recursos), 3) estrategia de continuidad, 4) equipos de recuperación, 5) plan de acción (puesta en marcha), 6) plan de vuelta a la normalidad, y 7) pruebas y actualización.

Si bien existen diversas metodologías, la presente consultoría acogió como referencia la norma ISO 22301:2012, *Seguridad de la sociedad. Sistemas de continuidad del negocio. Requisitos*, debido a tres razones. En primer lugar, la norma recoge las distintas metodologías y buenas prácticas en continuidad del negocio generadas en los últimos 20 años (ISO, 2012), y propone un sistema de gestión de la continuidad del negocio (SGCN), con un alcance mayor que el de un plan de continuidad. En segundo lugar, tiene reconocimiento internacional y es certificable, situación preferente para la entidad, dado que a futuro podría adquirir esta certificación. Tercero, la entidad tiene un sistema de gestión de la calidad certificado con la norma internacional ISO 9001, lo cual puede facilitar la incorporación de las prácticas de continuidad del negocio establecidas en la ISO 22301.

A continuación se presentan los principales elementos de la norma ISO 22301:2012, *Seguridad de la sociedad. Sistemas de continuidad del negocio. Requisitos*.

La norma se estructura en una introducción y diez cláusulas. La introducción recoge las generalidades, en las que se destaca la importancia de establecer y gestionar un sistema de gestión de continuidad del negocio (SGCN), relacionando la necesidad de establecer una política, gestionar los riesgos de continuidad, monito-

rear y evaluar el desempeño del SGCN y su mejora continua (ISO, 2012). La ISO 22301:2012 menciona las bondades de estructurar el SGCN con este esquema, por la consistencia que puede tener con otras normas ISO, y destaca la importancia de establecer las expectativas y necesidades de las partes interesadas de la organización como entrada para la preparación del SGCN. Finalmente, la Introducción habla de la relación de cada aspecto del PHVA (planear-hacer-verificar-actuar) con el resto de contenidos de la norma, en un esfuerzo por aclarar la relación del ciclo, en coherencia con los requerimientos de la continuidad del negocio (ISO, 2012).

El primer capítulo de la norma trata sobre su *alcance*, en el que fundamentalmente establece que existen requerimientos genéricos para que las organizaciones —de acuerdo con sus características y complejidades— establezcan e implementen un SGCN: "Este estándar internacional especifica requerimientos [...] un sistema de gestión de continuidad documentado [...] Los requerimientos [...] son genéricos [...] la aplicación de estos [...] depende de la complejidad [...] de la organización" (ISO, 2012, p. 7).

En el capítulo dos, la ISO 22301:2012 establece las *referencias normativas* para la aplicación de la norma.

En el capítulo tres se presentan *los términos y definiciones* (55 en total) de los diferentes aspectos tratados, y que dan sustento a esta norma sobre continuidad del negocio. Un gran número de las definiciones son comunes con otras normas ISO, lo cual permite ver la consistencia y articulación que trata de mantener la organización ISO en sus estándares internacionales (ISO, 2012).

El capítulo cuatro establece *la forma de comprender la organización*. En este capítulo, el análisis de los contextos interno y externo de la organización se vuelve condición necesaria para la gestión efectiva del SGCN: "Estos factores deben considerarse, al establecerse, implementarse y mantener el SGCN" (ISO, 2012, p. 16).

Las partes interesadas relevantes para la organización asumen un papel fundamental para el SGCN; de ahí la importancia de comprender sus necesidades y expectativas, incluyendo los aspectos regulatorios y normativos, ya que desempeñan un papel vital en términos de la continuidad, por lo cual la organización debe monitorearlas permanentemente. En este capítulo cuatro se describe también en mayor detalle la operacionalización, para lograr determinar el alcance del SGCN en la organización (ISO, 2012). En este

capítulo, la norma requiere también que todos los aspectos sean documentados permanentemente y de manera sistemática, y también que se establezcan y expliquen las exclusiones del SGCN. "Al definir el alcance, la organización debe documentar y explicar las exclusiones" (ISO, 2012, p. 17).

El capítulo cinco presenta el *liderazgo* que debe existir en la organización, proveniente de diferentes actores y según nivel jerárquico, para lograr la gestión efectiva del SGCN. Las altas directivas y la gerencia de la organización asumen un papel protagónico en este sentido, pues están llamadas a lograr que se implemente la continuidad del negocio y que de ella se apropie el resto de colaboradores de la empresa; además, "personas en la alta gerencia [...] deben demostrar liderazgo respecto al SGCN" (ISO, 2012, p. 18).

Es importante mencionar que la alta gerencia está llamada a definir los roles y responsabilidades que los demás colaboradores deben asumir respecto al SGCN; debe definir la política y velar por que el sistema sea compatible con el direccionamiento estratégico de la organización y con la norma de continuidad (ISO, 2012).

El capítulo seis establece la planeación del SGCN, al evidenciar lo importante que es tener en cuenta los aspectos establecidos al comprender la organización —por ejemplo, el análisis de contexto interno y externo, las partes interesadas, los aspectos regulatorios, pero también los riesgos y oportunidades—, para establecer gestiones eficaces frente a los mismos y determinar objetivos de continuidad consistentes con la política de continuidad (ISO, 2012). Los anteriores objetivos deben cumplir criterios de claridad, ser medibles, demostrar el avance en materia de continuidad y estar documentados, pero también debe disponerse de los recursos y definir los responsables para su logro (ISO, 2012).

El capítulo siete establece el *apoyo* al interior de la organización en relación con el SGCN. Específicamente, se desarrollan aspectos tales como los recursos, la competencia, la toma de conciencia, la comunicación y la documentación del sistema de continuidad.

En relación con los *recursos*, se requiere que la organización establezca y provea los que sean necesarios para la gestión del sistema de continuidad (ISO, 2012).

Igualmente, cuando en el capítulo siete se habla de competencia, se refiere a las acciones que debe emprender la organización para que el personal logre realizar sus funciones adecuadamente

y que no se impacte la gestión de la organización; es decir, que no se generen interrupciones o incidentes en materia de continuidad. La toma de conciencia se centra en la necesidad de que los colaboradores de la organización entiendan la importancia y actúen en coherencia con el SGCN (ISO, 2012).

En el capítulo siete se destaca en seguida la importancia de la *comunicación interna y externa* que debe gestionar la empresa en relación con la continuidad, y se establece la necesidad de que se definan procedimientos de comunicación con las partes interesadas de la organización, ante eventos de interrupción de la prestación de servicios; es decir, "qué se comunicará, cuándo se comunicará, con quién se comunicará" (ISO, 2012, p. 22).

Finalmente, en el mismo capítulo siete, se desarrolla el aspecto de la documentación del SGCN y se establecen requerimientos centrados principalmente en tres aspectos: documentar lo relacionado con el sistema, crear y mantener actualizada esta documentación, y desplegar un procedimiento de control frente a la misma (ISO, 2012).

En el capítulo ocho se establece la *operación*, estructurada en cuatro ejes: el primero, el *planeamiento operacional y el control*, en el que se establecen —a partir del PHVA— los procesos para la continuidad: "La organización debe planificar, implementar y controlar los procesos necesarios" (ISO, 2012, p. 24). Un aspecto importante tiene que ver con la necesidad de gestionar de manera adecuada el cambio: "La organización debe controlar el cambio planeado y revisar las consecuencias de los cambios no intencionados, tomando acciones para mitigar cualquier efecto adverso" (ISO, 2012, p. 24).

El segundo eje, *análisis de impacto del negocio y evaluación del riesgo*, se centra en el establecimiento de los requerimientos para una gestión sistemática de estos dos aspectos. En *la medición de impacto* se destaca la necesidad de evaluar impactos de actividades de interrupción y tiempos de reanudación de las mismas en el negocio (ISO, 2012). Respecto a estos riesgos de interrupción, el segundo eje habla de la necesidad de una evaluación y administración eficiente de los mismos, recomienda aplicar la ISO 31000:2009, que define principios y directrices genéricos sobre la gestión del riesgo (ISO, 2012).

El tercer eje, *estrategia de continuidad del negocio*, debe establecerse a partir del análisis de impacto y riesgo, pero con una mirada estratégica que permita distinguir las actividades críticas, estable-

cerlas como prioridad y blindarlas con mecanismos que eviten o mitiguen adecuadamente eventos de interrupción, lo que implica disponer de los recursos necesarios (ISO, 2012).

El cuarto eje, *establecer e implementar procedimientos para la continuidad del negocio*, aborda fundamentalmente la respuesta organizacional ante la ocurrencia de interrupciones en la organización, cómo se comunicarán estas interrupciones a las partes interesadas, la activación de los planes específicos de continuidad y los procedimientos de recuperación por las interrupciones ya generadas. Un aspecto importante de este eje tiene que ver con el requerimiento que se hace a las organizaciones de realizar ejercicios y ensayos de los procedimientos de continuidad que han establecido, así como mecanismos de ajuste y su mejora (ISO, 2012).

El capítulo nueve, "Evaluación del desempeño", se refiere a los aspectos de monitoreo, medición, análisis y evaluación de la continuidad del negocio en la organización. En este sentido, deben establecerse mecanismos sistemáticos que permitan su gestión adecuada. Entre estos mecanismos sobresale la auditoría, por lo cual el programa anual de auditorías de la organización debe contemplarlas, pero también la revisión del SGCN por la alta dirección de la empresa. Todos estos aspectos deben estar documentados y son condición necesaria para conocer situaciones, como el cumplimiento de los objetivos y la política de continuidad, el desempeño de los procesos en materia de continuidad, la adecuación, conveniencia y efectividad del SGCN (ISO, 2012, p. 33), y en general, tomar decisiones basadas en evidencia en relación con los aspectos de continuidad en la organización.

Finalmente, el capítulo diez, "Mejoramiento", trata dos aspectos: no conformidad y acción correctiva. En el capítulo se exponen los requerimientos para su gestión adecuada, de las que el análisis causal de las no conformidades es el instrumento fundamental para establecer tratamientos, a partir de acciones correctivas pertinentes que eliminen las causas de las no conformidades (ISO, 2012).

El otro aspecto tiene que ver con el mejoramiento continuo e implica un permanente esfuerzo organizacional de mejora frente al SGCN. La norma recomienda que, a partir de elementos como el liderazgo, la planeación y la evaluación del desempeño de la continuidad, se logre este propósito (ISO, 2012).

1.5.3 Marco teórico-conceptual de la continuidad del negocio

El concepto de *continuidad del negocio* aparece en los años 1970 y se liga a los sistemas de información, dado el auge del manejo mediante computadores de los aspectos financieros y contables de las empresas. Se desarrolla entonces un modelo de protección de datos que deriva en el Plan de Recuperación de Desastres (DRP, por su sigla en inglés), el cual se centra exclusivamente en medidas de protección y recuperación frente al riesgo de pérdida de información (Paul, 2009). Esta concepción evoluciona en la década de los 1990, pues se concibe a la organización como un todo que requiere protección similar y de recuperación ante desastres de los centros de cómputo, lo que lleva a la concepción actual de *continuidad del negocio* (Espinosa *et al.*, 2012). Se refuerzan estos aspectos en términos de planes de continuidad del negocio, tras sucesos como el atentado de las Torres Gemelas en Nueva York, que implicó pérdida de vidas, bienes materiales e información (M. H., 2007; Gaspar, 2008; Espinosa *et al.*, 2012; Servat, 2012).

Se comienza de esta manera a tener una mirada más holística del tema y aparecen actores en el tema de la continuidad, como el Business Continuity Institute o el Contingency Planning & Management, con publicaciones especializadas y organizaciones que asesoran en la materia (Espinosa *et al.*, 2012).

Toma importancia, en este sentido, la teoría de la contingencia en relación con las organizaciones. Según Sánchez (1992), si estas no desarrollan capacidad de adaptación de su estructura a las contingencias de su entorno, los resultados no serán satisfactorios, concepción similar a la que plantea Parga (2007), según quien la organización requiere de una preparación para responder de manera apropiada y oportuna a estos riesgos, y en la que el Plan de Continuidad del Negocio (BCP) adquiere gran importancia.

Desde la perspectiva del BCP, una adecuada gestión de la continuidad del negocio implica un buen análisis de riesgos (Parga, 2007), que debe partir de la identificación de los escenarios de falla a los cuales está expuesta la organización. Para el caso de esta consultoría, se acogió la concepción de escenarios de falla que plantea el Business Continuity Institute (2012) y se definieron de la siguiente manera:

- *Escenario de falla tecnológica.* Se incluyen en este escenario eventos como fallas en el fluido eléctrico, sabotaje informático, fallas en el centro de datos, problemas técnicos, fallas en equipos tanto de procesamiento y telecomunicaciones, como eléctricos, servicios de soporte a sistemas de producción y/o servicios, inhabilidad de *software* y *hardware*, afectación de la disponibilidad de los servicios y/o recursos tecnológicos por *hackers*, virus.
- *Escenario de inhabilidad de la sede.* Este escenario recoge eventos como daños en la infraestructura de la sede, artefactos explosivos, marchas, motines, imposibilidad de acceder a la sede.
- *Escenario de inhabilidad de la línea de atención.* En relación con la entidad, se entiende como la inhabilidad de la línea de atención o intervención de las PPR.
- *Escenario de desabastecimiento de bienes y servicios.* Se incluyen acá eventos como problemas de terceros involucrados en la producción o soporte de un servicio, problemas con los proveedores, incumplimiento en los pagos a proveedores, entre otros.
- *Escenario de desastre nacional o regional.* Incluye eventos relacionados con sismos, tormentas eléctricas, incendios, inundaciones.
- *Escenario de inhabilidad legal.* Se consideran en este escenario eventos relacionados con el marco jurídico regulatorio de la función institucional y del proceso de reintegración (servicios y beneficios), que puedan afectar la continuidad en la operación.
- *Escenario de inhabilidad financiera.* Eventos relacionados con la disponibilidad de recursos financieros para el apalancamiento de las metas y funciones de la entidad y de los procesos.
- *Escenario de paro de personal.* En este escenario se incluyen eventos como actos hostiles, problemas organizacionales, huelgas o sabotaje.

- *Escenario de sucesión de poder.* Incluye eventos como cambio de gobierno, cambio de dirección y de la línea de mando, que puedan afectar la continuidad en las operaciones.

Los términos *eventos de continuidad* o *eventos disruptivos* se refieren a la ocurrencia o cambio de un conjunto de circunstancias; de allí que el riesgo se caracterice por referencia a los eventos potenciales o se exprese en términos de la combinación de las consecuencias de un evento. Finalmente, la *identificación de riesgos* implica la identificación de las fuentes de riesgo, los eventos, sus causas y sus posibles consecuencias (ISO, 2012).

La identificación de los eventos de continuidad permite a la entidad generar una lista de las fuentes de riesgos y de los eventos que pueden materializarse e interrumpir el logro de cada uno de los objetivos (Icontec, 2004).

Como se observa, los escenarios definidos relacionan eventos de continuidad o eventos disruptivos (*incidentes* o *accidentes*, para la norma de continuidad) que tratan sobre la ocurrencia o cambio de circunstancias para la entidad, y que tienen la capacidad potencial de interrumpir su normal operación.

Siguiendo a Parga (2007), el análisis de estos escenarios de falla, como parte de la gestión del BCP, permite la identificación de los riesgos y el planteamiento de acciones contingentes que posibiliten continuar la operación y recuperar las condiciones normales de funcionamiento en el menor tiempo posible.

En términos de riesgos y continuidad del negocio, también existen estándares, como los de Cobit (*Control objectives for information and related technology*), ITIL (Information Technology Infrastructure Library) e ISO 27000 (International Organization for Standardization), pero los enfocan desde la gestión de tecnologías de la información y plantean la necesidad de conocer los riesgos que puedan interrumpir las operaciones, con el fin de ejecutar estrategias de continuidad (Machuca y Sasco, 2012).

Existen otros modelos que, aunque no tienen como foco la continuidad del negocio, brindan procedimientos genéricos para que las organizaciones gestionen sus riesgos. Entre estos modelos están el COSO, el estándar australiano AS/NZS 4360:1999, la norma técnica colombiana NTC 5254:2004, *Gestión del riesgo*, y la norma ISO 31000:2009, *Gestión de riesgos - Principios y guías*. Vale destacar

que esta última norma define el riesgo como "el efecto de la incertidumbre sobre los objetivos" y es el referente recomendado por la norma de continuidad ISO 22301:2012 para la gestión del riesgo.

La administración de riesgos, tal como la establece la ISO (2012), se presenta en la figura 2.

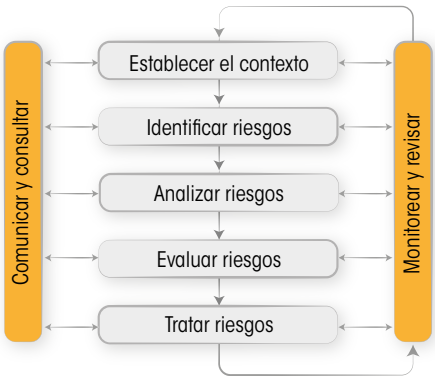

Figura 2. Vista general de la administración de riesgos.
Fuente: ISO (2012).

Como se muestra, *establecer el contexto* implica conocimiento de todos los aspectos que engloban la actividad de la organización; asimismo, la *identificación de riesgos* no solamente los reconoce a estos, sino también sus causas y efectos. Por su parte, el *análisis del riesgo* es el proceso en el que se establece la probabilidad de que un hecho suceda y el impacto que generan sus consecuencias. La *valoración de los riesgos* confronta los resultados del análisis del riesgo con las medidas de control que han sido identificadas, para establecer el tratamiento y fijar las políticas de administración de riesgos, que se estructura en cuatro ejes: transferir, retener, reducir o evitar el riesgo. Finalmente, la monitorización y la revisión implican establecer indicadores de seguimiento sobre las medidas que se adoptan para la gestión de riesgos.

Para la gestión de riesgos en el sector público colombiano, tiene gran importancia el Departamento Administrativo de la Función Pública, con la promulgación de su *Guía para la administración del riesgo* (DAFP, 2014), que define el riesgo como la posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos, y toma como referentes la norma ISO 31000:2009

y el modelo COSO. La Guía establece la siguiente clasificación de riesgos:

- *Riesgo estratégico.* Se asocia con la forma como se administra la entidad. Su manejo se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición clara de políticas, y el diseño y conceptualización de la entidad por la alta gerencia.
- *Riesgos de imagen.* Están relacionados con la percepción y la confianza de la ciudadanía hacia la institución.
- *Riesgos operativos.* Abarcan riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, la definición de los procesos, la estructura de la entidad y la articulación entre dependencias.
- *Riesgos financieros.* Se relacionan con el manejo de los recursos de la entidad, que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, los manejos de excedentes de tesorería y el manejo de los bienes.
- *Riesgos de cumplimiento.* Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y, en general, con su compromiso ante la comunidad.
- *Riesgos de tecnología.* Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras, y con el cumplimiento de la misión.
- *Riesgos de corrupción.* Relacionados con acciones y omisiones, el uso indebido del poder, de los recursos o de la información, para la obtención de un beneficio particular o de un tercero.

La *Guía para la administración del riesgo* del DAFP no establece acciones específicas para riesgos de continuidad, los cuales implican la probabilidad de ocurrencia de eventos que interrumpan la operación de los procesos y afecten la entrega de bienes o servicios a los clientes de la entidad. Sin embargo, la metodología propuesta por la Guía es aplicable a esta clase de riesgos, por lo cual se acogieron sus lineamientos en esta consultoría en cuanto a la identificación, valoración y clasificación de riesgos, los cuales se detallan

en el capítulo 3, donde se exponen los resultados en relación con los riesgos de continuidad.

Toda esta discusión acerca de la continuidad del negocio pareciera evidenciar el tránsito hacia una concepción más integral, que puede quizá reflejarse en posturas de autores y organismos como Servat (2012), que la define como parte del sistema de gestión gerencial, puesto que establece, implementa, opera, evalúa, mantiene y mejora la continuidad del negocio, al dar "confianza a terceros, ya que ha identificado los procesos esenciales que sustentan los productos o servicios que se desea proteger respecto a escenarios de amenazas producto del análisis del riesgo" (p. 1). Para otros autores, como Machuca y Sasco, un BCP es un proceso interno cuyo objetivo es asegurar que los procesos críticos de negocio estén disponibles para clientes, proveedores y otros *stakeholders* que necesiten acceder a ellos (Machuca y Sasco, 2012).

También está la postura de organismos como la ISO, para la cual la gestión de continuidad del negocio es un proceso holístico que identifica amenazas potenciales de una organización y los impactos que estas pueden causar en las operaciones del negocio. Además, proporciona un marco de trabajo para construir una organización más resistente, con capacidad para responder de forma efectiva y proteger los intereses de las partes clave interesadas, su reputación, imagen de marca y actividades de valor añadido (ISO, 2012). Esta concepción es la acogida por la presente consultoría.

Capítulo 2

La Agencia, su estructura y gestión frente a la norma internacional ISO 22301:2012

En este capítulo se realiza una aproximación a la estructura y gestión de la ARN, a la luz de los aspectos y requisitos que plantea la ISO 22301:2012, *Seguridad de la sociedad. Sistemas de continuidad del negocio. Requisitos*. Para tal fin, se revisó un volumen significativo de documentos y se recogieron elementos de las entrevistas aplicadas, que permitieron perfilar las acciones implementadas —o quizá las brechas— relacionadas con la continuidad del negocio frente a dicha norma.

2.1 La planeación estratégica institucional en relación con la ISO 22301:2012

La Agencia se encuentra adscrita a la Presidencia de la República (Presidente de la República, 2011, 2017) y su marco corporativo se enfoca en aportar a la paz, seguridad y convivencia del país, a partir de una visión que busca consolidar la organización como un referente internacional y una misión que impulsa el retorno a la legalidad —de forma sostenible— de la población desmovilizada. La Agencia tiene tres objetivos estratégicos: potencializar capacidades en los desmovilizados, propiciar espacios

de convivencia y reconciliación, y lograr corresponsabilidad de actores externos frente a la reintegración.

El marco corporativo no contempla objetivos de fortalecimiento institucional, lo que se explica porque cuando se estableció, la Agencia era un programa de Presidencia de la República y no una entidad.

Este marco se integra y despliega en el Plan Estratégico 2015-2018, lo cual implica un análisis de contexto interno y externo, que, al revisarlo en coherencia con la ISO de continuidad, puede relacionarse con acciones en esta materia, como los protocolos de seguridad para colaboradores de la Agencia y las personas desmovilizadas. Aunque los Grupos Territoriales y Puntos de Atención (GT/PA), que forman parte de la Agencia, trabajan en zonas donde existen bandas criminales u otros grupos armados ilegales, esas acciones de seguridad no se contemplan en los planes de los GT/PA, sino en procedimientos del sistema integrado. En relación con el contexto interno, se recogen aspectos relacionados con los sistemas de información de la entidad, pero predomina una mirada que centra el tema de la continuidad en la conservación de la información de la organización, en contravía de una mirada holística del tema, tal como lo plantea la ISO de continuidad.

El actual plan estratégico de la Agencia contiene tres objetivos estratégicos y un eje transversal (fortalecer la gestión institucional para la implementación del proceso de reintegración) que, por englobar las acciones de fortalecimiento institucional, y visto desde la perspectiva de la ISO de continuidad, puede ser el enlace entre la política de continuidad y los objetivos de la organización, y posibilitar un carácter sistemático en la planeación de la Agencia, al incorporar el aspecto de fortalecimiento institucional y reconocer el vacío del primer plan estratégico, que fue construido cuando la Agencia era la Alta Consejería para la Reintegración (ACR), un programa de la Presidencia de la República.

En general, la Agencia tiene 44 planes principales: Plan Estratégico Sectorial, Plan Estratégico 2015-2018, Plan de Acción Institucional, Plan de Anticorrupción y de Atención al Ciudadano, 16 planes operativos para cada dependencia del nivel central y 25 planes operativos de GT/PA.

El encadenamiento de los planes se estructura como se ve en la figura 3.

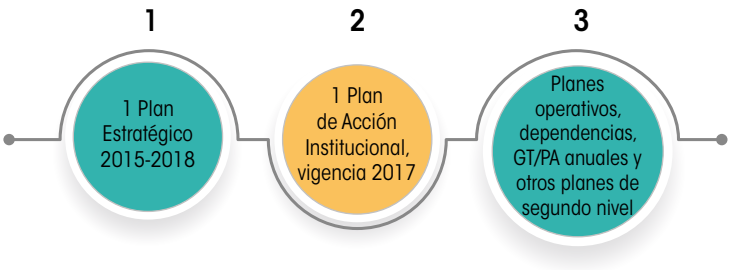

Figura 3. Encadenamiento de planes de la ARN.
Fuente: elaboración propia.

En el informe de gestión del primer trimestre de 2017, se evidencia que, según sus contenidos, los planes de las dependencias y de los GT/PA se orientan a la consecución de productos (95 y 137, respectivamente). Para el caso de los planes de las dependencias, se encuentran escasos temas relacionados con continuidad, tales como Plan de Trabajo del Sistema de Gestión de Seguridad en el Trabajo (SGSST) 2017, Plan de Conservación Documental (PCD), Plan de Mantenimiento y Soporte, la estrategia de defensa de los intereses judiciales de la entidad e iniciativas normativas que impacten el proceso de reintegración.

Otros productos que se identifican en la planeación de la Agencia son: índices calculados y validados (reincidencia, vulnerabilidad, y factores de inactivaciones y ausencias), análisis jurídico y contexto normativo del proceso de reintegración, evaluación del modelo de intervención, análisis de variables críticas que impactan el proceso y la política de reintegración, e información del contexto regional analizada para mejoras del proceso de reintegración en las regiones. Estos pueden constituirse en aspectos clave de análisis de contexto que permitan implementar acciones en materia de continuidad, tal como lo establece la norma de continuidad al hablar de la necesidad de considerar el contexto externo para determinar el alcance del SGCN.

En el caso de los planes operativos de los GT/PA, los productos están dirigidos a conseguir los logros y metas establecidos en relación con la ruta de reintegración y la corresponsabilidad; por ejemplo, estrategias de empleabilidad para desmovilizados, enfoques diferenciales, productivos, procesos comunitarios, de reconciliación, pero no incluyen acciones relacionadas con la continuidad

del negocio en relación con los aspectos de la ISO de continuidad (Planes operativos GT/PA 2016-2017).

En la Agencia se avanza hacia la implementación de instrumentos de planeación estratégica, como el *balance score card* (BSC). Esto se deja ver en hechos como el de que el *software* administrador del sistema de gestión contiene un módulo de BSC. En la estructuración final del BSC podría integrarse la continuidad del negocio y de esta manera connotarlo como estratégico, lo que posibilitaría apalancar en mayor grado el tema.

Tampoco se evidenciaron instrumentos de planeación, como la cadena de valor institucional definida para la organización, que refleje el cambio necesario con hitos críticos, para lograr los servicios y beneficios entregados a los desmovilizados, instrumento que puede ser punto de partida para identificar las acciones críticas "priorizadas, urgentes, vitales, esenciales, claves", necesarias de mantener ante interrupciones o incidentes de continuidad, como lo menciona de manera permanente la norma ISO 22301:2012 (ISO, 2012).

2.2 La estructura organizacional en relación con la norma ISO 22301:2012

Los diferentes planes de la entidad reflejan la estructura organizacional de la Agencia (figura 4). La estructura evidencia tres macrodependencias como ejes articuladores e integradores: Dirección General, Secretaría General, y Dirección Programática de Reintegración, lo cual denota una estructura organizacional vertical.

Para operar con esta estructura, la Agencia tiene su sede central ubicada en Bogotá, punto de concentración de sus directivas y desde donde se imparten las directrices, políticas, lineamientos de operación, y se asignan los recursos financieros a las 24 sedes territoriales (GT/PA), que atienden de manera directa a los desmovilizados y que se pueden identificar en la estructura de la figura 4.

Si se miran a partir de la ISO 22301:2012, son estas directivas quienes deben evidenciar compromiso y liderazgo en la continuidad del negocio y que esto sea compatible con la dirección estratégica de la organización, para lo cual deben proveer recursos.

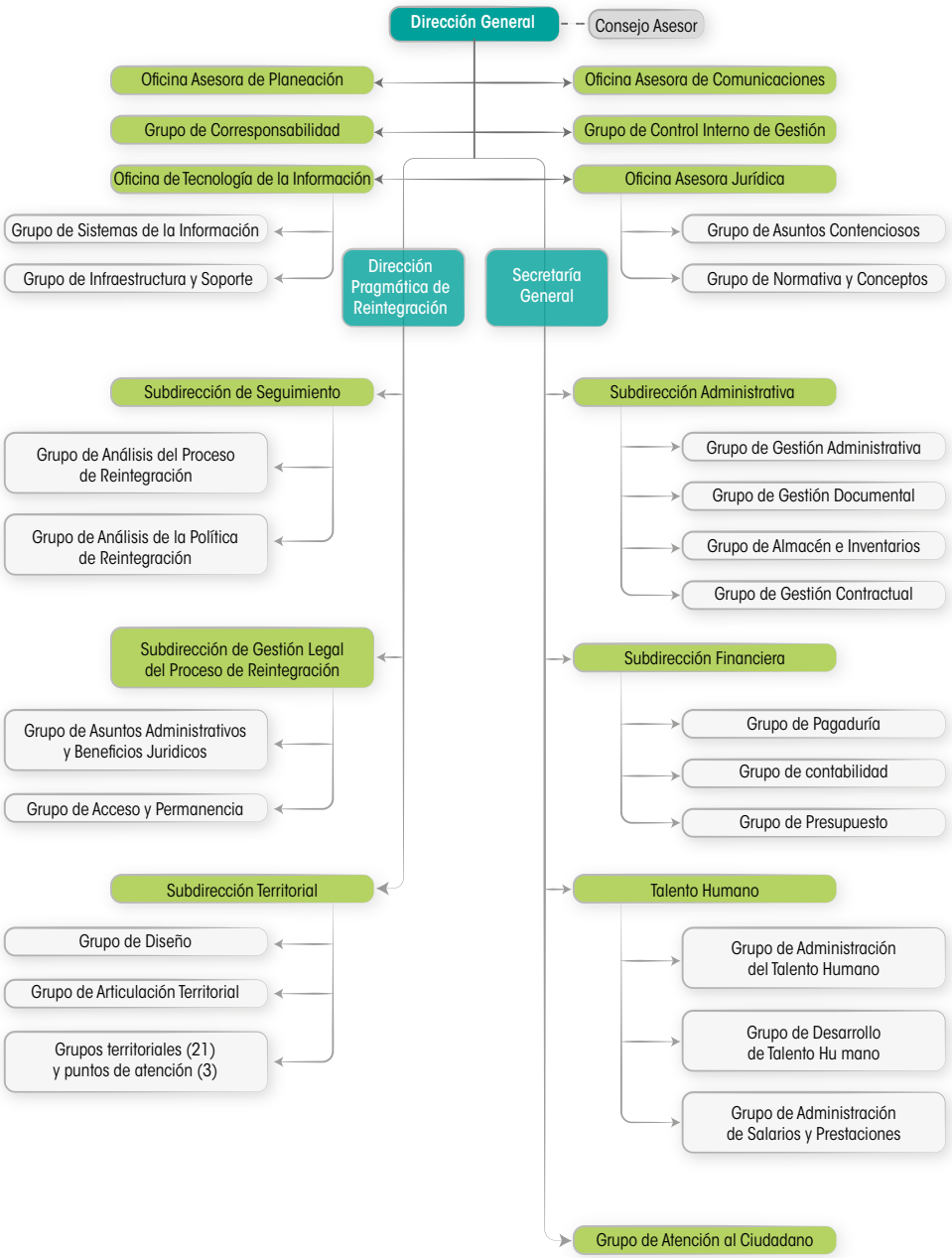

Figura 4. Estructura organizacional de la ARN.
Fuente: sitio web de la ARN.

Sin embargo, en el presupuesto 2017 de la Agencia se observa la ausencia relativa de partidas presupuestales para avanzar decididamente en acciones de continuidad del negocio (ACR, 2017), al igual que en su Plan Estratégico (ACR, 2015a), de forma que se pueda imprimirle un sello estratégico a la continuidad, aunque sí se reconocen aspectos relacionados, como la Estrategia GEL, sobre todo en lo que respecta a la seguridad y protección de la información.

Al revisar las funciones establecidas a los grupos de trabajo según la estructura organizacional —en relación con la ISO de continuidad, que habla de identificar funciones vinculadas a incidentes perturbadores—, se evidencian algunas funciones en los grupos de la Agencia que podrían relacionarse con continuidad del negocio.

Para el caso de los grupos o dependencias misionales, en la Subdirección de Seguimiento y en el Grupo de Articulación se recogen el análisis de riesgos de continuidad de los desmovilizados en la reintegración y la gestión de casos de riesgo, respectivamente.

Las demás funciones están inscritas a dependencias de apoyo. Por ejemplo, las acciones para la seguridad de la información y los planes de contingencia que aseguren la disponibilidad de infraestructura tecnológica, la información y los servicios en esta materia están dentro de las funciones de la Oficina de Tecnologías de la Información (OTI). A la Oficina Asesora Jurídica se le asignan acciones de gestión de riesgos jurídicos, el liderazgo y la implementación de políticas de daño antijurídico. El Grupo de Gestión Administrativa está encargado de los seguros de la entidad y de proveedores. Al Grupo de Gestión Documental se le asigna la conservación y protección de archivos. El Grupo de Almacén e Inventarios tiene a su cargo el mantenimiento y cuidado de bienes muebles e inmuebles. El Grupo de Gestión Contractual tiene asignadas acciones como la gestión de riesgos y las garantías de los contratos de la Agencia. Y Talento Humano está encargado de acciones de medicina preventiva, higiene y seguridad industrial (ACR, 2015b).

Volviendo a la ISO 22301:2012, estos aspectos se relacionan con la continuidad del negocio y, si la Agencia quisiera avanzar hacia un SGCN, la función transversal a todos los anteriores gru-

pos de trabajo (apoyar la implementación y sostenibilidad del Sistema de Gestión Integral y sus componentes) se presenta como una oportunidad.

Para el cumplimiento de sus funciones, la Agencia cuenta con recursos del presupuesto general de la Nación, que permiten atender a los desmovilizados otorgándoles beneficios sociales y económicos reglamentados mediante resoluciones 0754 de 2013 (ACR, 2013) y 1356 de 2016 (ACR, 2016c).

Se distinguen los beneficios sociales de acompañamiento psicosocial, gestión en salud, gestión en educación y formación para el trabajo, que también cobijan a los familiares. También están los beneficios económicos: apoyo económico a la reintegración, estímulo económico a la empleabilidad, estímulo económico para planes de negocio (capital semilla) y estímulo económico para educación superior.

La Agencia apalanca también otros servicios como gestiones ante autoridades por casos de riesgo, gestión de servicio social (consistente en 80 horas de servicio social que realizan las personas en proceso de reintegración y que benefician a comunidades receptoras), ejecución de proyectos comunitarios y de prevención del reclutamiento, articulación con entidades para facilitar la documentación legal de los desmovilizados, como cedulación, registro civil, antecedentes judiciales y beneficios jurídicos ante los jueces de la República, así como acciones para conocer la verdad del conflicto armado colombiano, pero sin consecuencias judiciales.

Este abanico de servicios y beneficios son los que debe mantener la Agencia, de manera ininterrumpida, para los desmovilizados, a partir de una eficaz y eficiente gestión de los escenarios de falla y riesgos de continuidad del negocio, tal como lo establece la ISO 22301:2012.

Los servicios y beneficios se inscriben en la ruta de reintegración concebida como el plan de trabajo definido conjuntamente entre la Agencia y el desmovilizado para la construcción de su proyecto de vida y la superación de su vulnerabilidad (ACR, 2013). Esta ruta la componen ocho dimensiones (figura 5).

Figura 5. Dimensiones de la ruta de reintegración.
Fuente: sitio web de la ARN.

2.3 El sistema de gestión de la Agencia frente a la ISO 22301:2012

La Agencia tiene implementado un sistema de gestión que apalanca el cumplimiento de su marco estratégico y está formado por el "Sistema de Gestión de la Calidad, el Modelo Estándar de Control Interno (MECI), el Modelo Integrado de Planeación y Gestión, y el Sistema de Gestión de Seguridad y Salud en el Trabajo" (ACR, 2016d). Este sistema de gestión está certificado por las normas ISO 9001 (Sistema de Gestión de la Calidad - Requisitos) y NTC GP 1000 (Norma Técnica de Calidad para la Gestión Pública).

El sistema de gestión, tal como está configurado, constituye una oportunidad para avanzar en la implementación de los requerimientos y prácticas de continuidad del negocio de la ISO 22301:2012, ya que se estructura con los parámetros de las normas ISO. Este aspecto es resaltado por la norma de continuidad, al mencionar que así se asegura "un grado de consistencia con otros

sistemas de gestión de estándares, tales como la ISO 9001:2008" (ISO, 2012, p. 5).

De esta manera, se aprovecharía el trabajo ya realizado al interior de la entidad en la implementación y consolidación de su sistema de gestión, compuesto por 16 procesos. Aquí se entiende por proceso el conjunto de actividades mutuamente relacionadas que transforman elementos de entrada en resultados (ISO, 2015) y que está representado en la figura 6.

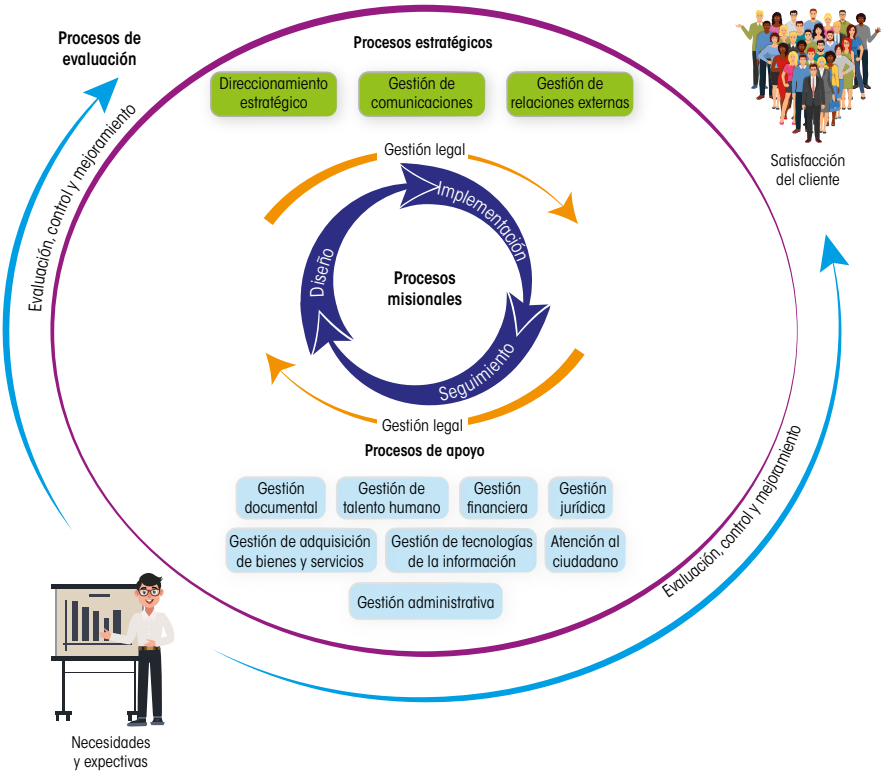

Figura 6. Mapa de procesos ARN.
Fuente: elaboración propia con base en el sitio web de la ARN.

Los procesos están esquematizados en documentos llamados *caracterizaciones*, que permiten tener una mirada global de cada uno, con lo cual se pueden identificar sus principales componen-

tes a partir del ciclo PHVA, aspecto que acoge la ISO de continuidad y que se presenta como coyuntura válida para integrar, de manera sistemática, acciones de continuidad a los procesos.

Estos documentos son controlados y sus diferentes versiones evidencian la dinámica y el intento organizacional de madurar y consolidar el sistema. Esto es evidente cuando se observa que el 68,75 % de los procesos presentan caracterizaciones con 5 o 6 versiones, y el 31,25 % con 3 versiones.

Los cuatro procesos misionales que gestionan y concentran los beneficios y servicios a las personas en proceso de reintegración presentan, en general, en sus caracterizaciones 5 o 6 versiones, lo cual evidencia un permanente ajuste en pro de la mejora continua. La discriminación de este aspecto, por proceso, se puede observar en la tabla 1.

Tabla 1. Versiones de caracterización de procesos

Proceso	Versión de la caracterización
Atención al ciudadano	5
Gestión administrativa	3
Gestión documental	3
Seguimiento	5
Implementación	6
Gestión de tecnologías de la información	5
Gestión de relaciones externas	3
Gestión financiera	3
Diseño	5
Gestión de comunicaciones	5
Direccionamiento estratégico	5
Gestión legal	3
Gestión de adquisición de bienes y servicios	5
Gestión del talento humano	5
Gestión jurídica	5
Evaluación, control y mejoramiento	5

Fuente: elaboración propia con base en documento de caracterización de procesos de la ARN.

La política del sistema de gestión enfatiza el compromiso de gestión en procura de la mejora continua para lograr impactos positivos en sus clientes. Así lo dice la Agencia en su *Manual del Sistema Integrado de Gestión para la Reintegración (Siger)*:

> En la Agencia [...] estamos comprometidos con la implementación y mantenimiento del Sistema Integrado de Gestión [...] en términos de calidad y seguridad y salud en el trabajo, orientado hacia el mejoramiento continuo, de manera que nos permita cumplir los [...] objetivos con nuestros clientes y partes interesadas. (ACR, 2016d, p. 25)

Se cuenta con siete ojetivos, de los cuales dos refieren de manera explícita acciones relacionadas con la continuidad del negocio (ACR, 2016d):

- Fomentar la seguridad y salud de todos los colaboradores, partes interesadas y ciudadanos mediante la mejora continua del sistema integrado de gestión para la reintegración.
- Identificar los peligros y riesgos de gestión, corrupción, seguridad y salud en el trabajo, evaluarlos y valorarlos y establecer los respectivos controles.

Al analizar los dos objetivos puede evidenciarse que comparten temas de salud y seguridad en el trabajo. Desde esta óptica, en caso de que se avanzara hacia un SGCN, podrían incorporarse a la política del sistema y taxativamente construir un objetivo de continuidad del negocio, en coherencia con lo planteado por la ISO 22301:2012.

Se evidencia que en este manual se plantean acciones relacionadas con continuidad, como las políticas en relación con la seguridad y protección de la información, y frente a la seguridad y salud en el trabajo. Se anota que en el transcurso de la consultoría se identificó que la Agencia avanza en la implementación del sistema de gestión de seguridad de la información tomando como referencia la ISO 27001, por lo cual, en relación con el sistema, sufrirán cambios la política, los objetivos, el manual del sistema y otros documentos que sustentan la operación de los procesos.

Pese a que no está integrado al sistema de gestión, en la actualidad la Agencia cuenta con el *Manual del Sistema de Gestión de Seguridad de la Información*, en el cual se hace explícita una política de continuidad del negocio, lo que evidencia un enfoque que no se restringe solo a la información. Dentro de los apartados de la política se menciona el siguiente: "Los responsables deben establecer los lineamientos para minimizar los efectos de las posibles interrupciones de la operación (sean estas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos)" (ACR, 2016a).

Al respecto, se pueden mencionar dos aspectos: por un lado, se tiene una política —requisito exigido por la norma de continuidad ISO 22301:2012— y, por otro, se tiene una concepción que se acerca a lo que propone esta norma, en el sentido de mantener una mirada holística sobre la continuidad del negocio, lo cual se evidencia aún más cuando se detallan los lineamientos de esta política, que promulga la identificación y valoración de riesgos, los escenarios y el plan de continuidad, aspectos que, sin embargo, presentan brechas entre lo promulgado y lo efectivamente realizado.

Resulta a la vez curioso que se conciba una política de continuidad del negocio que desborde el tema de la información, pero que se encuentre establecida en el *Manual del SGSI* de la entidad y no en el *Manual del Sistema Integrado*, con lo cual se le daría una connotación más estratégica y transversal a todo el sistema.

A pesar de que esta política existe y se ha comunicado por la alta gerencia al resto de la entidad —por la publicación del *Manual del SGSI*, única evidencia encontrada—, y que se pueden considerar como dos requisitos cumplidos según la norma ISO 22301:2012, por las respuestas de los entrevistados se evidencia su poco conocimiento y una cultura organizacional en la que la continuidad del negocio tiene poca apropiación y conocimiento por los colaboradores, lo que de alguna manera puede denotar una relativa debilidad de la *toma de conciencia* frente a la política de continuidad y su rol ante incidentes alteradores, como lo requiere la norma ISO de continuidad.

Puntualmente, en el sistema de gestión se evidencian acciones relacionadas con la continuidad, como las que lidera el proceso

de Talento humano, y que van encaminadas a lograr un entorno laboral más seguro mediante la identificación y gestión de peligros, la realización de acciones de inspección en seguridad, equipos, extintores, elementos de protección personal y atención de emergencias. En particular podemos decir:

- No se logró evidenciar una lista detallada de funcionarios con los datos necesarios de contactos (árbol de llamadas) para casos de emergencias.
- Existe un grupo de brigadistas —15 en sede central y 3 en promedio por GT/PA— que han recibido entrenamiento sobre atención de emergencias, a partir de la realización de campamentos con personal especializado de la Cruz Roja o personal experto de la Policía Nacional.
- Se realizan ejercicios de simulacros, pero estos responden principalmente a los programados en todo el país por autoridades en la materia y no son iniciativa propia de la entidad y, menos aún, desde la perspectiva de la ISO de continuidad. Esta última resalta la importancia de realizar ejercicios y ensayos de procedimientos de continuidad en los que deben primar propósitos, objetivos y una planificación sistemática, evidenciados en la revisión de documentos que sustentan los procesos de la entidad y, de manera específica, los del proceso de Talento humano.
- También se destacan las acciones lideradas por el proceso de Gestión administrativa, encaminadas a la seguridad de las instalaciones de las sedes de la entidad, de su personal, y a la gestión y cuidado de bienes. Se resaltan acá instrumentos como el mapa de riesgos de seguridad, el manual de seguridad preventiva —dirigido a la integridad de la vida de los colaboradores— y el manual para el manejo y control administrativo de los bienes de propiedad de la entidad.
- Existen otras acciones como la implementación de una política de prevención de daño antijurídico en la Agencia, liderado por el proceso de Gestión jurídica.

2.4 La estrategia global de riesgos en relación con la ISO 22301:2012

La norma de continuidad otorga gran importancia a una gestión sistemática del riesgo, que identifique, analice y evalúe los riesgos de interrupción de eventos en la organización. La entidad acogió la metodología del DAFP, evidenciada en su *Manual de gestión del riesgo* (ACR, 2017), para la administración de sus riesgos. En este manual se recogen aspectos de la NTC-ISO 31000:2011, *Gestión del riesgo - Principios y directrices*, que a su vez recomienda la ISO 22301:2012 para la evaluación de riesgos respecto a la continuidad del negocio; en ella se afirma: "Esta norma se puede aplicar a cualquier tipo de riesgo, cualquiera sea su naturaleza, bien sea que tenga consecuencias positivas o negativas" (ISO, 2009).

Cada proceso tiene un mapa de riesgos. En total se establecieron 38 riesgos de gestión, que se tratan a partir de 164 acciones. Al discriminar por proceso se obtienen los resultados consignados en la tabla 2.

Tabla 2. Consolidado de riesgos de gestión por proceso

Proceso	N.° riesgos	N.° acciones	Tipo de riesgo				
			Estratégico	Cumplimiento	Operativo	Tecnológico	Financiero
Atención al ciudadano	1	4		1			
Gestión administrativa	4	17			4		
Gestión documental	2	11			2		
Seguimiento	3	6	2		1		
Implementación	3	34	2		1		
Gestión de tecnologías de la información	4	13	1			3	
Gestión de relaciones externas	1	1	1				
Gestión financiera	4	13					4
Diseño	1	5	1				
Gestión de comunicaciones	1	3	1				

Proceso	N.° riesgos	N.° acciones	Tipo de riesgo				
			Estratégico	Cumplimiento	Operativo	Tecnológico	Financiero
Gestión legal	1	29		1			
Gestión de adquisición de bienes y servicios	2	4			2		
Gestión del talento humano	4	4		1	3		
Gestión jurídica	3	8		3			
Evaluación, control y mejoramiento	3	5	1	2			
Totales	38	164	10	8	13	3	4

Fuente: elaboración propia con base en mapa de riesgos de los 16 procesos de la ARN.

El mapa lo forman riesgos de tipo estratégico, operativo, de cumplimiento, financiero y tecnológico, que se explican en el *Manual de gestión de riesgos* de la entidad (ACR, 2017).

El mayor número de riesgos se concentran en los tipos operativo, estratégico y de cumplimiento, con porcentajes de 34,21 %, 26,32 %, y 25,05 %, respectivamente. Desde esta perspectiva, la entidad reconoce en mayor grado los riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, la definición de los procesos, la estructura de la entidad y la articulación entre dependencias.

Al analizar la valoración de los riesgos, en los que se incluyen los riesgos de corrupción, se encontraron los resultados mostrados en la tabla 3.

Tabla 3. Valoración de riesgos por proceso

Proceso	Zona valoración riesgo			
	Extrema	Alta	Moderada	Baja
Direccionamiento estratégico		1		
Gestión de comunicaciones		1		
Evaluación, control y mejoramiento	1	2	1	
Diseño		1		

Continúa...

... viene

Proceso	Zona valoración riesgo			
	Extrema	Alta	Moderada	Baja
Seguimiento		3		
Atención al ciudadano			1	
Gestión de adquisición de bienes y servicios	2	2		
Gestión del talento humano		2	3	1
Gestión de tecnologías de la información		3	2	
Gestión jurídica		2		1
Gestión administrativa	2	2	1	
Gestión documental		3		
Gestión financiera	1	4		
Gestión de relaciones externas			1	
Gestión legal			1	

Fuente: elaboración propia con base en mapa de riesgos de los 16 procesos de la ARN.

La entidad valora sus riesgos principalmente en zona alta. Sin embargo, al revisar los riesgos según proceso, se encuentran pocos relativamente respecto a la continuidad del negocio y, menos aún, desde la perspectiva de la ISO 22301:2012. No obstante, los mapas de riesgo de los procesos de la Agencia se presentan como una gran oportunidad para avanzar en acciones en este sentido.

En el *Manual de riesgos* se reconoce el análisis del contexto de la entidad para la gestión del riesgo; lo denominan como *contexto estratégico* e implica "la identificación de amenazas (factores externos) y debilidades (factores internos) a los que está expuesta la Entidad y que pueden afectar el cumplimiento de los objetivos de la misma" (ACR, 2017). Este aspecto es coherente con la ISO de continuidad, que destaca la importancia del establecimiento del contexto para avanzar hacia un SGCN.

Al analizar los mapas de riesgos, algunos de estos últimos pueden relacionarse con continuidad. Entre ellos están los que tienen que ver con temas de información, como "no divulgar información oportuna, relevante y veraz sobre la Política de Reintegración Social y Económica (PRSE)", que se tratan con acciones como "monitoreo y seguimiento [...] de contenidos relacionados con la PRSE realizados por actores externos" para la toma de acciones. No obstante, no se encontró un manual de crisis de comunicaciones, para

obrar de manera sistemática ante este tipo de situaciones, si bien antaño se pretendió avanzar al respecto.

Para otros riesgos, como "deficiencias en la identificación y consolidación de información de contexto de las regiones donde se encuentran ubicadas las personas desmovilizadas" —que es un aspecto clave en la ISO de continuidad— y "pérdida de la información en cualquier tipo de soporte", se realizan actividades como un plan de conservación y estrategias de seguridad de la información física.

En los aspectos tecnológico y de sistemas de información, se encuentran otros riesgos como "no disponibilidad de los servicios tecnológicos, vulnerabilidades de seguridad, soporte no disponible, pérdida de integridad de los datos, uso indebido de los activos de información tecnológicos", que se pueden inscribir en un escenario de falla tecnológica.

Algunos riesgos se relacionan con los recursos de la entidad, como "apropiación indebida de recursos en la ejecución contractual", y para ellos se realizan acciones de identificación de contrataciones en las que existe mayor probabilidad de materializar este riesgo y establecer puntos de control. Los "pagos no debidos" se controlan realizando acciones de control en la contabilidad de la entidad"; la "pérdida irrecuperable de bienes de la Entidad por sustracción de [...] terceros y de los colaboradores" se gestiona con acciones de control de bienes y la adquisición de seguros. Además, el "corte o suspensión en el suministro de servicios públicos" se tramita con una adecuada administración de facturas de servicios, pero nunca se habla en la perspectiva de continuidad.

En los temas jurídicos se encuentran riesgos como la "inadecuada aplicación de la política de prevención de daño antijurídico por [...] los colaboradores de la entidad", para lo cual existe un comité de conciliación; ante la "falta o indebida emisión de conceptos jurídicos" y la "falta o fallas en la representación judicial y extrajudicial de la entidad" se realizan acciones rigurosas de seguimiento.

Frente a la seguridad y salud en el trabajo aparece el riesgo de "incumplimiento de las políticas operativas del Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST)", frente al cual se despliegan acciones de control para cumplir las acciones en esta materia.

Al analizar los contenidos de los contextos en los mapas de riesgo de los diferentes procesos, se encuentran aspectos como: siete procesos no reconocen eventos externos, el contexto político

toma mayor relevancia con nueve eventos identificados, le sigue el contexto social con ocho, el económico con siete, el tecnológico con seis, el ambiental y el legal con dos cada uno, para un total de 34 eventos externos que generan riesgos para la operación de los procesos de la Agencia. En relación con la continuidad, estos contextos pueden evidenciar aspectos como los que se enumeran a continuación.

Frente al contexto ambiental, se reconoce "infraestructura deteriorada o nula de las vías de acceso, que no permiten el desarrollo de las actividades del proceso de reintegración" y "catástrofes naturales y condiciones medioambientales [que] impiden el desarrollo o acceso al lugar de la actividad programada", aspecto que adquirió particular relevancia en el caso del Grupo Territorial de Putumayo, que se vio afectado por la avalancha ocurrida en Mocoa en abril de 2017, pues sus instalaciones estuvieron por varios días sin suministro de servicios públicos. Como consecuencia de este evento, el Grupo Territorial debió reducir las metas de su plan operativo y varios de sus colaboradores sufrieron pérdidas de vivienda (N. Sarria, comunicación personal, junio de 2017).

Para otras sedes de la Agencia —como es el caso de la sede principal, ubicada en el centro de Bogotá—, el contexto ambiental en un escenario de desastre nacional o regional cobra importancia, por ejemplo, ante un sismo de intensidad significativa. Esto acarrearía la suspensión parcial o total de la operación de esta sede, lo que impactaría negativamente a la Agencia, teniendo en cuenta que no existe sitio alterno de operación ante un evento de este tipo. De igual manera sucede con el resto de sedes.

El riesgo de sismo se sustenta en estudios como el realizado por la Universidad de los Andes (Universidad de los Andes, 2010) sobre microzonificación sísmica de Bogotá, en el que se considera a la localidad de la Candelaria, en el centro de la ciudad y donde justamente está ubicada la sede central de la Agencia, como una de las zonas que resultarían más afectadas en caso de terremoto.

Por su parte, el Fopae (2010) sostiene que Bogotá presenta un alto grado de vulnerabilidad sísmica, entendida como una baja capacidad de resistir adecuadamente esta amenaza. En este sentido, y teniendo en cuenta que en Bogotá se encuentran las principales entidades del gobierno nacional, regional y distrital, así como las industrias de producción, bienes y servicios más importantes del

país, su posible afectación puede llegar a causar un gran impacto en la economía del país.

La edificación donde funciona la sede central de la entidad en Bogotá no es ajena a esta amenaza. Por un lado, se encuentra en una de las zonas de mayor vulnerabilidad, el edificio de ocho pisos donde funciona esta sede tiene más de 50 años de construcción y no cumple con las normas actuales de construcción sismorresistente para Colombia (ASIS, 2010). Este aspecto iría en contravía de lo que plantea la ISO de continuidad, respecto a que la premisa de la organización debe ser "salvar a la gente, como primera prioridad".

De acuerdo con los colaboradores entrevistados de la OTI, la Agencia tiene dispuestos sitios alternos para los servidores que sustentan la operación de sus sistemas de información y las copias de seguridad de estos, así como para la documentación en físico de la entidad y de sus clientes directos. Además, la Agencia ha emprendido la modalidad del teletrabajo, pero como parte de las políticas de equilibrio entre la vida personal y laboral, y no en relación con la continuidad del negocio.

En el contexto tecnológico, se reconocen en general agresiones hacia los sistemas informáticos. Durante esta consultoría se presentó el ataque cibernético mundial del *ransomware* WannaCry, a lo cual se respondió con una serie de acciones, aunque la OTI reconoció que muchas de estas se confeccionaron en la coyuntura del ataque y que se actuó de manera reactiva ante el evento, ya que las acciones no estaban previstas en un plan sistemático, tal como lo plantea la ISO 22301:2012. No obstante, estas acciones mitigaron de manera efectiva la materialización de riesgos en relación con el escenario de falla tecnológica.

Hay que destacar, en relación con este contexto, un avance respecto al resguardo y protección de los activos de información, pues se plantea con este fin un Sistema de Gestión de Seguridad de la Información (SGSI), que fue adoptado en la entidad mediante Resolución Interna 0335 de 2017.

En el contexto económico se reconocen como riesgos para la continuidad principalmente los recortes presupuestales realizados por el Ministerio de Hacienda a través del Boletín N.° 177, "Austeridad presente en el Presupuesto General de la Nación 2017", en el que los gastos generales y la contratación de servicios personales son impactados negativamente. Esto ha sido una constante en los

históricos del presupuesto de la Agencia y se viene presentando desde 2013 (entre 2013 y 2017, el recorte promedio fue de 23 000 millones de pesos). Por las entrevistas se deja ver que la austeridad ha implicado ajustes y arreglos en los procesos de contratación y en los gastos generales de la entidad, lo que, desde la perspectiva de la ISO de continuidad, implica limitaciones en los recursos necesarios para avanzar hacia un SGCN. La situación es tal que, como ya se dijo, ni siquiera se logró contratar un experto en continuidad, tal como se tenía proyectado en 2017.

La austeridad se relaciona con la baja de los ingresos corrientes del Estado. Al respecto, en el periódico de la Universidad Nacional de Colombia se publicó:

> Serios riesgos trae para la economía del país una caída extrema en los precios internacionales del petróleo. El producto interno bruto (PIB) se reduciría en 13 % para 2021, la inflación subiría al 1,8 % anual y el desempleo volvería al 12 %. (Ortiz *et al.*, 2014, p. 1)

En este mismo contexto adquieren también importancia las condiciones socioeconómicas territoriales para lograr la reintegración de los desmovilizados.

En el contexto político se reconocen principalmente dos aspectos que se ligan a la continuidad: la implementación del acuerdo de paz con las Farc-EP y la cercanía de las elecciones presidenciales de 2018. Estas situaciones quizá influyeran en las entrevistas porque se escucharon cosas como "la estructuración, fusión, liquidación, supresión o absorción de la ARN" en boca de colaboradores del proceso de Gestión legal cuando se les preguntó sobre el escenario de sucesión de poder. Lo anterior se materializó en parte con la promulgación del Decreto 897 de 2017, que modificó la estructura y nombre de la Agencia, con el fin de que acogiera la reincorporación de las Farc-EP (Presidente de la República, 2017).

En el contexto social, se resalta la estigmatización hacia los desmovilizados y las difíciles condiciones de seguridad y de orden público para operar tranquilamente. Estos dos últimos se relacionan con la continuidad. Frente a estas situaciones, algunos GT han tenido que retirar metas inscritas en sus planes operativos, como ocurrió con el Grupo Territorial Antioquia-Chocó.

En general, la Agencia cuenta con una administración de riesgos de gestión y de corrupción, pero que no se conectan necesariamente con los riesgos de continuidad del negocio, pese a que tiene análisis de contexto externo e interno, y los riesgos que implicaría perfilar acciones en esta materia, incluyendo acciones de recuperación sistemáticas, como lo plantea la ISO de continuidad.

2.5 Marco regulatorio de la Agencia en relación con la ISO de continuidad

La Agencia no está obligada a cumplir los requisitos de la norma estándar internacional ISO 22301:2012. No es un mandato en Colombia que este tipo de entidades la adopten, pero sí deben cumplir la norma NTC-GP 1000:2009.

Para el caso de la normativa, cada proceso cuenta con un normograma, que recoge las disposiciones internas y externas que rigen su operación. Estas pueden ser resoluciones, decretos, acuerdos, documentos de política, leyes, declaraciones, pactos internacionales, entre otras. La situación evidencia una dinámica que se puede percibir cuando se observa el alto número de versiones de estos documentos en los diferentes procesos (tabla 4).

Tabla 4. Versiones de normograma por proceso

Proceso	Versiones de normograma
Direccionamiento estratégico	6
Gestión de comunicaciones	6
Evaluación, control y mejoramiento	3
Diseño	6
Implementación	3
Seguimiento	4
Atención al ciudadano	4
Gestión de adquisición de bienes y servicios	4

Continúa...

... viene

Proceso	Versiones de normograma
Gestión del talento humano	4
Gestión de tecnologías de la información	5
Gestión jurídica	6
Gestión administrativa	3
Gestión documental	4
Gestión financiera	3
Gestión de relaciones externas	1
Gestión legal	4

Fuente: elaboración propia con base en normograma de los 16 procesos de la ARN.

Al analizar esta diversidad de normativas frente a la ISO 22301:2012, que requiere de las organizaciones una gestión sistemática frente a temas legales y regulatorios en relación con la continuidad del negocio, se puede observar que, en su operación, la Agencia toma en consideración la siguiente normatividad:

- Normativas relacionadas con los temas de información y tecnologías que, en general, buscan seguridad de la información y protección de datos personales y de los activos de información de la entidad, entre las que se destacan:
  - Conpes de seguridad digital
  - Ley General de Archivo 594 del 2000
  - Decreto 2573 del 12 de diciembre de 2014, con la estrategia Gobierno en Línea, en especial su componente de seguridad y privacidad de la información
  - Decreto 1377 del 27 de junio de 2013, sobre protección de datos
  - Ley 1273 del 5 enero de 2009, sobre seguridad informática y prevención de delitos informáticos
  - Decreto 1080 de 2015, que regula el Sistema Nacional de Archivos y el Programa de Gestión Documental

- Normativa en materia de protección y aseguramiento de los recursos físicos y financieros de la entidad, a partir de la gestión de estrategias y riesgos contra la corrupción. Se trata de aspectos promulgados en directivas o decretos con fuerza de ley por Presidencia de la República, y en los que entidades como el DAFP, la Secretaría de Transparencia o las entidades de control adquieren gran importancia. Se destacan:
  - Ley 1474 de 2011 (Estatuto Anticorrupción)
  - Ley 87 de 1993, de control interno en las entidades y organismos de la rama ejecutiva, y Decreto 943 de 21 de mayo de 2014, que la actualiza
  - Ley 42 de 1993, sobre aseguramiento de los bienes de las entidades.
- Conpes 3716 de 2011, sobre la matriz de riesgos previsibles en materia de contratación
- Normativa sobre la protección de los colaboradores de la entidad, que forma parte de las disposiciones sobre esta materia en el país:
  - Decreto 723 de 2015, sobre la afiliación al sistema de riesgos laborales
  - Decreto 1072 de 2015, sobre el Sistema de Gestión de Seguridad y Salud en el Trabajo.
  - Resolución 2646 de 2008, sobre los riesgos psicosociales
- Normativa interna, como la Resolución 531 de 2012, por la que se adopta el Reglamento de Higiene y Seguridad Industrial, con base en las disposiciones del SGSST.
- Normativa muy interna que se dirige a las personas en proceso de reintegración, de la cual forman parte las resoluciones 0754 de 2013, y 1356 de 2016, que regulan los servicios y beneficios para esta población, y las disposiciones del Estado para la protección de la integridad física de las personas desmovilizadas y sus familias, según lo establecido en el Decreto 4912 de 2011.

En general, muchos de estos aspectos normativos pueden ser insumos para los requerimientos legales y regulatorios que menciona la ISO 22301:2012 a fin de avanzar hacia un SGCN.

2.6 Las partes interesadas de la Agencia respecto a la ISO 22301:2012

La ISO de continuidad establece que son parte interesada aquellas

> [...] personas u organización que puede afectar, ser afectada, o se percibe que puede ser afectada por una decisión o actividad [...]. Esto puede ser un individuo o grupo que tiene un interés en cualquier decisión o actividad de la organización. (ISO, 2012, p. 10)

Con esta definición sobre las partes interesadas de la Agencia, se reconoce en el documento "Caracterización de usuarios" a las *personas en proceso de reintegración* como su principal cliente, y para ello dispone de una serie de instrumentos que permiten caracterizarlas y definir sus necesidades y expectativas en relación con los servicios y beneficios que se les ofrecen.

Sin embargo, no parece existir un documento sistemático de caracterización de usuarios que describa las diferentes partes interesadas de la entidad, aunque se evidencia en la diversidad de documentos consultados —y en las entrevistas realizadas—, que existen diferentes actores frente a los cuales se emprenden o se realizan acciones de manera conjunta, en función de su posición y el rol que desempeñan, bien sea en relación con la entidad o con el colectivo social. De este conjunto de actores se podría realizar una aproximación inicial de las partes interesadas de la Agencia, que serían:

- Las familias de los desmovilizados, principalmente como beneficiarios del proceso de reintegración o facilitadores de la reintegración de los desmovilizados (ACR, 2013).
- Las comunidades receptoras de desmovilizados, como beneficiarias de la reintegración en la búsqueda de escenarios de reconciliación, aspectos evidentes en documentos como los planes operativos, el proyecto de inversión de la

entidad y el documento de enfoque de la reintegración, que explica la dimensión ciudadana.

- El sector privado y las organizaciones de economía social y solidaria, conocidas como el tercer sector, a los que se dirige en gran parte la estrategia de corresponsabilidad que tiene la Agencia, en busca de apoyos en diversos temas frente al proceso de reintegración, entre los cuales sobresalen los temas de emprendimiento, vinculación laboral, apoyos técnicos o financieros e investigaciones conjuntas (ACR, 2016b).

- Los entes territoriales, como las alcaldías y gobernaciones, con los cuales los GT/PA articulan acciones a favor de la reintegración. Sobresale en este campo la mencionada en el informe de gestión de la ACR (2016c), en relación con la inclusión de la Política Nacional de Reintegración Social y Económica (PNRSE) en 301 planes de desarrollo, para lograr acciones afirmativas hacia los desmovilizados y la articulación para que ellos realicen su servicio social obligatorio.

- La academia, los investigadores, los estudiantes, articulando o gestionando acciones para la generación de conocimiento en torno a los temas de la reintegración.

- Las organizaciones internacionales y los gobiernos de otros países, a los cuales se dirigen acciones para lograr cooperación técnica, financiera, política, intercambio de experiencias en desarme, desmovilización y reintegración (DDR), muchas de ellas alcanzadas a partir de giras de cooperación dentro o fuera del país. La Agencia Colombiana para la Reintegración (ACR) realizó cinco giras de cooperación técnica desde 2009, por medio de las cuales buscó promover el intercambio de lecciones aprendidas, buenas prácticas y desafíos en materias de DDR con países en situación de conflicto o posconflicto.

- Los medios de comunicación, a los que se dirigen acciones para lograr divulgación bajo la modalidad *free-press*, que permita visibilizar los aspectos del proceso de reintegración, explicarlo de manera adecuada e informar con ese criterio a la opinión pública.

- Otras organizaciones de la sociedad civil con las cuales se pueden realizar acciones, por ejemplo, investigaciones. Estas organizaciones cumplirían el papel de operadores del proyecto de inversión de la entidad, que recoge el modelo de intervención comunitaria y la estrategia "Mambrú no va a la guerra" para prevención del reclutamiento. También facilitarían el logro de los productos establecidos en los planes operativos de los GT/PA o de las dependencias del nivel central de la entidad.
- Las entidades públicas, encargadas de acciones de articulación territorial para la implementación y evaluación del proceso de reintegración, en las que sobresalen acciones del tipo convenio para intercambiar información y lograr los beneficios estipulados en la Resolución 0754 de 2013, acerca de educación, salud, protección, documentación personal y beneficios jurídicos a los desmovilizados. Las entidades públicas también se encargarían de realizar evaluaciones independientes sobre resultados de la reintegración.

Frente a la ISO 22301:2012, los requerimientos de las partes interesadas se constituyen en insumos valiosos para la gestión de la continuidad, tal como se evidencia en la figura 7.

La Agencia tiene, sin embargo, una brecha en el campo de las partes interesadas, pues no ha abordado sistemáticamente las necesidades y expectativas de estas partes en su sistema de gestión, que se encuentra certificado por la ISO 9001:2009 y puede ser insumo para avanzar hacia la inclusión de la continuidad del negocio en perspectiva de la ISO 22301:2012. Este aspecto es significativo si se tiene en cuenta que la ISO 9001:2015 (la nueva versión de la ISO 9001:2009) da gran importancia a las partes interesadas y propone otros requisitos y la Agencia debe transitar el camino de actualización y recertificación de su sistema de gestión.

La ISO de continuidad le otorga gran importancia a la comunicación con las partes interesadas ante eventos alteradores o incidentes de interrupción; sin embargo, no se pudieron hallar protocolos o acciones encaminadas en esta materia. No obstante, en 2014, según afirmación de los colaboradores del equipo de la Oficina Asesora de Comunicaciones, la Agencia trató de avanzar en la elaboración de un manual de crisis de comunicación, aunque esto

se hizo desde un punto de vista político, para desplegar acciones en caso de que actores que inciden en la opinión pública del país comprometieran la reputación o desinformaran sobre la entidad.

En términos generales, la Agencia muestra en su estructura y gestión acciones relacionadas con continuidad, tal como se ha expuesto, pero tiene una serie de brechas por cerrar, que le implican establecer nuevas acciones, de manera sistemática e integral, si pretende avanzar frente a los requerimientos de la ISO de continuidad.

Estas acciones —que se evidenciaron en relación con los requisitos de la norma de continuidad— se sintetizan en la "Lista de chequeo ISO 22301:2012", que permite tener una visión integrada y rápida sobre la Agencia en relación con los requisitos de la norma.

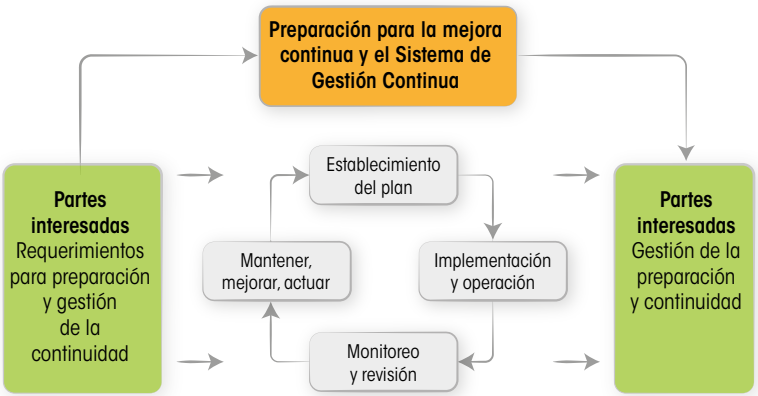

Figura 7. Ciclo PHVA aplicado al proceso de continuidad del negocio.
Fuente: ISO (2012).

Capítulo 3

Escenarios de falla y riesgos de continuidad del negocio en la entidad

En este capítulo se presentan los escenarios de falla y los riesgos de continuidad que los colaboradores entrevistados pudieron identificar y valorar. Se expone, en principio, un análisis general para la entidad y, posteriormente, para cada proceso.

Para favorecer la lectura y comprensión de los resultados presentados a continuación, primero se expondrán brevemente elementos de la metodología aplicados para la identificación y valoración de los escenarios de falla.

Identificación y valoración de escenarios de falla

Con el fin de identificar y valorar los escenarios de falla, se presentaron los escenarios de falla comunes en continuidad y, a partir de ellos, los colaboradores entrevistados identificaron los principales eventos disruptivos que pueden presentarse en cada uno de los procesos que pudiesen potencialmente interrumpir las operaciones y generar impacto sobre la entrega de servicios y beneficios a las PPR. Luego, se identificaron los riesgos de continuidad asociados a cada evento y escenario de falla y se plasmaron en la matriz de valoración de escenarios e identificación de riesgos.

En la aplicación de las entrevistas, no se identificaron eventos y riesgos de continuidad que pudieran sugerir o plantear la definición de otro escenario de falla que deba ser considerado.

Identificación y valoración de riesgos de continuidad

La identificación y valoración de riesgos de continuidad fue realizada por los colaboradores entrevistados en cada proceso, quienes, a partir del conocimiento que tienen de la entidad y del proceso al que pertenecen, identificaron y valoraron para dicho proceso los riesgos de continuidad asociados a cada evento disruptivo y escenario de falla previamente identificado.

Uno de los elementos del análisis del riesgo está orientado a establecer la probabilidad de ocurrencia y sus consecuencias, entendiendo la *probabilidad* como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de *frecuencia* —si se ha materializado— o de *factibilidad*, si es posible que se materialice teniendo en cuenta la presencia de factores internos y externos que puedan favorecer el riesgo (DAFP, 2014).

El *impacto* se entiende como las consecuencias que puede causar a la organización la materialización del riesgo (DAFP, 2014). El *análisis de impacto* es una técnica de evaluación que usan los niveles gerenciales para determinar los impactos potenciales asociados con una interrupción significativa de las operaciones de la organización. Las medidas cualitativas de probabilidad e impacto para valorar los escenarios de falla y riesgos de continuidad se definen en la tabla 5.

Tabla 5. Valoración de escenarios de falla y riesgos de continuidad

Probabilidad (PROB)		
Criterio	**Descripción**	**Calificación**
Raro	Eventos de interrupción de la operación que pueden ocurrir solo en circunstancias excepcionales.	1
Posible	Eventos de interrupción de la operación que pueden ocurrir en algún momento.	2
Probable	Eventos de interrupción de la operación que probablemente ocurrirán en la mayoría de las circunstancias.	3
Casi seguro	Eventos de interrupción de la operación que ocurrirán en la mayoría de las circunstancias.	4

Impacto (IMP)		
Criterio	Descripción	Calificación
Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.	1
Menor	Si el hecho llegara a presentarse, tendría bajo impacto sobre la entidad.	2
Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias sobre la entidad.	3
Mayor	Si el hecho llegara a presentarse, tendría grandes consecuencias sobre la entidad.	4

Fuente: elaboración propia con base en DAFP (2014).

Una vez calificada la probabilidad y el impacto del riesgo de continuidad objeto de análisis, se obtiene la información para establecer el nivel de riesgo según su ubicación en el *mapa de calor,* también conocido como *Matriz de calificación, evaluación y respuesta a los riesgos*. Esta matriz contiene un análisis cualitativo, que muestra la magnitud de las consecuencias (impacto) y la posibilidad de ocurrencia (probabilidad) (figura 8).

Probabilidad	Impacto			
	(1) Insignificante	(2) Menor	(3) Moderado	(4) Mayor
(1) Raro	Bajo	Bajo	Moderado	Alto
(2) Posible	Bajo	Moderado	Alto	Extremo
(3) Probable	Moderado	Alto	Alto	Extremo
(4) Casi seguro	Alto	Alto	Extremo	Extremo

Figura 8. Matriz de calificación, evaluación y respuesta a los riesgos.
Fuente: elaboración propia con base en DAFP (2014).

La ubicación del riesgo en la matriz puede orientar a la entidad en la definición de la política de tratamiento, la priorización de intervención y las acciones por implementar. El DAFP (2014) recomienda las siguientes políticas de tratamiento:

- *Zona de riesgo baja (B)*. Asumir el riesgo.
- *Zona de riesgo moderada (M)*. Asumir el riesgo. Reducir el riesgo.
- *Zona de riesgo alta (A).* Reducir el riesgo. Evitar, compartir o transferir.
- *Zona de riesgo extrema (E).* Reducir el riesgo. Evitar, compartir o transferir.

Luego de la valoración de los riesgos de continuidad y para facilitar su análisis y establecer recomendaciones, estos fueron agrupados por afinidad en seis categorías así: personas, procesos, tecnología, infraestructura física, gerenciales y financieros.

Cada una de las categorías anteriores recoge en su interior elementos considerados como desestabilizadores de la continuidad y se presentan a continuación en forma general:

- *Personas:* riesgos relacionados con la gestión de conocimiento, seguridad física o laboral, administración de personal.
- *Procesos:* riesgos relacionados con la gestión del proceso, proveedores y soporte de tecnología.
- *Tecnología:* riesgos relacionados con la confiabilidad, disponibilidad, integridad y recuperabilidad de la información.
- *Infraestructura física:* riesgos relacionados con la preparación ante emergencias, incendios, fluido eléctrico, seguridad, acceso y estado general de instalaciones.
- *Gerenciales:* riesgos de continuidad relacionados con políticas, directrices, rediseño organizacional.
- *Financieros:* riesgos relacionados con la provisión de recursos económicos.

Tipología del riesgo

Según el DAFP (2014), los riesgos pueden clasificarse por su tipología, así:

- Riesgos estratégicos
- Riesgos de imagen

- Riesgos operativos
- Riesgos financieros
- Riesgos de cumplimiento
- Riesgos de tecnología
- Riesgos de corrupción

Teniendo en cuenta estos lineamientos, se realizó un ejercicio de clasificación de los riesgos de continuidad según su tipología en la Matriz de valoración de riesgos (anexo), con el fin de facilitar la formulación de políticas de operación para su tratamiento y determinar el impacto durante el proceso de análisis del riesgo contemplado en la metodología del DAFP.

3.1 Escenarios de falla en la entidad

A partir de los resultados de la calificación asignada a los escenarios de falla en cada proceso, se calculó la valoración promedio de estos para la entidad, con el fin de identificar, de manera global, el nivel de riesgo que representa cada escenario. Los resultados se presentan en la tabla 6.

Tabla 6. Valoración de escenarios de falla en la ARN

Identificador	Escenarios	Probabilidad	Impacto	Nivel de riesgo	Zona de riesgo
1	Escenario de falla tecnológica	2	3	6	Alto
2	Escenario de inhabilidad de la sede	2	2	4	Moderado
3	Escenario de inhabilidad de línea de atención o intervención de las PPR	2	4	8	Extremo
4	Escenario de desabastecimiento de bienes y servicios	2	3	6	Alto
5	Escenario de desastre nacional o regional	2	3	6	Alto
6	Escenario de inhabilidad legal	3	4	12	Extremo

Continúa...

... viene

Identificador	Escenarios	Probabilidad	Impacto	Nivel de riesgo	Zona de riesgo
7	Escenario de inhabilidad financiera	4	3	12	Extremo
8	Escenario de paro de personal	2	3	6	Alto
9	Escenario de sucesión de poder	3	4	12	Extremo

Fuente: elaboración propia.

Al ubicar los resultados de la valoración de los nueve escenarios en el mapa de calor, se obtiene la figura 9.

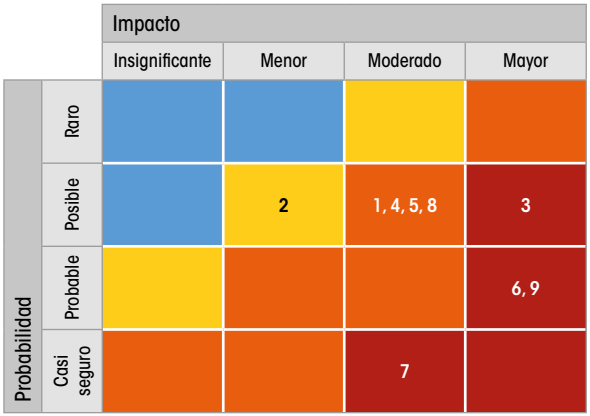

Figura 9. Mapa de calor de escenarios de falla en la ARN.
Fuente: elaboración propia según Matriz de valoración de riesgos.

En el mapa de calor se puede identificar que cuando los escenarios son evaluados de manera separada de los riesgos, resultan calificados en su mayoría con una probabilidad de *posible* y con un impacto de *moderado* a *mayor*. Además, como el nivel de riesgo es una combinación de probabilidad e impacto, predomina la ubicación de los escenarios en zonas de riesgo *alto* y *extremo*, y se encuentran en este cuadrante ocho de los nueve escenarios evaluados.

Uno de los criterios de priorización que se puede aplicar para intervenir los escenarios es su ubicación en el mapa de calor. Si se usa como referencia este criterio, los principales escenarios de falla en la entidad son los ubicados en zona de riesgo *extremo*: inhabilidad financiera, sucesión de poder, inhabilidad legal e inhabilidad

en la línea de atención o intervención. Por su parte, el escenario con menor severidad calificada es inhabilidad de sede, que alcanza apenas un nivel de riesgo moderado.

Al contrastar la evaluación independiente de los escenarios, tal como fue realizada por los colaboradores, con la evaluación de estos a partir de la valoración de los riesgos de continuidad contenidos en cada uno, los resultados difieren un poco. Esta resulta ser una evaluación de mayor utilidad, pues se calcula tomando en consideración los riesgos de continuidad identificados en cada escenario de falla. Para este caso, los resultados se muestran en la figura 10.

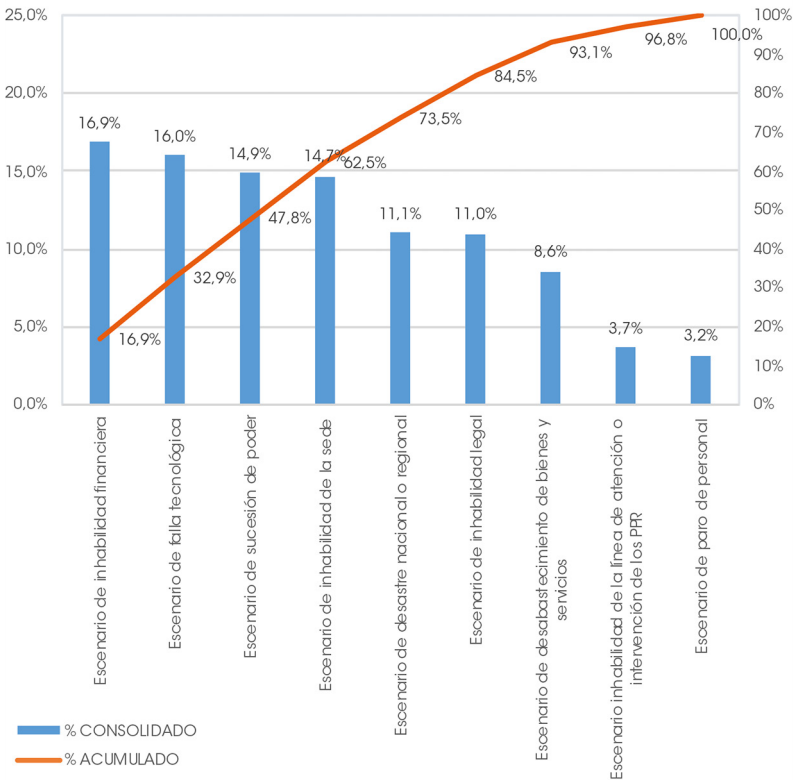

Figura 10. Participación de escenarios de falla según nivel de riesgo de continuidad en la ARN.
Fuente: elaboración propia según Matriz de valoración de riesgos.

Cuando se revisa la gráfica de participación de escenarios de falla en nivel de riesgos de continuidad en la ARN, se encuentra

que cuatro escenarios (inhabilidad financiera, falla tecnológica, sucesión de poder, e inhabilidad de la sede) agrupan el 62,5 % de la suma del nivel de riesgos de continuidad en la entidad y se constituyen en los principales escenarios de intervención, dado el nivel de riesgo asociado a estos.

Los demás escenarios (en su orden, desastre nacional o regional, inhabilidad legal, desabastecimiento de bienes y servicios, inhabilidad de la línea de atención o intervención de las PPR, y paro de personal) agrupan el 37,6 % del nivel de riesgos de continuidad.

Los riesgos asociados a cada escenario tienen como fuente factores externos y en esta clasificación se encuentran, en orden de importancia por su participación en el nivel de riesgos totales de la entidad, los escenarios de inhabilidad financiera (16,9 %), sucesión de poder (14,5 %) e inhabilidad legal (11 %). Los riesgos asociados a los demás escenarios son originados por factores internos de la entidad y, por tanto, para ellos podrían implementarse estrategias y acciones de control de manera más inmediata. En esta clasificación aparecen, según orden de importancia, los escenarios de falla tecnológica (16 %), inhabilidad de la sede (14,7 %), desastre nacional o regional (11,1 %), desabastecimiento de bienes y servicios (8,6 %), inhabilidad de la línea de atención o intervención de las PPR (3,7 %) y paro de personal (3,2 %).

Al revisar los resultados en función de la cantidad de riesgos identificados en cada escenario, se encontró que, de un total de 223 riesgos de continuidad identificados, el 53 % de ellos se encuentran asociados a los escenarios de falla tecnológica, inhabilidad de la sede, y desastre nacional o regional, los cuales agrupan el 51 % del total de riesgos identificados. Los resultados se pueden ver en la tabla 7.

Tabla 7. Frecuencia de riesgos en cada escenario de falla

Escenario	Cantidad de riesgos
Escenario de falla tecnológica	44
Escenario de inhabilidad de la sede	38
Escenario de desastre nacional o regional	31
Escenario de inhabilidad financiera	26
Escenario de sucesión de poder	25

Escenario	Cantidad de riesgos
Escenario de desabastecimiento de bienes y servicios	21
Escenario de inhabilidad legal	21
Escenario de inhabilidad de la línea de atención o intervención de los PPR	9
Escenario de paro de personal	8

Fuente: elaboración propia según Matriz de valoración de riesgos.

Al revisar los resultados en función del nivel de riesgo de cada escenario y la cantidad de riesgos en estos, se puede evidenciar la importancia que asumen, en su orden, los escenarios de falla tecnológica, inhabilidad financiera e inhabilidad de sede.

Los riesgos contenidos en el escenario de falla tecnológica están principalmente asociados al evento de fallas en los sistemas de información de la entidad y el centro de datos. Estos riesgos se clasifican en la categoría *tecnología* y están relacionados con la confiabilidad, disponibilidad, integridad y recuperabilidad de la información.

Los riesgos en relación con el escenario de inhabilidad financiera se asocian principalmente con el evento de limitación de recursos económicos. Estos riesgos se clasifican en la categoría *financieros,* en la cual se relacionan los riesgos de provisión de recursos económicos requeridos para el normal funcionamiento de la entidad.

Los riesgos frente al escenario de inhabilidad de la sede se asocian en su mayoría a eventos como marchas, problemas de orden público y amenazas de atentado. Estos riesgos se clasifican en la categoría *personas* y están relacionados con seguridad física o laboral, gestión de conocimiento y aspectos de la administración de personal.

En cuanto a los eventos disruptivos presentes en los escenarios de falla evaluados, en la tabla 8 se relacionan los más relevantes, teniendo en cuenta el criterio de frecuencia de aparición en los diferentes procesos. Estos eventos representan el 54 % del total identificado.

Tabla 8. Principales eventos de continuidad en la ARN

Principales eventos de continuidad	Frecuencia
Sismo con destrucción parcial o total de la edificación	15
Ajuste de estructura y actividades del personal	14
Marchas con problemas de orden público y amenazas de atentado	13
Fallas en infraestructura / Rotura de tuberías y canales	11
Fallas en sistemas de información y centros de datos	10
Sabotaje informático	10
Limitación de recursos económicos	8
Propagación de fuego en la sede central	8
Cambio del *staff* en la ARN	7
Presencia de inundaciones por fallas en tuberías y canales	7
Cambios en el marco jurídico regulatorio de la función institucional	6
Fallas en equipos de cómputo y *software*	6
Fallas en infraestructura (eléctrica, hidráulica, mecánica) por antigüedad de la sede	6

Fuente: elaboración propia según Matriz de valoración de escenarios e identificación de riesgos.

3.2 Riesgos de continuidad en la entidad

Se identificaron riesgos de continuidad —muchos de ellos con diferentes frecuencias, lo cual obedece a que un mismo riesgo pudo ser identificado en varios procesos y valorado de manera diferente—, distribuidos según frecuencia (figura 11).

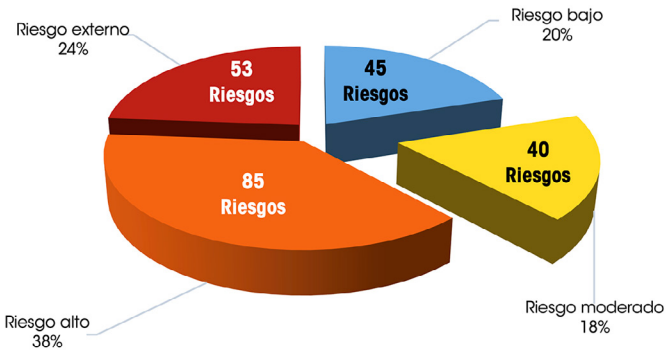

Figura 11. Composición del riesgo por zonas.
Fuente: elaboración propia según Matriz de valoración de riesgos.

Al representar los riesgos de continuidad en el mapa de calor, tomando en cuenta los criterios de probabilidad e impacto, se distribuyen como muestra la figura 12.

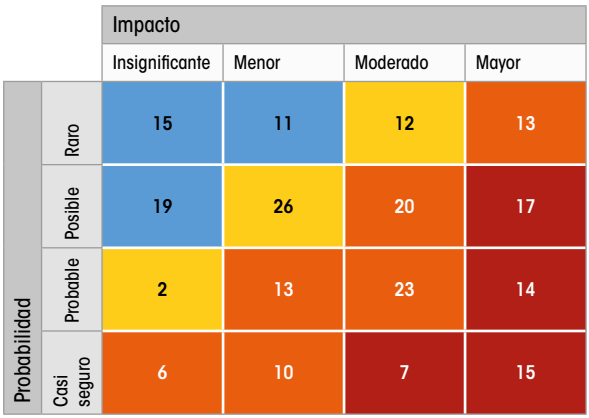

Figura 12. Mapa de calor - Riesgos de continuidad en la ARN.
Fuente: elaboración propia según Matriz de valoración de riesgos.

De acuerdo con la escala de valoración de riesgo aplicada y los resultados mostrados en el mapa de calor, la entidad tiene 53 riesgos de continuidad en la zona extrema, los cuales representan el máximo nivel de riesgo. Al revisar en detalle los riesgos de continuidad para la entidad ubicados en la zona extrema y los eventos asociados a estos encontramos:

En la categoría de riesgos *gerenciales,* se presentan ajustes en el direccionamiento estratégico, incumplimiento del plan nacional de desarrollo y del objeto de la Agencia, inobservancia normativa y de la función pública, rehechura de la planeación y el direccionamiento institucional, y cambio de los perfiles de los asesores. Estos riesgos son originados principalmente por eventos como redireccionamiento de la política de reintegración, cambios en el marco del proceso de reintegración —y, por ende, de la normatividad interna de la entidad—, ajustes y reducción de metas del plan estratégico, y cambio del *staff* en la entidad.

Identificados en la categoría de riesgos *financieros*, se destacan los riesgos de continuidad, tales como incumplimiento de compromisos normativos con riesgo para la entidad y sanciones o multas. Estos riesgos son originados por eventos de limitación de recursos económicos.

En la categoría de riesgos de *infraestructura física*, los principales riesgos de continuidad para la entidad son: daños a los activos de la sede, pérdida de información, demoras en cargue y reprocesos de la información, pérdida de servicios de comunicación, procesamiento de datos y reprocesos. Estos riesgos son originados principalmente en eventos como fallas en infraestructura o rotura de tuberías y canales, sismo con destrucción parcial o total de la edificación e interrupción del fluido eléctrico.

En la categoría de *personas*, se encuentran en zona extrema los riesgos de pérdida de la experiencia y de la memoria de la institución, afectación de la seguridad o la vida de funcionarios, daño a la sede o a colaboradores con interrupción del servicio, pérdida de la curva de conocimiento del proceso de reintegración y pérdida de oportunidad en los procesos por desarrollo de la curva de aprendizaje del nuevo personal. Dichos riesgos tienen su origen en eventos relacionados con cambio de la línea estratégica, marchas con problemas de orden público y amenazas de atentado, concurso de méritos por los cargos de la entidad, renovación o cambio del personal como consecuencia de concursos, y cambios en el marco jurídico regulatorio de la función institucional.

Agrupados en la categoría *procesos,* se presentan riesgos como demoras en atención a las PPR por falta de capacidad del proceso, insatisfacción en el servicio de las PPR, pérdida de información y de los activos requeridos para la prestación del servicio, intermitencia en el servicio, cese de operaciones en procesos, no cumplimiento de metas y compromisos con pérdida de confiabilidad en el proceso o pérdida de oportunidad en los procesos por desarrollo de la curva de aprendizaje de nuevo personal. Los eventos identificados como fuentes de estos riesgos son: cambios en el marco jurídico regulatorio de la función institucional, fallas en suscripción de convenios con demoras en entrega de bienes o servicios, ajuste de estructura y actividades del personal, pérdida o robo de equipos, limitación de recursos económicos y renovación o cambio del personal como consecuencia de concursos.

Por su parte, en la categoría *tecnología*, se encuentran en zona de riesgo extremo la fuga de información sensible del proceso de reintegración, pérdida de información, demoras en cargue y reprocesos de la información y demoras en acceso y manejo de información. Estos riesgos están asociados a eventos como fallas en

sistemas de información y centros de datos, sabotaje informático y fallas en equipos de cómputo y *software*.

En la tabla 9 se presentan los principales riesgos de continuidad para esta entidad. Aquí se tienen en cuenta aquellos con la máxima calificación de probabilidad (4) y la máxima calificación de impacto (4), para un nivel de riesgo de 16.

Tabla 9. Máximo nivel de riesgo

Escenario	Evento asociado	Riesgo de continuidad
Escenario de inhabilidad legal	Cambios en el marco jurídico regulatorio de la función institucional	Demoras en atención a las PPR por falta de capacidad del proceso
Escenario de inhabilidad legal	Cambios en el marco del proceso de reintegración	Ajustes en el contexto estratégico: administrativo, misional y tecnológico
Escenario de inhabilidad legal	Cambios en la normatividad interna de la ARN	Pérdida de sinergia entre procesos y necesidad de fijación de nuevos criterios técnicos
Escenario de inhabilidad financiera	Ajustes y reducción de metas del plan estratégico	Incumplimiento del plan nacional de desarrollo y del objeto de la ARN
Escenario de inhabilidad financiera	Ajustes a la política de la función pública	Incumplimiento normativo y de la función pública
Escenario de sucesión de poder	Redireccionamiento de la política del proceso de reintegración y de la estrategia	Rehacer la planeación y el direccionamiento institucional
Escenario de sucesión de poder	Cambio del *staff* en la ARN	Cambio de los perfiles de los asesores. No aseguramiento de competencias.
Escenario de falla tecnológica	Fallas en equipos de cómputo y *software*	Demoras en acceso y manejo de información
Escenario de inhabilidad financiera	Limitación de recursos económicos	Falta de disponibilidad de recursos
Escenario de inhabilidad financiera	Ajuste de estructura y actividades del personal	Incumplimiento del plan nacional de desarrollo y del objeto de la ARN
Escenario de sucesión de poder	Cambio del *staff* en la ARN	Rehacer la planeación y el direccionamiento institucional
Escenario de sucesión de poder	Renovación o cambio del personal como consecuencia de concursos	Pérdida de oportunidad en los procesos por desarrollo de la curva de aprendizaje del nuevo personal
Escenario de inhabilidad financiera	Limitación de recursos económicos	Cese de operaciones en procesos y de atención a visitantes
Escenario de inhabilidad financiera	Limitación de recursos económicos	Incumplimiento en compromisos normativos con riesgo para la entidad

Fuente: elaboración propia según Matriz de valoración de riesgos.

Localizados en la zona de riesgo alto, se encuentran 85 riesgos relacionados principalmente con la disponibilidad de recursos, cambios de lineamientos o directrices, pérdida de información, inhabilidad de *software*, daños en la infraestructura física, intermitencia o cese de operaciones en los procesos, daño de información física, afectación a la salud del trabajador, pérdida de confianza en la institución y en el proceso de reintegración, incumplimiento normativo y de la función pública, daños a los activos en la sede, pérdida de información física e interrupción del servicio a las PPR.

En la zona de riesgo moderado y bajo se encuentran 85 riesgos de continuidad, los cuales se relacionan principalmente con pérdida de servicios de comunicación y procesamiento de datos, bloqueo de canales formales de comunicación con las PPR, daño a la sede o a colaboradores con interrupción del servicio, bloqueo en el ingreso a la sede por huelga de trabajadores, daños a los activos en la sede y pérdida de información física, demoras en atención a las PPR por falta de capacidad del proceso, imposibilidad de acceder a la sede por motivos de orden público y falta de cumplimiento de proveedores.

Es importante aclarar que, en muchos de los casos, los procesos identificaron riesgos comunes, pero al valorarlos la calificación fue diferente. Lo anterior puede estar influido por la percepción y el conocimiento de los colaboradores entrevistados frente al proceso y el riesgo evaluado. Asimismo, en cada proceso, de acuerdo con su propósito y sus condiciones, la probabilidad de materialización del riesgo es diferente y en caso de que ocurra puede tener impactos diversos. Es así como encontramos riesgos de continuidad similares en las diferentes zonas de riesgo.

Otro de los resultados para el análisis de los riesgos en la entidad es su *frecuencia* de aparición. En este caso, se encontró que los riesgos relacionados con la pérdida de información, las demoras en acceso y manejo de información, la fuga de información sensible, y el daño a la sede o a colaboradores fueron identificados como los de mayor frecuencia en la mayoría de los procesos e incluso en un mismo proceso en diferentes escenarios de falla. Lo anterior puede deberse a que, como son riesgos transversales, todos o la mayoría de los procesos encuentran que están expuestos a ellos y pueden ser afectados por su materialización.

En la tabla 10 se muestran once riesgos, que suman una frecuencia de 113 apariciones, lo cual corresponde al 50,7 % de la totalidad de riesgos identificados y distribuidos en los principales riesgos de continuidad según su frecuencia.

Tabla 10. Principales riesgos según frecuencia

Principales riesgos de continuidad según frecuencia	Categoría del riesgo	Frecuencia
Pérdida de información, demoras en cargue y reprocesos de la información	Procesos	18
Daños a la sede o a colaboradores con interrupción del servicio	Infraestructura física	15
Daños a los activos en la sede y pérdida de información física	Infraestructura física	12
Afectación de la seguridad o la vida de funcionarios	Personas	10
Cese de operaciones en procesos y de atención a visitantes	Infraestructura física y Procesos	10
Demoras en acceso y manejo de información	Tecnología	10
Fuga de información sensible del proceso de reintegración	Tecnología	10
Cambios en la estructura de la ARN	Personas	8
Demoras en atención a las PPR por falta de capacidad del proceso	Procesos	8
Daño de información física y afectación a la salud del trabajador	Infraestructura física	7
Imposibilidad de acceder a la sede por daños en infraestructura con pérdida de documentos	Infraestructura física	5

Fuente: elaboración propia según Matriz de valoración de riesgos.

Al realizar la clasificación de los riesgos de continuidad identificados en la entidad, se encontró que las categorías de *procesos* e *infraestructura física* concentran la mayor cantidad de riesgos, lo que se puede entender porque los colaboradores identificaron —en los 16 procesos y en diferentes escenarios— eventos de continuidad y riegos asociados con la intermitencia en el servicio a las PPR o en la operación de los procesos, pérdida de capacidad del proceso, incumplimientos normativos, de metas y de informes y fallas en infraestructura física (eléctrica, hidráulica, mecánica) por antigüedad de las actuales instalaciones de la entidad.

Sin embargo, las categorías *gerenciales* y *financieros* contienen la mayor severidad de los riesgos identificados en relación con la frecuencia de riesgos contenida en estas categorías. Aquí se agrupan

riesgos y eventos relacionados con cambios en la política y el marco regulatorio del proceso de reintegración, cambios en el direccionamiento institucional y limitación de recursos financieros, principalmente. Los colaboradores los perciben con niveles de riesgo alto y extremo, dada la situación del contexto vigente de la entidad por las actuales negociaciones del proceso de paz.

Tabla 11. Frecuencia y nivel de riesgo por categorías

Categorias de riesgo	Frecuencia	Nivel de riesgo
Procesos: riesgos relacionados con la gestión del proceso, proveedores y soporte de tecnología.	70	465
Infraestructura física: riesgos relacionados con la preparación ante emergencias, incendios, fluido eléctrico, seguridad, acceso y estado general de instalaciones.	55	289
Personas: riesgos relacionados con la gestión de conocimiento, seguridad física o laboral y administración de personal.	38	236
Tecnología: riesgos relacionados con la confiabilidad, disponibilidad, integridad y recuperabilidad de la información.	35	181
Gerenciales: riesgos de continuidad relacionados con políticas, directrices y rediseño organizacional.	17	171
Financieros: riesgos relacionados con la provisión de recursos económicos.	8	68

Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3 Escenarios de falla y riesgos de continuidad por proceso

Los resultados que aquí se presentan recogen las percepciones, opiniones y valoración de escenarios de falla y riesgos de continuidad identificados por los colaboradores entrevistados en cada proceso. Se relacionan, además, dichos riesgos y escenarios con los eventos disruptivos que pueden presentarse en cada proceso y ser potenciadores de la materialización del riesgo identificado.

Adicionalmente, se presentan las recomendaciones que hacen los colaboradores de cada proceso frente a los riesgos valorados y que, según estos colaboradores, la entidad estaría en capacidad de implementar.

3.3.1 Proceso de direccionamiento estratégico

Este proceso tiene como propósito "establecer las políticas, directrices, planes y recursos que orienten la gestión de la entidad hacia el cumplimiento de la función institucional con eficacia, eficiencia y efectividad" (Caracterización del proceso de direccionamiento estratégico, versión 5, 2016).

Tomando como punto de partida el quehacer del proceso, los colaboradores entrevistados identificaron los riesgos que se muestran en la tabla 12, que pueden afectar la continuidad del proceso.

Tabla 12. Riesgos de continuidad - Direccionamiento estratégico

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Direccionamiento estratégico	1	Incumplimiento legal en reportes de información y oportuna comunicación (falla de sistema de información)	6	Alto
	2	Incumplimiento legal en reportes de información y oportuna comunicación (falla de telecomunicaciones)	6	Alto
	3	Pérdida de información, demoras en cargue y reprocesos de la información	8	Extremo
	4	Demoras en atención a las PPR por falta de capacidad del proceso	16	Extremo
	5	Ajustes en el contexto estratégico: administrativo, misional y tecnológico	16	Extremo
	6	Pérdida de sinergia entre procesos y necesidad de fijación de nuevos criterios técnicos	16	Extremo
	7	Incumplimiento del plan nacional de desarrollo y del objeto de la entidad	16	Extremo
	8	Incumplimiento normativo y de la función pública	16	Extremo
	9	Rehacer la planeación y el direccionamiento institucional	16	Extremo
	10	Cambio de los perfiles de los asesores, talento humano con experiencia	16	Extremo

Fuente: elaboración propia según Matriz de valoración de riesgos.

Teniendo en cuenta los riesgos identificados y valorados, los principales escenarios de falla son: inhabilidad legal, inhabilidad financiera y sucesión de poder, originados en la materialización de eventos como cambios en el marco jurídico regulatorio de la función institucional, cambios en el marco del proceso de reintegración, cambios en la normatividad interna de la ARN, ajustes y

reducción de metas del plan estratégico, ajustes a la política de la función pública, redireccionamiento de la política y del proceso de reintegración y cambio del *staff* de la entidad.

Alrededor de estos eventos se identificaron 10 riesgos de continuidad, de los cuales el 80 % se ubica en zona extrema y el restante en zona de riesgo alta. Esta ubicación obedece a que los riesgos fueron valorados por el proceso con probabilidad de ocurrencia casi segura y un impacto mayor sobre la continuidad del proceso.

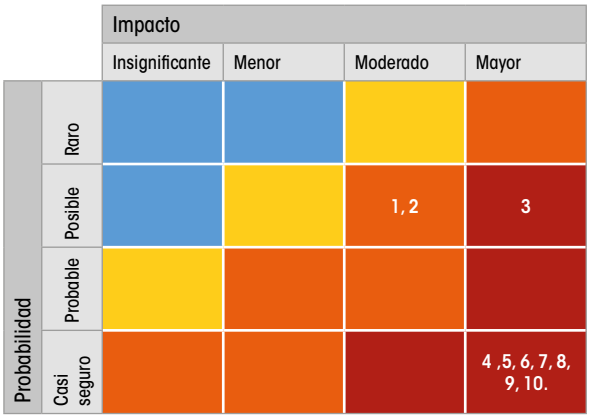

Figura 13. Mapa de calor - Direccionamiento estratégico.
Fuente: elaboración propia según Matriz de valoración de riesgos.

Por su frecuencia, el principal riesgo de continuidad es el incumplimiento legal en reportes de información y en la oportuna comunicación. Este riesgo se origina mayormente en el escenario de falla tecnológica como errores en los sistemas de información y telecomunicaciones, que afectan la obtención y procesamiento de información necesaria para la planeación, direccionamiento institucional y generación de informes; por ejemplo, los de cumplimiento de metas en los diferentes niveles de planeación, informes de tipo presupuestal o para organismos de control y vigilancia de la gestión institucional.

Este proceso se ve altamente impactado por factores externos a la entidad, como los cambios en la normativa, políticas y estrategias del gobierno nacional respecto al proceso de paz, lo cual hace que al interior de la entidad el gobierno deba realizar ajustes organizacionales (en materia presupuestal, estructura, políticas

institucionales, entre otros). Este tipo de cambios puede generar en la entidad, mientras se acopla al nuevo direccionamiento, intermitencia en los procesos y pérdida de oportunidad de estos en la entrega de productos o servicios a su cargo.

3.3.2 Proceso de gestión de comunicaciones

Este proceso se encarga de "diseñar y ejecutar la comunicación interna y externa para contribuir con el cumplimiento de la misión y el mejoramiento de la cultura organizacional de la entidad" (Caracterización del proceso de gestión de comunicaciones, versión 5, 2016).

Como resultado de las entrevistas, los colaboradores identificaron para este proceso los riesgos de la tabla 13 como aquellos que podrían llegar a afectar la continuidad parcial o total de este.

Tabla 13. Riesgos de continuidad - Gestión de comunicaciones

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión de comunicaciones	1	Pérdida de servicios de comunicación, procesamiento de datos y reprocesos	4	Moderado
	2	Fuga de información sensible del proceso de reintegración	8	Extremo
	3	Inhabilidad del *software* para manejar los programas que son base de trabajo	8	Alto
	4	Daño de información física y afectación a la salud del trabajador	2	Bajo
	5	Afectación de la seguridad o la vida de funcionarios	2	Bajo
	6	Bloqueo de canales formales de comunicación con las PPR	3	Moderado
	7	Afectación de la seguridad de funcionarios y pérdida de equipos	2	Bajo
	8	Falta de disponibilidad de recursos y equipos para la operación del proceso	2	Bajo
	9	Intermitencia en el servicio de comunicaciones y operación del proceso	2	Bajo
	10	Daño a la sede o a colaboradores con interrupción del servicio	3	Moderado

Continúa...

... viene

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión de comunicaciones	11	Afectación de la seguridad o la vida de funcionarios	2	Bajo
	12	Cambios en la estructura de la ARN (funciones de trabajo)	6	Alto
	13	Cambios en la estructura de la ARN (carga laboral)	6	Alto
	14	Cambios en la estructura de la ARN (política de austeridad)	9	Alto
	15	Falta de disponibilidad de recursos	9	Alto
	16	Bloqueo en el ingreso a la sede por huelga de trabajadores	4	Moderado
	17	Fallas en continuidad del proceso por cambio de lineamientos	9	Alto

Fuente: elaboración propia según Matriz de valoración de riesgos.

En el proceso de la Gestión de comunicaciones, la ARN está expuesta a diferentes escenarios de falla y riesgos de continuidad, entre los que se destacan —por su ubicación en zonas de riesgo alto y extremo— los escenarios de falla tecnológica, inhabilidad legal, inhabilidad financiera y sucesión de poder. Los eventos de continuidad identificados en este proceso son sabotaje informático, falta de licencias de *software* en programas que son base de trabajo, ajuste de estructura y actividades del personal, limitación de recursos económicos y cambios en el marco jurídico regulatorio de la función institucional. Dichos eventos pueden desencadenar la materialización de riesgos de continuidad para el proceso, principalmente fuga de información sensible del proceso de reintegración, inhabilidad de *software*, cambios en la estructura de la ARN, falta de disponibilidad de recursos, y fallas en continuidad del proceso por cambio de lineamientos.

En el mapa de calor de riesgos de continuidad (figura 14), se observa que el 41 % de estos se ubica en las zonas de riesgo alto y extremo. Este proceso califica en zona extrema el riesgo de fuga de información sensible del proceso de reintegración, originado en eventos de sabotaje informático.

Por su frecuencia, el principal riesgo de continuidad radica en los cambios en la estructura de la ARN, que podría significar el no disponer del personal suficiente para el desarrollo de las actividades del proceso y el cumplimiento de las metas.

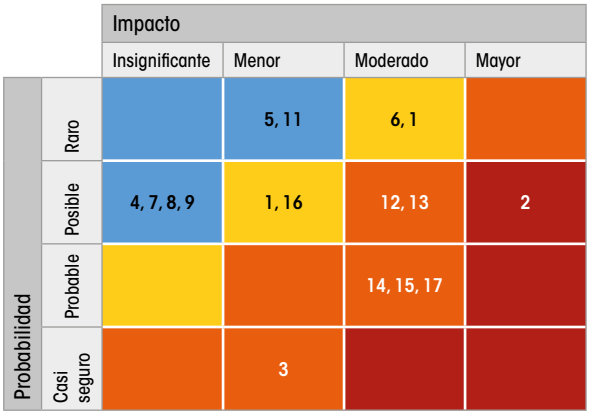

Figura 14. Mapa de calor - Gestión de comunicaciones.
Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3.3 Proceso de gestión de relaciones externas

El propósito de este proceso es "implementar acciones de posicionamiento y fortalecimiento de la política de reintegración a partir de la gestión con actores externos, para el mejoramiento del proceso de reintegración" (Caracterización en el proceso de gestión de relaciones externas, versión 3, 2016).

Los riesgos de continuidad que los colaboradores entrevistados identificaron para este proceso están consignados en la tabla 14.

Tabla 14. Riesgos de continuidad - Gestión de relaciones externas

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión de relaciones externas	1	Demoras en acceso y manejo de información	6	Alto
	2	Pérdida de servicios de comunicación, procesamiento de datos y reprocesos	3	Moderado
	3	Fuga de información sensible del proceso de reintegración	4	Alto
	4	Daños a los activos en la sede y pérdida de información física	12	Extremo
	5	Imposibilidad de acceder a la sede por motivos de orden público	1	Bajo

Continúa...

... viene

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión de relaciones externas	6	Daño de información física y afectación a la salud del trabajador (vectores)	8	Alto
	7	Daño de información física y afectación a la salud del trabajador (sismo)	4	Alto
	8	Pérdida de información, demoras en cargue y reprocesos de la información	8	Extremo
	9	Pérdida de imagen	8	Extremo
	10	Incumplimiento del plan nacional de desarrollo y del objeto de la ARN	12	Extremo
	11	No hay acompañamiento a regiones	9	Alto
	12	Pérdida de la experiencia y de la memoria de la institución	12	Extremo
	13	Pérdida de confianza en la institución y en el proceso de reintegración	9	Alto

Fuente: elaboración propia según Matriz de valoración de riesgos.

Por su ubicación en las zonas de riesgo alto y extremo, se identifican en este proceso como principales los escenarios de falla tecnológica, desastre nacional o regional, inhabilidad legal, inhabilidad financiera y sucesión de poder. En estos escenarios se identifican eventos disruptivos como sabotaje informático, fallas en infraestructura, sismo con destrucción parcial o total de la edificación, propagación de fuego en la sede central, cambios en el marco del proceso de reintegración, o cambio de la línea estratégica institucional.

En el mapa de calor se puede observar que el 84 % de los riesgos de continuidad identificados se encuentran en las zonas alta y extrema, con impactos entre moderado y mayor sobre la continuidad del proceso (figura 15).

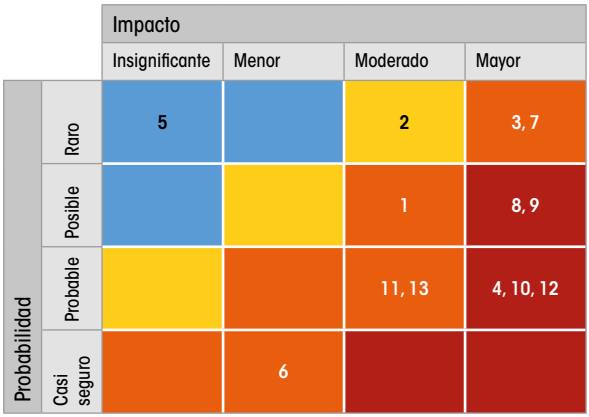

Figura 15. Mapa de calor - Gestión de relaciones externas.
Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3.4 Proceso de evaluación, control y mejoramiento

El propósito de este proceso es "evaluar en forma independiente la gestión institucional y asesorar en la definición e implementación de acciones, bajo los principios de autocontrol, autogestión y autorregulación, permitiendo la toma de decisiones para el mejoramiento continuo de la entidad" (Caracterización en el proceso de evaluación, control y mejoramiento, versión 5, 2016).

Los colaboradores de este proceso identificaron y valoraron los riesgos de continuidad; sus evaluaciones se muestran en la tabla 15.

Tabla 15. Riesgos de continuidad - Evaluación, control y mejoramiento

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Evaluación, control y mejoramiento	1	Pérdida de información, demoras en cargue y reprocesos de la información (Siger)	12	Extremo
	2	Pérdida de información, demoras en cargue y reprocesos de la información (SIR)	12	Extremo
	3	Fuga de información sensible del proceso de reintegración	12	Extremo
	4	Imposibilidad de acceder a la sede por daños en infraestructura con pérdida de documentos	4	Moderado

Continúa...

... viene

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Evaluación, control y mejoramiento	5	Daño de información física y afectación a la salud del trabajador	4	Moderado
	6	Afectación de la seguridad o la vida de funcionarios (problemas de orden público)	12	Extremo
	7	Intermitencia o retraso en la operatividad del proceso	4	Alto
	8	Daño a la sede o a colaboradores con interrupción del servicio	4	Moderado
	9	Afectación de la seguridad o vida de funcionarios (sismos)	4	Moderado
	10	Cambios en la estructura de la ARN	4	Alto
	11	Incumplimiento normativo y de la función pública (contratación de personal)	9	Alto
	12	Incumplimiento normativo y de la función pública (austeridad en el gasto)	9	Alto
	13	Bloqueo en el ingreso a la sede por huelga de trabajadores	3	Moderado
	14	Pérdida de la experiencia y de la memoria de la institución	4	Alto
	15	No independencia del proceso y falta de objetividad con implicaciones de corrupción	4	Alto

Fuente: elaboración propia según Matriz de valoración de riesgos.

Como principales escenarios de falla para este proceso se identifican, por su ubicación en zonas de riesgo alto y extremo, los siguientes: falla tecnológica, inhabilidad de la sede, inhabilidad legal, inhabilidad financiera y sucesión de poder. El escenario de falla tecnológica agrupa la mayor frecuencia de riesgos de continuidad, originados en la materialización de eventos como sabotaje informático y fallas en sistemas de información y centros de datos.

Entre los riesgos de continuidad a los que se expone el proceso, los más importantes son: pérdida de información, demoras en cargue y reprocesos de la información, fuga de información sensible del proceso de reintegración, intermitencia o retraso en la operatividad del proceso, cambios en la estructura de la ARN, incumplimiento normativo y de la función pública y pérdida de la experiencia y de la memoria de la institución.

En el mapa de calor se puede observar que el 62 % de los riesgos de continuidad identificados por los colaboradores del proceso se ubican en las zonas de riesgo alto y extremo, con impacto entre moderado y mayor (figura 16).

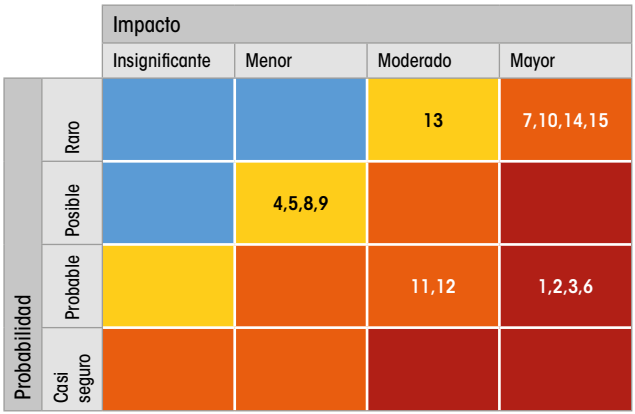

Figura 16. Mapa de calor - Evaluación, control y mejoramiento.
Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3.5 Proceso de diseño

Este proceso es responsable de "diseñar los lineamientos generales para el diseño (sic) de estrategias, lineamientos conceptuales, técnicos y metodológicos, herramientas y acciones requeridas del proceso de reintegración, de acuerdo con los mandatos legales y lineamientos establecidos por la entidad" (Caracterización en el proceso de diseño, versión 5, 2016).

Los colaboradores de las entrevistas identificaron y valoraron los riesgos de continuidad; los resultados se muestran en la tabla 15.

Tabla 16. Riesgos de continuidad - Diseño

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Diseño	1	Demoras en acceso y manejo de información (fallas en equipos de trabajo)	2	Bajo
	2	Demoras en acceso y manejo de información (fallas en telecomunicaciones)	2	Bajo
	3	Pérdida de información, demoras en cargue y reprocesos de la información	1	Bajo

Continúa...

... viene

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Diseño	4	Daños a los activos en la sede y pérdida de información física	2	Bajo
	5	Menor tiempo de trabajo en la sede central y afectación en la concentración en el trabajo	3	Moderado
	6	Daños a la sede o a colaboradores con interrupción del servicio	3	Moderado
	7	Cese de operaciones en procesos y en atención a visitantes	2	Bajo
	8	Intermitencia en el servicio (cambios en la planta de trabajadores)	4	Alto
	9	Cambios en la estructura de la ACR	2	Bajo
	10	Demoras en atención a las PPR por falta de capacidad del proceso	4	Alto
	11	Intermitencia en el servicio (disminución de viáticos)	4	Alto
	12	No hay acompañamiento a regiones	6	Alto
	13	Rehacer la planeación y el direccionamiento institucional	4	Moderado

Fuente: elaboración propia según Matriz de valoración de riesgos.

Como se observa en la tabla 15, los riesgos de mayor relevancia se encuentran en la zona de riesgo alto y están relacionados con la materialización de eventos, como ajustes de estructura en la entidad o actividades del personal y ajuste al proceso en servicio a regiones, lo cual puede exponer al proceso a riesgos como intermitencia en el servicio, demoras en atención a las PPR por falta de capacidad del proceso y no acompañamiento a regiones. Dichos riesgos se concentran principalmente en los escenarios de inhabilidad legal e inhabilidad financiera.

Al revisar el nivel de riesgo de los procesos tomando en consideración los ubicados en zonas alta y extrema, se encuentra que este proceso, por la valoración de sus riesgos, es el segundo con el nivel de riesgo más bajo. Lo anterior obedece a que los colaboradores consultados indicaron que los riesgos identificados en los seis escenarios pertinentes al proceso tienen un impacto insignificante en la continuidad del mismo y con probabilidades que van de posible a raro.

En el mapa de calor (figura 17) sobre ubicación de los riesgos de continuidad, se observa la agrupación de escenarios hacia la

izquierda, lo cual es consecuente con la apreciación del carácter insignificante o menor en el impacto que causarían, en caso de materializarse el riesgo.

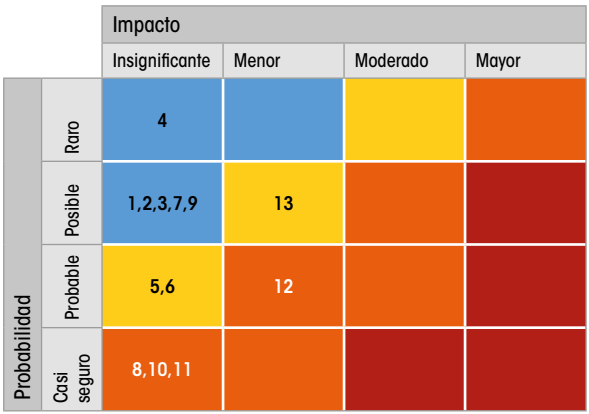

Figura 17. Mapa de calor - Diseño.
Fuente: elaboración propia según Matriz de valoración de riesgos.

Al considerar la frecuencia, el principal riesgo de continuidad es la demora en acceso y manejo de información, en razón de la dependencia a los equipos de cómputo para la realización del trabajo e igualmente a la necesidad de uso de telecomunicaciones en las actividades del proceso.

3.3.6 Proceso de implementación

El propósito de este proceso es "determinar los lineamientos técnicos y ejecutar las condiciones, beneficios, estrategias, metodologías y acciones a la población objeto, su grupo familiar y la comunidad receptora del proceso de reintegración, de manera oportuna y eficaz" (Caracterización del proceso de implementación, versión 6, 2016).

Tomando como punto de partida el quehacer del proceso, los colaboradores entrevistados identificaron los riesgos planteados en la tabla 17, que pueden afectar la continuidad del proceso.

Tabla 17. Riesgos de continuidad - Implementación

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Implementación	1	Pérdida de información, demoras en cargue y reprocesos de la información	12	Extremo
	2	Demoras en acceso y manejo de información (obsolescencia de equipos)	16	Extremo
	3	Demoras en acceso y manejo de información (demoras en soporte)	6	Alto
	4	Daño a la sede o a colaboradores con interrupción del servicio	12	Extremo
	5	Daños a los activos en la sede y pérdida de información física	9	Alto
	6	Cese de operaciones en procesos y de atención a visitantes	6	Alto
	7	Insatisfacción en el servicio de las PPR con reclamaciones judiciales	12	Extremo
	8	Intermitencia en el servicio	12	Extremo
	9	Intermitencia o retraso en la operatividad del proceso	2	Bajo
	10	Intermitencia en la operatividad del proceso, interrupción del servicio a las PPR	9	Alto
	11	Daño de información física y afectación a la salud del trabajador	6	Alto
	12	Pérdida de información, demoras en cargue y reprocesos de la información	6	Alto
	13	Cambios en la estructura de la ACR (nueva normatividad)	9	Alto
	14	Cambios en la estructura de la ACR (terminación de procesos a las PPR)	6	Alto
	15	Falta de disponibilidad de recursos	16	Extremo
	16	Cese de operaciones en procesos (incumplimiento de la misionalidad)	9	Alto
	17	Cese de operaciones en procesos (huelga)	3	Moderado
	18	Pérdida institucional de la curva de conocimiento del proceso de reintegración	12	Extremo
	19	Rehacer la planeación y el direccionamiento institucional	6	Alto

Fuente: elaboración propia según Matriz de valoración de riesgos.

Los riesgos contenidos en los escenarios de falla tecnológica e inhabilidad financiera son los que, de llegar a materializarse, presentan mayor severidad. Encontramos aquí los riesgos relacionados con fallas en equipos de cómputo y *software* (acceso y disponibilidad de la información) y limitación de recursos económicos requeridos para la ejecución del proceso de reintegración.

Otros escenarios que también son de importancia para el proceso Implementación son los de inhabilidad de la línea de atención o intervención de las PPR, desabastecimiento de bienes y servicios, y paro de personal. En estos escenarios se encuentran riesgos, como daño a la sede o a colaboradores con interrupción del servicio, insatisfacción en el servicio de las PPR con reclamaciones judiciales, intermitencia en el servicio, y pérdida institucional de la curva de conocimiento del proceso de reintegración. Estos riesgos están asociados a la materialización de eventos disruptivos como: marchas con problemas de orden público y amenazas de atentado, fallas en orientación oportuna del canal *call center*, fallas en suscripción de convenios o contratos con demoras en entrega de bienes o servicios o concursos de méritos por los cargos de la ARN.

Los riesgos de continuidad identificados y valorados en este proceso se encuentran casi en su totalidad en las zonas de riesgo alto y extremo, lo cual es comprensible si se tiene en consideración que este proceso es el responsable de la materialización de la oferta de servicios y beneficios de la entidad hacia la población objeto, y por tanto la materialización de un riesgo de continuidad podría afectar de manera directa a las PPR.

En el mapa de calor del proceso (figura 18), se puede observar la distribución de los riesgos en las diferentes zonas así: en zona de riesgo extremo el 35 %, en zona de riesgo alto el 53 % y en zonas de riesgo moderado y bajo el 5 % para cada una.

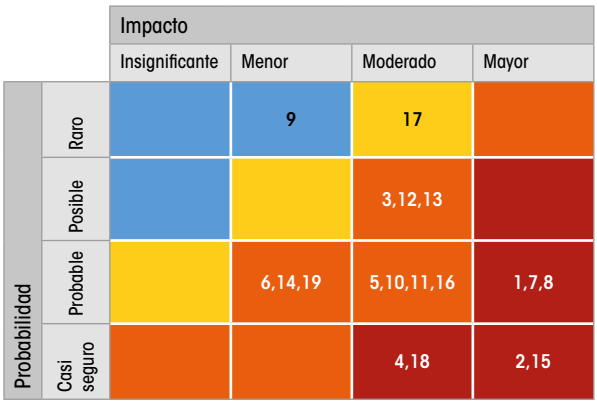

Figura 18. Mapa de calor - Implementación.
Fuente: elaboración propia según Matriz valoración riesgos.

El 90 % de los riesgos de continuidad en el proceso de implementación están en zonas de riesgo alto y extremo, lo cual debe ser analizado por la entidad a fin de definir acciones de priorización e intervención.

3.3.7 Proceso de seguimiento

El proceso de seguimiento se encarga de "desarrollar acciones de seguimiento y evaluación del proceso y la política de reintegración, proporcionando información y recomendaciones de manera oportuna como base para la toma de decisiones que contribuyan al mejoramiento de la función institucional" (Caracterización del proceso de seguimiento, versión 5, 2016)

Los colaboradores del proceso de Implementación identificaron y valoraron los riesgos de continuidad que se muestran en la tabla 18.

Tabla 18. Riesgos de continuidad - Seguimiento

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Seguimiento	1	Incumplimiento legal en reportes de información y oportuna comunicación	6	Alto
	2	Demoras en acceso y manejo de información	4	Moderado
	3	Fuga de información sensible del proceso de reintegración	4	Alto
	4	Daños a los activos en la sede y pérdida de información física	8	Alto
	5	Cese de operaciones en procesos y de atención a visitantes (marchas)	9	Alto
	6	Cese de operaciones en procesos y de atención a visitantes (infraestructura)	6	Alto
	7	Afectación de la seguridad o la vida de funcionarios	8	Extremo
	8	Cese de operaciones en procesos y de atención a visitantes (sismo)	4	Alto
	9	Ajustes en el contexto estratégico: administrativo, misional y tecnológico	4	Alto
	10	Cambios en la estructura de la ACR	8	Extremo
	11	Incumplimiento normativo y de la función pública	8	Alto

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Seguimiento	12	Incumplimiento del plan nacional de desarrollo y del objeto de la ACR	16	Extremo
	13	Rehacer la planeación y el direccionamiento institucional	2	Bajo
	14	Ajuste organizacional para responder a nuevas políticas	2	Bajo

Fuente: elaboración propia según Matriz de valoración de riesgos.

Los principales escenarios de falla que concentran los riesgos valorados en zonas de riesgo alto y extremo son: falla tecnológica, inhabilidad de la sede, desastre nacional o regional, inhabilidad legal e inhabilidad financiera. A estos escenarios encontramos asociados eventos disruptivos como fallas en sistemas de información y centros de datos, sabotaje informático, marchas con problemas de orden público y amenazas de atentado, fallas en infraestructura (eléctrica, hidráulica, mecánica) por antigüedad de la sede, sismo con destrucción parcial o total de la edificación, propagación de fuego en la sede central, cambios en el marco jurídico regulatorio de la función institucional y del proceso de reintegración, ajuste de estructura y actividades del personal, principalmente.

En el mapa de calor del proceso de seguimiento (figura 19) se puede observar que el 79 % de los riesgos del proceso se ubican en las zonas de riesgo alto y extremo.

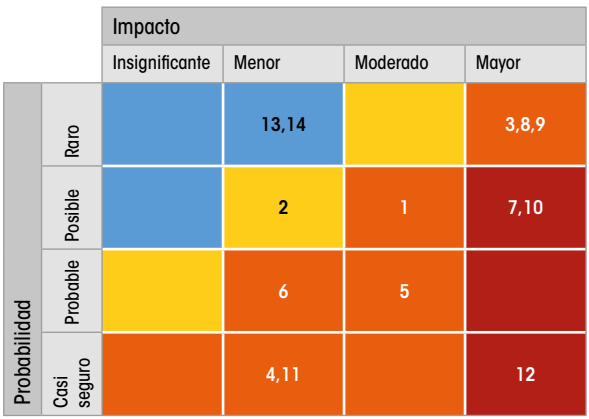

Figura 19. Mapa de calor - Seguimiento.
Fuente: elaboración propia según Matriz de valoración de riesgos.

Por su frecuencia, el principal riesgo de continuidad es el cese de las operaciones y de la atención a visitantes, en el caso de que no se permita el ingreso o uso de las instalaciones. Esto puede ser ocasionado por eventos como marchas o daño de la infraestructura de la sede central.

3.3.8 Proceso de gestión legal

El proceso de gestión legal es el encargado de "estructurar y liderar la gestión legal del proceso de reintegración mediante la orientación oportuna para el acceso y terminación del proceso, la aplicación de los beneficios jurídicos a las PPR, y la instrucción y decisión de los procesos administrativos sancionatorios" (Caracterización del proceso de gestión legal, versión 3, 2016).

Los riesgos de continuidad a los que está expuesto el proceso de gestión legal, de acuerdo con la identificación y valoración realizada por los colaboradores entrevistados, son los presentados en la tabla 19.

Tabla 19. Riesgos de continuidad - Gestión legal

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión legal	1	Pérdida de información, demoras en cargue y reprocesos de la información	1	Bajo
	2	Demoras en acceso y manejo de información	1	Bajo
	3	Inhabilidad de *software* a programas base de trabajo	3	Moderado
	4	Daños a los activos en la sede y pérdida de información física	4	Moderado
	5	Imposibilidad de acceder a la sede por orden público	6	Alto
	6	Afectación de la seguridad o la vida de funcionarios	8	Alto
	7	Insatisfacción de las PPR por el servicio con reclamaciones judiciales	6	Alto
	8	Intermitencia o retraso en la operatividad del proceso	6	Alto
	9	Cese de operaciones en procesos y de atención a visitantes (sismo)	2	Bajo
	10	Cese de operaciones en procesos y de atención a visitantes (inundación)	1	Bajo

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión legal	11	Demoras en atención a las PPR por falta de capacidad del proceso (aumento PQR)	4	Moderado
	12	Demoras en atención a las PPR por falta de capacidad del proceso (ajustes en el marco normativo)	4	Moderado
	13	Demoras en atención a las PPR por falta de capacidad del proceso (menor contratación de personal)	4	Moderado
	14	No hay acompañamiento a regiones	4	Moderado
	15	Ajuste organizacional para responder a nuevas políticas	6	Alto

Fuente: elaboración propia según Matriz de valoración de riesgos.

Conforme a los riesgos identificados, los principales escenarios de falla en los que se concentran los riesgos valorados en zona de riesgo alto son: inhabilidad de la sede, inhabilidad de la línea de atención, desabastecimiento de bienes y servicios, y sucesión de poder. Al interior de estos escenarios encontramos los eventos disruptivos que pueden materializar el riesgo para el proceso de gestión legal, que son: fusión, liquidación, supresión o absorción de la entidad con su respectiva reestructuración, marchas con problemas de orden público y amenazas de atentado, inseguridad en el sector donde se ubica la sede de la entidad, inhabilidad del *software*, insuficiente personal para atender la demanda de servicios de las PPR, fallas en infraestructura (eléctrica, hidráulica, mecánica) por antigüedad de la sede, entre otros.

Al ubicar los riesgos del proceso en el mapa de calor (figura 20), se observa que cinco de los quince riesgos identificados están en la zona de riesgo alto, esto es, el 33 % de los riesgos; el 67 % restante se encuentra en zonas de riesgo moderado y bajo.

Por su frecuencia, los principales riesgos de continuidad, para el proceso de Gestión legal son: el cese de operaciones en procesos y de atención a visitantes, ocasionado por eventos como sismos e inundaciones, y las demoras en atención a las PPR por falta de capacidad del proceso causadas por eventos como el desborde de PQR en el proceso o provocadas durante ajustes en el marco normativo de la ARN.

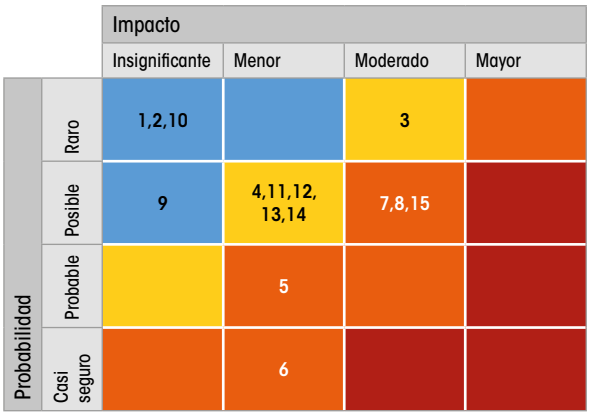

Figura 20. Mapa de calor - Gestión legal.
Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3.9 Proceso de atención al ciudadano

El propósito del proceso de atención al ciudadano es "desarrollar acciones orientadas a la identificación de necesidades, atención de requerimientos, promoción de la cultura del servicio y la evaluación de satisfacción de la ciudadanía frente a la gestión y los servicios que presta la entidad, con criterios de oportunidad, claridad, pertinencia con lo solicitado y respuestas de fondo" (Caracterización del proceso de atención al ciudadano, versión 5, 2016).

Los colaboradores de este proceso identificaron y valoraron los riesgos de continuidad mostrados en la tabla 20.

Tabla 20. Riesgos de continuidad - Atención al ciudadano

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Atención al ciudadano	1	Fuga de información sensible del proceso de reintegración	8	Extremo
	2	No hay comunicación con los clientes externos	3	Moderado
	3	Fuga de información sensible del proceso de reintegración	4	Alto
	4	Imposibilidad de acceder a la sede por orden público (marchas)	8	Alto

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Atención al ciudadano	5	Imposibilidad de acceder a la sede por orden público (toma de la sede)	4	Moderado
	6	Daños a los activos en la sede y pérdida de información física	4	Moderado
	7	Bloqueo de canales formales de comunicación con las PPR	3	Moderado
	8	Insatisfacción de las PPR con el servicio que genera reclamaciones judiciales	2	Bajo
	9	Intermitencia en el servicio	3	Moderado
	10	Cese de operaciones en procesos	8	Extremo
	11	Daño a la sede o a colaboradores con interrupción del servicio (sismo)	9	Alto
	12	Daño a la sede o a colaboradores con interrupción del servicio (incendio)	6	Alto
	13	Pérdida de imagen (aumento de PQR)	12	Extremo
	14	Pérdida de imagen (disminución de la capacidad del *call center* por presupuesto)	9	Alto
	15	Ajuste organizacional para responder a nuevas políticas	6	Alto
	16	Demoras en atención a las PPR por falta de capacidad del proceso	9	Alto

Fuente: elaboración propia según Matriz de valoración de riesgos.

Los riesgos valorados en zonas de riesgo extremo y alto son originados en los escenarios de falla tecnológica, inhabilidad legal, inhabilidad de la sede, desabastecimiento de bienes y servicios, desastre nacional o regional, inhabilidad financiera y sucesión de poder. Los principales eventos disruptivos asociados a estos escenarios y riesgos son: sabotaje informático, marchas con problemas de orden público y amenazas de atentado, incumplimiento en el servicio de *call center* por fallas de proveedores, sismo con destrucción parcial o total de la edificación, propagación de fuego en la sede central, aumento de PQR, ajuste de estructura y actividades del personal, redireccionamiento de la política del proceso de reintegración y de la estrategia, cambios en las políticas presupuestales ante nuevas políticas de reintegración, entre otros.

En el mapa de calor (figura 21) se muestra que 10 riesgos identificados y valorados se ubican en zonas de riesgo alto (43 %) y extremo (19 %), con impacto de moderado a mayor en la continuidad del proceso. Se destacan aquí los riesgos de fuga de información

sensible del proceso de reintegración, cese de operaciones en procesos y pérdida de imagen institucional (aumento de PQR), que quedan ubicados en zona de riesgo extremo.

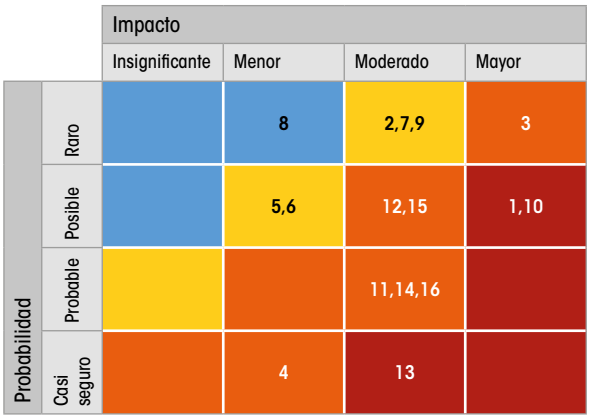

Figura 21. Mapa de calor - Atención al ciudadano.
Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3.10 Proceso de gestión jurídica

El propósito del proceso de gestión jurídica es "asesorar, coordinar y diseñar el desarrollo normativo, la defensa judicial o extrajudicial de la entidad, y el acompañamiento legal, para la implementación de la política de reintegración" (Caracterización del proceso de gestión jurídica, versión 5, 2016).

Acordes con la identificación y valoración de riesgos de continuidad realizada por los colaboradores del proceso, se obtuvieron los resultados planteados en la tabla 21.

Los principales escenarios de falla donde se ubican los riesgos valorados en la zona de riesgo alto son sucesión de poder y falla tecnológica. Se encuentran también aquí riesgos como ruptura de la continuidad de las políticas internas, afectación en continuidad por nuevas políticas y fuga de información sensible del proceso de reintegración.

Tabla 21. Riesgos de continuidad - Gestión jurídica

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión jurídica	1	Fuga de información sensible del proceso de reintegración	4	Alto
	2	Pérdida de información, demoras en cargue y reprocesos de la información	1	Bajo
	3	Afectación de la seguridad o la vida de funcionarios	1	Bajo
	4	Insatisfacción en el servicio de las PPR con reclamaciones judiciales	3	Moderado
	5	Daños a la sede o a colaboradores con interrupción del servicio	2	Bajo
	6	Sanciones o multas	2	Bajo
	7	Ruptura de la continuidad de las políticas internas	9	Alto
	8	Afectación en continuidad por nuevas políticas	6	Alto

Fuente: elaboración propia según Matriz de valoración de riesgos.

Al ubicar en el mapa de calor (figura 22) los riesgos identificados por el proceso, podemos observar que tres de ellos (37 %) se encuentran en zonas de riesgo alto y serían los principales candidatos a priorización teniendo en cuenta su severidad. Como se ve en la figura 22, este proceso presenta un bajo nivel de riesgo y se ubica como el tercero con nivel de riesgo más bajo.

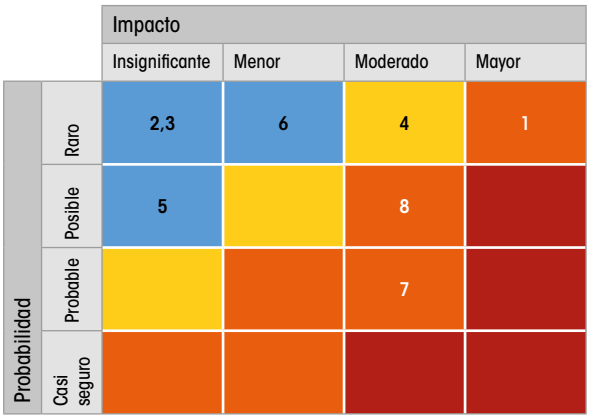

Figura 22. Mapa de calor - Gestión jurídica.
Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3.11 Proceso de gestión del talento humano

El proceso de gestión del talento humano es el encargado de "proveer a la entidad de servidores públicos competentes y satisfechos, que tengan un adecuado desempeño de sus funciones en el marco de las políticas de administración y desarrollo del talento humano, así como [de] realizar las gestiones pertinentes para investigar y sancionar las conductas disciplinarias que afecten el correcto funcionamiento de la entidad" (Caracterización del proceso de gestión del talento humano, versión 5, 2016).

Tras la identificación y valoración de riesgos de continuidad realizada por los colaboradores entrevistados, se obtuvieron los resultados de la tabla 22.

Tabla 22. Riesgos de continuidad - Gestión del talento humano

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión del talento humano	1	Pérdida de información, demoras en cargue y reprocesos de la información	1	Bajo
	2	Pérdida de servicios de comunicación, procesamiento de datos y reprocesos	1	Bajo
	3	Menor tiempo de trabajo en la sede central y afectación en la concentración en el trabajo	4	Alto
	4	Daños a los activos en la sede y pérdida de información física	2	Bajo
	5	Daño a la sede o a colaboradores con interrupción del servicio	2	Bajo

Fuente: elaboración propia según Matriz de valoración de riesgos.

Este proceso únicamente identificó cinco riesgos de continuidad, con uno solo calificado en zona de riesgo alto, y constituyó el proceso con el menor nivel de riesgos en la entidad.

En el mapa de calor del proceso de gestión del talento humano se muestra la distribución de los riesgos identificados de acuerdo con su valoración. Se encuentra que el escenario de inhabilidad de la sede es el que presenta la mayor importancia debido a que eventos originados en este escenario —como las marchas con problemas de orden público y las amenazas de atentado— pueden materializar el riesgo de menor tiempo de trabajo en la sede central y afectación en la concentración en el trabajo, el cual fue valorado

con una probabilidad de "casi seguro" y un impacto "insignificante". Sin embargo, esto lo ubica en zona de riesgo alto y, por tanto, sería un riesgo por intervenir en este proceso.

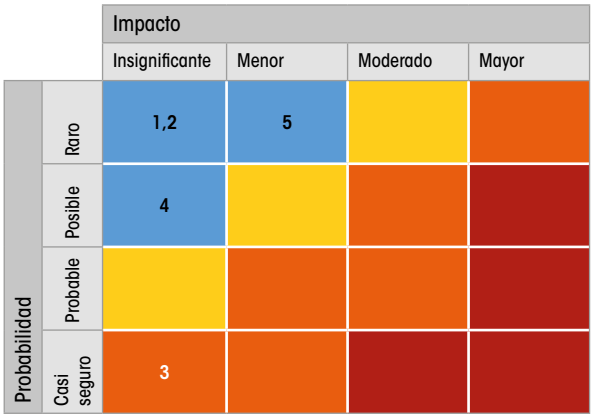

Figura 23. Mapa de calor - Gestión del talento humano.
Fuente: elaboración propia según Matriz valoración riesgos.

3.3.12 Proceso de gestión documental

El propósito del proceso de gestión documental consiste en

> administrar actividades que conlleven la implementación de políticas y metodologías eficientes para garantizar un correcto manejo documental que facilite la organización de los documentos durante todo su ciclo de vida y la preservación de la memoria institucional con fines probatorios e históricos. (Caracterización del proceso de gestión documental, versión 3, 2016)

Para este proceso, se identificaron y valoraron los riesgos de continuidad expuestos en la tabla 23. Los principales escenarios de falla son la sucesión de poder, inhabilidad financiera, falla tecnológica y desastre nacional o regional. Se encuentran asociados a estos escenarios eventos disruptivos como cambio del *staff* en la entidad, ajuste de estructura y actividades del personal, renovación o cambio del personal como consecuencia de concursos, fallas

en infraestructura (eléctrica, hidráulica, mecánica) por antigüedad de la sede o sismo con destrucción parcial o total de la edificación.

Tabla 23. Riesgos de continuidad - Gestión documental

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión documental	1	Pérdida de información, demoras en cargue y reprocesos de la información (problemas en equipos de trabajo)	4	Alto
	2	Pérdida de información, demoras en cargue y reprocesos de la información (fallas en centros de datos y servidores)	2	Bajo
	3	Fuga de información sensible del proceso de reintegración	4	Alto
	4	Cese de operaciones en procesos y de atención a visitantes	9	Alto
	5	Imposibilidad de acceder a la sede por daños en infraestructura con pérdida de documentos	8	Extremo
	6	Daño de información física y afectación a la salud del trabajador	8	Alto
	7	Pérdida de documentos, demora en la entrega o afectación de trámites	9	Alto
	8	No soporte de la información *Sigob* para continuidad del servicio	6	Alto
	9	Pérdida de información, demoras en cargue y reprocesos de la información (sismo)	12	Extremo
	10	Pérdida de información, demoras en cargue y reprocesos de la información (inundación)	8	Extermo
	11	Demoras en atención a las PPR por falta de capacidad del proceso	12	Extremo
	12	Rehacer la planeación y el direccionamiento institucional	16	Extremo
	13	Pérdida de oportunidad en los procesos por desarrollo de la curva de aprendizaje de nuevo personal	16	Extremo

Fuente: elaboración propia según Matriz de valoración de riesgos.

En el mapa de calor del proceso (figura 24) se observa que 12 de los 13 riesgos identificados (92 %) se encuentran en zonas de riesgo alto y extremo. Estos riesgos son susceptibles de priorización para intervención si se tiene en consideración su severidad.

Por su frecuencia, el principal riesgo de continuidad en este proceso es la pérdida de información, demoras en cargue y reprocesos de la información, materializados en eventos como fallas en centros de datos o servidores y durante sismos o inundaciones.

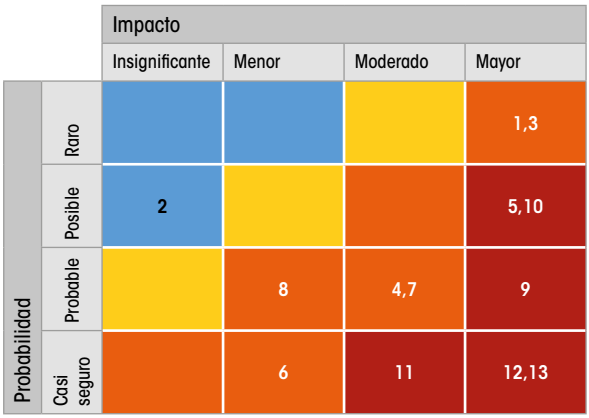

Figura 24. Mapa de calor - Gestión documental.
Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3.13 Proceso de gestión de tecnologías de la información

El propósito del proceso de gestión de tecnologías de la información es

> gestionar de manera integral las tecnologías de la información en la organización, prestando servicios acordes a las necesidades de la entidad y los avances en la materia, para contribuir al desarrollo de los procesos estratégicos, misionales y de apoyo a través de la tecnología. (Caracterización del proceso de gestión de tecnologías de la información, versión 5, 2016)

Los riesgos de continuidad a los que está expuesto este proceso, según la identificación y valoración de los colaboradores entrevistados, se exponen en la tabla 24.

Este proceso identificó riesgos de continuidad valorados en zona de riesgo extremo en ocho de los nueve escenarios evaluados. Se destacan —por la severidad de los riesgos contenidos— los escenarios de falla tecnológica, inhabilidad de la línea de atención o intervención de las PPR, desabastecimiento de bienes y servicios, inhabilidad legal, inhabilidad financiera y escenario de sucesión de poder. Al interior de estos escenarios, como potenciadores de

los riesgos de continuidad valorados en zona de riesgo extremo, se identificaron eventos disruptivos como interrupción del fluido eléctrico, pérdida o robo de equipos en campo, ajuste de estructura y actividades del personal, cambios en el marco jurídico regulatorio de la función institucional, limitación de recursos económicos, resistencia al cambio y renovación o cambio del personal como consecuencia de concursos.

Tabla 24. Riesgos de continuidad - Gestión de tecnologías de la información

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión de tecnologías de la información	1	Pérdida de servicios de comunicación, procesamiento de datos y reprocesos	12	Extremo
	2	Fuga de información sensible del proceso de reintegración	9	Alto
	3	Demoras en acceso y manejo de información	8	Extremo
	4	Imposibilidad de acceder a la sede por daños en infraestructura con pérdida de documentos	9	Alto
	5	Afectación de la seguridad o la vida de funcionarios	4	Moderado
	6	Daños a los activos en la sede y pérdida de información física (cañerías)	4	Moderado
	7	Pérdida de información y de los activos requeridos para la prestación del servicio	12	Extremo
	8	No prestación del servicio por el tiempo de respuesta de terceros contratados	12	Extremo
	9	Demoras en atención a las PPR por falta de capacidad del proceso	9	Alto
	10	Daño a la sede o a colaboradores con interrupción del servicio (sismo)	6	Alto
	11	Daño a la sede o a colaboradores con interrupción del servicio (incendio)	8	Extremo
	12	Daños a los activos en la sede y pérdida de información física (inundación)	4	Moderado
	13	Infringir la norma por desconocimiento	12	Extremo
	14	Cese de operaciones en procesos y de atención a visitantes	16	Extremo
	15	Incumplimiento en compromisos normativos con riesgo para la entidad	16	Extremo

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión de tecnologías de la información	16	Problemas de confiabilidad, calidad e integridad de la información	8	Extremo
	17	No existencia de información confiable para toma de decisiones	8	Extremo
	18	No cumplimiento de metas y compromisos con pérdida de confiabilidad en el proceso	12	Extremo
	19	Pérdida de oportunidad en los procesos por desarrollo de la curva de aprendizaje de nuevo personal	16	Extremo

Fuente: elaboración propia según Matriz de valoración de riesgos.

Para los riesgos ubicados en zona de riesgo alto, se identificaron los siguientes eventos disruptivos: sabotaje informático, fallas en infraestructura (eléctrica, hidráulica, mecánica) por antigüedad de la sede, falta de elementos o equipos de trabajo (desabastecimiento de bienes o servicios) y sismo con destrucción parcial o total de la edificación.

Al ubicar los riesgos en el mapa de calor (figura 25), es posible observar que 16 de los 19 riesgos identificados y valorados (84 %) se ubican en zonas de riesgo alto (21 %) y extremo (63 %), lo cual puede sugerir que este es un proceso que se debe intervenir de manera prioritaria, dado el nivel de riesgo al que se expone la entidad.

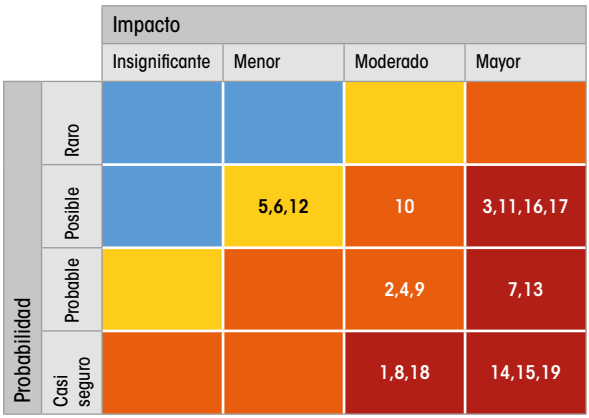

Figura 25. Mapa de calor - Gestión de tecnologías de la información.
Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3.14 Proceso de gestión en adquisición de bienes y servicios

El proceso sobre gestión en adquisición de bienes y servicios tiene como objetivo "planear y adquirir bienes y servicios que satisfagan las necesidades de las dependencias con oportunidad y calidad, contribuyendo así al cumplimiento de los propósitos de la entidad" (Caracterización de la gestión en adquisición de bienes y servicios, versión 5, 2016).

En las entrevistas, los colaboradores de este proceso identificaron y valoraron los riesgos de continuidad expuestos en la tabla 25.

Tabla 25. Riesgos de continuidad - Gestión en adquisición de bienes y servicios

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión en adquisición de bienes y servicios	1	Fuga de información sensible del proceso de reintegración	6	Alto
	2	Imposibilidad de acceder a la sede por daños en infraestructura con pérdida de documentos	6	Alto
	3	Afectación de la seguridad o la vida de funcionarios	6	Alto
	4	No disponibilidad de bienes y servicios requeridos para la operación	9	Alto
	5	Infringir la norma por desconocimiento (problemas con contratistas)	3	Moderado
	6	Cesación de los servicios o bienes contratados, afectación de la operatividad de los procesos con reclamaciones judiciales	3	Moderado
	7	Daño a la sede o a colaboradores con interrupción del servicio	9	Alto
	8	Pérdida de información, demoras en cargue y reprocesos de la información	6	Alto
	9	Infringir la ley por mala interpretación	6	Alto
	10	Infringir la norma por desconocimiento (atomización legal)	4	Alto
	11	Infringir la norma por desconocimiento (vacíos normativos de interpretación)	4	Alto
	12	Ajuste organizacional para responder a nuevas políticas	6	Alto
	13	Afectación en continuidad por nuevas políticas	6	Alto
	14	Pérdida de oportunidad en los procesos, por desarrollo de la curva de aprendizaje de nuevo personal	6	Alto

Fuente: elaboración propia según Matriz de valoración de riesgos.

Los riesgos identificados son originados principalmente en los escenarios de falla tecnológica, inhabilidad de la sede, desastre nacional o regional, inhabilidad legal y sucesión de poder. Como eventos disruptivos presentes en estos escenarios —y originadores de los riesgos identificados— están principalmente: sabotaje informático, fallas en infraestructura (eléctrica, hidráulica, mecánica) por antigüedad de la sede, marchas con problemas de orden público y amenazas de atentado, incumplimiento de contratos por proveedores, sismo con destrucción parcial o total de la edificación, inestabilidad jurídica en la contratación, vacíos normativos, fusión, liquidación, supresión o absorción de la entidad con su respectiva reestructuración, y renovación o cambio del personal como consecuencia de concursos, entre otros.

De acuerdo con la valoración realizada de los riesgos de continuidad identificados, la mayoría de estos se ubican en el mapa de calor (figura 26) en zona de riesgo alto con un 86 %, no se identifican riesgos en zona extrema y dos de ellos (14 %) se ubican en zona de riesgo moderado.

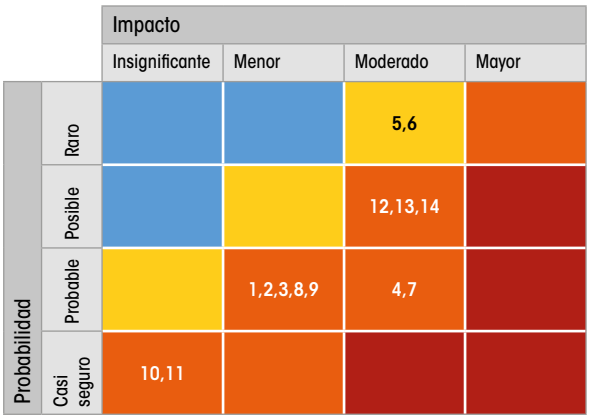

Figura 26. Mapa de calor - Gestión en adquisición de bienes y servicios.
Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3.15 Proceso de gestión financiera

El propósito del proceso de gestión financiera es "ejecutar y controlar con efectividad los recursos financieros apropiados a la

entidad para el cumplimiento de la misión institucional de acuerdo a la normatividad vigente" (Caracterización del proceso de gestión financiera, versión 3, 2016).

Los colaboradores entrevistados identificaron los riesgos consignados en la tabla 26, que pueden afectar la continuidad del proceso.

Tabla 26. Riesgos de continuidad - Gestión financiera

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión financiera	1	Pérdida de información, demoras en cargue y reprocesos de la información (en centros de datos)	2	Bajo
	2	Demoras en acceso y manejo de información	4	Moderado
	3	Pérdida de información, demoras en cargue y reprocesos de la información (en sistema SIIF)	2	Bajo
	4	Imposibilidad de acceder a la sede por daños en infraestructura con pérdida de documentos	2	Bajo
	5	Afectación de la seguridad o la vida de funcionarios	4	Moderado
	6	Pérdida de imagen	8	Extremo
	7	No disponibilidad de condiciones y servicios requeridos para la operación	4	Moderado
	8	Pérdida de la reputación de la entidad con demandas	4	Moderado
	9	Daño a la sede o a colaboradores con interrupción del servicio (sismo)	8	Extremo
	10	Daño a la sede o a colaboradores con interrupción del servicio (incendio)	8	Extremo
	11	Daños a los activos en la sede y pérdida de información física	4	Moderado
	12	Incumplimiento de planes estratégicos para la entidad	4	Moderado
	13	Sanciones o multas	12	Extremo
	14	Cese de operaciones en procesos	6	Alto

Fuente: elaboración propia según Matriz de valoración de riesgos.

Los principales escenarios de falla en relación con los riesgos identificados y valorados en zonas de riesgo extremo y alto son: inhabilidad financiera, inhabilidad de la línea de atención, desastre nacional o regional y paro de personal. Junto a estos escenarios, se relacionan los siguientes eventos disruptivos que, de presentarse, materializan los riesgos identificados: no contar con los recursos

para la ejecución de pagos, desbordamiento de canales no formales de información, aglomeración de las PPR en sedes, sismo con destrucción parcial o total de la edificación, propagación de fuego en la sede central, huelga del sindicato de la entidad, fallas en telecomunicaciones y sistemas de información, marchas con problemas de orden público y amenazas de atentado, entre otros.

En el mapa de calor del proceso (figura 27) se puede observar la distribución de los riesgos identificados y valorados. Así, el 36 % se ubica en zonas de riesgo extremo y alto, mientras el 43 % está en zona de riesgo moderado y el 21 % en zona de riesgo bajo. A partir de esta ubicación en el mapa de calor, la entidad puede determinar la priorización de los riesgos que va a intervenir.

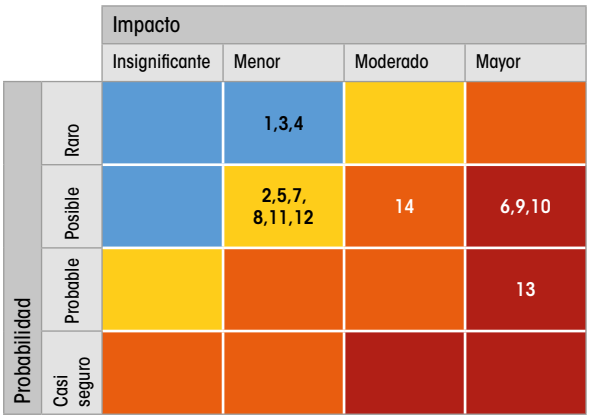

Figura 27. Mapa de calor - Gestión financiera.
Fuente: elaboración propia según Matriz de valoración de riesgos.

3.3.16 Proceso de gestión administrativa

El propósito del proceso de gestión administrativa es "administrar de manera eficaz y oportuna los recursos físicos y servicios generales, requeridos por los diferentes procesos de la entidad para el cumplimiento de la misión institucional" (Caracterización del proceso de gestión administrativa, versión 3, 2016).

Los riesgos de continuidad que los colaboradores entrevistados identificaron para este proceso están consignados en la tabla 27.

Tabla 27. Riesgos de continuidad - Gestión administrativa

Proceso	Identif.	Riesgo de continuidad	Nivel riesgo	Zona riesgo
Gestión administrativa	1	Pérdida de servicios de comunicación, procesamiento de datos y reprocesos	1	Bajo
	2	Pérdida de información, demoras en cargue y reprocesos de la información	1	Bajo
	3	Demoras en acceso y manejo de información	2	Bajo
	4	Daños a los activos en la sede y pérdida de información física (taponamiento de ductos y desagües)	2	Bajo
	5	Imposibilidad de acceder a la sede por orden público	2	Bajo
	6	Daño de información física y afectación a la salud del trabajador	2	Bajo
	7	Falta de cumplimiento de proveedores	6	Alto
	8	No disponibilidad oportuna de bienes y servicios requeridos para la operación	8	Alto
	9	No disponibilidad o falta de confiabilidad de la información requerida para la operación	1	Bajo
	10	Daño a la sede o a los colaboradores con interrupción del servicio (sismo)	4	Moderado
	11	Daño a la sede o a los colaboradores con interrupción del servicio (incendio)	1	Bajo
	12	Daños a los activos en la sede y pérdida de información física (inundaciones del piso)	2	Bajo
	13	No hay suficiencia presupuestal para desarrollar las actividades asignadas y el cumplimiento de metas	8	Alto
	14	Falta de cumplimiento de proveedores por deficiente planeación	2	Bajo
	15	Cese de operaciones en procesos y de atención a visitantes	1	Bajo
	16	Pérdida de la información o de bienes con probabilidad de pérdida del servicio	1	Bajo
	17	Demoras o intermitencia en los procesos	4	Moderado
	18	Resistencia del personal a las nuevas políticas y direccionamiento	8	Alto

Fuente: elaboración propia según Matriz de valoración de riesgos.

Teniendo en cuenta los riesgos con la más alta valoración, los principales escenarios de falla son: sucesión de poder, desabastecimiento de bienes y servicios e inhabilidad financiera. Relacionados con estos escenarios se encuentran los siguientes eventos disrup-

tivos potencializadores de los riesgos de continuidad identificados: inhabilidad de contratistas para prestar su servicio o la entrega de bienes, fallas y demoras en el proceso de contratación, ajuste de estructura y actividades del personal, cambio del *staff* en la entidad, sismo con destrucción parcial o total de la edificación y cambio de sede con traslado de activos, entre otros.

Como se observa en el mapa de calor de la figura 28, este proceso no tiene riesgos ubicados en zona de riesgo extremo. En la zona de riesgo alto se ubican cuatro (22 %) y serían los principales riesgos de este proceso para priorizar su intervención. En zona de riesgo medio se ubica el 13 % y en zona de riesgo bajo está el 75 % de los riesgos de continuidad del proceso.

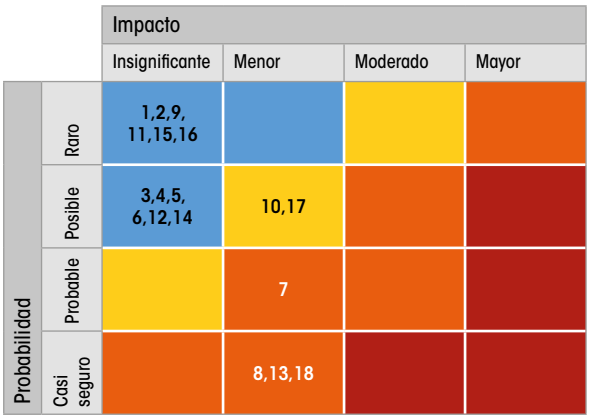

Figura 28. Mapa de calor - Gestión administrativa.
Fuente: elaboración propia según Matriz de valoración de riesgos.

Capítulo 4

Recomendaciones en materia de continuidad del negocio

A continuación, se presentan las recomendaciones de esta consultoría a la ARN. Es potestad de la Agencia acogerlas si pretende definir e implementar una gestión sistémica e integral de la continuidad del negocio.

4.1 Recomendaciones en perspectiva para la implementación de un sistema de gestión de continuidad del negocio

Este diagnóstico proporciona elementos de juicio a la ARN y a sus directivas para evaluar y definir la pertinencia de implementar un sistema de gestión de la continuidad del negocio (SGCN) que le proporcione razonable seguridad en la recuperación y restauración de las operaciones de la entidad, ante eventos que comprometan su normal funcionamiento, con lo que se garantiza de manera permanente la oferta de servicios y beneficios a las PPR.

Las etapas para la implementación de un SGCN serían:

- Definición de la estrategia de continuidad de la entidad
- Desarrollo y ejecución del plan de continuidad
- Revisión y mejora continua del SGCN

La implementación del SGCN aprovecharía las fortalezas institucionales que ya se han mencionado respecto a un sistema de gestión configurado bajo normas ISO —lo cual es consistente con la norma de continuidad—, pero también las competencias y la experiencia adquirida por el personal que ha liderado la implementación de dicho sistema, en especial desde el proceso de Direccionamiento estratégico.

4.2 Recomendaciones para implementar prácticas de continuidad desde la estrategia global de riesgos de la entidad

Partiendo de los resultados de la identificación y valoración de riesgos de continuidad, se recomienda iniciar acciones de mitigación y control, las cuales se podrían incluir en los actuales mapas de riesgo institucional y por proceso. La aplicación de la metodología DAFP para la identificación y valoración de riesgos de continuidad facilita la inclusión en los actuales mapas de riesgos de la entidad, que siguen la misma metodología.

De forma ideal, se debería intervenir la totalidad de los riesgos identificados; sin embargo, se deben tener en consideración situaciones como la limitación de recursos y de capacidad de la entidad y de los procesos para esa intervención. Así, se recomienda establecer criterios de priorización por nivel y frecuencia de riesgo; en este caso, se obtienen los siguientes resultados, que pueden ser consultados con más detalle en el anexo.

- Con el criterio de *frecuencia*, los principales escenarios de intervención serían falla tecnológica, inhabilidad de la sede y desastre nacional o regional, los cuales agrupan el 51 % del total de riesgos identificados.
- Con el criterio de *nivel de riesgo*, los principales escenarios de intervención serían inhabilidad financiera, falla tecnológica, sucesión de poder e inhabilidad de la sede, los cuales conforman el 62,5 % del nivel de riesgo de la entidad.

- Si se consideran los riesgos ubicados en zonas de riesgo extremo y alto, se deberían intervenir 132 riesgos, que representan el 62 % de la totalidad de riesgos identificados.
- Según los niveles calculados, los principales riesgos de continuidad (niveles alto y extremo) se presentan en tres procesos, con el 43,2 % de participación. El primero de ellos es el proceso de Gestión de tecnologías de la información, con 16 riesgos de continuidad y 15,5 % de participación; el segundo es el proceso de Direccionamiento estratégico con 10 riesgos de continuidad y 14,4 % de participación, y el tercero es el proceso de Implementación con 17 riesgos de continuidad y 13,3 % de participación.
- En orden de importancia, según frecuencia y nivel de riesgo en cada escenario de falla, la Agencia debe intervenir de manera prioritaria los escenarios de falla tecnológica, inhabilidad financiera e inhabilidad de sede, mediante tratamiento de los riesgos identificados en estos escenarios.

Los riesgos asociados a los escenarios de inhabilidad financiera, sucesión de poder e inhabilidad legal, que tienen una participación del 42,8 % del nivel de riesgo total, están ocasionados principalmente por situaciones externas a la entidad, lo cual plantea un mayor grado de dificultad para su intervención y tratamiento, debido a la poca gobernabilidad que tiene la entidad frente a estas situaciones. Sin embargo, se recomienda de manera general:

- Participar activamente en los escenarios de definición de política y lineamientos normativos y de gobierno que pudieran afectar a la entidad, a fin de intervenir en beneficio de esta o advertirlos al interior de la entidad de manera anticipada, de forma que le permita prepararse para afrontar dichos cambios con el menor impacto negativo.
- Potencializar la gestión de proyectos buscando otras fuentes de financiación que apalanquen la misionalidad y el fortalecimiento institucional; para este fin, la entidad podría establecer una línea de acción en su estrategia de corresponsabilidad.

- Ejercer estrictos controles en la ejecución de los recursos, a fin de maximizar su aprovechamiento, con lo cual se reduciría el impacto de políticas como la austeridad en el gasto. Este aspecto se puede fortalecer a partir de la promoción del control social.
- Fortalecer la estrategia de gestión de conocimiento que tiene la Agencia, implementando de manera sistemática acciones que recojan la memoria y el conocimiento institucional, para evitar su pérdida debido al concurso de méritos que actualmente realiza la Agencia y del potencial cambio de dirección de la misma.
- Realizar la preparación de los colaboradores de la entidad para afrontar los concursos de méritos, con el fin de reducir la rotación. Este aspecto se puede desarrollar a partir del Plan Institucional de Capacitación (PIC) o de convenios con entidades como la Escuela Superior de Administración Pública (ESAP).
- Emprender acciones de preparación de la entidad y de los procesos, para entender el entorno en el cual se mueve la entidad, y desarrollar capacidad de adaptación a los cambios de dicho entorno. Estas acciones se pueden gestionar desde la Subdirección de Seguimiento, que, según la resolución de grupos, tiene a cargo este tipo de funciones.

A continuación, se presenta una serie de recomendaciones generales, las cuales se establecen según el agrupamiento de riesgos por categorías.

4.2.1 Recomendaciones frente a riesgos clasificados en la categoría de *infraestructura física*

En esta categoría de riesgo se agrupan los relacionados con el estado de la infraestructura donde funciona la entidad, preparación frente a emergencias, incendios, fallas en el fluido eléctrico, seguridad física de instalaciones y accesos, entre otros.

Las principales recomendaciones en esta categoría son:

- Evaluación periódica de los riesgos: se sugiere actualizar los planes de emergencia y contingencia de la entidad frente a las variaciones presentadas, tales como cambio de sede e incidentes relacionados con el estado de la infraestructura actual (inundación, ruptura de canales, fallas en fluido eléctrico, entre otros).
- Mantenimiento de la infraestructura física de la actual sede, teniendo en cuenta su antigüedad. Es necesario un plan de mantenimiento preventivo que garantice el adecuado funcionamiento de los sistemas eléctricos, hidráulicos, mecánicos y de control biológico.
- Planificar y realizar acciones de detección, contención y atención de incendios en centros de datos, redes y bodegas, de manera que se mitigue el nivel de riesgos en estos recursos críticos para la operación de la entidad.
- Programar los mantenimientos de sistemas, equipos, centros de datos y, en general, de todos los recursos tecnológicos de que dispone la entidad, en horarios que no afecten la normal operación de los procesos.
- Revisar el espacio de trabajo de los funcionarios respecto a la proyección de servicios por cada piso, a fin de considerar la permanencia y tránsito de funcionarios y de visitantes frente a los riesgos que presenta su congestión, y los efectos en cadena o acumulativos con riesgos de incendios, sismos, atentados, falencias estructurales y de evacuación, con lo cual se disminuirían las consecuencias de su combinación.
- Contemplar el uso de otras sedes o inmuebles para la entidad como "sedes B" —es decir, un plan alterno de infraestructura— para casos de un daño parcial o total del edificio.
- Prever la posible contingencia de contratación de personal frente a eventos que afecten el recurso humano (sismo, incendio, entre otros), pues actualmente las políticas al respecto no contemplan un plan o método rápido de contratación ante los escenarios nombrados ni aseguran la no pérdida de capacidad de los procesos críticos.

4.2.2 Recomendaciones frente a riesgos clasificados en la categoría de *tecnología*

En esta categoría de riesgo se evaluaron tres aspectos que afectan la continuidad de las operaciones: confiabilidad, disponibilidad y recuperabilidad de la información.

- Dada la importancia de los sistemas de información en la continuidad del negocio, se recomienda realizar un análisis de riesgo en profundidad, que permita determinar la situación real de los sistemas de información de la entidad y analizar sus riesgos y vulnerabilidades, con el propósito de definir una estrategia de prevención y recuperación, así como la asignación y organización de los recursos necesarios.

- Teniendo en consideración que la entidad ya estableció —a través del *Manual del sistema de gestión de la seguridad de la información*— una serie de políticas, lineamientos y normas que se deben cumplir para su seguridad, se recomienda emprender acciones de comunicación y entrenamiento a los colaboradores para su conocimiento, apropiación y aplicación, así como acciones de verificación de cumplimiento de lo definido en el *Manual* en materia de seguridad de la información. Estos aspectos podrían quedar establecidos en la planeación institucional (planes de acción y planes operativos), liderados por los procesos de gestión de comunicaciones, tecnología de la información y talento humano.

- Gestionar los riesgos de seguridad de la información, estableciendo los controles requeridos acordes con el inventario y clasificación de los activos de información, en los cuales se determinan los niveles de protección necesarios para cada activo de este tipo.

- Asegurar la disponibilidad de información mediante la digitalización, con el objeto de facilitar su utilización y conservación. Esta medida se podría implementar a partir de la formulación de un proyecto de fortalecimiento institucional liderado por la Secretaría General de la Agencia.

- Dada la reiterada queja de los colaboradores entrevistados en cuanto a la demora en el cargue y procesamiento de información en los sistemas de información de la entidad, se recomienda estudiar la causa, a fin de tomar acciones pertinentes que deriven en sistemas de información más eficientes y eficaces.
- Garantizar el soporte técnico a los diferentes sistemas de información, bien sean desarrollados en la entidad o por terceros, y el control de las vigencias sobre las licencias de *software* que se usan en la entidad, de tal forma que permitan dar continuidad a la operación de estos sistemas.

4.2.3. Recomendaciones frente a riesgos clasificados en la categoría de *procesos*

En esta categoría de riesgo se agrupan los relacionados con gestión del proceso, los temas de proveedores y el soporte de tecnología.

- Desarrollar mecanismos de preparación de los procesos para operar en situaciones contingentes, ante la ocurrencia de cualquier evento disruptivo identificado, que pueda materializar un riesgo de continuidad.
- A partir de la identificación de eventos disruptivos que puedan afectar cada proceso y de los riesgos de continuidad asociados, se recomienda establecer un plan de respuesta y recuperación del proceso para afrontar cada amenaza identificada. Dicho plan debe tomar en consideración los recursos requeridos para el restablecimiento de las funciones críticas del proceso, como sistemas de TI, personal, instalaciones, proveedores y clientes.
- Si bien los procesos de la entidad ya cuentan con sus documentos de operación y control bajo condiciones normales, es importante que avancen hacia la documentación suficiente de las operaciones a cargo del proceso, para la respuesta y recuperación frente a cada evento disruptivo y los riesgos asociados. Hay que establecer, entre otras cosas, qué se hace, quién lo hace, cómo se hace, cuándo se hace,

qué se comunica y quién lo comunica. Este plan debe ser objeto de pruebas o simulacros para su validación.

- Es importante, además, determinar a quién llamar en cada categoría de incidente, por lo cual se debe tener un árbol de números telefónicos para que se hagan las llamadas correctas y en el orden adecuado. Todo lo anterior puede estar contenido en un documento de plan de respuesta y recuperación del proceso, el cual debe ser conocido, como mínimo, por todos los colaboradores del proceso y el equipo de dirección.
- La continuidad del negocio depende en parte de garantizar a los trabajadores acceso ininterrumpido a los datos y a las aplicaciones. En este sentido se reconoce que la entidad ha avanzado en políticas de trabajo móvil, aunque no pensando en la continuidad del negocio.
- Una interrupción tiene muchas repercusiones negativas para la entidad, pero esas posibilidades se disminuyen con el teletrabajo, pues la operación no está centralizada en un solo sitio. Por lo anterior, se recomienda fortalecer el teletrabajo en la ARN como estrategia de continuidad, disponiendo de los medios para que, individualmente, cada colaborador pueda seguir trabajando en caso de eventos de inhabilidad total de la sede.
- Comunicaciones internas y externas: para poder gestionar una crisis y mantener la confianza pública, al tiempo que se reducen los impactos negativos sobre la imagen de la entidad, es importante que exista un flujo claro de comunicación establecido. Por esta razón, se deben incluir, como parte del aseguramiento de la continuidad del negocio, procedimientos de comunicación tanto internos como con las partes interesadas, en caso de que se produzca un evento disruptivo de importancia.
- La capacidad de comunicarse de un modo efectivo en una contingencia es un aspecto esencial que contribuye a mantener la confianza pública en la entidad y en el proceso.
- En este sentido, es necesario que las acciones de continuidad del negocio de la entidad incluyan procedimientos de

comunicación que identifiquen, entre otros aspectos, a los responsables de comunicación adecuados para los eventos disruptivos identificados. Igualmente, se podría retomar el trabajo de elaboración del *Manual de crisis de comunicaciones*, en el que el enfoque de continuidad aparezca de manera integral.

- Cada proceso, según su naturaleza y objetivo, debe estructurar metodologías sistemáticas para identificar cambios del entorno que puedan afectar su operación y continuidad, minimizando de esta manera impactos negativos.
- Hay que identificar los proveedores de bienes y servicios críticos para el aseguramiento de la continuidad en la operación de cada proceso y de la entidad; establecer con ellos acuerdos de nivel de servicios y, de ser posible, tener proveedores de respaldo para estos bienes y servicios.

4.2.4 Recomendaciones frente a riesgos clasificados en la categoría de *personas*

En esta categoría se agrupan, entre otros, los riesgos relacionados con la seguridad física, laboral y de gestión del conocimiento. Se recomienda:

- Fortalecer la sistematización del conocimiento tácito en la Agencia. Este aspecto puede tener mayor despliegue a partir de la estrategia de gestión del conocimiento que tiene actualmente la Agencia, lo que deriva en una organización con una capacidad mayor de adaptación a las circunstancias cambiantes y contribuye así a la continuidad del negocio.
- Planificar suficientemente los cambios de sede, incluyendo criterios de selección respecto a la seguridad que ofrece la nueva construcción y el entorno para el personal que ocupa las instalaciones. Esta es una solicitud reiterativa de los colaboradores en todos los procesos.
- En aras de mantener un buen clima organizacional que pueda afectar positivamente los servicios que presta la entidad a sus clientes, se resalta la importancia de mantener

desde el equipo directivo una comunicación clara y directa con el personal frente al futuro inmediato de la entidad.

- Preparar a los colaboradores y al *call center* frente a los cambios en materia normativa y procedimental que modifican la oferta de servicios y beneficios, o los mecanismos de acceso a estos, de manera que se asegure una adecuada orientación a la PPR y no se afecte su proceso de reintegración.
- Asegurar la definición adecuada de las competencias requeridas para el desempeño exitoso de cada función y desarrollar procesos de selección transparente que garanticen el cumplimiento de los perfiles definidos. Una falla humana por desconocimiento puede materializar un riesgo de continuidad.
- Realizar permanente entrenamiento a los colaboradores, con lo cual se disminuye el riesgo de errores humanos en la operación atribuidos al desconocimiento, los cuales pueden provocar la degradación de un servicio hasta su pérdida.
- Reforzar la preparación de los colaboradores en las actividades de prevención y respuesta a emergencias ocasionadas por desastres naturales.

4.2.5 Recomendaciones frente a riesgos clasificados en la categoría *gerenciales*

En esta categoría se agrupan los riesgos relacionados con políticas, directrices, rediseño organizacional, entre otros aspectos de orden directivo:

- Frente al impacto que traerá consigo el concurso de méritos, se sugiere fortalecer la preparación de los colaboradores para afrontar este concurso, a fin de minimizar el riesgo de rotación de personal y, con esto, la pérdida de conocimiento que ya tienen los colaboradores actuales de la entidad, sus clientes y sus procesos.

- Teniendo en consideración la relevancia de los sistemas de información en la continuidad de las operaciones de la entidad, desde la alta dirección se debe asegurar un recurso humano suficientemente competente, capaz de enfrentar eventos inesperados que atenten contra la operación, seguridad y disponibilidad de los sistemas de información y las comunicaciones.
- Fortalecer los análisis de contexto a fin de prepararse para afrontar los efectos positivos y negativos de las fluctuaciones del entorno, como parte de la gestión de la política de reintegración.
- Implementar acciones que permitan desarrollar capacidad de adaptación al cambio en los colaboradores.
- Implementar estrategias de retención de personal, a fin de evitar la fuga de talentos y, con ella, la pérdida de conocimiento. La rotación de personal tiene incidencia en la curva de aprendizaje, en la que se pueden presentar fallas en el trabajo de los nuevos colaboradores por razones de aprendizaje, lo que a su vez incide en el servicio. En otras palabras, un colaborador nuevo con poco entrenamiento puede afectar negativamente la continuidad del servicio a las PPR.
- Establecer mecanismos rigurosos de priorización y uso eficiente de los recursos, definiendo indicadores de economía en la planeación institucional que pueden formar parte de instrumentos; por ejemplo, el plan estratégico o el plan de acción institucional de la Agencia.
- Estudiar la posibilidad de implementar una estrategia de *marketing* a partir de una buena comprensión de los mecanismos políticos y de las características del sector público, con el fin de mejorar el posicionamiento de la política de reintegración y de la gestión de la entidad en la implementación de dicha política. Con esto se busca incrementar los niveles de aceptación, respaldo y cooperación de todos los sectores con el proceso de reintegración y su continuidad. A su vez, se lograría mayor incidencia en los procesos de negociación con actores armados y en los temas de paz.

Las recomendaciones generales frente a los riesgos clasificados en la categoría de los *financieros* —los cuales agrupan los relacionados con la provisión de recursos económicos— ya se describieron en el numeral 4.2 y están orientadas principalmente a establecer controles en la ejecución de los recursos y fortalecer la gestión de proyectos buscando otras fuentes de financiación.

4.3 Recomendaciones específicas por proceso

A continuación, se plantean recomendaciones específicas para cada proceso, elaboradas a partir de las recomendaciones realizadas por los colaboradores indagados. Están orientadas al establecimiento de medidas de prevención y control para los riesgos valorados en zonas de riesgo alto y extremo. Para mayor detalle, se puede consultar la Matriz de valoración de riesgos.

4.3.1 Direccionamiento estratégico

A partir de las recomendaciones realizadas por los funcionarios entrevistados, se plantean las siguientes acciones: implementar políticas y acciones de seguridad de la información, desarrollar y mejorar la capacidad de adaptación institucional frente a cambios del entorno, entrenar a colaboradores y desarrollar estrategias de adaptación al cambio, asegurar el cumplimiento de perfiles de los colaboradores, establecer controles de cumplimiento de metas, normativas y compromisos institucionales.

4.3.2 Gestión de comunicaciones

En la gestión de comunicaciones se presentan, en general, riesgos de nivel medio y bajo. El trabajo depende, en esta gestión, de los equipos, el acceso a internet y el *software* específico para gestionar la comunicación de la entidad. Las recomendaciones son: establecer mayores controles de seguridad de la información, buscar fuentes alternas de recursos para asegurar la estabilidad financiera, planear el recurso con mantenimiento y soporte técnico, mantenimiento general de la sede y reforzamiento de estructura, y mayores prácticas de prevención y capacitación sobre riesgos.

4.3.3 Gestión de relaciones externas

En esta gestión, las acciones por desarrollar son: mayores controles de seguridad de la información, digitalización de la información, control en la ejecución eficiente de los recursos, realizar gestión del conocimiento y alta documentación, mejorar la gestión de sustentación de la necesidad de recursos para la entidad, monitoreo y posicionamiento de la política de reintegración, asegurar la existencia y conocimiento de planes de contingencia, entre otras.

4.3.4 Evaluación, control y mejoramiento

En la gestión de evaluación, control y mejoramiento, se deben implementar acciones como controles o políticas de seguridad que minimicen el riesgo de pérdida o fuga de la información, aseguramiento del soporte técnico para las herramientas informáticas con que cuenta la entidad, establecimiento de controles que permitan una adecuada planeación y ejecución del presupuesto, mayor participación de la entidad en negociaciones con grupos armados, capacitación permanente ante riesgos y simulacros, y generación de procesos transparentes de selección, entre otros.

4.3.5 Diseño

En la gestión de diseño se debe, entre otras cosas, disponer de computadores de apoyo para atender eventos de falla, adecuar infraestructura (arreglo de tuberías, canales, insonorización de la sede), cumplir perfiles de trabajo en los cargos contratados, planificar y asegurar tiempos de empalme en cargos, hacer seguimiento financiero y realizar mayor difusión y sensibilización nacional frente a la política de reintegración.

4.3.6 Implementación

En la gestión de implementación se deben desarrollar políticas de aseguramiento de la información, mayores alternativas de portabilidad de equipos de trabajo (mejorar acceso a la información desde diferentes sitios de trabajo), mejores criterios de ubicación de la sede (evitar exposición a marchas, atentados, riesgos de orden

público), capacitación/orientación oportuna y eficaz en el servicio de *call center*, optimización de procesos de contratación, priorización del recurso para la atención misional de las PPR, gestión del conocimiento y la memoria institucional, implementación de un plan de continuidad del proceso, planificación de nuevas contrataciones de sedes, revisando estado previo de la infraestructura, ajuste de los tiempos de respuesta de pagos a proveedores de bienes y servicios frente a los que maneja el Programa Anual Mensualizado de Caja (PAC).

4.3.7 Seguimiento

La gestión de este proceso depende del ingreso oportuno de información al sistema, de las bases de datos y de la gestión de los reportes. Los colaboradores entrevistados recomiendan, entre otras medidas, implementar políticas de seguridad de la información, fortalecer el sistema de información y realizar *backups*, planificar cambios en el direccionamiento, mejorar la infraestructura física de la sede, priorizar la asignación de recursos para el proceso según su impacto en la misión de la entidad y fortalecer las medidas de prevención ante desastres.

4.3.8 Gestión legal

Los colaboradores dependen del trabajo presencial en la sede central, de ahí que los factores que alteren el horario de su trabajo, así como sus recursos y la documentación, afecten la normal operación del proceso. Entre las recomendaciones que hacen los colaboradores están, entre otras: mejorar las condiciones de infraestructura y ubicación de la sede central; ajustar los procedimientos de atención, de manera que se mitigue la insatisfacción en el servicio de las PPR y las posibles reclamaciones judiciales; mejorar la preparación institucional para afrontar los cambios tanto en la normativa como en la política de reintegración; mejorar el respaldo y seguridad de la información, y priorizar los recursos misionales.

4.3.9 Atención al ciudadano

Presenta de manera priorizada los riesgos relacionados con la capacidad de respuesta a las PPR frente a cualquier incidente. Las acciones que recomiendan los colaboradores para este proceso son, entre otras: realizar un blindaje técnico de la información (seguridad de la información), implementar estrategias de teletrabajo, tener un segundo proveedor de bienes y servicios (respaldo), mejorar la infraestructura de la sede central (con adecuaciones para riesgos especiales de incendios), desarrollo de capacidad de adaptación ante cambios normativos y de política, y gestión de conocimiento y de memoria histórica institucional.

4.3.10 Gestión jurídica

Las acciones que los colaboradores recomiendan para este proceso son: mejorar la seguridad de la información frente a los diferentes perfiles de usuarios, blindar jurídicamente la entidad (sujetos a la norma), realizar análisis técnico que sustente el enfoque del proceso de reintegración frente a cambios en el marco jurídico o en la política de reintegración, optimizar el trabajo desde casa y optimizar también la movilidad a sedes de grupos territoriales.

4.3.11 Gestión del talento humano

Entre las recomendaciones realizadas por y para este proceso están: generación de *backups* de forma automática y no manual, con lo que se contribuye a la seguridad de la información; teletrabajo; programación y cumplimiento de los esquemas de mantenimiento de la infraestructura física de las instalaciones, y programación de prácticas de simulacros.

4.3.12 Gestión documental

Las acciones por desarrollar en este proceso, a partir de las recomendaciones realizadas por sus colaboradores, son, entre otras: políticas de seguridad de la información; digitalización de la información y respaldo informático; uso de sedes regionales como

plan alterno de trabajo e implementación del teletrabajo; digitalización de expedientes en el 100 % con repositorio local en todas las sedes; acuerdo de niveles de servicio con proveedores; campaña documental cultural para entrega oportuna de información; implementación de políticas de continuidad y planes de empalme, y mantenimiento de la infraestructura física de la sede.

4.3.13 Gestión de tecnologías de la información

Las acciones recomendadas por los funcionarios entrevistados son, entre otras: seguridad de la información (generación de respaldos de información, alta seguridad en los *backups* de información, mayor asistencia tecnológica a grupos territoriales, sensibilización y cultura organizacional en manejo de información, mecanismos de protección de datos sensibles, infraestructura informática adecuada, entre otras), adecuado mantenimiento a la infraestructura de la edificación y respaldo frente a fallas del fluido eléctrico, garantías en contratos con proveedores y con terceros, buenas prácticas internas de contratación, mayor acceso remoto a herramientas de trabajo, mayor seguridad en el tránsito de equipos para protección de la información, mejoramiento de los escenarios y proyección del presupuesto, proyección de sedes, optimización de recursos, preparación del recurso humano para los concursos de provisión de cargos a fin de reducir la fuga de conocimiento, y teletrabajo.

4.3.14 Gestión en adquisición de bienes y servicios

Las acciones de prevención y mitigación de riesgos de continuidad recomendadas para este proceso son: implementar mejores prácticas y política de seguridad de la información; teletrabajo; preparación del proceso para momentos de contingencia frente a eventos disruptivos; adecuado mantenimiento de las instalaciones; revisión y seguimiento de contratos para impedir que no haya disponibilidad de bienes y servicios requeridos para la operación; unificación de criterios en Colombia Compra Eficiente, y fortalecimiento institucional del conocimiento y la memoria histórica (gestión del conocimiento y de la memoria institucional).

4.3.15 Gestión financiera

Las acciones por desarrollar a partir de las recomendaciones realizadas por los funcionarios entrevistados son, entre otras: control de la ejecución del gasto, cumplimiento del cronograma de trabajo, digitalización de la información, adecuado mantenimiento de las instalaciones de la entidad, mejoramiento de la gestión ante el Ministerio de Hacienda con una adecuada sustentación de la necesidad de recursos, implementación de sistemas de atención y prevención de incendios, y puesta en marcha de planes de contingencia frente a riesgos.

4.3.16 Gestión administrativa

Las acciones propuestas por los funcionarios entrevistados como medidas de mitigación y control de los riesgos son, entre otras: protección de la información mediante generación de *backups*, garantía de la continuidad de contratación de servicios de soporte informático, mantenimiento adecuado de la infraestructura física de la sede (eléctrico, hidráulico, mecánico y biológico), oportuna atención a solicitudes internas de fumigación y control de plagas, alertas y seguimiento del cronograma de contratos (cumplimiento del Plan anual de adquisición de bienes y servicios), manejo sancionatorio de casos ante incumplimiento de proveedores y plan de contingencia de trabajo remoto (teletrabajo).

Capítulo 5

Conclusiones de la consultoría

A partir de los capítulos que componen el informe final de la consultoría, se presentan las siguientes conclusiones.

5.1 En relación con los aspectos generales de la consultoría

El problema identificado por la consultoría se gestiona con el presente diagnóstico y se constituye en una primera aproximación para conocer de manera sistemática las prácticas de continuidad, aunque restringida exclusivamente a la sede central de la entidad. Una visión más completa e integral implica metodológicamente un estudio posiblemente mixto —cualitativo y cuantitativo—, que alcance a todas las sedes de la ARN. Esto implicaría, entre otras cosas, una redefinición de la población y de la muestra de estudio, en las que se indague también a sus partes interesadas y a colaboradores de la entidad que implementan la reintegración en los territorios.

Sin desconocer lo anterior, esta consultoría permite tener una mirada comprensiva —coherente con el tipo de estudio que se planteó— de la continuidad del negocio en la sede central, con la que no contaba la ARN. Además, el referente ISO de continuidad del negocio, adoptado en el marco teórico-conceptual, permitió arrojar elementos válidos para la Agencia, con el fin de evaluarse y de adoptar —si así lo considera la ARN— acciones de gestión organizacional en la materia. En este sentido, los objetivos propuestos por la consultoría se cumplieron.

5.2 Respecto a la estructura y gestión de la ARN frente a la ISO 22301:2012

En general, la ARN presenta en su planeación estratégica poco despliegue de acciones en materia de continuidad del negocio. Esto se evidencia en instrumentos como su plan estratégico para la vigencia 2015-2018, en el plan de acción institucional para la vigencia 2017, y en los 34 planes operativos de las dependencias del nivel central y de los GT/PA. Los planes son coherentes con el esquema organizacional vertical que tiene la Agencia y con las funciones establecidas para los grupos de trabajo, lo cual evidencia en estas últimas una estructura funcional que no conduce a gestionar un desarrollo integral y holístico de continuidad del negocio en la entidad, aunque se reconocen —principalmente en los planes de las dependencias y en algunas de sus funciones— acciones relacionadas con continuidad y que tienen que ver principalmente con los activos de información, la salud y seguridad en el trabajo, los bienes y recursos financieros de la entidad.

La Agencia cuenta con un sistema de gestión integral que recoge el MECI, la NTC-GP 1000:2009 y el SGSST, formado por 16 procesos que se estructuran bajo el ciclo PHVA, que están debidamente documentados (aproximadamente 150 documentos sustentan la operación de estos procesos). Además, existe una experiencia de implementación de más de cuatro años que permitió la certificación en IS0 9001:2008. Esto se constituye en una fortaleza de la ARN en caso de pretender avanzar hacia un SGCN.

La ARN gestiona una estrategia global de riesgos y diferencia riesgos de gestión y de corrupción, con 47 riesgos en total y 164 acciones de tratamiento. Para ello acoge la metodología del DAFP, coherente con la ISO 31000, y tal como recomienda la norma 22301:2012 para la gestión de riesgos de continuidad. Si bien en la estrategia no se desarrolla la continuidad de manera explícita e integral, sí se reconoce que existen riesgos relacionados con la continuidad, especialmente en las gestiones de talento humano, tecnologías de la información, administrativa y adquisición de bienes y servicios. En todo caso, la estrategia global de riesgos se presenta como una gran oportunidad para avanzar en prácticas de continuidad del negocio, aunque no se hacen aproximaciones con cierto grado de rigurosidad

sobre los impactos negativos que traería su materialización ni los grados de tolerancia y tiempos de recuperabilidad.

Como entidad pública, la ARN no está obligada a cumplir la norma de continuidad, pero sí gravita sobre ella un vasto marco regulatorio que debe acoger o tener en cuenta para su operación (más de 200 normas se incluyen en los normogramas de los procesos de acuerdo con sus objetivos y naturaleza). Algunas de estas normativas tienen relación con continuidad del negocio, entre las que se destacan la relacionada con la seguridad y protección de la información institucional, la salud y seguridad en el trabajo, y la de protección y aseguramiento de los recursos físicos y financieros de la entidad.

Finalmente, al analizar las partes interesadas de la ARN en relación con la continuidad, se puede concluir que se presentan brechas en materia de comunicación, a la hora de sufrir eventos disruptivos en su operación. Asimismo, la Agencia desconoce las expectativas y necesidades de esas partes en esta materia, lo que la pone en desventaja ante la materialización de riesgos de continuidad.

5.3 Frente a los escenarios de falla y riesgos de continuidad

Los escenarios de falla con mayor valoración de los colaboradores fueron: inhabilidad financiera, falla tecnológica, sucesión de poder e inhabilidad de la sede, que agrupan el 62,5 % del nivel de riesgos de continuidad en la entidad.

Se identificaron 75 eventos disruptivos originadores de los riesgos de continuidad en relación con los nueve escenarios planteados. Los principales eventos según su frecuencia de presentación son: sismo con destrucción parcial o total de la edificación, ajuste de estructura y actividades del personal, marchas con problemas de orden público y amenazas de atentado, fallas en infraestructura de las instalaciones de la sede, sabotaje informático y fallas en sistemas de información y centros de datos.

Por su *nivel de riesgo*, los principales eventos son: cambios en el marco jurídico regulatorio de la función institucional, cambios en el marco del proceso de reintegración, cambios en la normatividad interna de la ARN, redireccionamiento de la política del

proceso de reintegración y de la estrategia, limitación de recursos económicos, y renovación o cambio del personal como consecuencia de concursos.

Se identificaron 223 riesgos, muchos de ellos con diferentes frecuencias, lo cual obedece a que un mismo riesgo pudo ser identificado en varios procesos y valorado de manera diferente, pero en todo caso se traducen en 69 riesgos diferentes.

Por su *frecuencia*, los principales riesgos de continuidad son: pérdida de información, demoras en cargue y reprocesos de la información, daño a la sede o a colaboradores con interrupción del servicio, daños a los activos en la sede y pérdida de información física, afectación de la seguridad o la vida de funcionarios, cese de operaciones en procesos y de atención a visitantes, demoras en acceso y manejo de información, y fuga de información sensible del proceso de reintegración.

Por su *nivel de riesgo*, se ubican 15 en zona extrema, relacionados con temas como incumplimiento normativo, ajuste institucional por cambio en el contexto de la entidad, seguridad de la información, limitación de recursos y aspectos relacionados con la gestión de conocimiento.

5.4 Sobre las recomendaciones en materia de continuidad realizadas a la ARN

La implementación de un SGCN tiene potencial si se consideran la experiencia y el saber ya adquiridos en el establecimiento, la mejora continua del sistema de gestión integral con el que cuenta la entidad y su consistencia con las normas ISO.

Respecto a implementar prácticas de continuidad desde la Estrategia Global de Riesgos de la entidad, estas pueden asumir en la actualidad un valor más práctico y menos costoso para la Agencia, si se consideran la dinámica diaria de gestión de riesgos y la obligatoriedad de su seguimiento, evaluación y actualización. De ahí que las recomendaciones generales, las hechas por riesgo según categoría y las específicas para cada proceso son insumos valiosos para tal fin, considerando, además, que recogen los aspectos que identificaron y propusieron los propios colaboradores de la entidad.

Referencias

Agencia Colombiana para la Reintegración. (2013). Resolución 0754 de 2013. Diario Oficial 48862.

Agencia Colombiana para la Reintegración. (2015a). *Plan Estratégico 2015-2018.*

Agencia Colombiana para la Reintegración. (2015b). Resolución 2152 de 2015. *Por la cual se crean los grupos de trabajo internos de la ACR*.

Agencia Colombiana para la Reintegración. (2016a). *Manual del Sistema de Gestión de Seguridad de la Información (SGSI)*. https://bit.ly/2KwtwLQ

Agencia Colombiana para la Reintegración. (2016b). *Informe de gestión.* https://bit.ly/2OnLami

Agencia Colombiana para la Reintegración. (2016c). Resolución 1356 de 2016. *Por la cual se modifican unos artículos y se deroga el artículo 38 de la Resolución 0754 de 2016*. https://bit.ly/2CXgEKF

Agencia Colombiana para la Reintegración. (2016d). *Manual del Sistema Integrado de Gestión para la Reintegración (Siger)*. https://bit.ly/2KxhMJd

Agencia Colombiana para la Reintegración. (2017). *Manual de Gestión del Riesgo*. https://bit.ly/2QswuF3

Agencia para la Reincorporación y la Normalización. (2017). *Presupuesto desagregado por áreas. Vigencia 2017*. https://bit.ly/2qsFhMz

Alta Consejería para la Reintegración. (2009). *La contribución de Cartagena al desarme, desmovilización y reintegración*. https://bit.ly/2XvSxMz

Asociación Colombiana de Ingeniería Sísmica. (2010). *Reglamento colombiano de construcción sismorresistente NSR-10*. Ministerio de Ambiente, Vivienda y Desarrollo Territorial.

Barnes, J. (2001). *A guide to business continuity planning*. John Wiley & Sons.

Business Continuity Institute. (2008). Lancashire Resilience Forum. https://bit.ly/37ib9nI

Clavijo, D. (2010). *El proyecto de la investigación. Haciendo posible la tesis de grado*. U. L. S.

Departamento Administrativo de la Función Pública. (2014). *Guía para la administración del riesgo.* https://bit.ly/37mMcaE

DiMattia, S. (2001). Planning for continuity. *Library Journal*, *126*(19), 32-34.

Espinosa, J., Guasp, M. y Lerma, A. (2012). Gestión integral de crisis: la nueva continuidad del negocio. *Revista Red Seguridad*, (58).

Fopae. (2010). Actualización y sistematización de escenarios de daños por terremoto para Bogotá [informe final, fase 2]. https://bit.ly/2QBuwC7.

Gaspar, J. (2006*). El plan de continuidad del negocio: Guía práctica para su elaboración*. Ediciones Díaz de Santos.

Gaspar, J. (2008). Un banco de tres patas: planes de continuidad de negocio en el sector financiero. *Revista Mensual de Bolsas y Mercados Españoles*, (174), 58–60.

Instituto Colombiano de Normas Técnicas y Certificación. (2004). Norma Técnica Colombiana NTC 5254. *Gestión del Riesgo*.

Machuca, S. y Sasco, G. (2012). *Coloured Petri Nets como apoyo a la Gestión de proyectos de continuidad del negocio*. Sedici.

M. H. (2007). Los planes de continuidad de negocio, una herramienta en expansión. *Revista Mensual de Bolsas y Mercados Españoles*, (160), 58–61. https://bit.ly/2r7YZgy

Organización Internacional de Estandarización. (2009). ISO 31000. *Gestión de riesgos - Principios y guías*.

Organización Internacional de Estandarización. (2012). ISO 22301:2012. *Societal security. Business continuity management systems. Requirements*. https://bit.ly/34f2kJe

Organización Internacional de Estandarización. (2015). ISO 9000:2015. *Quality Management Systems-Fundamentáis and Vocabulary*.

Ortiz, C., Higuera, J., Huérfano, H. y Díaz, C. (2014). Caída de precios del petróleo golpea a Colombia. *UN Periódico 184*. Universidad Nacional.

Parga, M. (2007). Gestión global de la continuidad de negocio. *Revista Mensual de Bolsas y Mercados Españoles*, (163), 18–22. https://bit.ly/2KD6qTV

Paul, K. (2009). Business continuity, a history of challenges. *Survival Insights*. https://bit.ly/2O4AnOR

Porter, M. E. (1996). What is strategy? *Harvard Business Review*, *74*(6), 61–78.

Presidente de la República de Colombia. (2011, 3 de noviembre). Decreto 4138 de 2011. Diario Oficial 48242.

Presidente de la República de Colombia. (2017, 29 de mayo). Decreto Ley 897 de 2017. Diario Oficial 50248.

Sánchez, J. C. (1992). La aproximación contingente en la teoría organizacional: ¿hacia un nuevo enfoque? *Revista de Psicología del Trabajo y de las Organizaciones*, *8*(21), 39-50.

Servat, A. A. (2012). Nuevo estándar internacional en continuidad del negocio, ISO 22301:2012. *Revista Gestión*, (1999-5709), 26–31. https://bit.ly/3699Ibr

Universidad de los Andes. (2010, 26 de octubre). *Microzonificación sísmica de Bogotá* [proyecto].

Universo Fórmulas. (2015). *Muestreo discrecional o por juicio*. https://bit.ly/2OoMgOy

La preparación editorial de *Diagnóstico de continuidad del negocio en la Agencia para la Reincorporación y la Normalización (ARN), sede central, Bogotá* estuvo a cargo de Ediciones Universidad Central.

En la composición del texto se utilizaron fuentes ITC Veljovic Std y ITC Avant Garde Gothic Std. Se publicó en diciembre de 2021, en la ciudad de Bogotá.

Diagnóstico de continuidad del negocio en la Agencia para la Reincorporación y Normalización (ARN), sede central, Bogotá

Este libro, resultado de una tesis destacada de la Maestría en Gestión de Organizaciones, presenta un diagnóstico de continuidad del negocio en la sede central de la Agencia para la Reincorporación y Normalización (ARN, antes ACR), con tres objetivos en mente: entender la organización a partir de la ISO 22301:2012; identificar y valorar los escenarios de falla y los riesgos de continuidad, y formular recomendaciones. Se definió un diseño cualitativo, que implicó la revisión de un gran volumen de documentos institucionales y la aplicación de entrevistas a colaboradores de la entidad. Los resultados evidencian que la Agencia ha avanzado principalmente en establecer acciones de continuidad en materia de sus activos de información; en menor medida lo ha hecho hacia la seguridad de sus colaboradores e instalaciones, y tiene significativas brechas por cerrar en su estrategia global de riesgos cuando se le mira a partir de la continuidad del negocio.

El desarrollo y los resultados presentados son también una guía para este tipo de diagnósticos, útiles tanto para las organizaciones públicas como para las privadas en diversos sectores.

UNIVERSIDAD CENTRAL