

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

1. INTRODUCCIÓN

Toda organización está expuesta a situaciones imprevistas que pueden alterar su funcionamiento normal, afectar a las personas, comprometer sus activos y poner en riesgo la continuidad de sus operaciones. Las emergencias, ya sean de origen natural, humano o tecnológico, exigen una preparación adecuada que permita actuar de forma rápida, coordinada y eficiente, protegiendo la vida, la infraestructura, la información y los procesos misionales.

La Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo) reconoce la importancia de anticiparse, prepararse y responder de manera estratégica y estructurada frente a cualquier eventualidad que comprometa la seguridad humana, la continuidad operativa y la integridad institucional. Por ello, implementa un Plan Integral de Prevención, Preparación y Respuesta ante Emergencias, articulando los componentes de Seguridad y Salud en el Trabajo (SG-SST), gestión documental, sostenibilidad ambiental y tecnologías de la información, en coherencia con su Sistema Integrado de Gestión (SIG).

En el marco del SG-SST, este plan promueve condiciones seguras en el entorno laboral, fomenta una cultura preventiva y fortalece la capacidad de respuesta institucional frente a cualquier situación que ponga en riesgo la salud y la vida de los trabajadores, contratistas, visitantes y comunidad. Las emergencias afectan no solo la infraestructura física y los procesos operativos, sino, sobre todo, el bienestar del recurso humano, por lo cual se requiere preparación continua, procedimientos estandarizados y una movilización eficiente de recursos internos y externos.

Desde la dimensión documental, los archivos institucionales son un activo estratégico para la gestión, la memoria institucional y la transparencia. La pérdida de información compromete la trazabilidad, la rendición de cuentas y la continuidad misional. Por ello, este plan contempla un Plan de Emergencias Documentales, en articulación con el Plan Institucional de Archivos – PINAR, que permite prevenir, mitigar y atender situaciones que pongan en riesgo el acervo documental, asegurando su recuperación, preservación y acceso.

En cuanto al componente ambiental, RenoBo asume su corresponsabilidad frente a la protección del entorno y la prevención de impactos negativos derivados de situaciones de emergencia. En línea con el Plan Institucional de Gestión Ambiental (PIGA), se establecen medidas preventivas y correctivas para reducir la vulnerabilidad ambiental, proteger los recursos naturales y garantizar una operación sostenible y resiliente.

En materia tecnológica, la alta dependencia de los sistemas de información y servicios digitales exige contar con un Plan de Contingencia Tecnológica, que garantice la disponibilidad, integridad y recuperación de los activos digitales críticos. Este componente incluye la identificación de riesgos tecnológicos, el diseño de procedimientos de restauración y la definición de tiempos máximos de recuperación, en el marco de una estrategia de continuidad operativa y protección de datos.

Este documento, por tanto, reúne los lineamientos estratégicos, normativos y operativos que integran la respuesta institucional frente a emergencias, fortaleciendo la resiliencia organizacional y reafirmando el compromiso de RenoBo con la protección de su gente, su memoria institucional, sus recursos tecnológicos, el medio ambiente y la ciudad que transforma cada día.

2. LINEAMIENTOS PARA LA PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Para la Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo), garantizar un entorno seguro para trabajadores, contratistas, visitantes y partes interesadas es una prioridad institucional. Por ello, se dispone de instalaciones adecuadas, recursos físicos y tecnológicos, y una cultura organizacional basada en la prevención, la preparación y la respuesta efectiva ante cualquier tipo de emergencia.

Las directivas de la Empresa, en articulación con la Brigada de Emergencias y la Dirección Administrativa y de TICS, reafirman su compromiso con la implementación del Plan Integral de Emergencias, a través de los siguientes lineamientos:

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Seguridad y protección de las personas:

- ✓ Preservar la vida y la integridad de todos los actores institucionales frente a cualquier amenaza o emergencia.
- ✓ Garantizar el cumplimiento de la normativa legal vigente en materia de prevención, preparación y atención de emergencias.
- ✓ Asegurar una respuesta rápida y efectiva que permita la continuidad operativa y la pronta recuperación de los procesos afectados.

Gestión ambiental responsable:

- ✓ Velar porque todas las acciones en emergencias incorporen criterios de protección del medio ambiente.
- ✓ Evaluar los riesgos ambientales e identificar puntos críticos mediante un plan específico que contemple procedimientos ante eventualidades.
- ✓ Capacitar al personal sobre medidas de atención ambiental, estableciendo mecanismos de comunicación con las autoridades competentes.
- ✓ Evaluar y actualizar de manera periódica el Plan de Emergencias Ambientales, en concordancia con el PIGA institucional.

Protección de la memoria documental:

- ✓ Implementar acciones para prevenir y mitigar amenazas de origen natural, antrópico o accidental que puedan comprometer los archivos institucionales.
- ✓ Establecer estrategias de sostenibilidad documental que aseguren la recuperación y continuidad de la información crítica.

Continuidad tecnológica y protección de datos:

- ✓ Mantener en operación los procesos de misión crítica y servicios de TI ante cualquier eventualidad.
- ✓ Contar con un Plan de Emergencias de Tecnologías de la Información que permita la restauración eficiente de sistemas inoperables.
- ✓ Resguardar la información institucional frente a pérdida, hurto o destrucción, mediante medidas físicas y lógicas de protección.

Enfoque articulador y mejora continua:

- ✓ Asegurar la integración del Plan de Emergencias al Sistema Nacional para la Prevención y Atención de Desastres, fortaleciendo planes locales y acuerdos de apoyo mutuo.
- ✓ Garantizar la actualización permanente del plan bajo estándares de calidad y en el marco del Sistema Integrado de Gestión (SIG).
- ✓ Promover una cultura institucional de prevención mediante capacitación, comunicación continua y simulacros.

En cumplimiento de estos lineamientos, RenoBo reafirma su compromiso con la protección de las personas, la sostenibilidad del entorno, la preservación de su patrimonio documental y la garantía de continuidad operativa, alineando su gestión con la normativa vigente y las políticas corporativas.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Establecer las medidas de prevención, preparación, respuesta y control que permitan a la Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo) actuar de manera oportuna y efectiva frente a la posible materialización de amenazas que generen situaciones de emergencia, poniendo en riesgo la salud, la vida y el bienestar de su población (trabajadores, contratistas, visitantes, comunidad y terceros).

El objetivo es garantizar la ejecución de acciones rápidas, seguras y confiables que salvaguarden:

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- ✓ La integridad de las personas involucradas.
- ✓ Los bienes materiales e infraestructura de la organización.
- ✓ La continuidad operativa y la protección de los sistemas de información y datos institucionales.
- ✓ La sostenibilidad de los archivos ante amenazas de origen natural, animal o antrópico.
- ✓ La mitigación del impacto ambiental generado por la emergencia.
- ✓ La preservación de la imagen institucional y la confianza ciudadana en la organización.

3.2 OBJETIVOS ESPECÍFICOS

Con el fin de fortalecer la capacidad de respuesta institucional, la Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo) establece los siguientes objetivos específicos para la gestión integral de emergencias:

Seguridad, prevención y respuesta operativa

- ✓ Identificar y valorar anticipadamente las amenazas que puedan afectar a las instalaciones y sus ocupantes.
- ✓ Responder de forma oportuna ante escenarios de riesgo que comprometan la integridad de trabajadores, contratistas, usuarios y visitantes.
- ✓ Fortalecer la cultura de prevención, protección y autocuidado institucional a través de medidas preventivas, correctivas y de control.
- ✓ Cumplir con los requerimientos establecidos por las entidades de control en materia de emergencias.
- ✓ Establecer planes de mejora derivados del análisis de vulnerabilidad institucional.
- ✓ Señalizar rutas de evacuación e identificar los sistemas de atención básica como extintores, camillas, botiquines y sillas de ruedas.

Gestión Documental en emergencias

- ✓ Actualizar la matriz de riesgos del proceso de Gestión Documental conforme al Acuerdo 006 de 2014.
- ✓ Identificar riesgos y definir procedimientos generales para responder ante emergencias que afecten la memoria documental.
- ✓ Reducir la vulnerabilidad de los documentos de archivo, mediante prácticas seguras de conservación.
- ✓ Minimizar la pérdida de documentos ante desastres naturales o antrópicos.
- ✓ Mantener actualizado el inventario único documental, junto con los recursos físicos, técnicos y humanos para su protección.
- ✓ Diseñar e implementar el Plan de Emergencia Documental para asegurar la recuperación del acervo en caso de desastre.
- ✓ Crear el listado de documentos esenciales y priorizarlos en caso de rescate.
- ✓ Capacitar al personal en el tratamiento adecuado de los archivos durante emergencias.
- ✓ Normalizar y socializar los procedimientos de atención antes, durante y después de emergencias documentales.
- ✓ Realizar simulacros específicos aplicados al material documental.

Continuidad de tecnologías de la información

- ✓ Generar un diagnóstico actualizado de la infraestructura tecnológica de la Empresa.
- ✓ Establecer lineamientos y procedimientos de contingencia para garantizar la funcionalidad de los sistemas de información.
- ✓ Asegurar la recuperación oportuna de servicios tecnológicos críticos ante fallas o eventos disruptivos.
- ✓ Implementar medidas para proteger herramientas como internet, correo electrónico y bases de datos institucionales.
- ✓ Garantizar la continuidad del servicio a funcionarios, contratistas, ciudadanos y demás usuarios internos o externos.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- ✓ Prevenir la pérdida de información y mantener la calidad, integridad y veracidad de los datos institucionales.

4. ALCANCE

El Plan Integral de Prevención, Preparación y Respuesta ante Emergencias de la Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo) aplica a todas las sedes físicas de la entidad, incluyendo el depósito de archivo y las oficinas administrativas, así como a todas las personas que se encuentren dentro de dichas instalaciones al momento de una emergencia: trabajadores, contratistas, visitantes y partes interesadas.

El alcance del plan comprende la identificación y evaluación exhaustiva de los riesgos a los que la Empresa está expuesta, así como la definición de los procedimientos para:

- Notificación interna y externa de la emergencia.
- Activación del equipo de respuesta institucional.
- Evacuación segura del personal.
- Control y mitigación de los efectos adversos.
- Comunicación efectiva con autoridades competentes.
- Implementación de medidas de recuperación y retorno a la operación normal.

Este plan también establece los niveles de coordinación y actuación requeridos para responder de manera estructurada y eficiente ante cualquier tipo de emergencia, incluyendo aquellas de origen natural, tecnológico, humano o antrópico.

La planificación contempla acciones diferenciadas para la atención de personas con discapacidad, movilidad reducida, o condiciones especiales de visión y audición, asegurando el principio de accesibilidad e inclusión en todos los procedimientos.

Finalmente, el Plan tendrá aplicación continua durante los trescientos sesenta y cinco (365) días del año, las veinticuatro (24) horas del día, garantizando cobertura permanente y capacidad de respuesta en cualquier momento.

5. LEGAL

Ver Normograma de la Empresa de Renovación y Desarrollo Urbano de Bogotá.

6. ALCANCE Y COBERTURA

6.1 CARACTERÍSTICAS Y REQUISITOS

El Plan Integral de Prevención, Preparación y Respuesta ante Emergencias de la Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo) está compuesto por un conjunto de subplanes articulados, diseñados para atender de manera específica los distintos tipos de amenazas que puedan afectar la operación institucional. Estos subplanes integran los lineamientos de gestión establecidos en el Sistema Integrado de Gestión (SIG) y responden a la naturaleza diversa de los riesgos a los que está expuesta la organización.

Los componentes del plan son:

- **Plan de Preparación y Respuesta ante Emergencias en Seguridad y Salud en el Trabajo (SG-SST):** Establece las acciones de prevención, mitigación, atención y recuperación frente a situaciones que comprometan la salud y la vida de los trabajadores, contratistas, visitantes o comunidad.
- **Plan de Preparación y Respuesta ante Emergencias Documentales:** Define los procedimientos orientados a salvaguardar la memoria institucional y el acervo documental de la Empresa ante eventos que puedan generar pérdida, deterioro o destrucción de documentos físicos o digitales, en articulación con el Plan Institucional de Archivos – PINAR y el Acuerdo 006 de 2014.
- **Plan de Preparación y Respuesta ante Emergencias Ambientales (PIGA):** Alineado con el Plan Institucional de Gestión Ambiental, incluye las medidas necesarias para prevenir, contener y mitigar impactos ambientales negativos generados por

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

emergencias, garantizando el cumplimiento normativo ambiental y la sostenibilidad operativa.

- **Plan de Preparación y Respuesta ante Emergencias de Tecnologías de la Información:**

Establece las estrategias para proteger la infraestructura tecnológica, los sistemas de información y la integridad de los datos institucionales. Contempla escenarios de falla, ciberataques o desastres que comprometan la continuidad digital de los servicios.

Cada uno de estos componentes responde a requisitos normativos específicos, contiene protocolos de activación, roles definidos, rutas de evacuación, estrategias de comunicación y medidas de recuperación. La integración de estos planes permite una respuesta coordinada, multisectorial y eficaz frente a cualquier eventualidad.

6.2 RESPONSABILIDADES

El Plan Integral de Prevención, Preparación y Respuesta ante Emergencias de la Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo) define las responsabilidades de los actores clave que garantizan su implementación, sostenibilidad y mejora continua. Cada responsable deberá cumplir con sus funciones de manera articulada, bajo los lineamientos del Sistema Integrado de Gestión (SIG):

- **Representante legal por medio de la Dirección Administrativa y de TICS**

- Suministrar los recursos financieros, técnicos y logísticos necesarios para el diseño, implementación y verificación del Plan.
- Verificar el cumplimiento del Plan a todos los niveles de la organización.
- Participar en los procesos de selección, contratación y gestión del personal requerido para la ejecución del plan, incluyendo capacitaciones y entrenamientos.

- **Responsable de Seguridad y Salud en el Trabajo**

- Diseñar, implementar y hacer seguimiento al componente SG-SST del Plan de Emergencias.
- Garantizar su actualización periódica y el cumplimiento de los objetivos establecidos en materia de prevención de riesgos laborales.

- **Responsable de Gestión Documental**

- Diseñar, implementar y verificar el funcionamiento del Plan de Emergencias Documentales.
- Asegurar la actualización permanente del plan y su alineación con el PINAR y la normativa archivística vigente.

- **Responsable de Gestión Ambiental**

- Diseñar, implementar y hacer seguimiento al Plan de Emergencias Ambientales en articulación con el PIGA.
- Verificar su actualización anual y garantizar la prevención y mitigación de impactos ambientales.

- **Responsable de Gestión de tecnologías de la información**

- Diseñar, implementar y mantener actualizado el Plan de Emergencias de TI.
- Verificar la capacidad de respuesta tecnológica ante fallas, incidentes o amenazas, asegurando la continuidad de los servicios digitales y la protección de la información.

- **Servicios Logísticos y Administrativos**

- Garantizar la disponibilidad y mantenimiento de los recursos físicos necesarios para la atención de emergencias (extintores, camillas, botiquines, señalización, alarmas, hidrantes, etc.).

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- Verificar periódicamente el estado y funcionamiento de los sistemas de evacuación y protección física.
- Coordinar el suministro de insumos básicos durante simulacros o eventos reales de emergencia.
- Apoyar la logística de evacuación, accesibilidad y atención prioritaria a personas con movilidad reducida o condiciones especiales.
- Gestionar la reposición y mantenimiento de los equipos asignados a la Brigada de Emergencias.

➤ **COPASST**

- Realizar inspecciones programadas y no programadas a los equipos y condiciones relacionados con la atención de emergencias.
- Notificar oportunamente cualquier acto o condición insegura identificada durante sus inspecciones.

➤ **Representante Legal (a través de la Dirección Administrativa y de TICS)**

- Suministrar los recursos financieros, técnicos y logísticos necesarios para el diseño, implementación y verificación del Plan.
- Verificar la aplicación del Plan en todos los niveles de la organización.
- Participar en la selección y contratación del personal necesario para la implementación del plan (incluyendo capacitaciones y entrenamientos).

➤ **Jefes de Área o Superiores Jerárquicos**

- Velar por el cumplimiento del plan en los procesos bajo su responsabilidad.
- Verificar que se realicen las actualizaciones correspondientes al plan en sus áreas.
- Facilitar la participación del personal asignado a la Brigada de Emergencias en los programas de capacitación.
- Participar en procesos de contratación relacionados con la implementación del plan (capitaciones, consultorías, entrenamientos).

➤ **Comité de Emergencias y Contingencias**

- Conocer el contenido del Plan, participar en su divulgación y coordinar su activación en caso de emergencia.

➤ **Brigada de Emergencias**

- Participar activamente en procesos de capacitación, entrenamiento y socialización del Plan.
- Realizar inspecciones de seguridad a los equipos de atención de emergencias.
- Activar el Plan y ejecutar los protocolos establecidos durante eventos de emergencia.

➤ **Comité Paritario de Seguridad y Salud en el Trabajo – COPASST**

- Realizar inspecciones planificadas y no planificadas a los equipos y condiciones de emergencia.
- Reportar actos y condiciones inseguras que puedan afectar la efectividad del plan.

➤ **Trabajadores**

- Participar activamente en los procesos de capacitación y simulacros de emergencia.
- Proveer información clara y veraz sobre su estado de salud cuando sea requerido para la planificación de emergencias.
- Conocer las rutas de evacuación, recursos disponibles y puntos de encuentro asignados.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- Cumplir las instrucciones impartidas por la Brigada de Emergencias durante situaciones reales o ejercicios de simulación.

6.3 ESTRUCTURA ORGANIZACIONAL PARA LA PREPARACIÓN, ATENCIÓN Y RESPUESTA DE EMERGENCIAS

La Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo) adopta el Sistema Comando de Incidentes (SCI) como estructura operativa para coordinar la preparación, atención y respuesta ante emergencias, en articulación con el Sistema Nacional de Gestión del Riesgo de Desastres (SNGRD).

Este modelo facilita una atención organizada y eficiente, mediante roles definidos, comunicación clara y coordinación entre áreas, sin importar el tipo o magnitud de la emergencia.

Estructura del Comité de Emergencias y Contingencias:

Comandante del Incidente:

Jefe de la Brigada de Emergencias. Lidera la respuesta y toma decisiones durante la emergencia.

Responsables por componente:

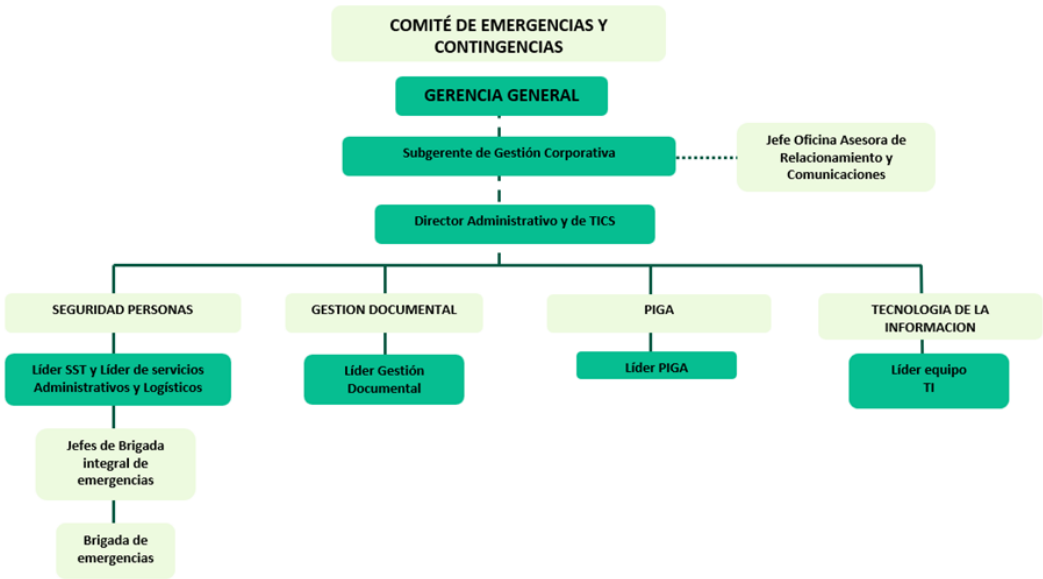
Cada responsable lidera su plan específico durante la emergencia:

- ✓ Seguridad y Salud en el Trabajo
- ✓ Gestión Documental
- ✓ Gestión Ambiental
- ✓ Tecnologías de la Información
- ✓ Servicios Logísticos y administrativos

Enlace interinstitucional:

Facilita la coordinación con entidades externas como IDIGER, bomberos, Policía, entre otros.

Este Comité de Emergencias y Contingencias estará compuesto por:



6.4 DIRECCIÓN Y CONTROL

Una vez notificada una situación de emergencia, corresponderá al Comité de Emergencias y Contingencias tomar la determinación de activar este Plan. Desde ese momento el Comité tomará el control y la dirección de las operaciones.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

La oficina asesora de comunicaciones, estará en contacto continuo con la Dirección Administrativa y de TICS, para hacer los reportes oficiales a los trabajadores y partes interesadas de la empresa.

Se activará el plan de preparación y respuesta ante emergencias teniendo en cuenta la situación presentada, el responsable será el líder del proceso asignado.

7. DEFINICIONES

Acervo documental: Conjunto de documentos de un archivo, conservados por su valor sustantivo, histórico o cultural.

Amenaza: Probabilidad de que un fenómeno de origen natural, tecnológico o humano, potencialmente capaz de causar daño y generar pérdidas, se produzca en un determinado tiempo y lugar.

Análisis de vulnerabilidad: Es el proceso mediante el cual se basa el inventario de recursos físicos, técnicos y humanos, con el objeto de poder determinar los eventuales efectos de distintas modalidades de emergencias y desastres para señalar la manera de cómo se puede responder ante una amenaza.

Archivo central: Unidad administrativa que coordina y controla el funcionamiento de los archivos de gestión y reúne los documentos transferidos por los mismos una vez finalizado su trámite y cuando su consulta es constante.

Archivo de gestión: Archivo de la oficina productora que reúne su documentación en trámite, sometida a continua utilización y consulta administrativa.

Ayuda mutua: Convenio privado, voluntario, condicionado, recíproco (bilateral o multilateral) y sin fines de lucro, suscrito entre diferentes Empresas y la Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo), y organizaciones privadas y del estado con actividades o amenazas similares o compatibles.

Biodeterioro: Alteración de los materiales que constituyen un bien debido a la actividad metabólica de una o más poblaciones de microorganismos u organismos vivos pertenecientes a distintos grupos sistemáticos.

Brigada: Una brigada es un grupo de personas debidamente organizadas y capacitadas para prevenir o controlar una emergencia.

Catástrofe: Es toda emergencia que, por su magnitud, traspasa las fronteras de la Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo), llegando a afectar una zona, una región o un país y desestabilizando su normal funcionamiento, superando la capacidad de respuesta.

Combustión: Reacción de oxidación lo suficientemente fuerte e intensa para producir luz y calor.

Competencia: Atributos personales y de actitud demostrada, para aplicar el conocimiento y las habilidades.

Conato de incendio: Evento que puede ser controlado y dominado de forma sencilla y rápida por el personal de grupos establecidos (Brigadas) haciendo uso de los medios de protección disponibles en el área, dependencia o sector.

Conservación Documental: Conjunto de medidas de conservación preventiva y conservación – restauración, adoptadas para asegurar la integridad física y funcional de los documentos de archivo con soporte análogo.

Conservación/Restauración: Acciones que se realizan de manera directa sobre los bienes documentales, orientadas a asegurar su conservación a través de la estabilización de la materia. Incluye acciones urgentes en bienes cuya integridad material física y/o química se encuentra en riesgo inminente de deterioro y/o pérdida, como resultado de los daños producidos por agentes

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

internos y externos, sean estas acciones provisionales de protección para detener o prevenir daños mayores, así como acciones periódicas y planificadas dirigidas a mantener los bienes en condiciones óptimas.

Contingencia ambiental: Situación o evento no deseado y generalmente imprevisto que afecta negativamente al medio ambiente.

Control: Acciones reactivas de respuesta a la fase de impacto de la emergencia.

Derrame: Vertimiento accidental (no previsto) de un producto, contenido en un recipiente o recinto físico, ajeno a la operación formal.

Desastre: Daño o alteración grave de las condiciones normales de vida, causado por fenómenos naturales o antrópicos que supera la capacidad de respuesta.

Desempeño: Resultados medibles del sistema de gestión en seguridad y salud ocupacional, relativos al control de los riesgos de seguridad y salud ocupacional de la organización, basados en la política y los objetivos del sistema de gestión en seguridad y salud ocupacional.

Detección: Espacio de tiempo desde cuando un evento sucede y alguien se da cuenta. Es la fase de evacuación en que se dice que es el tiempo que transcurre cuando se presenta la emergencia y alguien la detecta.

Deterioro: Alteración o degradación de las propiedades físicas, químicas y/o mecánicas de un material, causada por envejecimiento natural u otros factores

Disposición final de documentos: Decisión resultante de la valoración hecha en cualquier etapa del ciclo vital de los documentos, registrada en las tablas de retención y/o tablas de valoración documental, con miras a su conservación total, eliminación, selección y/o reproducción. Un sistema de reproducción debe garantizar la legalidad y la perdurabilidad de la información.

Documentos electrónicos: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares.

Emergencia: Todo evento identificable en el tiempo, que produce un estado de perturbación funcional en el sistema, por la ocurrencia de un evento indeseable, que en su momento exige una respuesta mayor a la establecida mediante los recursos normalmente disponibles, produciendo una modificación sustancial pero temporal, sobre el sistema involucrado, el cual compromete a la comunidad o el ambiente, alterando los servicios e impidiendo el normal desarrollo de las actividades esenciales.

Emergencia general: Evento que precisa de la intervención de toda la Brigada de Emergencias de la **Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo)**, y la ayuda de grupos de apoyo externo. Implica la evacuación inminente.

Emergencia parcial: Evento que para ser controlado requiere la intervención del Grupo Operativo de Emergencias del sector y sus efectos se limitan a este.

Equipos de protección personal: Elementos de uso personal que de acuerdo a su labor protegen la integridad física de los trabajadores.

Escenario: Lugar donde ocurre o se desarrolla un evento.

Evacuación: Conjunto de procedimientos y acciones por el cual se protege la vida e integridad física de las personas, animales o cosas en el evento de verse amenazadas, mediante el desplazamiento de un sitio de mayor riesgo a un sitio de menor riesgo en el menor tiempo.

Evaluación de riesgos: Proceso general de estimar la magnitud de un riesgo y decir si este es tolerable o no.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Fases de la evacuación: Detección del riesgo, alarma, preparación de la evacuación y evacuación (salida del personal).

Folio: hace referencia a la mínima parte de un expediente, debido a que los expedientes se encuentran compuestos por folios o hojas.

Identificación del riesgo: Proceso para el reconocimiento de situaciones que generan riesgos y la definición de sus características.

Impacto: Acción directa de una amenaza o riesgo en un grupo de personas.

Incidente: Evento o suceso repentino que sobreviene por causa o con ocasión del trabajo, y que en circunstancias diferentes habría podido producir en el trabajador una lesión orgánica, perturbación funcional, invalidez, muerte, daño o pérdida de la propiedad o que tuvo el potencial para llegar a ser un accidente.

Incidente ambiental: Evento que bajo condiciones no controladas puede llevar a un accidente ambiental, generando pérdidas e impactos negativos sobre varios o todos los elementos del medio ambiente.

Kit de derrames: Es un conjunto de herramientas, suministros y Equipo de Protección Personal que ayudará a cualquier persona entrenada a responder a un derrame, efectuándolo de manera segura y eficiente.

Mitigación: Acciones desarrolladas, antes, durante y después de un siniestro, tendientes a contrarrestar sus efectos críticos y asegurar la supervivencia del sistema, hasta tanto se efectúe la recuperación.

PAM: Plan de Ayuda Mutua.

Plan de acción: Es un trabajo colectivo que se establece en un documento, las medidas preventivas para evitar los posibles riesgos específicos de la Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo), y que indican las operaciones, tareas y responsabilidades de toda la comunidad para contrarrestar las situaciones de inminente riesgo.

Plan de contingencia: Componente del plan de prevención, preparación y respuesta a emergencias de la Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo), que contiene los procedimientos para la pronta respuesta en caso de que se presente un evento específico.

Plan de Prevención, Preparación y Respuesta a Emergencias Integral: Es aquel en el cual se establece la estrategia para estar preparados y responder a una situación de emergencia o desastre, con potencialidad de generar pérdidas humanas, daños al medio ambiente, pérdidas materiales o económicas. Define la gestión establecida para mantener actualizada y vigentes, las políticas, estructura organizacional, objetivos, recursos, competencias, responsabilidades, procedimientos de actuación, seguimiento, control y revisiones periódicas con el fin de garantizar su eficacia cuando se requiera, con el objetivo de minimizar los daños potenciales de dicho evento.

Plan de evacuación: Conjunto de acciones y procedimientos tendientes a que las personas amenazadas por un riesgo, real o ficticio, protejan su vida e integridad física, mediante el desplazamiento hasta un sitio o lugar previamente seleccionado, aprobado y divulgado, con un mínimo riesgo y un mínimo de tiempo.

Planificación: Es la preparación previa de cualquier actividad, teniendo en cuenta experiencias anteriores, recursos actuales y conocimientos teóricos, de tal manera que pueda enfrentarse a cualquier otro evento adecuadamente.

Planos de evacuación: Es el documento esquemático y graficado donde están plasmadas las rutas de evacuación de las instalaciones físicas de la empresa, Los elementos de contingencia, la (s) ruta (s) de evacuación y el (los) punto(s) de encuentro.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Plan operativo normalizado: Es la base para la realización de tareas necesarias y determinantes para el control de un tipo de emergencia. Define el objetivo particular y los responsables de la ejecución de cada una de las acciones operativas en la respuesta a la emergencia.

Prevención: Acción de preparación y disposición, que se hace anticipadamente para evitar un riesgo o ejecutar una medida.

Rescate: Acción de liberar, recuperar, salvar, con cierto grado de dificultad y riesgo, dirigido a algo o alguien que se encuentra en peligro.

Residuo peligroso: Se denomina residuo peligroso a aquel que contiene propiedades intrínsecas que presentan riesgos para la salud y para el medio ambiente.

Respuesta: Ejecución de las acciones previstas en la etapa de planeación.

Riesgo: Es una fuente o situación con potencial riesgo de daño en términos de lesión, enfermedad o muerte, daño a la propiedad, al ambiente de trabajo o a una combinación de estos.

Riesgo significativo: Combinación de probabilidad y consecuencias de que ocurra un evento peligroso específico con potencialidad de desestabilizar a la organización.

Riesgo tolerable: Riesgo que se ha reducido a un nivel que la organización puede soportar respecto a sus obligaciones legales y su propia política de Seguridad y Salud ocupacional.

SCI: Sistema Comando de Incidentes.

Seguridad: Condición de estar libre de un riesgo, de daño inaceptable.

Simulacro: Ejercicio real de juego con roles y funciones, que se llevan a una simulación en un escenario real o construido lo más fiel posible, con fines de preparación y mitigación a un riesgo determinado.

Sistema Integrado de Conservación: Es el conjunto de planes, programas, estrategias, procesos y procedimientos de conservación documental y preservación digital, bajo el concepto de archivo total, acorde con la política de gestión documental y demás sistemas organizacionales, tendiente a asegurar el adecuado mantenimiento de cualquier tipo de información, independiente del medio o tecnología con la cual se haya elaborado, conservando atributos tales como unidad, integridad autenticidad, inalterabilidad, originalidad, fiabilidad y accesibilidad, desde el momento de su producción y/o recepción, durante su gestión, hasta su disposición final, es decir, en cualquier etapa de su ciclo vital.

8. GENERALIDADES

8.1 INFORMACIÓN BÁSICA DE LA EMPRESA

INFORMACIÓN BÁSICA DE LA ORGANIZACIÓN		
Razón social		NIT
Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo)		830.144.890
Dirección		Teléfono
Sede principal: Cra 10 No. 17-18 Edificio Colseguros Pisos 22,23,24 y 16		(+60 1) 359 94 94
Departamento	Municipio	Localidad
Cundinamarca	Bogotá	Santa Fé
Actividad Económica		Representante legal
RU6820		Carlos Felipe Reyes Forero
Responsable SST		Coordinador PPRE
Andrea Beltrán		Mauricio Liévano Pino
Horario de trabajo		Lunes a viernes de 7:30 am a 4:30 pm con 1 hora de almuerzo
Nivel de riesgo		I, IV, V
Número de trabajadores		64 servidores públicos 34 en teletrabajo
Número de contratistas		300 contratistas en promedio – No presenciales

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Geo referenciación sede principal	
La Empresa de Renovación y Desarrollo Urbano de Bogotá D.C. se encuentra ubicada en la Cra 10 No. 17- 18 Pisos 16(medio piso),22,23 y 24. Edificio Colseguros en Bogotá, Cundinamarca, se llega mediante la utilización de las rutas urbanas de la ciudad.	
Límites	
Costado oriental	Carrera 09
Costado occidental	Carrera 10
Costado sur	Cll 17 con Carrera 10
Costado norte	Cll 18 con Carrera 10
Vías de acceso sede principal	



El edificio se encuentra ubicado en el centro de Bogotá, está rodeado de diferentes sectores de comercio, oficinas, parqueaderos diferentes industrias y edificaciones gubernamentales las cuales generan diferentes potenciales de peligro como incendio, terrorismo, fenómenos naturales entre otros.

EDIFICIO CENTRO COLSEGUROS P.H.	
El edificio cuenta con las siguientes características:	
• 27 pisos • 3 sótanos. • 773 m2 por piso. • 3 puertas de acceso. • ascensores. • Cada piso cuenta con una salida de emergencias. • 2 plantas eléctricas (una para la iluminación y la otra para los ascensores y maquinas del edificio) con alcance de servicio de 48 horas, alimentada por 1.600 galones. • Área protegida por EMI. • 2 sistemas de extinción (agua nebulizado - gabinete tipo A y tipo B). • Puertas de salida de emergencias en cada piso de 76 cm de ancho y con barra antipánico. » Certificado en ISO 45001: 2018. » 3 baños por piso (3 baterías sanitarias para mujeres y hombres mas 2 orinales) mas 2 baños privados por piso. • Blindobarras desde el sótano hasta la terraza del edificio atravesando los racks. RENOBO contará con un local comercial para atención al ciudadano de 564 M2. Entre los principales recursos disponibles en el edificio Centro Colseguros, se cuenta con sistemas de alerta, señalización y alarma, descritos a continuación:	
AGUA	E.A.A.B.
LUZ	CODENSA S.A
TELEFONO	EMPRESA DE TELEFONOS DE BOGOTA ETB
GAS	GAS NATURAL S.A
Planta eléctrica	
El Edificio cuenta con dos plantas eléctricas marca POWERLINK ubicadas en la zona central del sótano 2 con acceso desde el costado oriental.	
Este equipo, en caso de fallas en el fluido eléctrico, ofrece el 100% de la energía para el funcionamiento tanto de las oficinas	

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

como de las zonas comunes. El sistema cuenta con una transferencia de tipo automático la cual enciende la planta inmediatamente se interfiere el fluido eléctrico y un sistema de paralelismo para el funcionamiento simultáneo de los dos equipos.

El sistema cuenta con un ducto de extracción que va hasta la cubierta, evitando de esta forma la contaminación a los edificios aledaños. También cuenta con un tanque de combustible con una capacidad de funcionamiento de hasta 10 horas de operación, y que está ubicado al norte de la planta con su respectivo cárcamo para control de derrames.

Sistema de bombeo de agua

El edificio cuenta con un tanque de reserva de agua (ubicado en el sótano) del proveedor IGIHM S.A. el cual suministra este líquido para las dos (2) redes:

- Red de agua potable
- Red contra incendio

Cada red cuenta con un equipo de bombas que toma el agua del tanque y lo distribuye hacia las salidas establecidas en las zonas comunes y en cada oficina, según el caso. Adicionalmente el edificio cuenta con dos pozos eyectores con dos bombas cada uno.

También cuenta con un sistema de presión tanto para agua potable como de red contra incendio, cada uno tiene su equipo independiente de bombeo, por otra parte, se encuentra el equipo eyector el cual es utilizado para retirar el agua proveniente de aguas lluvias o el exceso de agua que traigan los vehículos que lleguen a los diferentes parqueaderos.

Equipos especiales que se encuentran en el edificio

En el edificio encontramos los siguientes equipos que brindan apoyo al desarrollo de los servicios básicos:

- Subestación eléctrica según normas CODENSA S.A. E.S.P.
- Planta eléctrica de suplencia total.
- Strip telefónico según normas de la ETB.
- Equipos de bombeo del sistema eyector del edificio.
- Tanque de reserva de agua potable y para red contra incendios.
- Equipo de ventilación mecánica.
- Equipo de seguridad y control.
- Sistema de detección y extinción de incendios.
- Sistema de seguridad y control con red de CCTV.
- Equipos duplicadores de parqueo.
- Equipo de citofonía.
- Desfibrilador portátil.

Inventario Recursos Internos Actuales

En total la empresa cuenta con 33 extintores:

Sede centro piso 22, 23, 24	Cantidad
Extintores multipropósito de 10 lbs	12
Extintores Co2 20 lbs	16

Además de los extintores la empresa cuenta con los siguientes elementos para la atención y la respuesta ante emergencias.

SEDE PRINCIPAL

CANTIDAD	DESCRIPCIÓN
3	Paletas de PARE – SIGA
1	Motobomba
3	Gabinets red contra incendios
Si	Detectores de humo (sensores)
1	Sistema de alarma
1	Linterna
6	Chalecos de brigadista asignados
Ok	Señalización
Ok	Brigada de Emergencias
7	Camillas
4	Botiquín tipo A
2	Botiquín tipo B

- Sistema de detección de incendio y alarma

Este sistema está compuesto de los siguientes elementos: detectores de humo de tipo óptico, tanto en las oficinas como en las zonas comunes, estaciones manuales de alarma, sirenas y luces (strober) de emergencia, módulos de control y monitoreo NFPA y gabinetes con citófono para comunicación. Los detectores de humo funcionan de manera automática en conjunto con los módulos de monitoreo y control, Las estaciones manuales y gabinetes con citófono están diseñados para ser accionados por el usuario del edificio en caso de detectarse un conato de incendio. Estos elementos están conectados a un panel de control con baterías independientes, ubicado dentro de un gabinete especial para este fin. Adicionalmente, el edificio cuenta con un circuito independiente para iluminación en caso de emergencia.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- Gabinetes de emergencia			
Los gabinetes de emergencia se encuentran ubicados en todos los pisos del edificio teniendo en cuenta la capacidad de cada uno de ellos, para lo cual se encuentran dos en cada uno de los pisos ubicados en el ala del costado norte, y el ala del costado sur, estos gabinetes se encuentran incrustados y en los muros y contienen un extintor de 10 libras tipo ABC una pica de emergencia una llave y una manguera que está conectada con la red directa de contraincendios del Edificio.			
Inventario Recursos Externos			
En caso de emergencias, la Empresa cuenta con la siguiente red externa, que puede brindar servicios de apoyo en caso de materializarse alguna amenaza tal y como está reflejado en la siguiente tabla:			
ENTIDADES	NOMBRE	TELEFONO	DIRECCION
	Clínica Centenario	6017460111	CALLE 13 N° 17-21
	Clinica San Francisco de Asis	6015190707	Cl. 16 #16-80
	Clinica Cafam	6013077011	Sede Centro: Carrera 8 # 15-73
	Estación de Bomberos Central la Pepita	6013822500	Cl. 11 #20A-10
	CAI Colseguros	6013296992	Cra. 12 #17 - 66
	CAI Rosario	6012860744	Cra. 4 #12c - 95
	DEFENSA CIVIL	6017006465	Calle 52 No 14 - 67
	CRUZ ROJA	7460909 Ext 400	Av cra 68 No 68B - 31

9. PLAN DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS DESDE SEGURIDAD Y SALUD EN EL TRABAJO

9.1. ANÁLISIS DE AMENAZAS Y DETERMINACIÓN DE LA VULNERABILIDAD

9.1.1 Objetivos del análisis de amenazas y determinación de la vulnerabilidad desde Seguridad y Salud en el Trabajo

- Establecer el patrón de comportamiento, ubicación, consecuencias y características de los fenómenos de tipo natural, tipo antrópico, o por los procesos de trabajo que en cualquier momento pueden generar alteraciones repentinas en las actividades normales de la Empresa.
- Determinar el nivel de exposición y la predisposición a la pérdida de un elemento o grupo de elementos ante una amenaza específica, teniendo en cuenta los elementos sometidos a riesgo como son: personas, recursos, sistemas y procesos.
- Realizar un inventario específico de riesgos para la identificación de agentes generadores ligados a las instalaciones y actividades que puedan afectar en un momento dado el normal desarrollo de las actividades.

9.2. ANÁLISIS DE VULNERABILIDAD

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Vulnerabilidad: Característica propia de un elemento o grupo de elementos expuestos a una amenaza, relacionada con su incapacidad física, económica, política o social de anticipar, resistir y recuperarse del daño sufrido cuando opera dicha amenaza.

El análisis de vulnerabilidad contempla tres elementos expuestos, cada uno de ellos analizado desde tres aspectos:

CLASIFICACIÓN DE CRITERIO	PUNTO A CALIFICAR
Personas	Gestión Organizacional Capacitación y Entrenamiento Características de Seguridad
Recursos	Suministros Edificación Equipos
Sistemas y Procesos	Servicios públicos Sistemas alternos Sistemas de recuperación

Una vez determinada la vulnerabilidad, se determina el nivel de riesgo para las amenazas prioritarias calificadas como inminentes y probables, relacionado la amenaza y la vulnerabilidad de los elementos expuestos.

Estimación de las probabilidades

A continuación, se presentan los aspectos a considerar para la valoración general de las amenazas:

Históricos: Durante el año 2024 se realizaron diferentes protestas en las ciudades y en varias de ellas se tomó como punto de encuentro la cra 10ma con calle 19, generando caos a la salida del trabajo, actos vandálicos, bloqueos en vías principales de la ciudad.

No se han presentado antecedentes de conatos de incendios en las instalaciones de la empresa.

Geográficos: El edificio no se encuentra cercano a fuentes hídricas que puedan generar inundaciones, no tiene cercanía a los cerros orientales que puedan generar derrumbes.

Adicionalmente la ciudad de Bogotá está expuesta a la actividad sísmica generada por los diversos sistemas de fallas geológicas activas existentes en el país, en mayor o menor grado en función de la distancia de la capital a estos sistemas, tales como el sistema de Falla Frontal de la Cordillera Oriental (Falla Guaicáramo, Falla Algeciras), Falla Usme, Honda e Ibagué.

Bogotá se encuentra localizada en una zona de amenaza sísmica intermedia, dado que se encuentra ubicada aproximadamente a 40 km de distancia del sistema de Falla Frontal de la Cordillera Oriental (Falla del Piedemonte Llanero) que es la fuente sísmica activa más cercana a la ciudad y que tiene el potencial de generar sismos de magnitudes importantes.

La empresa se encuentra ubicada en uno de los puntos viales más importantes de la ciudad sobre la carrera 10ma , en donde convergen diferentes vías principales de la ciudad tales Cra 7ma, Av caracas, Av calle 19.

Tecnológicos: Los riesgos tecnológicos están presentes toda vez que la empresa cuenta con diferentes equipos eléctricos que permiten el desarrollo de las actividades de la misma. En el desarrollo de estas actividades pueden materializarse diferentes riesgos como fallas en sistemas de seguridad, telecomunicaciones, sistemas de información, energía, calentamiento o enfriamiento, notificación de emergencias, entre otros.

Origen antrópico: Este riesgo es aquel que se materializa como consecuencia de factores humanos y es causa en gran parte de las emergencias en el trabajo y puede ser consecuencia de aspectos como: bajo entrenamiento, descuido, conductas inapropiadas, abuso de sustancias o fatiga, entre otros.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Adicionalmente debemos contemplar los riesgos de origen público, los cuales son resultantes de acciones antrópicas que podrían poner en riesgo la seguridad y vida de los funcionarios de la empresa, acciones como (atracos, robos, asonadas, paros, actos vandálicos, entre otros).

- **Frecuencia de Exposición a la amenaza:** Está determinada por la probabilidad de ocurrencia del evento que puede originar la pérdida. De acuerdo a la frecuencia con que pueda ocurrir.
- **Generalidades de la amenaza:** Las amenazas que pueden afectar el desarrollo de actividades en la empresa son generadas por eventos naturales y/o antrópicos, de carácter interno o externo con la probabilidad de afectar diferentes sitios singularmente o en combinación. La amenaza tiene diferentes grados de intensidad y severidad.

Para realizar la priorización de los riesgos según su gravedad y organizar la información básica con el fin de dimensionar el Plan de emergencia y contingencia que desarrollará la empresa, se utilizó la matriz de priorización de riesgos que a continuación se menciona:

Clasificación de las amenazas

ITEM	AMENAZAS	ORIGEN DE LA AMENAZA
1	Falla estructural por sismo	De acuerdo con la zonificación de las instalaciones, éstas se encuentran en medio de una zona de nivel de riesgo intermedio según la microzonificación sísmica de Bogotá dada su cercanía con los cerros orientales.
2	Falla estructural por eventos atmosféricos (granizada)	Es la anomalía o irregularidad que presenta una construcción por el cambio brusco en la configuración inicial, provocada en este caso por un evento de carácter atmosférico (granizada o vendaval), lo que pueden ocasionar desde goteras hasta la falla estructural de cubiertas, ruptura de vidrios, levantamiento y desprendimiento de techos.
3	Incendio	El incendio es la ocurrencia de fuego no controlado y la explosión es la liberación de energía generada por la ocurrencia de fenómenos fisicoquímicos, generalmente después de una explosión sobreviene un incendio. Este fenómeno puede afectar a estructuras y seres vivos. Se pueden originar por fallas en el sistema eléctrico, derrames de combustible o escapes de gases inflamables en presencia de una chispa o fuego.
4	Explosión por atentado terrorista	La existencia de grupos al margen de la ley que pueden atacar en cualquier momento y en forma indiscriminada con simples artefactos artesanales como bombas incendiarias, petardos, granadas o incluso con vehículos cargados con explosivos, puede tener consecuencias de pérdidas materiales y humanas de gran impacto.
5	Hurtos o atracos	Por la existencia de este flagelo en nuestro país, originado por la delincuencia común u organizada, las entidades que funcionan en el edificio, pueden ser blanco de la delincuencia. Teniendo en cuenta las últimas manifestaciones sociales en donde se ha tomado como punto de encuentro la calle 100 con Autopista Norte, aumenta la posibilidad de actos vandálicos o robos y atracos cerca a las instalaciones de la empresa.
6	Riesgos de tránsito	Generado por colisiones, choques, atropellamientos en vía pública.
7	Bloqueo de vías	Es la congregación de un número de personas, que se reúnen en un lugar y cuyo objetivo es la protesta por cualquier inconformidad, o simplemente por la inundación de la vía en época invernal.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

ITEM	AMENAZAS	ORIGEN DE LA AMENAZA
8	Riesgo biológico	Exposiciones laborales capaces de originar algún tipo de infección, alergia o toxicidad.

Metodología de análisis de amenazas y determinación de riesgos

Para el Análisis de las Amenazas y Determinación de los Riesgos de la Empresa se tuvieron en cuenta los siguientes aspectos:

Visitas de observación por las áreas en estudio para el levantamiento de un inventario general en cuanto a: recursos internos actuales, análisis de amenazas, determinación de la vulnerabilidad y la identificación de agentes que puedan generar una emergencia en la edificación donde se encuentra ubicada.

Una vez identificadas las amenazas se procedió a evaluarlas, combinando el análisis probabilístico, con el comportamiento físico de la fuente generadora, utilizando información de eventos ocurridos en el pasado y se calificó de forma cualitativa esta información; la cual se encuentra en el siguiente cuadro de evaluación de amenazas y vulnerabilidad.

Amenazas identificadas

AMENAZA	INTERNO	EXTERNO	FUENTE DE AMENAZA	CLASIF	COLOR
Falla estructural por sismo			De acuerdo con la zonificación de las instalaciones, éstas se encuentran en medio de una zona lacustre según la microzonificación sísmica de Bogotá.	Posible	
Falla estructural por eventos atmosféricos (granizada – vendaval)			Es la anomalía o irregularidad que presenta una construcción por el cambio brusco en la configuración inicial, provocada en este caso por un evento de carácter atmosférico (granizada o vendaval), lo que pueden ocasionar desde goteras hasta la falla estructural de cubiertas, ruptura de vidrios, levantamiento y desprendimiento de techos.	Posible	
Riesgos de tránsito			Dado por colisiones o choques de vehículos, atropellamientos en vía pública.	Probable	
Incendio			El incendio es la ocurrencia de fuego no controlado y la explosión es la liberación de energía generada por la ocurrencia de fenómenos fisicoquímicos, generalmente después de una explosión sobreviene un incendio. Este fenómeno puede afectar a estructuras y seres vivos. Se pueden	Probable	

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

AMENAZA	INTERNO	EXTERNO	FUENTE DE AMENAZA	CLASIF	COLOR
			originar por fallas en el sistema eléctrico, derrames de combustible o escapes de gases inflamables en presencia de una chispa o fuego.		
Explosión por atentado terrorista			La existencia de grupos al margen de la ley que pueden atacar en cualquier momento y en forma indiscriminada con simples artefactos artesanales como bombas incendiarias, petardos, granadas o incluso con vehículos cargados con explosivos, puede tener consecuencias de pérdidas materiales y humanas de gran impacto.	Probable	
Hurtos o atracos			Por la existencia de este flagelo en nuestro país, originado por la delincuencia común u organizada, las sedes donde funciona la empresa, pueden ser blanco de la delincuencia.	Probable	
Bloqueo de vías			Es la congregación de un número de personas, que se reúnen en un lugar y cuyo objetivo es la protesta por cualquier inconformidad o paro.	Probable	

Análisis de resultados de identificación y priorización de amenazas específicas

Una vez realizada la valoración de los posibles riesgos a los que se encuentran expuestos los trabajadores de la Empresa en el desarrollo de las labores cotidianas, se pueden determinar en el análisis de vulnerabilidad las siguientes conclusiones:

- En general todas las áreas no han tenido una calificación como inminente, la mayoría de las amenazas identificadas están calificadas como probable o posible.
- El área que tendría una mayor probabilidad de ocurrencia de emergencias particularmente sería la emergencia por disturbios, atracos, vandalismo, paros nacionales, teniendo en cuenta las últimas situaciones de orden social presentadas en la ciudad.
- La probabilidad de materialización de emergencia por colapso de la estructura es bajo teniendo en cuenta la zonificación en la cual está ubicada la empresa.
- La amenaza con mayor susceptibilidad de pérdidas materiales en el edificio sería una emergencia por sismo, teniendo en cuenta la zonificación sísmica de Bogotá y los recientes movimientos telúricos que se han presentado en el continente.
- El área que presentaría mayor severidad en pérdidas en todos los eventos y promediando los posibles impactos sería la estructura del edificio y el evento que generaría mayores pérdidas sería el de explosión por algún acto vandálico producto de movilizaciones o de la situación social del país.
- Respecto al control existente, se debe priorizar el control del riesgo de colapso de estructuras, accidente por riesgo público o sismo.

Medidas de intervención frente a las amenazas

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Las medidas de control determinadas por la Empresa para prevenir los posibles eventos identificados, evaluados y priorizados en el análisis de vulnerabilidad presentado, son:

Medidas de intervención frente a amenazas

AMENAZA	MEDIDA DE INTERVENCIÓN	TIPO
Falla estructural por sismo	Planes Operativos Normalizados para atención en caso de fallas estructurales por sismo. Conformación de la brigada de evacuación y respuesta ante emergencias. Simulacros de evacuación.	Preventiva
Falla estructural por eventos atmosféricos (granizada – vendaval)	Capacitar al personal de soporte operativo sobre el Plan de Emergencias de las instalaciones, al igual que a los integrantes de la Brigada una vez esté constituida en primeros auxilios básicos en caso de materialización de riesgos por daños estructurales.	Preventiva
Riesgos de tránsito	Capacitar al personal de acuerdo al Plan Estratégico de Seguridad Vial con el fin de prevenir la materialización del riesgo.	Preventiva
Incendio	Capacitar a los funcionarios y Brigadistas, acerca de la existencia del riesgo de incendio, manejo de extintores, inspecciones para detectar condiciones de riesgo y uso de los sistemas de control existentes.	Preventiva
Explosión por atentado terrorista	Capacitar al personal en el Plan de contingencia por atentados, llamar al 123 y a las autoridades competentes.	Preventiva
Hurtos o atracos	Realizar capacitación en prevención del Riesgo Público. Mantener comunicación con autoridades y Plan de Ayuda Mutua.	Preventiva
Bloqueo de vías	Fortalecer la comunicación con las autoridades policiales. Tomar acciones preventivas antes de paros y bloqueos nacionales.	Preventiva

9.3. BRIGADA DE EMERGENCIAS

Se denomina Brigada de Emergencia al grupo de trabajadores que se encuentran debidamente organizados, entrenados y equipados para estar en la absoluta capacidad de identificar las condiciones de riesgo que puedan generar determinadas emergencias y así mismo se encuentran entrenados para actuar oportunamente controlando o minimizando las consecuencias de dichos riesgos identificados.

Esta brigada es conformada con el fin de promover un cambio de actitud en el personal, con la finalidad de fomentar una cultura preventiva, la cual se fundamente y respalde en la necesidad de controlar y manejar de manera organizada las condiciones laborales inadecuadas que puedan causar desastres que afecten la salud o seguridad de los trabajadores o así mismo, los bienes materiales de la empresa.

El profesional de Seguridad y Salud en el Trabajo establece y organiza la formación jerárquica y funcional de la Brigada de Emergencia, incluyendo la designación de sus respectivos jefes de los grupos de brigadas, según un organigrama previo, de este modo el profesional de Seguridad y Salud en el Trabajo, coordina con los jefes de cada área dentro de la empresa a fin de conformar la Brigada de Emergencias que estará capacitada para la atención de:

- Primeros Auxilios

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- Prevención y extinción de incendios
- Evacuación y Rescate

También se debe considerar que el Profesional de Seguridad y Salud en el Trabajo mantenga una lista actualizada de los brigadistas acreditados y vigentes.

La brigada debe reunirse a fin de coordinar las acciones a tomarse en caso de un imprevisto siendo recomendable como mínimo 2 veces al año, esta reunión será coordinada con el Profesional de Seguridad y Salud en el Trabajo.

El perfil para pertenecer a la Brigada de Emergencias es el siguiente:

Poseer de manera natural sin ser obligado voluntad, pro actividad ánimo y espíritu de colaboración, y contar con conocimiento sobre evacuación, rescate, primeros auxilios, control de derrames e incendios. Así mismo, se debe encontrar en buenas condiciones físicas y psicológicas a fin de participar óptimamente en las operaciones de la brigada y en las prácticas de entrenamiento. Algunas características a considerar como favorables para ser parte de una brigada son:

- **Condiciones físicas**
 - Estar en la edad donde la capacidad física no se vea disminuida, entre 18 a 60 años de edad.
 - Deben poseer una relación peso-estatura adecuada.
 - No padecer problemas cardiovasculares ni respiratorios que compliquen la salud del brigadista durante una emergencia.
- **Condiciones Psíquicas**
 - Poseer estabilidad emocional.
 - Tener aptitudes de liderazgo.
 - Tener disposición de colaboración, capacidad de aprendizaje. Poseer iniciativa propia, capacidad para tomar decisiones.
 - No padecer claustrofobia, vértigo u otra afección.
 - Tener aptitud para el trabajo en equipo.
 - Tener aceptación de sus compañeros.
- **Condiciones complementarias recomendables**
 - Haber pertenecido, en empleos anteriores, a grupos de esta naturaleza, lo cual facilitaría enormemente el aprendizaje o entrenamiento orientado a alcanzar los objetivos básicos de un brigadista.
 - Si es o fue en su momento bombero, también implica una ventaja, para aprovechar los conocimientos de éste, en beneficio de los demás integrantes de la brigada.
 - También resultaría positivo si ha participado en cursos de primeros auxilios o respuesta ante emergencias.
 - De ocurrir la emergencia en horas laborables, es su deber permanecer en la Empresa, realizando tareas que le correspondan de acuerdo al Plan.

9.4. RESPONSABILIDADES DEL COMITÉ DE EMERGENCIAS Y CONTINGENCIAS Y BRIGADA DE EMERGENCIAS

En este numeral se establece para cada persona o grupo de personas responsables las indicaciones puntuales frente a una situación de emergencias; esto se hace con el fin de facilitar el aprendizaje, el entrenamiento, el desarrollo de procedimientos más específicos y, por lo tanto, la respuesta adecuada.

En la Empresa se cuenta con una brigada integral, con la capacidad de reacción frente a los diferentes tipos de emergencias que se pueden materializar, los cuales son: incendios, atención de primeros auxilios y evacuación.

CARGO	RESPONSABILIDAD
Comité de Emergencias y Contingencias	✓ Motivar la participación de los miembros de sus áreas de trabajo en todas las actividades que se convoquen para

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

CARGO	RESPONSABILIDAD
	fortalecer el plan de emergencias. ✓ Dar ejemplo en el cumplimiento de las normas de seguridad y el interés por la eficaz ejecución del plan. ✓ Aportar los recursos humanos, físicos y financieros necesarios para ayudar a asegurar la adecuada ejecución del plan. ✓ Planear y organizar las diferentes acciones y recursos para la eficaz atención de una eventual emergencia. ✓ Conocer el funcionamiento de la empresa, las instalaciones, las emergencias que se puedan presentar y los planes normativos y operativos de la misma. ✓ Realizar reuniones periódicas para mantener actualizado el plan. ✓ Activar la cadena de llamadas de los integrantes del comité. ✓ Evaluar las condiciones y magnitud de la emergencia. ✓ Establecer contacto con los grupos de apoyo y los directivos de la empresa y si es necesario con los organismos externos (Bomberos, Defensa Civil, Cruz Roja, Comités de emergencias, etc.)

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

CARGO	RESPONSABILIDAD
Brigadistas frente a una situación de primeros auxilios	✓ Determinar qué tipo de elementos de primeros auxilios son necesarios para la empresa. ✓ Realizar entrenamiento periódico sobre atención de pacientes. ✓ Atender en sitio seguro al personal afectado y lesionado. ✓ Clasificar al personal de acuerdo a la gravedad de su lesión para una mejor y más eficaz atención (Triage). ✓ Preparar al personal clasificado en nivel prioritario para su pronta evacuación hacia un centro hospitalario. ✓ Llevar el control estadístico de pacientes, lesiones presentadas, atención suministrada, a donde se remitió etc. ✓ Mantener adecuadamente dotados y llevar control del uso de los botiquines. ✓ Participar activamente en las brigadas y campañas de salud que se organicen en la empresa como parte del Sistema de Gestión de la Seguridad y Salud en el Trabajo. ✓ Reorganizar los elementos utilizados, velando por la reposición del material gastado.
Brigadistas frente a una situación de evacuación y rescate	✓ Conocer el Plan de emergencias y capacitar a los funcionarios de la empresa. ✓ Implementar y difundir el sistema de alarma. ✓ Señalizar y mantener despejadas las vías de evacuación. ✓ Dirigir en forma ordenada y correcta la salida de las personas en caso necesario. ✓ Mantener un control efectivo sobre las personas para evitar aglomeraciones y estados de pánico. ✓ Proceder en forma segura y técnica al rescate de las personas que se encuentren heridas o atrapadas. ✓ Verificar una vez finalizada la evacuación que dentro de las instalaciones no quede ninguna persona. ✓ Instruir a todo el personal en el Plan de evacuación. ✓ Mantener un listado actualizado de las personas que laboran en su área. ✓ Evaluar el proceso de evacuación dado, determinando si estaba o no de acuerdo con el plan.

9.5. CONFORMACIÓN DE LA BRIGADA

La Brigada de Emergencia debe estar conformada por trabajadores de la empresa de todas las áreas, y deben estar en la capacidad de dar respuesta a las contingencias que se presenten en la Empresa.

Una vez elegidas las personas miembros de la Brigada de Emergencias, se capacitarán en primeros auxilios, prevención y extinción de incendios, evacuación y rescate.

La Empresa ha constituido la Brigada de Emergencias de manera integral, todos los brigadistas están en la facultad de atender cualquier tipo de emergencia sea de incendios, evacuación o primeros auxilios y los miembros se actualizan de manera anual.

9.6. PLAN DE EVACUACIÓN

Se debe instruir al personal sobre la identificación de emergencias que ameriten evacuación. En caso de ser necesario, los brigadistas darán la instrucción de evacuación y dirigir a los trabajadores, contratistas y visitantes de la empresa, al punto de encuentro y notificar al Comité de Emergencias y Contingencias para determinar si es necesaria la ayuda externa.

Tipo y Codificación de la Alarma de Evacuación

Sede principal

El sistema de alarma del Edificio en donde se encuentra RENOBO es:

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- ✓ Sonora.
- ✓ Es un medio masivo.
- ✓ Es identificada por todo el personal.
- ✓ La sirena es automática y está en todos los puntos del edificio.

El Plan de evacuación de la organización se compone de cuatro fases que son:

1. **Detección de la emergencia**

Tiempo transcurrido desde que se origina el peligro hasta que alguien o algo lo reconocen. El tiempo depende de:

- La clase de riesgo.
- Los medios de detección disponibles.
- Uso y ocupación en la edificación.
- Día y hora del evento.

2. **Alarma**

Tiempo transcurrido desde que se detecta el peligro hasta que se toma la decisión de evacuar y se informa a los ocupantes. El tiempo depende del:

- Sistema de alarma.
- Adiestramiento del personal.

3. **Preparación de la salida de ser necesario**

Tiempo transcurrido desde que se da la alarma hasta que sale la primera persona. El tiempo depende del entrenamiento.

- Verificar quiénes y cuántas personas hay.
- Disminuir nuevos riesgos.
- Proteger valores.
- Recordar el punto de encuentro.

4. **Salida**

Tiempo transcurrido desde que sale la primera persona, hasta que sale la última. El tiempo depende de:

- Número de personas.
- Distancia a recorrer.
- Capacidad de las vías.
- Limitante de los riesgos.

Punto de encuentro

En caso de situaciones de emergencia que requiera la evacuación del personal de las instalaciones de la Empresa, se deben tener definidos los puntos de encuentro que se utilizarán para la agrupación de todo el personal.

Punto de encuentro Sede principal

En la **Empresa de Renovación y Desarrollo Urbano de Bogotá (RenoBo)**, se ubicó un punto de encuentro parcial en la PLAZOLETA al lado de la torre ubicada sobre la Carrera 10, este para emergencias que no ameriten la evacuación total del edificio. Cuando el tipo de emergencia o desastre amerite evacuación total, este sitio se utilizara para la agrupación y conteo de todo el personal en el parque SANTANDER ubicado en la Carrera 7 con Calle 15.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS



SE RECOMIENDA EVACUAR EN:	ACCIONES DE NO EVACUACIÓN	NO SE RECOMIENDA EVACUAR
Incendio Explosión interna Debilitamiento de estructuras físicas Después de un sismo Amenaza de bomba y según recomendaciones de la Policía Nacional Inundación (si no es seguro) Roturas de tuberías (si no es seguro)	Refugiarse al interior y si la emergencia lo amerita ubicarse debajo de mesas, escritorios, sillas lejos de ventanales o si se encuentra en corredores agacharse y cubrirse la cabeza con las manos.	Durante un movimiento sísmico Explosión externa Toma armada Robo

Tiempo total de evacuación

El tiempo total de evacuación se toma como el tiempo que se requiere para realizar toda la evacuación de las instalaciones, desde que se da la alarma hasta que sale la última persona.

El tiempo de llegada al punto de encuentro, desde el punto más lejano dentro de las instalaciones, se determinará de acuerdo con información presentada a continuación.

Para estimar este tiempo de evacuación se debe tener en cuenta las siguientes variables:

- El tiempo de detección (T_d). Tiempo que se toma en iniciar la alarma desde que se detecta la emergencia.
- El tiempo de alarma (T_A). Tiempo que toma para que se haga la emisión por los medios de alerta respectivos.
- El tiempo de retardo e identificación de las vías de evacuación (T_R). Tiempo que toma a las personas, asimilar la voz de alarma y ubicar la salida de emergencia, este tiempo depende de la preparación del personal y de la señalización.
- El tiempo actual de evacuación (T_E). Tiempo que toma al personal recorrer los caminos de evacuación al punto de encuentro.

La suma de todas estas variables da como resultado el tiempo que toma realizar la evacuación completa.

Entrenamiento y difusión

El Comité de Emergencias y Contingencias debe recibir una capacitación anual mínimo de dos (2) horas en Sistema Comando de Incidentes, así tengan completamente definidos sus roles

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

frente a una emergencia. La Brigada de Emergencias debe recibir un entrenamiento integral con una capacitación bimestral.

Periódicamente debe difundirse en diferentes medios (visuales o auditivos), las acciones a seguir al momento de presentarse una emergencia.

Señalización

La organización cuenta con señalización en todas sus instalaciones, que indican las rutas de evacuación, ubicación de extintores, botiquines, camillas, planos de evacuación, etc.

Simulacros de emergencia

Los simulacros permiten poner en práctica un plan y una organización previstos por el personal de respuesta a emergencia (Brigada), para evaluar su desarrollo y realizar los ajustes necesarios.

Algunos de los aspectos que se tratan de verificar en un simulacro son:

- Comunicaciones de emergencias.
- Procedimiento general de alarma.
- Accionamiento de sistemas de protección contra incendios.
- Comportamiento y tiempo de reacción de los ocupantes de la edificación o instalación.
- Movilización y posicionamiento de equipos de emergencias.
- Tiempo de reacción de las Brigada para Emergencias.
- Procedimientos y decisiones claves del comandante de incidentes.
- Procedimientos y decisiones claves de la Brigada para Emergencias.
- Cumplimiento de procedimientos de seguridad en el área en emergencia.
- Interacción con grupos de apoyo externo.
- Nivel de intervención de los grupos de apoyo externo.

El objetivo es verificar en sitio y tiempo real, la capacidad de respuesta de las personas y la organización operativa del Plan para emergencias ante un evento de posible ocurrencia, basado en los procedimientos para emergencias.

Metodología

- Seleccionar un escenario creíble para una emergencia simulada.
- Preparar un documento de planeación general del simulacro.
- Suponer una situación típica en el escenario con algunas variantes en su desarrollo que permitan verificar la iniciativa y criterios de los participantes.
- Establecer cuál debería ser la respuesta adecuada para cada situación planteada.
- Seleccionar suficientes Veedores (internos o externos) para el análisis y calificación del ejercicio, a cada uno de los cuales se les asignan funciones específicas.
- Preparar formatos para la evaluación suficientes para cada uno de los veedores, teniendo en cuenta las funciones específicas.
- Realizar charlas de inducción previas con los veedores, para aclarar aspectos del ejercicio.
- Prevenir con suficiente anticipación a los entes de apoyo externo (Bomberos, policía, ejército, grupos antiexplosivos, entre otros).
- Dar la alarma de inicio al simulacro.
- Realizar el registro fílmico o fotográfico.
- Llevar un seguimiento a todas las comunicaciones realizadas.
- Dar por terminado el simulacro.
- Realizar reunión con los veedores para consolidar las observaciones y mediciones
- Realizar reunión general con todos los integrantes operativos del Plan, socializando los aspectos negativos y positivos observados durante el ejercicio.
- Elaborar un informe de resultados con sus correspondientes recomendaciones.

Supervisión y control

Periódicamente se ha de comprobar la correcta disponibilidad y adecuación del Plan de Prevención, Preparación y Respuesta a Emergencias Integral y la actualización de aquellos puntos que se detecten desfasados mediante las acciones de supervisión y control desplegadas por los siguientes medios:

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- Inspecciones
- Auditorias
- Renovación del análisis
- Análisis de simulacros periódicos

Con el objetivo de verificar la efectividad del simulacro de evacuación se realiza un informe de preparación y evaluación de simulacros.

10. PLAN DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS O DAÑOS ESTRUCTURALES

10.1 Introducción

Las emergencias estructurales representan un riesgo significativo para la integridad física de las personas, los bienes y la continuidad operativa de la Empresa. Estas emergencias pueden originarse por fallas en la infraestructura, sismos, sobrecargas, deterioro de materiales o eventos externos que comprometan la estabilidad de las instalaciones.

10.2 Objetivo General

Establecer las acciones preventivas, de preparación y respuesta ante emergencias estructurales, con el fin de salvaguardar la vida e integridad de las personas, reducir daños materiales y asegurar la continuidad operativa de la Empresa.

10.3 Objetivos Específicos

- Identificar los riesgos estructurales potenciales en la edificación.
- Establecer protocolos de actuación ante situaciones de emergencia estructural.
- Definir las funciones y responsabilidades del equipo de respuesta ante emergencias.
- Implementar estrategias de mitigación que reduzcan la probabilidad y el impacto de estas emergencias.
- Capacitar al personal en evacuación y respuesta oportuna ante eventos estructurales.

10.4 Alcance

Este plan aplica a todas las instalaciones físicas, personal, visitantes y contratistas que se encuentren en las edificaciones bajo responsabilidad de la Empresa. Abarca desde la identificación del riesgo estructural hasta la fase de recuperación post-emergencia.

10.5 Impactos del Riesgo

Las emergencias estructurales pueden generar:

- Pérdidas humanas por colapsos parciales o totales.
- Daños materiales severos a infraestructura, equipos y documentos críticos.
- Interrupción de operaciones por inhabilitación de las instalaciones.
- Afectación reputacional por una gestión inadecuada del riesgo.
- Impacto económico, por reparación de daños y costos asociados a la interrupción del servicio.

10.6 Estrategias para Mitigar el Riesgo

- Inspecciones técnicas periódicas a la infraestructura por personal especializado.
- Mantenimiento preventivo y correctivo de elementos estructurales.
- Reforzamiento estructural en zonas críticas según diagnóstico técnico.
- Cumplimiento de normativas de construcción sismo-resistente y códigos vigentes.
- Simulacros de evacuación periódicos, con enfoque específico en emergencias estructurales.
- Señalización y rutas de evacuación visibles y funcionales.
- Capacitación al personal en primeros auxilios, evacuación y puntos de encuentro.

10.7 Equipo de Respuesta ante Emergencias Estructurales

10.7.1 Composición del Equipo

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- Coordinador general de emergencias
- Líder de Revisión de infraestructura
- Líder de Brigada de emergencias
- Líder de comunicaciones
- Personal de apoyo logístico
- Brigadistas voluntarios

10.7.2 Funciones del Líder de Revisión de Infraestructura

Evaluar la seguridad estructural inmediata:

Realizar una inspección visual preliminar de las zonas afectadas para identificar daños evidentes que comprometan la estabilidad de la edificación.
Determinar si las instalaciones pueden seguir siendo utilizadas o deben ser evacuadas/restringidas.

Coordinar con profesionales técnicos especializados:

Gestionar el acompañamiento de ingenieros estructurales, arquitectos o personal calificado para una evaluación técnica más profunda, si es necesario.

Delimitar zonas de riesgo:

Señalizar, acordonar y restringir el acceso a áreas comprometidas estructuralmente para evitar incidentes secundarios.

Emitir un informe preliminar de daños:

Documentar hallazgos de manera clara, con fotografías y descripción de afectaciones estructurales visibles y sugerir acciones correctivas o recomendaciones inmediatas.

Apoyar la toma de decisiones para retorno seguro:

Brindar información técnica al Coordinador General de Emergencias para decidir si es viable el retorno a las actividades o se requiere reubicación temporal.

Revisar rutas de evacuación e infraestructura crítica:

Verificar que escaleras, pasillos, salidas de emergencia, techos y estructuras de soporte no presenten afectaciones que pongan en riesgo al personal.

Coordinar reparaciones urgentes o estabilización temporal:

En caso de afectaciones menores, gestionar acciones inmediatas para garantizar la seguridad (refuerzos provisionales entre otros).

Participar en simulacros y capacitaciones:

Aportar desde su experiencia técnica a los procesos de formación y preparación del personal en escenarios de emergencia estructural.

10.8 Evaluación de Riesgos y Estrategias para Mitigarlos

Riesgo Identificado	Probabilidad	Impacto	Nivel de Riesgo	Estrategia de Mitigación
Colapso parcial por sismo	Media	Alto	Alto	Revisión estructural periódica y reforzamiento sísmico
Grietas en muros	Alta	Medio	Alto	Mantenimiento correctivo inmediato
Sobrecarga en entresijos	Media	Alto	Alto	Control de peso, redistribución de cargas
Humedad en estructuras	Alta	Medio	Alto	Impermeabilización y reparación
Corrosión en elementos metálicos	Media	Medio	Medio	Aplicación de recubrimientos anticorrosivos
Colapso en ventanas	Alta	Alto	Alto	Realizar revisiones visuales y técnicas del estado.
Colapso, ruptura o fuga en tuberías	Alta	Alto	Alto	Realizar inspecciones visuales con herramientas de detección.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

11. PLAN DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS DOCUMENTALES

11.1 INTRODUCCIÓN

El Plan de Emergencias Documentales es una herramienta fundamental que permite a las instituciones garantizar la protección, conservación y recuperación de los documentos de valor legal, histórico, administrativo o de cualquier otra índole, en caso de que eventos inesperados o desastres pongan en riesgo su integridad. Este plan es esencial para el manejo eficaz de la información, permitiendo que las organizaciones puedan enfrentar con seguridad cualquier crisis, garantizando la preservación de su patrimonio documental y la continuidad de sus actividades operativas.

En el contexto de la normativa archivística colombiana, el Acuerdo 001 de 2015 del Archivo General de la Nación (AGN) establece los principios y directrices para la gestión de la función archivística en el Estado, incluyendo la implementación de sistemas de conservación documental que contemplen medidas específicas para la respuesta ante emergencias. Este acuerdo subraya la importancia de contar con políticas y procedimientos bien definidos para la protección de los archivos, para asegurar que, frente a cualquier eventualidad, la documentación institucional no solo sea preservada, sino que pueda ser rápidamente recuperada para continuar con las actividades de la entidad.

Asimismo, el Plan de Emergencias Documentales debe alinearse con los lineamientos establecidos en la Ley 594 de 2000 (Ley General de Archivos), que establece los requisitos básicos para la gestión documental en el ámbito público, incluyendo la obligación de adoptar medidas preventivas y de protección ante riesgos, y la obligación de garantizar que los documentos sean preservados de manera efectiva, con miras a su recuperación total después de cualquier incidente disruptivo.

Este plan no se limita a definir procedimientos para la protección física y digital de los documentos, sino que debe incorporar un enfoque integral que contemple diversas medidas de seguridad, tales como la instalación de sistemas de respaldo y la implementación de protocolos rigurosos para la gestión de la información. Además, el plan debe establecer claras líneas de responsabilidad, definir los roles de los miembros del equipo encargado de la respuesta ante emergencias y garantizar una rápida movilización de los recursos necesarios para contener el daño y preservar la documentación. También debe incluir estrategias para la restauración y recuperación de documentos dañados, y prever mecanismos de acceso a la información crítica en situaciones adversas.

El Plan de Emergencias Documentales debe contemplar un enfoque de continuidad operativa, lo que implica que las entidades no solo deben ser capaces de proteger sus documentos, sino también mantener su capacidad de cumplir con funciones esenciales, incluso en condiciones extremas. Esto es vital para evitar la paralización de procesos y garantizar que la entidad pueda seguir operando con normalidad a pesar de cualquier eventualidad.

Además, la correcta implementación de este plan es un componente esencial de la gestión archivística moderna, ya que no solo facilita el cumplimiento de la normatividad vigente, sino que también protege la memoria institucional y permite la recuperación rápida de información, lo que resulta crucial para la toma de decisiones, la transparencia y el acceso a la información pública.

Es importante señalar que el acervo documental físico de la empresa Renobo se encuentra bajo la custodia de Servicios Postales Nacionales (SPN), en el marco de un contrato administrativo que regula las condiciones de almacenamiento, conservación y protección de los documentos. Como productora de la documentación, Renobo tiene la responsabilidad de velar por el cumplimiento de los lineamientos establecidos en el Plan de Emergencias Documentales, garantizando que el servicio contratado por SPN se ajuste a las normativas y directrices pertinentes, asegurando así la correcta gestión y preservación de su acervo documental en todo momento, incluso ante situaciones de emergencia.

11.2. OBJETIVO

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

El Plan de Emergencias Documentales en RENOBO es garantizar la protección, recuperación y continuidad de los documentos críticos de la entidad ante emergencias o desastres. Este plan busca asegurar que, ante eventos inesperados como desastres naturales, fallos tecnológicos, ciberataques o errores humanos, los documentos importantes sean preservados y puedan ser recuperados de manera rápida y eficiente, minimizando su impacto en las operaciones y el cumplimiento de las obligaciones legales y operacionales de RENOBO.

11.2.1 Objetivos Específicos:

- **Proteger la Información Crítica:** Asegurar la preservación de documentos esenciales (físicos y electrónicos) para el funcionamiento de RENOBO y el cumplimiento de sus obligaciones legales.
- **Establecer Procedimientos de Recuperación Eficaces:** Definir pasos claros para la restauración de la información, garantizando una recuperación eficiente y oportuna.
- **Minimizar la Interrupción de las Operaciones:** Mantener la continuidad operativa mediante estrategias que aseguren la disponibilidad de los documentos a través de respaldos adecuados.
- **Prevenir la Pérdida de Información:** Implementar medidas preventivas, como copias de seguridad y seguridad cibernética, para minimizar los riesgos de pérdida de documentos.
- **Cumplir con los Requerimientos Legales y Regulatorios:** Garantizar que RENOBO cumpla con las normativas relacionadas con la conservación y gestión documental, incluso en emergencias.
- **Capacitar al Personal:** Asegurar que todos los empleados reciban formación en gestión documental en emergencias para una respuesta rápida y eficaz.
- **Evaluar y Mejorar el Plan Continuamente:** Realizar revisiones periódicas del plan para adaptarlo a nuevas necesidades, avances tecnológicos y riesgos emergentes.
- **Seguimiento a las Actividades del Prestador del Servicio de Custodia:** Implementar un sistema de seguimiento y supervisión continuo de las actividades realizadas por el prestador del servicio de custodia de documentos, asegurando que se cumplan con los estándares de seguridad, conservación y disponibilidad de la información. Este seguimiento incluye la verificación de los procedimientos de custodia, los informes periódicos sobre el estado de los documentos y la revisión de las copias de seguridad. Además, se establecerá una comunicación constante con el prestador para garantizar que todos los procesos estén alineados con los objetivos de protección documental de RENOBO, y que cualquier incidencia o riesgo identificado sea abordado de manera oportuna.

11.3. ALCANCE.

El Plan de Emergencias Documentales en RENOBO abarca la protección, preservación, recuperación y continuidad de toda la documentación crítica de la entidad, tanto física como digital. El plan cubre todos los documentos esenciales para el funcionamiento y cumplimiento de las obligaciones legales de RENOBO, estableciendo procedimientos claros ante emergencias o desastres, como desastres naturales, fallos tecnológicos o ciberataques. Incluye la supervisión de las actividades del prestador de servicios de custodia, asegurando que se mantengan altos estándares de seguridad, conservación y recuperación de documentos. Además, contempla la capacitación del personal involucrado y la evaluación continua de los procedimientos y recursos para garantizar la efectividad del plan. También asegura el cumplimiento con las normativas legales y regulatorias aplicables en materia de conservación y protección de la información.

11.4 IDENTIFICACIÓN Y DESCRIPCIÓN DE RIESGOS INFORMACIÓN FÍSICA

Riesgo: Pérdida de Documentación Física

Descripción del Riesgo: La pérdida de documentación física es un riesgo crítico que puede afectar la integridad y disponibilidad de la información archivada, lo que puede derivar en dificultades operativas y legales. Este riesgo puede manifestarse en varias formas, incluyendo la destrucción accidental, el extravío, el deterioro por condiciones ambientales inadecuadas, o la falta de un sistema adecuado de control y conservación.

Causas Comunes:

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- ❖ **Condiciones inadecuadas de almacenamiento:** La falta de controles ambientales adecuados (como temperatura y humedad) puede causar deterioro en documentos físicos, como el amarilleo, la ruptura o el daño por hongos.
- ❖ **Condiciones relacionadas con el mantenimiento del depósito en el que se encuentra en custodia del acervo documental:** Las instalaciones del depósito deben ser resistentes y seguras, con estructuras capaces de soportar cargas pesadas (por ejemplo, estanterías y archivadores). La infraestructura debe contar con sistemas de detección y/o mitigación de incendios, rociadores, alarmas, y medidas preventivas para minimizar riesgos de siniestros.
- ❖ **Desastres naturales o eventos accidentales:** Inundaciones, incendios u otros desastres pueden dañar o destruir documentos almacenados físicamente.
- ❖ **Errores humanos:** La manipulación incorrecta o el archivo inadecuado de documentos puede llevar a su pérdida o destrucción accidental.
- ❖ **Falta de capacitación o conciencia del personal:** Si el personal no está debidamente capacitado en gestión documental, puede haber negligencia en el manejo adecuado de los archivos, aumentando el riesgo de pérdida.

Impactos del Riesgo:

- ❖ **Pérdida de información clave:** La desaparición de documentos importantes puede afectar la toma de decisiones, los procesos operativos y los requisitos legales.
- ❖ **Multas o sanciones:** La pérdida de documentos relacionados con la transparencia, la fiscalización o la auditoría podría resultar en sanciones o multas para la entidad.
- ❖ **Daño a la reputación:** La pérdida de documentos importantes puede dañar la imagen y credibilidad de la entidad ante la sociedad y otras organizaciones.
- ❖ **Retrasos y dificultades en la gestión:** La falta de acceso a información clave puede generar retrasos en proyectos o en la resolución de trámites administrativos.

Estrategias para Mitigar el Riesgo:

- ❖ **Condiciones de almacenamiento adecuadas:** Asegurar que los documentos se almacenen en condiciones controladas (temperatura, humedad, seguridad) que minimicen el riesgo de deterioro.
- ❖ **Digitalización de documentos:** Promover la digitalización de documentos físicos para crear copias de seguridad electrónicas que permitan recuperar la información en caso de pérdida física.
- ❖ **Capacitación continua del personal:** Brindar capacitación constante al personal sobre buenas prácticas de archivo y gestión documental para evitar errores humanos.
- ❖ **Planes de contingencia:** Desarrollar y mantener planes de emergencia para la protección de archivos en caso de desastres naturales, incendios u otros incidentes.
- ❖ **Control y monitoreo regular:** Establecer un programa de auditorías periódicas para revisar la integridad de los archivos y la eficacia de los controles existentes.

11.5 IDENTIFICACIÓN Y DESCRIPCIÓN DE RIESGOS INFORMACIÓN ELECTRÓNICA Y/O DIGITAL.

Riesgo: Pérdida de Documentación electrónica y/o digital.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Descripción del Riesgo: El riesgo asociado a la información electrónica hace referencia a la posibilidad de que los datos almacenados en formato digital se vean comprometidos, deteriorados o se pierdan debido a diversos factores, tanto internos como externos. Estos riesgos pueden tener un impacto directo en la operatividad de la Empresa, afectando su capacidad para tomar decisiones, cumplir con sus obligaciones legales, y mantener la transparencia y el acceso a la información.

Los riesgos relacionados con la información electrónica pueden clasificarse en varias categorías, que incluyen factores técnicos, de ciberseguridad, humanos, ambientales, y operacionales. A continuación, se describen los principales riesgos de manera general:



Causas Comunes

Causas Técnicas.

- ❖ **Fallas de hardware:** Los discos duros, servidores y dispositivos de almacenamiento pueden fallar debido a defectos de fabricación, desgaste o mal funcionamiento, lo que puede resultar en la pérdida de datos.
- ❖ **Corrupción de archivos:** Errores en la transmisión de datos, interrupciones durante la escritura de archivos o fallos en el sistema de almacenamiento pueden causar corrupción de los archivos, volviéndolos ilegibles o inaccesibles.
- ❖ **Errores de software:** Los fallos en los programas utilizados para almacenar o gestionar la documentación electrónica pueden ocasionar la eliminación o la corrupción de los archivos, especialmente si el software no se actualiza regularmente o tiene fallos de programación.
- ❖ **Falta de redundancia o sistemas de respaldo:** La ausencia de copias de seguridad adecuadas o de sistemas de redundancia puede hacer que, en caso de un fallo en el sistema primario, los datos se pierdan sin posibilidad de recuperación.

Causas de Ciberseguridad.

- ❖ **Ataques cibernéticos:** Hackeos, malware, ransomware y otros tipos de ciberataques pueden provocar la pérdida, corrupción o encriptación de los datos, dejándolos inaccesibles hasta que se pague un rescate (en el caso del ransomware).
- ❖ **Accesos no autorizados:** La falta de controles de acceso adecuados puede permitir que personas no autorizadas eliminen o alteren información crítica, ya sea intencionalmente o por error.
- ❖ **Vulnerabilidades de seguridad:** La presencia de fallos en el sistema de seguridad, como contraseñas débiles, configuraciones incorrectas o software desactualizado, puede hacer que los sistemas sean más vulnerables a ataques o pérdidas de datos.

Causas Humanas

- ❖ **Errores humanos:** Los colaboradores pueden cometer errores al gestionar o almacenar datos, como eliminar archivos por accidente, sobrescribir documentos importantes o guardar información en ubicaciones incorrectas.
- ❖ **Falta de capacitación:** La falta de conocimientos adecuados sobre la gestión de información electrónica y las mejores prácticas de seguridad puede llevar a la mala gestión de los documentos digitales.
- ❖ **Acciones malintencionadas:** El sabotaje o las actividades maliciosas por parte de empleados pueden causar la pérdida de documentación crítica o la alteración de los archivos.

Causas Ambientales

- ❖ **Desastres naturales:** Inundaciones, incendios, terremotos o tormentas pueden destruir los servidores y centros de almacenamiento, causando la pérdida física de la información almacenada en dispositivos de hardware.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- ❖ **Condiciones desfavorables de almacenamiento:** Los equipos de almacenamiento mal mantenidos, expuestos a temperaturas extremas, humedad o polvo, pueden fallar y resultar en la pérdida de datos.
- ❖ **Desastres tecnológicos:** Cortes de energía prolongados o problemas con los generadores de respaldo pueden afectar la operación de los sistemas de almacenamiento de datos, causando la pérdida de archivos electrónicos no guardados correctamente.

Causas Operacionales

- ❖ **Falta de políticas de gestión de datos:** La ausencia de políticas claras sobre el manejo, almacenamiento y conservación de la documentación electrónica puede generar caos en la gestión de la información, lo que facilita la pérdida o eliminación de datos importantes.
- ❖ **No implementación de sistemas de respaldo:** No contar con procedimientos regulares de respaldo, o hacer un respaldo insuficiente, puede hacer que la información se pierda permanentemente cuando ocurre un fallo en el sistema.
- ❖ **No actualización de infraestructura tecnológica:** El uso de sistemas obsoletos o mal configurados puede aumentar el riesgo de pérdida de datos debido a fallos de hardware o software, o la falta de capacidad para soportar volúmenes de datos más grandes o complejos.
- ❖ **Falta de planes de recuperación ante desastres:** No contar con un plan formal de recuperación de datos o procedimientos de contingencia puede dificultar la restauración de la documentación en caso de incidentes graves.

Causas relacionadas con la Integración de Sistemas

- ❖ **Problemas de interoperabilidad:** La incompatibilidad entre sistemas antiguos y nuevos puede generar fallos en la transferencia o el acceso a datos, lo que puede resultar en la pérdida de información durante el proceso de migración o integración.
- ❖ **Manejo inapropiado de los metadatos:** La incorrecta asignación de metadatos o la falta de estructuración adecuada de los datos puede dificultar la búsqueda y recuperación de archivos, aumentando el riesgo de pérdida de información clave.

Causas relacionadas con la Falta de Monitoreo y Auditoría

- ❖ **Ausencia de auditorías regulares:** No realizar auditorías periódicas para verificar la integridad y seguridad de los datos puede hacer que los problemas de pérdida o corrupción de datos pasen desapercibidos hasta que sea demasiado tarde.
- ❖ **Falta de monitoreo de acceso y actividad:** No contar con sistemas de monitoreo para rastrear el acceso a los archivos y detectar actividades inusuales puede permitir que los archivos sean eliminados o alterados sin ser detectados.

11.6 EQUIPO DE RESPUESTA ANTE EMERGENCIAS DOCUMENTALES

Es un grupo interdisciplinario y especializado dentro de RENOBO, encargado de coordinar, ejecutar y supervisar todas las actividades relacionadas con la protección, recuperación y conservación de la documentación crítica en situaciones de emergencia. Este equipo es clave para garantizar que, ante cualquier evento que ponga en riesgo la integridad de los documentos de la entidad, las acciones sean tomadas de manera rápida, eficiente y organizada.

Composición del equipo:

- ❖ **Coordinador de Emergencias Documentales:** Es la persona encargada de liderar el equipo, tomar decisiones críticas durante las emergencias, coordinar las acciones entre los diferentes miembros del equipo y con otros departamentos de la entidad, y garantizar que se sigan los procedimientos establecidos en el plan. Para los documentos físicos, esta tarea será realizada por el **Supervisor del Contrato de Custodia** y/o el **Apoyo a la Supervisión**, quienes serán responsables de gestionar y coordinar la protección, recuperación y conservación de los documentos físicos en situaciones de emergencia, asegurando que se sigan los protocolos adecuados de seguridad y recuperación establecidos en el plan de emergencias.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- ❖ **Responsable de Gestión Documental:** Encargado de la supervisión y aseguramiento de la correcta ejecución de los procedimientos de gestión documental y recuperación de la información. También asegura que todos los documentos esenciales estén correctamente clasificados y almacenados para facilitar su pronta recuperación. Esta actividad será realizada por el **Líder Operativo del Proceso de Gestión Documental**, quien garantizará que todos los documentos físicos y electrónicos se gestionen de acuerdo con los procedimientos establecidos para su protección y recuperación en situaciones de emergencia.
- ❖ **Responsable de Tecnología y Sistemas:** Este miembro desempeña un papel crucial en la recuperación de la documentación electrónica, garantizando la integridad y disponibilidad de los datos digitales en caso de emergencia. Se encarga de la gestión y ejecución de respaldos digitales periódicos, asegurando que todos los documentos electrónicos estén adecuadamente respaldados y sean fácilmente recuperables en caso de pérdida. Además, es responsable de la restauración de bases de datos y sistemas críticos, la protección de la infraestructura tecnológica frente a posibles amenazas externas e internas, y la mitigación de riesgos tecnológicos como ciberataques, fallos de servidores, o vulnerabilidades de sistemas. Esta actividad será realizada por el **Líder del Proceso TIC**, quien supervisará la correcta implementación de las políticas de seguridad digital, realizará pruebas de recuperación de datos, y coordinará las acciones necesarias para restaurar la operatividad de los sistemas tecnológicos afectados durante una emergencia.
- ❖ **Responsable de Custodia y Seguridad de Documentos:** Este miembro es responsable de crear y establecer los lineamientos para la protección de los documentos antes, durante y después de una emergencia, asegurando que se mantengan en condiciones óptimas para su recuperación en cualquier situación. Supervisa y asegura que se sigan rigurosamente los protocolos de seguridad establecidos para la protección de los archivos, implementando medidas preventivas y correctivas según sea necesario. Esta actividad será realizada por el **Líder Operativo del Proceso de Gestión Documental**, quien será responsable de desarrollar y garantizar que los lineamientos de seguridad, tales como el acceso controlado a las áreas de almacenamiento, el manejo adecuado de los documentos y la protección frente a riesgos físicos, sean implementados y actualizados para proteger la integridad de los documentos.
- ❖ **Personal de Soporte Operativo:** Integrantes del equipo encargados de la ejecución de las tareas operativas, como la clasificación de documentos dañados, la restauración física de archivos, y el apoyo en la implementación de medidas de contingencia durante una emergencia.
- ❖ **Responsable de Comunicación:** Se encarga de gestionar las comunicaciones internas y externas durante una emergencia, asegurando que todas las partes interesadas (empleados, proveedores, autoridades) estén informadas de las acciones en curso.
- ❖ **Responsable de Capacitación:** Este miembro se enfoca en la formación del personal en los procedimientos de respuesta ante emergencias documentales, asegurando que todos los empleados estén debidamente entrenados sobre cómo actuar en caso de una emergencia y en el uso adecuado de las herramientas y protocolos establecidos. Esta actividad será coordinada con el proceso de Talento Humano, en el marco de la implementación del Plan Institucional de Capacitaciones. Las capacitaciones serán desarrolladas por los colaboradores del Proceso de Gestión Documental y los responsables de la custodia, en el contexto del contrato de servicios, asegurando que el personal reciba la formación necesaria para afrontar eficazmente cualquier situación de emergencia.

Funciones del Equipo:

- ❖ **Desarrollar y Ejecutar Procedimientos:** Asegurar que se sigan los procedimientos establecidos en el Plan de Emergencias Documentales.
- ❖ **Monitoreo y Evaluación:** Evaluar continuamente la efectividad del plan, realizando simulacros, pruebas y ajustes según las necesidades.
- ❖ **Gestión de Recursos:** Asegurar que todos los recursos necesarios para la protección y recuperación de documentos estén disponibles y sean operativos.
- ❖ **Comunicación y Coordinación:** Mantener una comunicación efectiva con todos los departamentos y con el prestador del servicio de custodia, así como con las autoridades pertinentes.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- ❖ **Informe y Seguimiento:** Tras una emergencia, el equipo es responsable de elaborar informes detallados sobre los incidentes ocurridos, las acciones tomadas y las lecciones aprendidas, para mejorar el plan y las respuestas futuras.

Este equipo debe estar preparado para actuar de manera inmediata y eficiente, garantizando que la documentación esencial de RENOBO se preserve y recupere con el mínimo impacto en las operaciones de la Empresa.



11.7 EVALUACIÓN Y CLASIFICACIÓN DE DOCUMENTOS

- ❖ **Identificación de documentos críticos:** Hacer un inventario de los documentos más importantes que deben ser protegidos, como los legales, financieros, contratos, registros históricos y cualquier otro documento esencial para el funcionamiento de la entidad.
- ❖ **Clasificación de documentos:** Establecer una jerarquía de importancia para los documentos, diferenciando entre los que requieren protección inmediata y aquellos cuya pérdida puede tener un impacto menor.
- ❖ **Prioridad en la recuperación:** Definir un orden de recuperación basado en la importancia y la criticidad de los documentos.

11.8. ESTRATEGIAS DE PREVENCIÓN Y PROTECCIÓN

RENOBO, a través de la implementación del Sistema Integrado de Conservación Documental, realizará el seguimiento y monitoreo de las acciones orientadas a los programas de conservación preventiva, los cuales buscan garantizar la integridad física, química y digital de los documentos entre ellos los que se relacionan a continuación:

1. Capacitación y sensibilización.
2. Inspección y mantenimiento de sistemas de almacenamiento e instalaciones físicas.
3. Saneamiento ambiental: desinfección, desratización y desinsectación.
4. Monitoreo y control de condiciones ambientales.
5. Almacenamiento y realmacenamiento.
6. Prevención de emergencias y atención de desastres.

Dicho seguimiento se llevará a cabo directamente sobre las acciones y responsabilidades del custodio de la información, quien tiene a su cargo la aplicación de medidas técnicas, administrativas y operativas que aseguren la adecuada conservación de los documentos en el marco de los riesgos identificados por la normativa vigente, conforme a lo establecido en el Acuerdo 001 de 2024 “Por el cual se establece el Acuerdo Único de la Función Archivística, se definen los criterios técnicos y jurídicos para su implementación en el Estado Colombiano y se fijan otras disposiciones.”

11.9. ATENCIÓN DE EMERGENCIAS

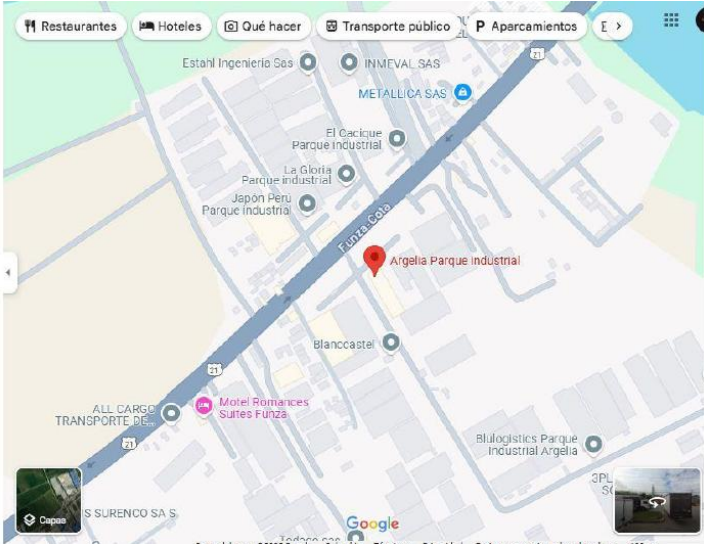
10.9.1 Rutas de evacuación



PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS



11.9.2. Vías de Acceso y linderos sectoriales.



11.9.3 Punto de encuentro principal.

En caso de emergencias y/o sucesos inesperados por acción humana o de la naturaleza el punto de encuentro se encuentra ubicado al exterior de la bodega, en la zona de parqueo de la edificación.



Nota 1. Para el caso de la información que se encuentra bajo custodia directa de la Empresa en el edificio de Colseguros, se atenderán estrictamente las rutas de evacuación previamente definidas. Asimismo, se ejecutarán todas las actividades de prevención, protección y respuesta establecidas en el presente Plan de Emergencias, con el fin de garantizar la salvaguarda de la información física y la integridad de las personas responsables de su manejo.

Nota 2. La información física de la Empresa —incluida aquella correspondiente a los fondos documentales— se encuentra resguardada conforme a los protocolos establecidos. Su custodia

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

ha sido delegada a un tercero especializado, quien actúa en cumplimiento de los lineamientos contractuales y normativos vigentes. En caso de una emergencia que comprometa dicha información, la Empresa garantizará el acompañamiento institucional necesario, así como la implementación oportuna y efectiva del presente Plan de Emergencias.

Dicho plan contempla medidas preventivas, correctivas y de contingencia, orientadas a salvaguardar la integridad, disponibilidad y confidencialidad de la información física, asegurando su recuperación y la continuidad operativa, de acuerdo con los lineamientos de gestión del riesgo y protección documental.

Este compromiso institucional forma parte de las acciones integrales para la preservación del patrimonio documental y del cumplimiento de las obligaciones legales y normativas en materia de gestión documental, incluida la delegación de la custodia a un tercero idóneo para tal fin.

Elementos disponibles para la atención de emergencias.

DESCRIPCIÓN	CANTIDAD	UBICACIÓN
Extintor Multipropósito ABC	57	Deposito – Funza
Extintor Satélite Multipropósito 150 LB	3	Deposito – Funza
Extintor de agente limpio o sistemas de apagado automático	18	Deposito – Funza
Camillas	1	Área oficinas segundo piso
Inmovilizadores	1	Área oficinas segundo piso
Botiquín Portátil	1	Piso 1 área depósito, en zona de baños.

11.10. ACTIVIDADES PARA LA ATENCIÓN DE EMERGENCIAS DOCUMENTALES

Es necesario asignar roles y responsabilidades para la ejecución del Plan de Emergencias Documentales. Las actividades contempladas en dicho plan, así como la gestión de los materiales requeridos, estarán a cargo del custodio de la información, quien será responsable de su correcta implementación.

Asimismo, debe definirse un espacio exclusivo para la recuperación de documentos y/o archivos que se encuentran actualmente en las instalaciones. Este espacio debe ser amplio, con adecuada ventilación, libre de agentes contaminantes y protegido frente a cualquier afectación de tipo climático.

Evaluación del Plan

El seguimiento al Plan de Emergencia Documental se efectúa en los informes del Sistema Integrado de Conservación de la Empresa y la herramienta de seguimiento definida para tal fin.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

12. PLAN DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS AMBIENTALES - PIGA

12.1. RIESGOS AMBIENTALES

Para analizar los riesgos ambientales que podría tener la Empresa, se deben identificar los problemas ambientales presentes en la zona de influencia de la sede administrativa, estos están asociados principalmente a la contaminación atmosférica y auditiva, esto se debe a la ubicación, ya que nos encontramos en un sector comercial con gran afluencia vehicular.

Estos dos tipos de contaminación pueden tener efectos negativos tanto en la salud pública como en la calidad de vida de las personas que trabajan en esta zona, los cuales se relacionan a continuación:

Contaminación atmosférica:

- ❖ Emisiones de vehículos: El alto volumen de tráfico vehicular, especialmente de vehículos con motores a gasolina o diésel, contribuye a la emisión de gases contaminantes como dióxido de carbono (CO₂), óxidos de nitrógeno (NOx) y partículas en suspensión, que afectan la calidad del aire.

Contaminación auditiva:

- Ruidos por el tráfico: El ruido constante generado por el paso de vehículos, especialmente en horas pico, puede afectar a los colaboradores, provocando estrés y dificultades para concentrarse.
- Ruidos comerciales: La actividad comercial intensa, como la música a alto volumen, los anuncios publicitarios o los ruidos generados por la carga y descarga de mercancías, también contribuyen a la contaminación auditiva.

Tabla SGA: Identificación de riesgos Ambientales

EVENTO	PROBABILIDAD	CONSECUENCIA	NIVEL DE RIESGO
Inundaciones	BAJA	MENOR	4 - RIESGO ACEPTABLE
SISMO	BAJA	MENOR	4- RIESGO ACEPTABLE
Derrame sustancias peligrosas	MUY BAJA	MÍNIMA	1 - RIESGO ACEPTABLE
Mal Manejo de Residuos	BAJA	MENOR	4 - RIESGO ACEPTABLE
Ruido contaminación externa	ALTA	MAYOR	32 - RIESGO ALTO
Emisiones atmosféricas - Contaminación externa	ALTA	MAYOR	32 - RIESGO ALTO

El análisis de los riesgos ambientales para la empresa debe considerar las condiciones específicas del entorno y la ciudad en la que se encuentra. En este caso, los eventos mencionados, como inundaciones, ruido, emisiones atmosféricas, sismos, derrames y el manejo inadecuado de residuos, son cruciales para evaluar el impacto potencial sobre la operación de la Empresa y la salud de sus trabajadores. A pesar de encontrar que el ruido por contaminación externa y las emisiones atmosféricas tienen un riesgo alto dada la ubicación de la Empresa, dentro de las oficinas se perciben ondas de sonido leves y las emisiones por la calidad atmosférica solo se perciben al recorrer las vías principales como lo son la Carrera 10 y la Calle 19.

Responsable PIGA

- Velar por el control y prevención de los riesgos ambientales al interior de la empresa, realizando un seguimiento mensual, semestral y anual.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

11.2 EMERGENCIA EN CASO DE FUGA DE AGUA

En caso de una fuga de agua en el interior de la empresa, es importante tomar medidas rápidas y efectivas para minimizar el daño y garantizar la seguridad de las personas. Se deben tener en cuenta los siguientes lineamientos en caso de una emergencia:

A. Verificar la seguridad de las personas:

- ❖ Acción inmediata: En cuanto se detecte la fuga, lo primero es asegurar que no haya personas en peligro. Si la fuga es extensa y representa un riesgo inmediato (por ejemplo, riesgo de electrocución si hay cables o equipos eléctricos cercanos), se debe evacuar rápidamente el área afectada.
- ❖ Comunicación: Notificar de inmediato a todas las personas en las cercanías sobre la emergencia, indicando que deben evacuar si es necesario y dirigirse hacia las zonas seguras establecidas previamente.

B. Cerrar la fuente de agua:

- ❖ Acción rápida: Localizar la válvula de suministro de agua más cercana al lugar de la fuga y cerrar el flujo de agua lo más rápido posible para evitar que la fuga se agrave.

C. Controlar daños y contener el agua

- ❖ Acción inmediata: Intentar contener la fuga utilizando barreras, toallas, trapos o cualquier material absorbente disponible, y colocar recipientes como cubos, cubetas o desagües para recoger el agua. Si es posible, dirigir el agua hacia un área que no cause mayores daños (como drenajes).
- ❖ Materiales disponibles: Asegurarse de que haya equipos adecuados para contener agua de manera efectiva, como barreras de contención, mangueras para drenaje, o incluso equipos de bombeo si la fuga es considerable.
- ❖ Monitoreo constante: Durante el proceso de control, es importante monitorear que el agua no se extienda a otras áreas de la empresa, especialmente aquellas con equipos sensibles o materiales valiosos.

D. Llamar al personal de mantenimiento calificado

- ❖ Acción profesional: Si la fuga es resultado de un problema en las tuberías o en los sistemas de plomería, se debe contactar al personal de mantenimiento especializado. Es importante no intentar reparar la fuga de manera improvisada si no se tiene el conocimiento y las herramientas adecuadas, ya que esto puede empeorar la situación.
- ❖ Intervención rápida: Los equipos de mantenimiento deben estar disponibles para responder a emergencias de forma rápida. La empresa debe contar con contactos de mantenimiento que estén disponibles las 24 horas.

E. Evaluación de daños

- ❖ Examen detallado: Una vez que la fuga esté bajo control, es esencial realizar una evaluación exhaustiva de los daños causados por el agua. Esto incluye revisar áreas como:
- ❖ Equipos electrónicos o eléctricos que puedan haber estado en contacto con el agua.
- ❖ Mobiliario (mesas, sillas, alfombras, etc.) que podría haber sufrido daños.
- ❖ Sistemas informáticos y documentos importantes que pudieran haber estado expuestos.
- ❖ Documentación: Es crucial documentar todos los daños para efectos de seguros, reparación y análisis posterior. Tomar fotos, hacer una lista detallada de los daños y realizar un informe escrito.

F. Limpieza y secado

- ❖ Limpieza inmediata: Una vez evaluado el daño, proceder con la limpieza y secado de las áreas afectadas. Usar toallas secas. Evitar el uso de productos de limpieza agresivos que puedan dañar aún más los materiales o superficies.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- ❖ Inspección adicional: Después de secar, realizar una inspección para asegurarse de que no haya humedad residual en las paredes, techos o estructuras cercanas que pueda dar lugar a daños a largo plazo.

G. Prevención de futuros incidentes

- ❖ Revisión de sistemas de plomería: Programar revisiones periódicas de las instalaciones de plomería, válvulas de cierre, y sistemas de drenaje para garantizar que estén en buen estado.

11.3 ATENCIÓN DE CONTINGENCIAS PARA RESIDUOS SÓLIDOS Y PELIGROSOS

Ruptura de bombillas: En caso de rotura de bombillas en la empresa, es importante tomar medidas rápidas y adecuadas para garantizar la seguridad de las personas y minimizar la exposición a sustancias potencialmente peligrosas, como el mercurio.

A. Evacuación del área

- ❖ Acción inmediata: En caso de que la ruptura de la bombilla ocurra en un área ocupada, es crucial evacuar a las personas de inmediato para evitar la exposición a fragmentos de vidrio y posibles vapores de mercurio.
- ❖ Tiempo limitado: Asegurarse de que la evacuación se realice de manera rápida pero ordenada, sin que los empleados toquen o se acerquen a los fragmentos de vidrio. Las áreas adyacentes también deben ser evacuadas si el mercurio se dispersa.

B. Uso de equipo de protección personal (EPP)

Protección adecuada: Antes de proceder con la limpieza, todos los encargados de la limpieza deben usar el equipo de protección personal adecuado, que debe incluir:

- ❖ Guantes de protección: Para evitar el contacto directo con los fragmentos de vidrio o el mercurio.
- ❖ Gafas de seguridad: Para proteger los ojos de posibles fragmentos volátiles o polvo.
- ❖ Mascarilla o protección respiratoria: Para evitar inhalar partículas finas de mercurio o polvo de la bombilla rota.

C. Restricción de acceso

- Delimitar el área afectada: Es crucial restringir el acceso a la zona afectada para evitar que otras personas se acerquen a los fragmentos de vidrio o entren en contacto con sustancias peligrosas.
- Señalización visible: Colocar señales de advertencia (como cintas de advertencia o carteles) en las áreas cercanas a la ruptura para alertar a los empleados del peligro y evitar el paso.

D. Recolección de fragmentos

- ❖ Método adecuado: Utilizar guantes de protección o pinzas para recoger cuidadosamente los fragmentos de vidrio, evitando que se rompan más o se dispersen. Los fragmentos deben colocarse en una bolsa de plástico resistente.
- ❖ Evitar el uso de aspiradoras o escobas: No se deben usar aspiradoras o escobas para la limpieza, ya que pueden dispersar el mercurio y otros fragmentos pequeños de vidrio, lo que podría empeorar la situación y poner en riesgo la salud.

E. Limpieza del área

- ❖ Uso de cinta adhesiva o papel pegajoso: Una vez que los fragmentos grandes de vidrio han sido recogidos, utilizar cinta adhesiva o un papel pegajoso para recoger los fragmentos más pequeños o el polvo residual.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- ❖ Paño húmedo para la limpieza final: Después de haber recogido todos los fragmentos visibles, pasar un paño húmedo sobre la superficie afectada para eliminar cualquier residuo de vidrio o mercurio. Es importante evitar que el polvo se disperse durante el proceso de limpieza.
- ❖ Precaución adicional: Durante la limpieza, asegurarse de que todo el material contaminado se recoja cuidadosamente sin esparcirlo por otras áreas.

F. Recolección y disposición adecuada

- ❖ Recolección segura: Colocar todos los materiales utilizados para la limpieza (como guantes, paños, fragmentos de vidrio y cualquier otro material contaminado) en una bolsa de plástico resistente.
- ❖ Sellado seguro de la bolsa: La bolsa debe ser sellada de manera segura para evitar la liberación de contaminantes. Luego, debe ser etiquetada adecuadamente como residuo peligroso y almacenada de acuerdo con las normativas locales de manejo de residuos peligrosos.

G. Notificación y reporte

- ❖ Informar a la Dirección Administrativa y de TIC's: Es esencial notificar a la Dirección sobre el incidente. Esto debe incluir detalles precisos sobre la ubicación de la ruptura, las acciones tomadas y cualquier medida adicional que se haya implementado.
- ❖ Registrar el incidente: Asegurarse de que se registre el incidente en el sistema de gestión de seguridad de la empresa, para dar seguimiento y garantizar que no se repitan situaciones similares en el futuro.
- ❖ Análisis post-incidente: Posteriormente, se debe realizar un análisis del incidente para evaluar las causas de la ruptura y revisar las medidas preventivas para evitar futuros accidentes de este tipo.

El manejo adecuado de un derrame de tóner en la Empresa es esencial para garantizar la seguridad de las personas y prevenir posibles impactos negativos en el entorno de trabajo. A continuación, se detalla un protocolo para gestionar un derrame de tóner:

A. Protección personal (EPP):

- ❖ Guantes de protección: Usar guantes adecuados (preferiblemente de nitrilo o similares) para evitar el contacto directo con el tóner.
- ❖ Gafas de seguridad: Proteger los ojos de posibles salpicaduras o partículas suspendidas en el aire.
- ❖ Mascarilla o respirador: Si es posible, usar una mascarilla para evitar la inhalación de partículas de tóner que puedan estar en suspensión en el aire, ya que algunos tóners contienen sustancias que pueden ser perjudiciales si se inhalan en grandes cantidades.

B. Ventilación adecuada:

- ❖ Aireación del área: Si el derrame ocurre en un área cerrada o mal ventilada, abrir puertas y ventanas para permitir la circulación del aire. Esto ayudará a dispersar las partículas en suspensión y reducir la concentración de polvo de tóner en el ambiente.

C. Contención del derrame:

- ❖ Método adecuado de recolección: Usar utensilios limpios y secos, como una pala o un papel absorbente, para recoger el tóner derramado. Evitar el uso de escobas o cepillos, ya que pueden dispersar el tóner por el aire.
- ❖ Contener el derrame rápidamente: Intentar contener el derrame dentro de una zona limitada para evitar que se extienda a áreas más grandes. Si el derrame es pequeño, se puede utilizar un borde o una barrera para evitar que el tóner se esparza.

D. Limpieza del área

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- Uso de paños o papel absorbente: Una vez que se haya contenido el tóner derramado, usar paños limpios o papel absorbente para recoger los residuos de tóner. Evitar el uso de agua para limpiar la superficie afectada, ya que el tóner puede disolverse o fijarse, lo que dificultará la limpieza posterior.
- Método suave de limpieza: Limpiar con movimientos suaves para evitar que el tóner se derrame más o se libere al aire. Asegurarse de que toda la superficie afectada esté limpia y libre de residuos.

E. Recolección y disposición adecuada

- **Recolección de residuos:** Colocar todo el material utilizado para la limpieza (paños, papel absorbente, guantes, etc.) en una bolsa de plástico resistente.
- **Sellado de la bolsa:** Cerrar y sellar la bolsa de manera segura para evitar la liberación de partículas de tóner al ambiente.
- **Etiquetado como residuo peligroso:** Etiquetar adecuadamente la bolsa como residuo peligroso según las normativas locales de manejo de desechos, y asegurarse de que se almacene en un área segura hasta su disposición adecuada.

F. Limpieza del equipo (si es necesario):

- **Desconectar el equipo:** Si el derrame ocurre dentro de la impresora o el equipo de impresión, asegúrese de apagar el equipo antes de comenzar la limpieza. Desconectarlo de la fuente de alimentación eléctrica para evitar riesgos eléctricos o cortocircuitos.
- **Seguir las instrucciones del fabricante:** Consultar el manual del fabricante de la impresora o equipo afectado para seguir las instrucciones específicas sobre cómo limpiar el equipo de manera segura. En algunos casos, los fabricantes proporcionan directrices claras para limpiar el tóner sin dañar el equipo.
- **Precauciones adicionales:** Al limpiar el interior de la impresora o equipo, utilizar herramientas adecuadas, como brochas suaves o aspiradoras especiales para polvo, según lo permita el fabricante.

G. Notificación y reporte:

Informar a las áreas responsables: Notificar de inmediato a la Dirección Administrativa y de TIC's sobre el derrame de tóner. Es importante incluir detalles precisos sobre:

- La ubicación del derrame.
- El tamaño del derrame y las acciones tomadas para contenerlo y limpiarlo.
- Las medidas adicionales necesarias para prevenir futuros derrames.

Registrar el incidente: Documentar el incidente adecuadamente para poder llevar un registro de los derrames y las acciones tomadas. Esto servirá tanto para cumplir con las normativas internas de seguridad como para identificar posibles áreas de mejora en los procedimientos de manejo de tóner.

Seguimiento: Si es necesario, tomar medidas adicionales para revisar las condiciones del equipo de impresión, como la calibración o la inspección de los cartuchos de tóner, para prevenir futuros derrames.

H. Acciones preventivas adicionales:

- **Almacenaje adecuado de tóner:** El tóner debe almacenarse en un lugar seguro, seco y bien ventilado, siguiendo las recomendaciones del fabricante, para evitar derrames accidentales. Además, deben guardarse en su embalaje original hasta su uso.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

13. PLAN DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS DE TECNOLOGÍAS DE LA INFORMACIÓN

Este documento presenta en detalle la situación tecnológica como resultado del proceso de levantamiento de información realizado a nivel de infraestructura tecnológica con el que cuenta la Empresa y los manuales de instalación de los sistemas de información en caso de restauración de la plataforma tecnológica de la Empresa

El propósito de este plan es mantener la continua ejecución de los procesos de misión crítica y sistemas de información tecnológica de la empresa en el caso extraordinario que un evento pudiera ocasionar que los sistemas fallen en el mínimo de su producción. El Plan de Contingencia contiene las necesidades y requerimientos de tal forma que la Empresa pueda estar preparada para responder a un evento y, en su caso, hacer eficiente la restauración de los sistemas que hayan estado inoperables por el evento.

Por otro lado, siendo la información uno de los activos vitales de la empresa, el resguardo de los datos es una acción de vital importancia ante la posibilidad de pérdida, destrucción o hurto; lo que implica la implementación de un Plan de Contingencia, que propendan por la protección de los mismos.

12.1 PLAN DE CONTINGENCIA

El Plan de contingencia deberá ser revisado periódicamente. Así mismo, es revisado/evaluado cuando se materializa una amenaza.

Este plan de contingencia comprende:

- Medidas preventivas para evitar la materialización de una amenaza.
- Medidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es contrarrestar los efectos adversos de la misma.
- Medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Teniendo en cuenta los siguientes aspectos:

- Contar con un Centro de Datos, donde se aloje el servidor controlador de dominio de propiedad de la Empresa y que entre en funcionamiento en caso de que el servidor local falle o esté indisponible.
- El equipo del proceso Gestión de TIC será el encargado de gestionar el restablecimiento de los servicios TI en caso de desastre.

Acciones a seguir:

- Determinar los requerimientos de los procesos, verificando el análisis de riesgos y el análisis de impacto en él.
- Gestionar los procedimientos de backup para resguardar los datos y servicios de procesamiento locales.
- Mantener y poner a prueba su solución de recuperación.
- Continuar con la disposición de los sistemas críticos de la Empresa en la modalidad de SaaS, para disponibilidad de la información ante un evento fortuito.

12.2 SERVIDORES / SERVICIOS DE MISIÓN CRÍTICA / APLICACIONES

SISTEMA	NOMBRE DEL SISTEMA
Conectividad LAN	Conexión de Red Interna
DNS	Servicio de resolución de nombres
Aplicaciones	Sistemas de Información
Servidores	Equipos de Hardware de procesamiento de información
Backup	Medios de copias de respaldo

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

SISTEMA	NOMBRE DEL SISTEMA
Equipos de RED	Equipos Activos de red y conectividad

Servidores

El siguiente cuadro presenta los servidores con los que cuenta la empresa, nombre, dirección IP, con el fin de mantener claridad sobre las implicaciones de las recomendaciones en el momento de su aplicación y la posibilidad de llevarlas a cabo.

Servicio de Colocación con ETB Data Center Santa Bárbara		
SERVIDOR	NOMBRE	Tipo de Servidor
Servidor alojamiento servidores virtuales	BOGEMPRESA (RENOBO)HV01	Físico
Servidor de Dominio, DNS y Directorio Activo	BOGEMPRESA (RENOBO)MVDC01	Virtual

Servicio de Hosting Web ETB			
SERVIDOR	NOMBRE	IP (Interna)	Tipo de Servidor
Portal Web Institucional	Empresa (Renobo) web	186.28.253.78	Hosting Web servicio ETB - Virtual
Sistema de gestión documental – producción	TAMPUS	https://gestiondocumental.etb.net.co/	Nube
Sistema de gestión documental – pruebas	TAMPUS	https://gestiondocumental.etb.net.co/Instancias/ ERU_Prub/	Nube
Sistema ERP	JSP7 - Gobierno	https://jsp7eruv3.aspsols.com/	Nube
Sistema de Georeferenciación	servidor 1		Plan Máquina Virtual Básica
Sistema de Georeferenciación	servidor 2		Plan Máquina Virtual Básica
Sistema de Georeferenciación	servidor 3		Plan Máquina Virtual Básica
Sistema de Georeferenciación	servidor 4		Plan Máquina Virtual Básica

EDIFICIO Colsegutos – Cuartos Tecnicos		
SERVIDOR	NOMBRE	Tipo de Servidor
Servidor alojamiento servidor virtual, aplicación APOTEOSYS y carpetas compartidas	APLICACIONES	Físico
Servidor aplicaciones Históricas ACAPELLA, Intranet Metrovivienda, SIIM,	SERAPP	Físico
Servidor aplicaciones históricas SP6, SIAF	SP6	Físico
File server – controlador de dominio	BOGEMPRESA (RENOBO)HV04	Físico
Controlador de dominio	BOGEMPRESA (RENOBO)VM0401	Virtual
Servidor de almacenamiento PPAL	BOGNASPPAL	Físico
Servidor de almacenamiento Backup	BOGNASBK	Físico
Servidor alojamiento servidores virtuales	METROVIVIENDA	Físico
Servidor alojamiento servidores virtuales	PROXMOX	Físico

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Servidor alojamiento servidores virtuales	FUSIÓN	Físico
Servidor alojamiento servidores virtuales	CLOUD	Físico

Sistema de Gestión Documental empresa (RENOBO - Histórico)	Sgd Empresa (Renobo)	Virtual
Sistema SIAF histórico	SIAF	Virtual
Sistema Siim2 histórico	Siim2Prod	Virtual
Intranet empresa (RENOBO)NET	newintranet	Virtual
Sistema JSP7-Gobierno Historico		Virtual
Copia respaldo históricos	Histmetro Empresa (Renobo)	Virtual
Sistema JSP7-Gobierno Producción	BOGEMPRESA (RENOBO)HV03	Virtual
Portal Web Metrovivienda – ERU histórico	webmetro	Virtual

Sistema GLPI	Glpí Empresa (Renobo)	Virtual
Histórico Intranet empresa (RENOBO)	HistIntranet EMPRESA (RENOBO)	Virtual
OCS Inventory Intranet empresa (RENOBO)		Virtual

Aplicaciones

El siguiente cuadro presenta las aplicaciones implementadas en la empresa y que se encuentran en producción, con el fin de mantener claridad sobre las implicaciones de las recomendaciones en el momento de su aplicación y la posibilidad de llevarlas a cabo.

ÁREA DE SISTEMAS APLICACIONES – EMPRESA (RENOBO)			
SERVIDOR	NOMBRE APLICACIÓN	DESCRIPCIÓN	PRINCIPALES USUARIOS
Servidor Sistema Administrativo y Financiero	JSP7-Gobierno	Sistema Administrativo y Financiero de la Empresa	Supervisores de Contrato. Todos los usuarios de la Dirección de Contratación Los usuarios de la Direccion Administrativa y de TICS .
Servidor de Intranet	Empresa REDNOBO	Intranet con las noticias de la empresa, Organigrama, Directorio, Sistema Integrado de Gestión, entre otros.	Todas las dependencias de la empresa
Sistema de mesa de Ayuda e inventario de equipos	GLPI (Gestión Libre de Parc Informati que (en español Gestor libre de Equipos Informáticos)),	Es un software libre para la gestión de servicios de TI (ITSM), servicios de apoyo a la gestión (sistema de gestión de fallos y ServiceDesk) y automatización de inventario de los equipos de cómputo de la empresa.	Todas las dependencias de la empresa
Servidor Sistema de Gestión documental – Histórico	Empresa (RENOBO)	Sistema basado en Caliope 0.9 de la fundación Correlibre cuyas funciones es el Proceso de Gestión Documental (Radicación Salida, Entrada e Interno; y creación de Expedientes virtuales)	Todas las dependencias de la empresa
Hosting Web Portal Web Institucional – SAAS – PAAS (nube)	Empresa (Renobo)	Portal web institucional de la empresa	Público en general
SAAS – PAAS (nube)	TAMPUS	Nuevo sistema de gestión documental	Todas las dependencias de la Empresa y consulta externa para usuario con radicado
PAAS	Visor Geográfico	Sistema de información geográfica	Dependencias misionales.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Almacenamiento y Backup

El siguiente cuadro presenta los dispositivos que se encuentran para la toma de backups de los datos que se manejan en la empresa, con el fin de mantener claridad sobre las implicaciones de las recomendaciones en el momento de su aplicación y la posibilidad de llevarlas a cabo.

LOCAL

SERVIDORES DE ALMACENAMIENTO Y BACKUP
Servidor NAS principal - 70TB Servidor NAS
Backup - 60TB
BACKUPS
Discos duros externos 12 TB

12.3 IDENTIFICACIÓN DE RIESGOS

Para la identificación de los riesgos de seguridad de la información la empresa tiene definida la **Política para la Administración de Riesgos (PL-08)** en la cual se dan los lineamientos respectivos.

12.4 PLANES DE RECUPERACIÓN Y RESPALDO

Algunas de las medidas con las que cuenta la empresa para realizar la recuperación y respaldo del área de TI son las siguientes:

- Copias de los documentos por usuario y correo a entrega de paz y salvo o cuando se realiza solicitud de jefes o supervisores (Ver *PD-51 Copias de respaldo*).
- Copia de seguridad de los aplicativos del sistema de información financiero y administrativo; sistema de mesa de ayuda, sistema de gestión documental e intranet. (Ver *PD-51 Copias de respaldo*).
- El portal web está alojado en un hosting web de la ETB y cuenta con el servicio de backup y restauración propia de ese hosting según el servicio contratado (Política Backup Máquina virtual: Incremental Diario + Full Semanal + Retención Mensual + 1 Restauración el cual consiste en un snapshot de la máquina virtual).
- File server Owncloud para usuarios, permite centralizar la información y facilitar la administración y protección.
- Dos servidores NAS en sincronización de principal y respaldo, con software y especializado que permite de duplicación y restauración.
- Contrato de mantenimiento preventivo y correctivo de PC´s, e impresoras.
- Contrato de mantenimiento preventivo y correctivo de administración de equipos de comunicación.
- Contrato de alquiler de equipos para cubrir la demanda de la empresa.
- Contrato Interadministrativo con ETB para los servicios: DataCenter tipo tier III colocación de un servidor, Hosting Web con Backup y restauración, monitoreo, conectividad principal con internet dedicado, máquinas virtuales aprovisionadas con SO windows server para el sistema de georeferenciación.
- Contrato Interadministrativo con ETB para el servicio de Gestión Documental en la nube con la correspondiente política de Backup y Restauración.

12.5 PLAN DE CONTINUIDAD DE INFRAESTRUCTURA

Red de Datos

Equipos Activos

El siguiente cuadro presenta los equipos activos de red de la empresa y que se encuentran disponibles para la conectividad, comunicación y seguridad de la información; con el fin de mantener claridad sobre las implicaciones de las recomendaciones en el momento de su aplicación y la posibilidad de llevarlas a cabo.

Marca	Modelo	Ubicación
-------	--------	-----------

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Fortinet	FortiSwitch 148F-POE	Piso 16
	FORTI_AP_431F	
Fortinet	FortiSwitch 148F-POE	Piso 22
	FortiSwitch 148F-POE	
	FortiSwitch 148F-POE	
	FORTI_AP_431F	
	FORTI_AP_431F	
	FORTI_AP_431F	
Fortinet	FortiSwitch 148F-POE	Piso 23
	FortiSwitch 148F-POE	
	FortiSwitch 148F-POE	
	FORTI_AP_431F	
	FORTI_AP_431F	
	FORTI_AP_431F	
Fortinet	FortiSwitch 148F-POE	Piso 24
	FortiSwitch 148F-POE	
	FortiSwitch 148F-POE	
	FORTI_AP_431F	
	FORTI_AP_431F	
	FORTI_AP_431F	
DELL	S4112F-ON -	
	S4112F-ON -	

Comentarios Generales sobre la Configuración

- ✓ Existen diversos elementos de control, claves de acceso a cada dispositivo.
- ✓ Los equipos tienen capacidades de seguridad, configurados con limitación en el acceso.
- ✓ La configuración se encuentra centralizada en consola Web lo que permite una administración más segura.
- El acceso a los equipos lo realiza únicamente el personal autorizado del grupo TIC.

La Red de datos es la que permite transmitir información de un computador a otro. Las aplicaciones que posee la empresa son sistemas de información en la Web, pero también se tiene aplicaciones históricas que se deben consultar y son cliente/servidor, además de carpetas compartidas lo que se hace indispensable la interacción entre diferentes dispositivos a los servidores de la empresa, por lo que el servidor es uno de los componentes importantes de la Red. El cableado es estructurado y topología estrella.

El elemento activo de comunicaciones son los switch de datos, el cual permite trasladar a cada nodo (host) los paquetes de datos para que se intercambie información en toda la Red.

Actualmente la empresa cuenta con dos canales dedicados para el servicio de Internet con salida desde la sede principal con un ancho de banda de 400MB y disponibilidad del 99.7%.

Se cuenta con los servicios de conectividad WAN a través de una red IP/MPLS para el transporte de los datos, voz y video, el cual permite la conectividad de la sede principal. En el edificio Colseguros piso 22, 23 y 24, a la sede principal de procesamiento en el DataCenter del operador de servicios ETB, lo anterior, permite garantizar el acceso de los usuarios a los sistemas de información, intranet, Internet, correo electrónico y sistemas propios, por medio de:

- Canal dedicado de INTERNET de 400 Mbps, para navegación y publicación de servicios Web.
- Canal dedicado de DATOS de 50 Mbps en la sede principal que constituye la integración de los canales de Colocación ETB y las sedes de la empresa y Archivo.
- Canal dedicado de INTERNET de 10 Mbps, para publicar servicios web, desde los servidores propios de empresa que estarán en COLOCACION.
- Canal dedicado de Datos de 1 Mbps, para consultar e interactuar en doble vía una aplicación en la Sede Secretaría Distrital de Planeación.
- Canal dedicado de Datos de 15 Mbps, para servicios de voz, datos e internet desde la Sede principal hacia la sede Archivo.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Así, también la Empresa cuenta con un segundo proveedor de servicios de conectividad Internet, con un servicio que presta el canal de Internet principal.

Estos servicios son de suma importancia, ya que permite conectividad para que los funcionarios puedan tener acceso a los sistemas de información con los que cuenta la empresa y de esa forma socializar algunas actividades que pueden generar un valor agregado.

El objetivo de la Red en la Empresa es el de compartir recursos de Hardware y Software para maximizar el uso de los dispositivos.

Es por ello, que es importante el poder detectar las fallas en la red de datos, ya que de esa forma se permitirá que la empresa pueda entregar el 100% de sus recursos disponibles a la comunidad. Por lo anterior, se cuenta con un servicio de monitoreo por parte de ETB (Entuity) que genera alarmas cuando el canal principal o el backup de internet está caído o no se ve el servicio, también genera alarmas sobre los servidores que están en colocación en el DataCenter de Santa Bárbara.

Diseño de la red de datos

Como se mencionó anteriormente, la red de datos posee una topología estrella, en donde el cuarto de telecomunicaciones del piso 22 cuenta con el aprovisionamiento de los proveedores ETB y CLARO para el servicio de conectividad Internet y MPLS, los pisos 23 y 24 se comunican por medio de una conexión por fibra de 10-100Gbps.

Con esta infraestructura se cubre los pisos 22, 23 y 24 de la sede principal en el edificio Colseguros, permitiendo que se pueda transmitir la información por medio de los diferentes computadores de la empresa los cuales poseen una tarjeta de Red, el cual es un dispositivo que se encuentra al interior del computador, y es la interfase entre la máquina y el medio de transmisión.

Además, la Empresa cuenta con la conectividad para la sede de Archivo que permite la interacción a nivel de LAN y se suministra el servicio de Internet.

Cableado estructurado

El cableado estructurado es la plataforma de comunicaciones en la red que posee la empresa, este cableado usualmente es UTP (cable de par trenzado no apantallado) es el medio de transmisión de la información de un nodo a otro. Es posible que, por problemas de cableado, se tengan problemas de conectividad, sin embargo, el cableado entregado está debidamente certificado por la empresa que realizó su instalación; y en caso de falla o deterioro el proveedor de arrendamiento de sedes realiza la corrección e instalación necesarios.

Equipos activos de comunicación

El elemento activo de comunicación que utiliza la empresa es el switch de datos, elemento que permite la transmisión de tramas (paquetes de datos) desde la tarjeta de Red del Transmisor a la tarjeta de Red del Receptor. Este elemento activo de comunicaciones no debe estar apagado, ya que en ese momento se tendría una caída en la Red de datos.

La empresa cuenta con 9 switches de 48 puertos y 2 switches Core de 12 puertos, cada puerto posee unos leds (indicadores visuales) que señalan el estado de funcionamiento de cada puerto, en el momento en que está activo el puerto, el led del mismo debe estar encendido. Cada puerto conecta a un nodo o computadora por lo que una de las formas de detectar que hay falla de comunicación es observar el puerto, obviamente, cada puerto debe estar marcado con el punto de Red respectivo.

Detección de fallas

- **Por problemas eléctricos:** Si hay problemas de suministro de fluido eléctrico, posiblemente se apague el elemento activo de comunicaciones, por lo tanto, el resultado será una caída en la red de datos.
- **Por problemas en el switch de datos:** Si el elemento activo tiene una falla de tipo eléctrico

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- éste no encenderá y se tendrá un problema similar al caso anterior.
- **Por problemas de puerto:** es posible que, por alguna variación de voltaje, se queme una cantidad limitada de puertos, frente a lo cual se deben verificar los leds que indican conectividad.
 - **Por problemas en la tarjeta de Red:** puede existir la posibilidad de que la tarjeta de Red esté fallando, una forma rápida de verificar su funcionamiento es identificar si el led de la tarjeta de Red está funcionando, en caso contrario es posible que la NIC no esté operando adecuadamente. Otro caso probable es que esté desactivado desde el sistema operativo.

Alternativas de solución

- En el caso de falla en el suministro de energía eléctrica, se cuenta con UPS por cada cuarto técnico que da un tiempo de 10 minutos mientras se restablece el servicio. Por otro lado, el edificio Colseguros cuenta con una planta eléctrica propia que suplente el servicio de energía durante un periodo de 12 horas mientras se restablece el servicio.
- Por problemas de switch de datos: Si el responsable de sistemas ha detectado que el elemento activo no enciende, se debe verificar si es posible reemplazarlo utilizando para ello la garantía. En caso contrario, se deben realizar las gestiones necesarias para entregar un elemento activo para reemplazar el dañado.
- Por problemas de puerto: se debe verificar que el led de la tarjeta con que está conectado el puerto está encendido, si al realizar un ping al Server éste no contesta, es posible que el puerto está fallando, otra verificación es cambiar la conexión de la tarjeta a otro punto de red, el cual conectará a otro puerto, si al realizar un ping al Server éste contesta, se puede concluir que el puerto es el que está fallando, lo mismo se puede realizar si hay problemas con los puntos de red.
- Por problemas en la tarjeta de Red: La tarjeta puede estar deshabilitada desde el Sistema Operativo, será necesario revisar si éste está habilitado o no, en el caso que esté deshabilitado, habilitarlo inmediatamente desde el sistema operativo. Si está habilitada la tarjeta de red y no hay comunicación, será necesario reinstalar el “driver” de la tarjeta de Red, o revisar si posee dirección IP.
- Realizar un contrato de mantenimiento preventivo y correctivo de administración de equipos de comunicación.

Servidores físicos en el DataCenter de ETB

En el DataCenter de ETB Santa Bárbara se dispone de 1 servidor en colocación con un servicio tipo Tier III, es decir con disponibilidad 99,9829%, 1,6 horas de interrupción al año y redundancia N+1. Por otro lado, se tiene un monitoreo 7*24 por medio de la configuración SNMP de los mismos, que permite un seguimiento constante de las diferentes eventualidades que se pueden registrar por la red, como uso del puerto, caída de conectividad o del servidor, entre otros.

A continuación, se mencionan los servidores físicos que están en colocación:

Servicio de Colocación con ETB Data Center Santa Bárbara		
SERVIDOR	NOMBRE	Tipo de Servidor
Servidor alojamiento servidores virtuales	BOGEMPRESA (RENOBO)HV01	Físico

Detección de fallas

Independientemente de los beneficios del DataCenter se pueden tener fallas como las configuraciones propias de cada servidor en las diferentes aplicaciones instaladas para el servicio que provee cada uno, incluyendo los servidores virtuales de los sistemas que están actualmente en producción. Además, problemas de Hardware, tales como, problemas con los discos duros, tarjetas de Red, Motherboard, entre otros.

El objetivo, es poder detectar qué tipo de problema posee el servidor y con ello, determinar qué acción tomar, en ese sentido, es necesario retomar algunas fallas generales que pueden darse en el Server.

Por problemas de Hardware:

- Fuente de Poder.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- Motherboard.
- Sistemas de almacenamiento.
- Tarjetas de Red.
- Periféricos del Server.

Por problemas de Software:
Sistema Operativo incluyendo paquetes, driver, aplicaciones y servicios.

Alternativas de Solución

- En el caso de falla en el suministro de energía eléctrica, se cuenta con UPS por cada cuarto técnico que da un tiempo de 10 minutos mientras se restablece el servicio. Por otro lado, el edificio Colseguros cuenta con una planta eléctrica propia que suplente el servicio de energía durante un periodo de 12 horas mientras se restablece el servicio.
- Por problemas de switch de datos: Si el responsable de sistemas ha detectado que el elemento activo no enciende, se debe verificar si es posible reemplazarlo utilizando para ello la garantía. En caso contrario, se deben realizar las gestiones necesarias para entregar un elemento activo para reemplazar el dañado.
- Por problemas de puerto: se debe verificar que el led de la tarjeta con que está conectado el puerto está encendido, si al realizar un ping al Server éste no contesta, es posible que el puerto está fallando, otra verificación es cambiar la conexión de la tarjeta a otro punto de red, el cual conectará a otro puerto, si al realizar un ping al Server éste contesta, se puede concluir que el puerto es el que está fallando, lo mismo se puede realizar si hay problemas con los puntos de red.
- Por problemas en la tarjeta de Red: La tarjeta puede estar deshabilitada desde el Sistema Operativo, será necesario revisar si éste está habilitado o no, en el caso que esté deshabilitado, habilitarlo inmediatamente desde el sistema operativo. Si está habilitada la tarjeta de red y no hay comunicación, será necesario reinstalar el “driver” de la tarjeta de Red, o revisar si posee dirección IP.
- Realizar un contrato de mantenimiento preventivo y correctivo de administración de equipos de comunicación.
- Problemas con el SO y sus servicios: En muchas ocasiones, los problemas no son de Hardware, sino también de Software, en este caso es importante identificar el Sistema Operativo que se tiene instalado y el proceso de actualización de paquetes, además de las aplicaciones necesarias según el servicio que posee cada servidor físico. A continuación, se describen los sistemas operativos de los seis servidores:

Servicio de Colocación con ETB Data Center Santa Bárbara		
SERVIDOR	NOMBRE	Sistema Operativo
Servidor alojamiento servidores virtuales	BOGEMPRESA (RENOBO)HV01	Windows Server 2012

Servidor físico y virtual en el DataCenter de ETB

El servidor físico que está en colocación en el DataCenter de ETB, tiene configurado un servidor virtual donde se encuentra el controlador de dominio.

Detección de fallas

Independientemente de los beneficios del DataCenter se pueden presentar fallas como las configuraciones propias de cada servidor virtual en las diferentes aplicaciones instaladas para el servicio que provee cada uno. Además, problemas de Hardware, tales como, problemas con los discos duros, tarjetas de Red, Motherboard, entre otros.

El objetivo, es poder detectar qué tipo de problema posee el servidor y con ello, determinar qué acción tomar, en ese sentido, es necesario retomar algunas fallas generales que pueden darse en el Server.

- Por problemas de Hardware:
- Fuente de Poder.
 - Motherboard.
 - Sistemas de almacenamiento.
 - Tarjetas de Red.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- Periféricos del Server.

Por problemas de Software:
Sistema Operativo incluyendo paquetes, driver, aplicaciones y servicios.

Alternativas de Solución

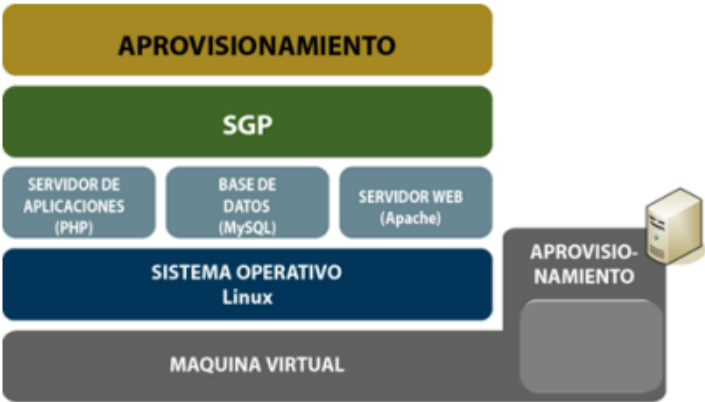
- Fuente de poder: Se cuenta con fuentes redundantes por cada servidor y tiene aprovisionado dos UPS independientes para cada fuente.
- Por problemas de NIC: Normalmente, el Server posee dos tarjetas de Red, uno para la Intranet y el otro para el acceso a Internet. Se debe verificar si el led de la tarjeta de Red está funcionando, en caso contrario es posible que la NIC no esté operando adecuadamente. Otro caso probable es que esté desactivado desde el sistema operativo. Se cuenta con un servicio de ojos y manos remotas que permite verificar según el led cuál es el problema que se está presentando.

Réplicas de sistemas de información

Para el sistema JSP7- Gobierno (Administrativo y Financiero) se tiene configurado en alta disponibilidad debido a que el sistema se encuentra distribuido en varios servidores tipo Docker.

Servicio de Hosting con ETB Data Center
Sistema de Gestión documental TAMPUS

La infraestructura aprovisionada es la siguiente:



Servidores en la sede principal de la empresa

Se cuenta con servidores en los cuartos de telecomunicaciones del piso 22, 23 y 24 los cuales tienen sistemas de información y datos históricos de las empresas fusionadas.

Los mencionados servidores cuentan con contrato de mantenimiento preventivo de hardware de los mismos, además del continuo monitoreo y actualización del sistema operativo. A continuación, se relacionan sus sistemas operativos:

EDIFICIO Colseguros - Cuarto de Tecnico Empresa (RENOBO)		
SERVIDOR	NOMBRE	Sistema Operativo
Servidor alojamiento servidor virtual, aplicación APOTEOSYS y carpetas compartidas	APLICACIONES	Windows Server 2008 r2
Sistema JSP7-Gobierno Pruebas	JSP7PRUEBAS	Windows Server 2008 r2
Servidor aplicaciones Históricas ACAPELLA, Intranet	SERAPP	Windows Server 2003

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

EDIFICIO Colseguros - Cuarto de Tecnico Empresa (RENOBO)		
SERVIDOR	NOMBRE	Sistema Operativo
Metrovivienda, SIIM,		
Servidor aplicaciones históricas	SP6	Windows Server 2003
SP6, SIAF		
Sistema OwnCloud	OwnCloud	Ubuntu Server 16.04.3 LTS
File server	BOGEMPRESA (RENOBO)HV04	Windows Server 2016 Std
Controlador de dominio	BOGEMPRESA (RENOBO)VM0401	Windows Server 2016 Std
Servidor de almacenamiento PPAL	BOGNASPPAL	Windows Server Storage 2016 STD
Servidor de almacenamiento Backup	BOGNASBK	Windows Server Storage 2016 STD

Servicio de Colocación con ETB Data Center Santa Bárbara		
SERVIDOR	NOMBRE	Sistema Operativo
Histórico Intranet EMPRESA (RENOBO)	HistIntranet empresa (RENOBO)	10.115.245.61 GNU/Linux - Ubuntu 16.04.3

Sobre los sistemas de información y aplicaciones que actualmente están en producción, se garantizar que estén en funcionamiento 7*24 ya que algunos de ellos se pueden acceder desde Internet lo que implica que los usuarios que tienen usuario y contraseña institucionales acceden a estos sistemas fuera del horario laboral, lo anterior, conlleva a tener una serie de contingencias no solo en que se dé continuidad del servicio sino en la veracidad y conservación de los datos que en ellos se registran y tramitan.

Servicio de Internet

El servicio de Internet permite tener acceso a los recursos de Internet tales como páginas gubernamentales, bases de datos, correo electrónico, etc.

El plan actual con el que cuenta la Empresa se constituye de 2 canales en alta disponibilidad:

- Un canal dedicado de 400 Mbps que actúa como canal principal y esta contratado con uno de los proveedores mas estables del mercado.
- Un segundo canal dedicado de 400MB en alta disponibilidad que actúa como backup contratado con nuestro aliado tecnológico ETB.

Además de un monitoreo constante sobre el Router Internet y Router de canal de datos, además del consumo del mismo por medio de la herramienta ENTUITY como parte del servicio contratado a ETB.

Los canales cuentan con una disponibilidad del 99.7%.

Frente a los servicios alojados en el Data Center permite garantizar el servicio a los usuarios en un 99,9%.

Alternativas de solución

- El servicio de monitoreo es proactivo 7x24, con reporte automático al correo del proceso Gestión de TIC de manera que se pueden tomar acciones en conjunto con el proveedor en la revisión del problema y solución cuando se presente fallas en el servicio.

Plan de Continuidad en caso de corte eléctrico

Acciones Preventivas a la contingencia

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Las siguientes acciones corresponden a la administración del edificio Colseguros y se refieren a la disponibilidad de la planta que suministra electricidad al edificio en su conjunto, concretamente a nuestros espacios compuestos por los pisos 16, 22, 23 y 24.

- Contar con una planta de emergencia que suministre energía conectada al centro de cableado.
- Supervisar semanalmente el nivel óptimo de combustible, agua, baterías, etc.
- Contar con un plan de mantenimiento semestral con supervisiones mensuales.
- Supervisar el combustible de respaldo en el área de servicios generales del edificio.
- Contar con equipo de emergencia contra incendios en el local de la planta.
- Contar con el mapa eléctrico del área en la planta y archivado, identificando los contactos respaldados y regulados.
- Realizar un contrato de mantenimiento preventivo y correctivo de la UPS.

UPS

- Contar con dos UPS en los cuartos técnicos para los pisos 22, 23 y 24 de la sede que cubren las necesidades y la cantidad de equipos activos que se conecten.
- Plan de mantenimiento dado caso contrato con un tercero.
- Contar con el mapa eléctrico del área, identificando los contactos regulados y respaldados.

Generales

- Contar con un monitoreo de la infraestructura de TI.
- Gestionar los respaldos de emergencia a la información del servidor mail, DNS, configuraciones de Equipo Activo principal y respaldo.
- Solicitar revisión periódica (semestral) del estado y óptimo funcionamiento de los bancos de respaldo eléctrico en los equipos del proveedor de medios.
- Asignar jerarquía a los equipos Activos y Servicios para ejecutar medidas mayores (darlos de baja).
- Determinar las fases de una contingencia de esta índole.

Acciones durante la contingencia

En caso de interrupción del suministro eléctrico en lapsos cortos consecutivos:

- Comunicarse con los servicios logísticos del edificio para la supervisión de la Planta de emergencia.
- Monitorear las UPS cada 10 minutos. para programar acciones mayores.
- Valorar la decisión de apagar los equipos activos y/o servicios para evitar daños y/o pérdida de información y de equipos.

En caso de una interrupción del suministro eléctrico no mayor a una hora:

- Comunicarse con los servicios logísticos del edificio para la supervisión de la Planta de emergencia.
- Monitorear la UPS cada 10 min. para programar acciones mayores.
- Apagar los equipos no prioritarios como impresoras, monitores o PC que no demanden su uso.
- Desconectar electrodomésticos (cafeteras, equipo de sonido, refrigerador, horno de microondas, ventiladores, etc.).

En caso de una interrupción del suministro eléctrico mayor a una hora:

- Dar aviso de la contingencia a los usuarios prioritarios (Gerencia, directores, y atención al usuario).
- Preparar el apagado de los equipos prioritarios (equipo activo).
- Comunicarse con servicios generales del edificio para la supervisión de la planta de emergencia con mayor énfasis.
- Monitorear la UPS cada 5 min. para programar acciones mayores.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- Dar de baja al equipo activo y servicios con mediana prioridad con respecto a las fases definidas.

Acciones después de la Contingencia

- Brindar un tiempo de gracia (depende de la magnitud de la contingencia) para restablecer los equipos activos y servicios.
- Restablecer los equipos activos y servicios que se dieron de baja, en forma paulatina.
- Validar el correcto funcionamiento de los equipos activos y servicios.
- Identificar los posibles daños de los equipos activos.
- Notificar a los usuarios afectados el restablecimiento de los servicios y su condición.
- Evaluar los daños de los equipos activos, planta eléctrica, UPS u otros.

12.6 PLAN DE EMERGENCIA ESTRATEGIAS DE CONTINUIDAD DE TI

Una vez evaluados los riesgos y los requerimientos de la operación de los componentes de TI (mediante el Análisis de Impacto a Negocio – BIA), en esta actividad se proponen las diferentes estrategias de continuidad de TI incluyendo los siguientes aspectos:

Consideraciones para la Continuidad de TI

- Documentación de los Sistemas, configuración e información de los proveedores.
- Asegurar copias de respaldo de los datos institucionales de gestión de usuario.
- Coordinar la solución de Continuidad acorde con el *Manual de Políticas de seguridad y privacidad de la información* (MN-04).
- Coordinar la solución de Continuidad con los controles de seguridad de los Sistemas de información.
- Considerar contingencias para la infraestructura de datos institucionales.
- Coordinar con Proveedores.
- Realizar Acuerdos de Nivel de Servicio con los Proveedores.
- Estandarizar equipos de red LAN.

Soluciones Tecnológicas de Continuidad

- Copias de respaldo de los Sistemas de información y Datos Institucionales.
- Identificar puntos comunes de fallas.
- Obtener imagen de los Hosting Web implementados.
- Implementar balanceo de carga en los sistemas de información aplicables.
- Implementar redundancia en componentes críticos (Controlador de dominio).
- Implementar soluciones de almacenamiento.
- Integrar accesos remotos y tecnologías inalámbricas.
- Realizar monitoreo.
- Replicar datos Institucionales de usuario final.
- Usar UPS (Uninterruptible Power Supplies).

12.7 PLAN DE MANTENIMIENTO

Procedimiento de Activación y Escalamiento

La fase de Notificación y Activación define las acciones iniciales a tomar ante un evento de interrupción o no disponibilidad del componente de TI, e incluye las actividades de Notificación al proceso de Gestión de TIC, evaluación del daño e implementación o activación del Plan.

Reanudación, Recuperación y Restauración

Aunque no existen procedimientos si se realizan tareas de:

- Reanudar temporalmente las operaciones de TI.
- Recuperar el daño hecho al sistema original y se actualiza la información.
- Recuperar las capacidades de procesamiento en operación normal.

Publicación y Divulgación

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

La etapa de Publicación y Divulgación de las tareas de preparación y respuesta ante emergencias de tecnologías de la información busca que la información referente a la continuidad de las operaciones de TI llegue a todos los colaboradores.

Manejo documental

Las siguientes consideraciones deben tenerse en cuenta para las actividades de preparación y respuesta ante emergencias de tecnologías de la información de la empresa:

- Las actividades van encaminadas al uso interno de la empresa.
- Las actividades se encuentran plasmadas en los procedimientos del proceso Gestión de TIC publicados en la Intranet de la empresa.

Información general de qué hacer en caso de un evento

El Proceso de Gestión de TIC coordina con el proveedor externo y/o revisa internamente los equipos propios y determina los procedimientos de notificación de eventos de acuerdo con lo configurado en los sistemas de información y monitoreo.

Responsabilidades o roles frente a una emergencia

FUNCIONARIO	Contacto	ROL / RESPONSABILIDAD
Proceso Gestión de TIC	sistemas@renobo.com.co	Coordinar, planear y ejecutar el plan de acción en cuanto a sistemas de información, recursos informáticos y red con su respectivo respaldo.
Dirección Administrativa y TIC	hvelandiap@renobo.com.co	Coordinar, verificar y asignar los responsables frente a una emergencia.
Profesional de Gestión de Servicios Logísticos	serviciosadministrativos@renobo.com.co	Contar con el inventario de los recursos físicos y asegurar que en caso de pérdida de alguno se cuente con el método de reposición.

12.8 ELEMENTOS, ACTIVIDADES Y RESPONSABLES DEL PLAN DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS DE TECNOLOGÍAS DE LA INFORMACIÓN

Elemento	Actividad	Responsable
Coordinación y seguimiento	Implementar el Plan, coordinar con especialistas y usuarios la ejecución del Plan y controlar y reportar su ejecución durante el procedimiento.	Comité de Emergencias y Contingencias
Recursos para atender la contingencia	Preparación para la ocupación y operación de todos los sitios alternativos. Esto incluye todos los servicios adicionales y aspectos de seguridad. Proveer el personal adicional para realizar las actividades para atender la contingencia en forma acelerada.	Dirección Administrativa y de TICS
Recuperación	Evaluar los daños, recuperar lo que no se dañó y evitar más daños. Proveer datos detallados para los seguros.	Dirección Administrativa y de TICS (Gestión de TIC, Gestión de Servicios Logísticos)
Hardware del sistema	Montar los servidores, estaciones de trabajo y redes internas de comunicación necesarios para restablecer los servicios del Sistema de Información.	Dirección Administrativa y de TICS (Gestión de TIC)
Software del sistema	Instalar y poner en funcionamiento una versión probada del sistema operativo actual y otros sistemas de control para	Dirección Administrativa y de TICS (Gestión de TIC)

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Elemento	Actividad	Responsable
	el hardware existente o nuevo al sitio actual o alterno.	
Telecomunicaciones	Reconstruir o montar la red de telecomunicaciones. Esto incluye proveer recursos de comunicación a los sitios existentes y alternativos.	Dirección Administrativa y de TICS (Gestión de TIC – Contratos de Telecomunicaciones e infraestructura de cableado estructurado)
Operaciones	Proveer una instalación funcionando y manejar el equipo nuevo o existente en el sitio nuevo o alternativo. Esto incluye el backup de los sistemas de información.	Dirección Administrativa y de TICS (Gestión de TIC y Gestión Financiera)
Preparación de datos	Establecer los servicios de preparación y captura de datos. Montaje de copias de respaldo y revisión de integridad.	Dirección Administrativa y de TICS (Gestión de TIC)
Transporte	Suplir todas las necesidades de transporte para el personal, el hardware, la documentación y otros materiales de cómputo.	Dirección Administrativa y de TICS
Administración	Proveer todos los servicios para el personal y materiales necesarios para la operación (papelería, por ejemplo)	Dirección Administrativa y de TICS

12.9 PRESERVAR LA INFORMACIÓN CONTABLE – RECURSOS TECNOLÓGICOS

La preservación de la información contable está cubierta al 100% dado que el sistema Administrativo y Financiero JSP7-Gobierno se encuentra implementado en la nube, esto quiere decir que se cubre de la siguiente manera:

1.

Un backup anual por año a corte de 31 de diciembre.
2.

Un backup mensual a corte a los últimos doce meses.
3.

Un backup semanal al último mes.

LISTADO DE PROVEEDORES PROCESO GESTIÓN DE TIC

A continuación, se asocia el listado de los proveedores de la empresa en todo lo referente a recursos tecnológicos, con un dato de contacto, pues ellos son parte de los procesos de solución para mitigar los riesgos evidenciados en el plan:

Contrato Infraestructura de Telecomunicaciones, colocación, hosting Web

Proveedor	Contacto	Dirección	Teléfono
Empresa de Teléfonos de Bogotá SA ESP	Help Desk	helpdeskETB@etb.com.co	018000 123737 Op 2

Infraestructura física, eléctrica cuartos de telecomunicaciones, cableado estructurado sede principal

Proveedor	Contacto	Dirección	Teléfono
Grupo ASD	Nathaly Pineda	npineda@grupoasd.com	

Mantenimiento preventivo y Correctivo de Hardware

Proveedor	Contacto	Dirección	Teléfono
IT Soluciones y servicios	Alice Gómez	comercial2@itsolucionesyservicios.com	320 8352174

Software

Software	Proveedor	Contacto	Correo electrónico	Teléfono
Lumion	MicroCAD S.A.S	Maria Zuleima Mosquera Díaz	capacitacion@microcad.com.co	Tel: (57) (4) 2932121 ext.101 // 4448149 // Fax: 3202889 // Cel: 3015849472
ArcGis y City	Esri Colombia	Camila Galán	cgalan@esri.co	(601) 650 1550 ext

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Software	Proveedor	Contacto	Correo electrónico	Teléfono
Engine		C.		3367
Antivirus	Datasec	soporte	soporte@datasec.com.co	3103159346

Alquiler Pcs

Proveedor	Contacto	Correo electrónico	Teléfono
NecSoft		soporte@necsoftpc.com	3160283083

Planta telefónica

Proveedor	Contacto	Correo electrónico	Teléfono
M@icrotel	Diana Carolina Romero	serviciotecnico@maicrotel.com	6438330 Ext 116
	Carlos Vaquero		3124183428

JSP7 – Sistema Administrativo y Financiero

Proveedor	Contacto	Correo electrónico	Teléfono
ASP SOLUTIONS	Eugenio Millán	eugenio.millan@aspsols.com	3173926034 3008035350
	Juan Carlos Rugeles	jcrugeles@aspsols.com	
Soporte Microsoft	Microsoft Colombia		(571) 326 4700

LISTADO DE CONTACTOS INTERNOS

Proceso Gestión de TIC

Nombre	Teléfonos
Yolanda Urrea	3012064648
Yuli Beltrán	3054783445
Tatiana Ortiz	3057527845
Sophia Morales	3003334129
Zamir Velasquez	3112788344
Holman Barrera	3175019663
Freiman Herreño	3107677979
Nilson Andrés Villalo	3212091526
Juan Pablo Suarez	3112528096
Andres Buitrago	3204125433
Iván Ceballos	3175769847
Fernando Ospina	3167424133

14. PROCEDIMIENTOS OPERATIVOS NORMALIZADOS “PON’S”

Los procedimientos operativos normalizados son acciones específicas de respuesta “Normalizadas”, que permiten a todos los organismos y personas que intervienen en la atención de un incidente, actuar de forma similar, coordinadamente, facilitando las comunicaciones y optimizando el uso de los recursos disponibles.

A continuación, se relacionan los escenarios de riesgo de mayor probabilidad que pueden presentarse en las locaciones de la Empresa y se presentan los procedimientos operativos normalizados:

- PON para atención de una emergencia
- PON para atención de un accidente de tránsito

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

- PON para evacuación
- PON para derrame
- PON para hurto
- PON para incendio
- PON para primeros auxilios
- PON para sismo

Para cada uno de estos riesgos, la Empresa establece los siguientes Procedimientos Operativos Normalizados (PON):

PLAN OPERATIVO NORMALIZADO PARA ATENCIÓN DE UNA EMERGENCIA

OBJETIVO

Realizar la notificación de un incidente o emergencia para que se implementen las acciones pertinentes conforme los Procedimientos Operativos Normalizados que se han establecido y la posterior evaluación de las acciones realizadas y posterior restablecimiento de las actividades habituales del área afectada.

ALCANCE

Aplica a todas las sedes, dependencias y personas (habituales o flotantes) de la Empresa. Está sujeto al entrenamiento y equipos con que cuente la Brigada de Emergencias, así como de aquellas entidades que se puedan requerir para el control de la situación.

RECURSOS, SUMINISTROS Y SERVICIOS A UTILIZAR

Se debe contar con disponibilidad de brigadistas de emergencia, equipos conforme lo requerido en los PON's, directorio telefónico de entidades de emergencia, equipos de comunicaciones, y disponibilidad de vehículo institucional en caso de emergencia.

1. PROCEDIMIENTOS OPERATIVOS NORMALIZADOS "PON'S"

Los procedimientos operativos normalizados son acciones específicas de respuesta "Normalizadas", que permiten a todos los organismos y personas que intervienen en la atención de un incidente, actuar de forma similar, coordinadamente, facilitando las comunicaciones y optimizando el uso de los recursos disponibles.

A continuación, se relacionan los escenarios de riesgo de mayor probabilidad que pueden presentarse en las locaciones de la Empresa y se presentan los procedimientos operativos normalizados:

- PON para atención de una emergencia
- PON para atención de un accidente de tránsito
- PON para evacuación
- PON para derrame
- PON para hurto
- PON para incendio
- PON para primeros auxilios
- PON para sismo

Para cada uno de estos riesgos, la Empresa establece los siguientes Procedimientos Operativos Normalizados (PON):

PLAN OPERATIVO NORMALIZADO PARA ATENCIÓN DE UNA EMERGENCIA

OBJETIVO

Realizar la notificación de un incidente o emergencia para que se implementen las acciones pertinentes conforme los Procedimientos Operativos Normalizados que se han establecido y la posterior evaluación de las acciones realizadas y posterior restablecimiento de las actividades habituales del área afectada.

ALCANCE

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Aplica a todas las sedes, dependencias y personas (habituales o flotantes) de la Empresa. Está sujeto al entrenamiento y equipos con que cuente la Brigada de Emergencias, así como de aquellas entidades que se puedan requerir para el control de la situación.

RECURSOS, SUMINISTROS Y SERVICIOS A UTILIZAR

Se debe contar con disponibilidad de brigadistas de emergencia, equipos conforme lo requerido en los PON’s, directorio telefónico de entidades de emergencia, equipos de comunicaciones, y disponibilidad de vehículo institucional en caso de emergencia.

DIAGRAMA DE FLUJO	ACCIÓN A REALIZAR	RESPONSABLE
	Cualquier persona que detecte una emergencia evalúa la proporción de la misma	Funcionarios, Contratistas, Visitantes
	Da aviso inmediato al brigadista de emergencia o al personal de Seguridad para que se inicien las acciones de respuesta pertinentes.	Funcionarios, Contratistas, Visitantes
	La persona que reporta el incidente puede actuar como primer respondiente para tratar de controlar la emergencia conforme la situación, su capacitación y entrenamiento.	Funcionarios, Contratistas, Visitantes
	La brigada de emergencias esta activa, el primer integrante de la brigada en llegar al lugar de la emergencia, asume la coordinación de la atención del incidente, verificando el tipo de emergencia, su magnitud, equipos y áreas involucradas	Brigadista
	Se activa el (los) Procedimiento(s) Operativo(s) Normalizado(s) - PON a que haya lugar.	Brigadista
	Informar al área de Talento Humano a través de la persona encargada del Sistema de	Brigadista, Funcionario, Contratista
	Realizar el aislamiento preventivo del área afectada e inicia las actividades de control	Brigadista, Funcionario, Contratista
	Una vez llega el resto de la Brigada de Emergencia se asignan tareas y se procede a la intervención requerida conforme las características del incidente y el PON a ejecutar.	Brigadista
	Una vez desarrolladas las acciones del PON y garantizado el control del incidente o emergencia se realiza la evaluación del mismo y de su intervención	Brigadista, Líder SGSST
	Se establece enlace con el personal que pertenece al nivel estratégico correspondiente para el reporte del incidente y asumir las acciones de recuperación de la zona afectada.	Subgerencia de Gestion Corporativa Líder SGSST

PLAN OPERATIVO NORMALIZADO PARA ATENCIÓN DE UN ACCIDENTE DE TRÁNSITO

OBJETIVO

Realizar el manejo adecuado de un accidente vehicular con o sin lesionados reduciendo la posibilidad de efectos adverso adicionales a los producidos por el incidente.

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

ALCANCE

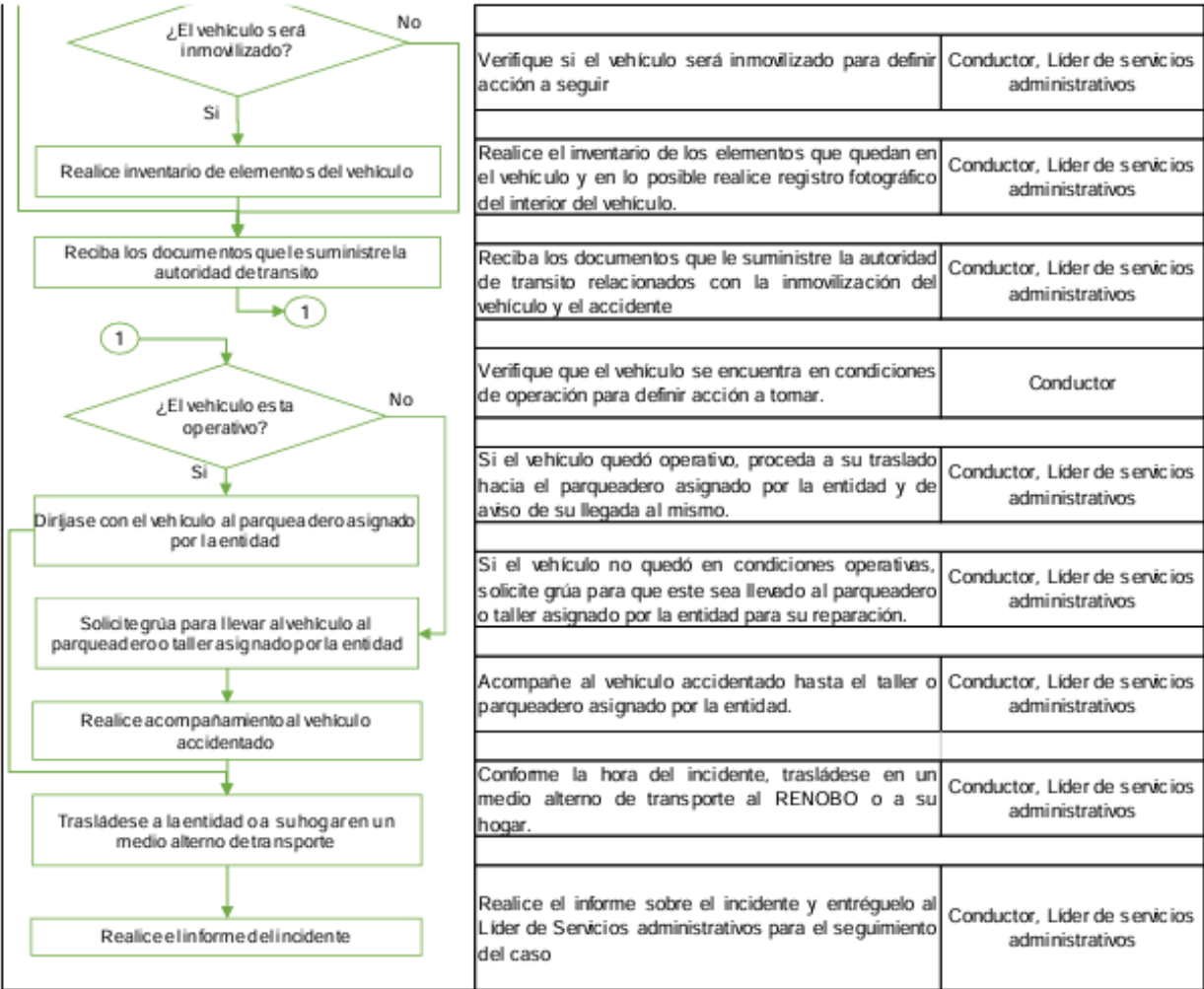
Aplica a todos los vehículos que prestan sus servicios a las diferentes dependencias y personas de la Empresa. Este comprende el entrenamiento brindado a cada conductor conforme el área asignada y los equipos con los cuales está dotado el vehículo.

RECURSOS, SUMINISTROS Y SERVICIOS A UTILIZAR

Tarjeta de Propiedad del Vehículo, Licencia de Conducción del vial o conductor, Seguro Obligatorio de Accidentes de Tránsito - SOAT, Herramientas y Equipo de Seguridad del vehículo, Botiquín, Soporte Líder de recursos físicos.

DIAGRAMA DE FLUJO	ACCIÓN A REALIZAR	RESPONSABLE
Quédese en la escena y notifique el accidente de Tránsito	Al momento de accidentarse en el vehículo, quédese en la escena y notifique al área de servicios administrativos de RENOBO	Conductor
Asegure la escena del incidente con luces de parqueo y conos	Encienda luces de parqueo y ubique los conos o triángulos reflectivos a una distancia igual o mayor a 10 metros de la ubicación del automóvil siniestrado.	Conductor
¿Conductor y/o Pasajeros Tienen Lesiones? No Si	Verifique que si usted, así como sus pasajeros tienen lesiones. Solicite la activación de la póliza, así como el apoyo de personal de tránsito y servicio de salud	Conductor, Líder de servicios administrativos , Líder SGSST
Active el NUSE 123 para atención de emergencias en salud	Active el sistema de emergencias local a través del Número Único de Servicio de Emergencia - NUSE 123	Conductor, Líder de servicios administrativos , Líder SGSST
No mueva el vehículo hasta elaborar el croquis del incidente	No mueva el vehículo hasta que se realice el croquis del incidente, solo podrá mover el vehículo cuando la autoridad de tránsito lo solicite o requiera. Realice	Conductor, Líder de servicios administrativos
No concilie, sea prudente al discutir el incidente.	Sea precavido al discutir el incidente y no realice ningún tipo de acuerdo. Espere al delegado de la aseguradora y/o de servicios administrativos de	Conductor, Líder de servicios administrativos

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS



PLAN OPERATIVO NORMALIZADO PARA EVACUACIÓN

OBJETIVO

Alejar en el menor tiempo posible al personal permanente y flotante que se encuentra en las instalaciones de la empresa por encontrarse expuesto a una amenaza y a la materialización del riesgo que ella conlleva, conduciendo a este personal hasta un lugar seguro alejado del incidente o emergencia.

ALCANCE

Aplica a todas las sedes, dependencias y personas (habituales y/o visitantes) de la empresa. Está sujeto al entrenamiento y equipos con que cuente la brigada de emergencias, así como de aquellas entidades que se puedan requerir para el control de la situación.

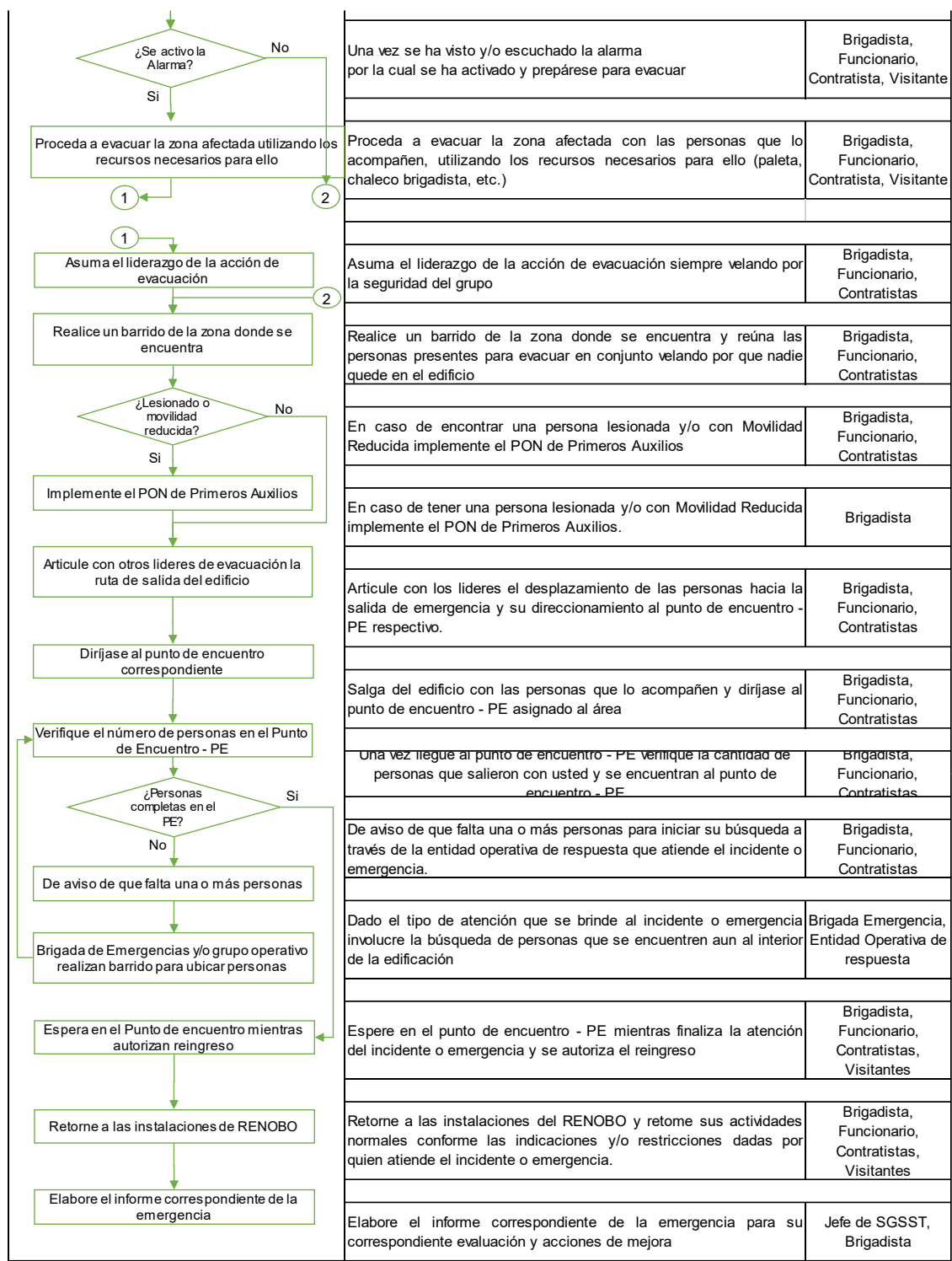
RECURSOS, SUMINISTROS Y SERVICIOS A UTILIZAR

Se requieren paletas de señalización, chalecos para los brigadistas, botiquines portátiles, Camillas, Espacio(s) definido(s) como Punto(s) de Encuentro, Señal de punto de encuentro - PE, Brigadistas de Emergencia

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

DIAGRAMA DE FLUJO	ACCIÓN A REALIZAR	RESPONSABLE
Notificación de una Emergencia Valide la Información y ubicación del incidente o emergencia Proceda a activar la Brigada de emergencias ¿Cuenta con brigadista? No Si Alerte las áreas conexas y al personal cercano a la zona comprometida Active la Alarma si la emergencia presentada así lo requiere Evalúe la estrategia y ruta de evacuación	Se realiza la notificación de una emergencia o incidente por parte de una persona que se encuentra en la sede de RENOBO Es pertinente validar la situación que ha sido reportada para definir la activación de la alarma y de la brigada de emergencia. Conforme la validación realizada, proceda a activar la brigada de emergencias. Verifique si esta acompañado por un brigadista de la entidad que lo apoye en el proceso y las acciones a desarrollar Alerte al personal de las áreas cercanas a la zona comprometida o afectada por la emergencia para que inicien el procedimiento de evacuación. Realice la notificación de la Emergencia a través de la alarma definida por la entidad (visual y sonora) si esta lo amerita. Conforme el área o zona afectada evalúe la ruta por la cual realizara la evacuación y la estrategia bajo la cual actuara.	Funcionario, Contratistas, Visitante Funcionario, Contratistas, Visitante Brigadista, Funcionario, Contratista Funcionario, Contratistas, Visitante Brigadista, Funcionario, Contratista Brigadista, Funcionario, Contratista Brigadista, Funcionario, Contratista

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS



PLAN OPERATIVO NORMALIZADO PARA DERRAME

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

OBJETIVO

Establecer los lineamientos necesarios para la preparación y atención de un incidente y/o emergencia ambiental que se pueda presentar de acuerdo a la evaluación de vulnerabilidades y amenazas identificadas en el desarrollo de las actividades de la empresa.

ALCANCE

Aplica a todas las sedes, dependencias, personas (habituales y/o visitantes) y servicios de la empresa que involucran el manejo o intervención ante el derrame de algún tipo de líquido. Está sujeto al entrenamiento y equipos con que cuente la brigada de emergencias, así como de aquellas entidades que se puedan requerir para el control de la situación con impacto ambiental.

RECURSOS, SUMINISTROS Y SERVICIOS A UTILIZAR

Brigada de emergencias, capacitación en la contención básica de líquidos, equipo de contención de líquidos (conforme su tipo).

DIAGRAMA DE FLUJO	ACCIÓN A REALIZAR	RESPONSABLE
Identifique el liquido que se derramo, fuente de la fuga, cantidad, ubicación, uso.	Identifique el liquido que se derramo (combustible, aceite, cloro, Varsol, etc.), la fuente de la fuga, cantidad, ubicación, uso. Informe del caso	Funcionario, Contratistas, Visitante
Evalúe la situación, determine riesgos asociados, identifique la afectación e informe	Evalúe la situación, determine riesgos asociados, identifique el tipo de afectación (interna o externa) para la empresa e informe	Brigadista, Funcionario, Contratistas - PIGA
Identifique el tipo de intervención requerida (interna y/o externa)	Identifique el tipo de intervención requerida (interna y/o externa), active la brigada de emergencias solicite los recursos necesarios y de ser necesario active cuerpo de socorro especializado.	Brigadista, PIGA
Evite la inhalación de vapores, fuentes de ignición, caminar sobre el producto	Evite la inhalación de vapores, fuentes de ignición, caminar sobre el producto para no contaminar otras áreas.	Brigadista, Funcionario, Contratistas, Visitante, PIGA
¿El producto fue contenido?	Verifique si el producto ya fue contenido	Brigadista, PIGA
Detenga la fuga en caso de poder hacerlo sin riesgo.	Detenga la fuga (cierre la llave, ponga un tapón, etc.) en caso de poder hacerlo sin riesgo, no actúe solo. Use materiales absorbentes no combustibles	Brigadista, PIGA
Verifique el curso que tomo el liquido y proceda a confinarlo, evite que siga su recorrido.	Verifique el curso que tomo el derrame del liquido y proceda a confinarlo, evite que siga su recorrido de tal forma que no afecte cuerpos de agua o suelos.	Brigadista, PIGA
En caso de tener un lesionado active el PON de Primeros Auxilios, descontamine la persona.	En caso de tener personas lesionadas por el derrame, active el PON de Primeros Auxilios y descontamine la persona.	Brigadista, Funcionario, Contratistas, Visitante, PIGA
Controlada la fuga realice el re envase, trasiego y recuperación del liquido derramado	Una vez controlada la fuga disponga los equipos necesarios para realizar el re envase, trasiego y recuperación del liquido derramado. Siempre mantenga	Brigadista, PIGA
Recoger y disponer de manera adecuada los productos utilizados para contener y confinar el liquido	Los productos utilizados para contener y confinar el liquido derramado se deben recoger en caneca o bolsas adecuadas, han de ser rotulados y disponerse	Brigadista, PIGA
Verifique estado del personal en el incidente. Si es necesario active PON de Primeros Auxilios.	Una vez controlado el incidente verifique estado físico de quienes intervinieron en la atención del incidente. De ser necesario active el PON de Primeros Auxilios.	Brigadista, PIGA, Lider SGSST
Reacondicione sitio afectado y equipos, elabore el informe del incidente	Reacondicione sitio(s) afectado(s) y equipo(s), y realice el informe del incidente	Brigadista, PIGA, Lider SGSST

PLAN OPERATIVO NORMALIZADO PARA HURTO

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

OBJETIVO

Minimizar las lesiones en las personas, así como las pérdidas en la infraestructura que se puedan presentar como consecuencia de un asalto, robo o hurto por parte de uno o varios individuos.

ALCANCE

Aplica a todas las sedes, dependencias y personas (habituales y/o visitantes) de la empresa. Está sujeto al entrenamiento y equipos con que cuente la Brigada de Emergencias, así como de aquellas entidades que se puedan requerir para el control de la situación.

RECURSOS, SUMINISTROS Y SERVICIOS A UTILIZAR

Sistema de alarma no sonora, personal de seguridad física.

DIAGRAMA DE FLUJO	ACCIÓN A REALIZAR	RESPONSABLE
Detecte la situación de hurto, robo o asalto.	Detecte la situación de riesgo por hurto, robo o asalto en las instalaciones y/o vehículo(s) de la entidad.	Funcionarios, Contratistas
Mantenga la calma y no realice ningún acto imprudente	Mantenga la calma y no realice ningún acto que ponga en peligro a otras personas	Funcionarios, Contratistas
De aviso al personal de seguridad si es posible llame al 123 y reporte el incidente y pida ayuda	De aviso a seguridad física de la entidad. De ser posible llame al NUSE 123 para reportar el incidente y solicite ayuda al personal de la Policía nacional	Funcionarios, Contratistas
Observe la mayor cantidad de detalles para identificar a los asaltantes	Observe la mayor cantidad de detalles (facciones, ropa, dirección en que huyen, placa de vehículos utilizados, etc.) que puedan ayudar a identificar a los asaltantes y dar con el paradero de los asaltantes	Funcionarios, Contratistas
Protéjase en caso de presentarse actos violentos con o sin armas	En caso de un enfrentamiento que implique violencia con o sin armas letales, busque un lugar seguro y protéjase hasta cuando este seguro de que la situación ha sido controlada por la Policía Nacional.	Funcionarios, Contratistas Seguridad Física de la sede
No ¿Los delincuentes se fueron?	Una vez finalizado el hurto o asalto, verifique que los delincuentes se hayan retirado.	Funcionarios, Contratistas
Si tiene algún herido o lesionado active el PON de primeros auxilios	En caso de tener una persona herida o lesionada active el PON de primeros auxilios	Brigadista Lider SGSST Servicios
Evite cargas por encima de los hombros, giros y/o inclinaciones del tronco	Apoye el proceso de investigación de la Policía Nacional para la toma de información. El personal afectado por el asalto o hurto deberá brindar la información que se relacione con el caso	Subgerencia G. Corporativa Funcionario Contratista
Elabore el informe respectivo y denuncia de lo sucedido.	Elabore el informe respectivo y denuncia de lo sucedió a la empresa o entidad competente. Adelante proceso de reposición de elementos robados.	Subgerencia G. Corporativa

PLAN OPERATIVO NORMALIZADO PARA INCENDIO

OBJETIVO

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

Realizar la contención de un incendio conforme la capacidad y entrenamiento de la Brigada de Emergencias asegurando a su vez, la evacuación del personal amenazado por la conflagración y el apoyo externo necesario para la extinción definitiva del fuego.

ALCANCE

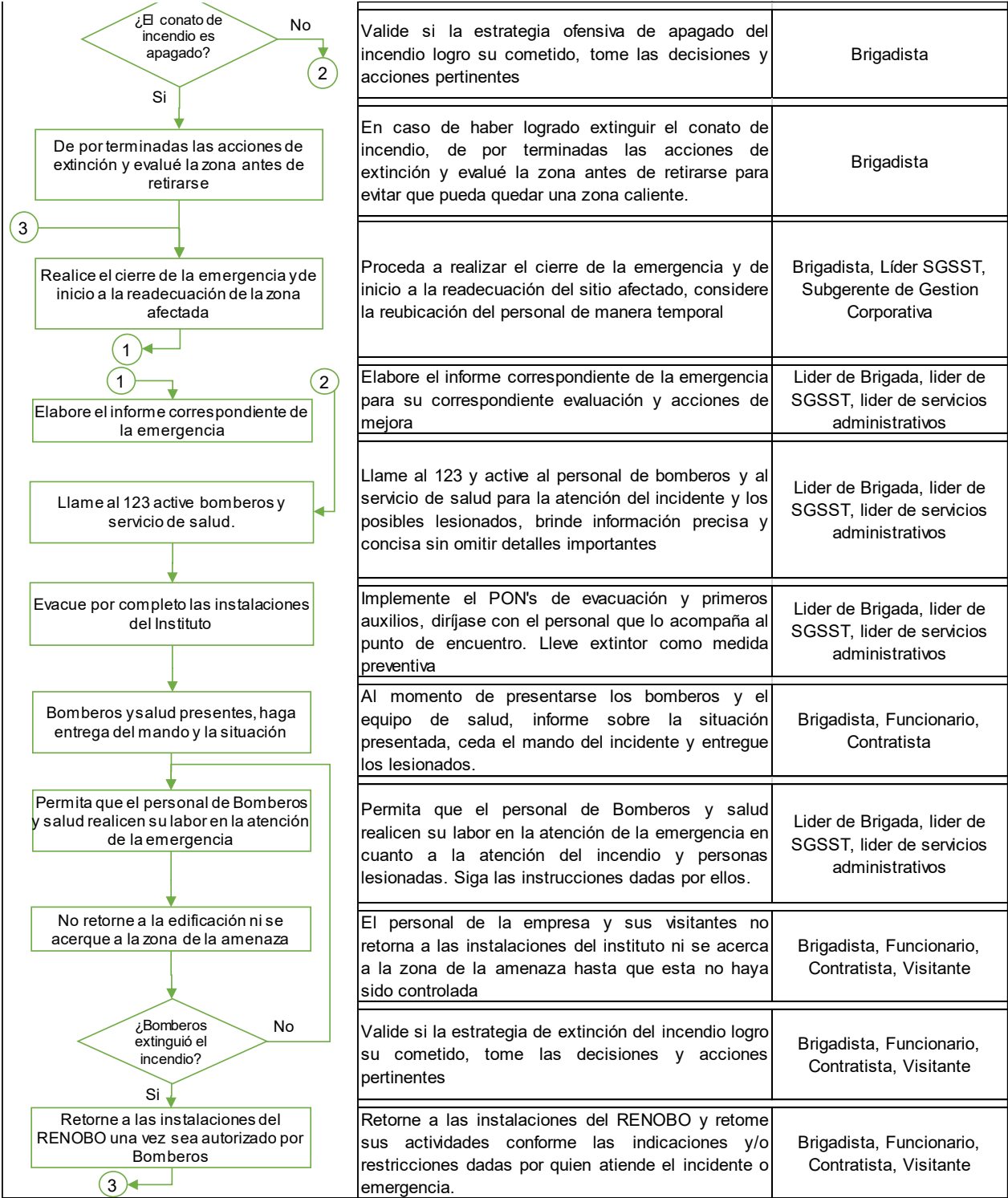
Aplica a todas las sedes, dependencias y personas (habituales y/o visitantes) de la empresa. Está sujeto al entrenamiento y equipos con que cuente la Brigada de Emergencias, así como de aquellas entidades que se puedan requerir para el control de la situación.

RECURSOS, SUMINISTROS Y SERVICIOS A UTILIZAR

Se requieren chalecos para los brigadistas, extintores, gabinetes equipados, alarma contraincendios, detector contraincendios, Brigadistas de Emergencia.

DIAGRAMA DE FLUJO	ACCIÓN A REALIZAR	RESPONSABLE
Valide la veracidad de la Emergencia	Valide la veracidad de la amenaza, y a recopilar la mayor cantidad de información posible (origen, causas, tamaño, ubicación, posible afectación)	Funcionario, Contratista, Visitante
Notifique la Emergencia al representante de la entidad o al brigadista	Advierta sobre la situación de riesgo al lider de brigada con el cual se encuentra, al brigadista de emergencia, o a la persona de seguridad	Funcionario, Contratista, Visitante
Aléjese del sitio del incidente que presenta el conato de incendio	Si no cuenta con la preparación ni entrenamiento apropiados aléjese de la zona del fuego alejando a las demás personas del lugar	Funcionario, Contratista, Visitante
Aísle la zona afectada y suspenda el fluido eléctrico del lugar	Aísle la zona y suspenda el fluido eléctrico del lugar, en caso de no saber donde se hace, solicítelo al personal de seguridad o al brigadista de emergencias.	Brigadista, Funcionario, Contratista
Evalúe la situación y decida el tipo de control (ofensivo o defensivo)	Realice evaluación de la situación, tenga en cuenta nivel de riesgo, entrenamiento y equipos disponibles y decida el tipo de control posible. Siempre prima la seguridad de las personas	Brigadista, Funcionario, Contratista
Prepare el personal para evacuar las instalaciones de Renobo	Siga las instrucciones de los brigadistas y prepárese para evacuar, inicie PON's de evacuación y primeros auxilios.	Brigadista, Funcionario, Contratista

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS



PLAN OPERATIVO NORMALIZADO PARA PRIMEROS AUXILIOS

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

OBJETIVO

Facilitar la respuesta y atención a cualquier persona que resultare lesionada al interior de las instalaciones de la empresa o por efecto de un accidente al momento de encontrarse desarrollando alguna de las funciones propias de su ocupación.

ALCANCE

Aplica a todas las sedes, dependencias y personas (habituales y/o visitantes) de la empresa. Está sujeto al entrenamiento y equipos con que cuente la Brigada de Emergencias, así como de aquellas entidades que se puedan requerir para el control de la situación.

RECURSOS, SUMINISTROS Y SERVICIOS A UTILIZAR

Brigadista de primeros auxilios, botiquín, camilla, inmovilizadores cefálico y cervical, Soporte Líder de brigada de emergencias, Líder SGSST, Líder servicios administrativos.

DIAGRAMA DE FLUJO	ACCIÓN A REALIZAR	RESPONSABLE
Informe del incidente o accidente al Brigadista del área o al Líder de SGSST	Al ocurrir un incidente o accidente al interior de las instalaciones de RENOBO informe al brigadista de emergencias, y en caso que un funcionario o contratista se lesione o vea afectada su salud en cumplimiento de sus funciones al exterior de la entidad avise al Líder de SGSST	Líder SGSST, Brigadista, Funcionario, Contratista
Verifique que la persona tenga pulso y respire, así mismo, su estado conciencia.	Verifique que la persona tenga pulso y respire, así como el estado conciencia (¿habla con usted o no lo hace?).	Brigadista, Funcionario, Contratista
Solicite un botiquín para la atención primaria de la persona	Solicite el botiquín para la atención primaria de la persona lesionada	Brigadista, Funcionario, Contratista
No ¿Esta entrenado en primeros Auxilios?	Conforme la preparación y entrenamiento con la que usted cuente, defina el camino de acción a seguir.	Brigadista, Funcionario, Contratista
Realice Valoración Primaria y estabilice al paciente	Si cuenta con la preparación y entrenamiento apropiada realice la valoración primaria y estabilice al paciente. No pierda contacto con el paciente	Brigadista, Funcionario, Contratista
¿El paciente se estabilizo y mejoro?	Verifique el estado del paciente y si este se estabilizo y mejoro su condición de salud. Tenga en cuenta el tipo de lesión o afectación a la salud	Brigadista, Funcionario, Contratista

PLAN OPERATIVO NORMALIZADO PARA SISMOS

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

OBJETIVO

Realizar el manejo adecuado del incidente con el fin de evitar lesionados y reducir la posibilidad de daños materiales en las instalaciones.

ALCANCE

Aplica a todas las sedes, dependencias y personas (habituales y/o visitantes) de la empresa. Está sujeto al entrenamiento y equipos con que cuente la Brigada de Emergencias, así como de aquellas entidades que se puedan requerir para el control de la situación.

RECURSOS, SUMINISTROS Y SERVICIOS A UTILIZAR

Se debe contar con disponibilidad de brigadistas de emergencia, equipos conforme lo requerido en los PON's, directorio telefónico de entidades de emergencia y equipos de comunicaciones.

DIAGRAMA DE FLUJO	ACCIÓN A REALIZAR	RESPONSABLE
Inicio y detección del Sismo Suspenda actividades y refúgiase en un lugar seguro y cercano finalización del Sismo ¿Hay Lesionados? Si Ejecuta PON de Primeros Auxilios Inspección de instalaciones ¿Se requiere evacuación? No Si Ejecuta PON Evacuación ¿Requiere ayuda externa? No Si Solicite la ayuda específica requerida. Proceda a las acciones correspondientes de recuperación Elaborar informe del incidente	Una vez identifique un sismo, suspenda sus tareas o actividades e implemente acciones de protección resguardándose de objetos que caen, alejándose de las ventanas. No intente evacuar durante el sismo. Una vez finalice el sismo espere un instante Verifique si cerca a usted hay personas lesionadas o afectadas por las consecuencias del movimiento telúrico. Si luego de finalizado el sismo observa personas lesionadas, ejecute PON para Manejo de Lesionados. Verifique las condiciones de la estructura y si observa daños prepárese a evacuar y este atento a las indicaciones de la brigada de emergencias. Defina si es necesario evacuar la edificación. Siga las indicaciones de la brigada de emergencias y ejecute el PON de evacuación. Conforme las condiciones de la estructura e incidentes conexos, verifique si requiere apoyo de una entidad operativa externa. Solicite la ayuda a la entidad operativa y/o de apoyo que le permita atender de manera adecuada el incidente. Si las condiciones de seguridad no están dadas para retomar labores, el director como nivel estratégico establecerá las acciones a seguir. Proceda a elaborar el informe del incidente o emergencia y de las acciones implementadas	Funcionario, Visitantes Funcionario, Visitantes Funcionario, Visitantes Brigada Emergencias Funcionario, Visitantes Brigada Emergencias Brigada Emergencias Brigada Emergencias Jefe de Emergencias Brigada Emergencias Jefe de Emergencias Brigada Emergencias Director, Asistencia Técnica, Brigada Emergencias Lider SGSST, lider de servicios administrativos y lider de brigada

PLAN INTEGRAL DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	01/11/2023	Documento original aprobado en el marco del Comité Institucional de Gestión y Desempeño del 1 de noviembre de 2023. Acta No. 22 de 2023.
2	30/07/2025	Ajustes del Plan por cambio de sede. Documento aprobado en el marco del Comité Institucional de Gestión y Desempeño del 30 de julio de 2025.