El servicio público es de todos

Función Pública

FUNCIÓN PÚBLICA

Documento Técnico del Plan de Continuidad del Negocio

VERSIÓN 6

Enero 2022

Versión	Fecha Versión	Observación
1	05 de febrero 2017	Creación del documento
2	01 de Marzo 2017	Versión 2 del Documento Técnico del Plan de Continuidad del Negocio
3	31 de Mayo 2019	Tercera versión del Documento Técnico del Plan de Continuidad del Negocio
4	21 de Octubre 2020	Adecuación del documento técnico a la norma técnica colombiana NTC/ISO IEC 22301
5	09 de Noviembre 2021	Se detalla el modelo de operación del plan de continuidad y las responsabilidades específicas del comité de emergencias. Se incluyen las fichas descriptivas de protocolo de acción por escenario de emergencia
6	20 de Enero 2022	Se anexa formato de actividades detectivas, preventivas, reactivas y correctivas para gestionar adecuadamente las situaciones que sean calificadas como emergencia y puedan comprometer la seguridad del personal, la prestación de servicio o la continuidad de las funciones misionales.

Tabla de contenido

Presentación

Con el fin de contar con una herramienta que nos permita prevenir o reaccionar adecuadamente ante posibles incidentes que pongan en riesgo al personal que prestasus servicios para la Entidad, los visitantes de la sede principal, afectar el debido desarrollo de las actividades propias de Función Pública, impedir la prestación y continuidad del servicio a los Grupos de Valor o el cumplimiento de los compromisos establecidos en la planeación estratégica institucional, la Entidad ha consolidado el conjunto de acciones que se emprenden para dar respuesta a estos eventos en el Plan de continuidad del negocio. Estas acciones diseñadas y ejecutadas de forma planificada, permitirían responder de manera eficiente ante una emergencia, restablecer en el menor tiempo la prestación de los servicios y mitigar el impacto negativo de la pérdida de recursos.

El plan de continuidad del negocio tiene en cuenta las obligaciones legales aplicablesa la Función Pública que establecen la Ley de Seguridad y Salud en el Trabajo, la Ley de Control Interno (análisis del entorno y manejo de riesgos), los lineamientos del eje transversal de seguridad de la política de seguridad digital, la Ley de Calidad, la Ley general de archivos, y comprende actividades detectivas, preventivas, reactivas y correctivas, articuladas a la planeación estratégica y operativa de cada vigencia segúnla función y responsabilidad de cada proceso.

La consolidación del plan incluye la elaboración de guías de trabajo: la primera la constituye el documento técnico que define los elementos críticos a controlar a partir del análisis de los riesgos asociados, los responsables, etapas, definiciones y generalidades; la segunda son las actividades específicas y secuenciales, fechas de ejecución, recursos requeridos (humanos, físicos, tecnológicos, económicos) y el análisis de brechas de cada una de ellas, teniendo en cuenta las restricciones económicas de la Función Pública.

Marco Legal

El desarrollo del plan de continuidad de negocio para el departamento administrativo de la función pública se fundamenta en la necesidad de preservar la disponibilidad y continuidad de los servicios que presta la entidad, dentro del marco de la implementación de la política de gobierno digital y los lineamientos generales en el uso de servicios digitales ciudadanos. Igualmente, la estrategia de continuidad de negocio institucional está articulado con el modelo integrado de planeación y gestión a través de la 3ª. Dimensión: Gestión con valores para resultados. Finalmente, la estrategia de continuidad de negocio institucional facilita la integración de las estrategias preservación de la seguridad y la vida de los grupos de valor de la Entidadal incorporar los lineamientos de gestión y tratamiento de riesgos y desastres de la Ley 1523 de 2012, política nacional de gestión del riesgo de desastres y las

obligaciones en materia de Sistema de Gestión de la Seguridad y Salud en el Trabajo(SG-SST) del decreto 1072 de 2015.

Ley 1955 de 2018, por el cual se expide el Plan Nacional de Desarrollo 2018 -2022."Pacto por Colombia, Pacto por la Equidad".

> Artículo 147. Transformación Digital Pública. Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para estepropósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. En todos los escenarios la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la Cuarta Revolución Industrial, entre otros.
>
> 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.
>
> 11. Inclusión y actualización permanente de políticas de seguridad y confianzadigital.

Decreto 1078 de 2015. por medio del cual se expide el Decreto Único Reglamentariodel Sector de Tecnologías de la Información y las Comunicaciones.

> "TÍTULO 17 lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
>
> ARTICULO 2.2.17.1.6. Principios. Además de los principios previstos en el artículo 209 de la Constitución Política, en el artículo 2 de la Ley 1341 de 2009, en el artículo 3 de la Ley 1437 de 2011, en el artículo 4 de la Ley 1581de 2012 y los atinentes a la Política de Gobierno Digital contenidos en el artículo 2.2.9.1.1.3 del capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015 la prestación de los servicios ciudadanos digitales se orientará por los siguientes principios:
>
> 6. Seguridad, privacidad y circulación restringida de la información: Toda la información de los usuarios que se genere, almacene, transmita o trate en el marco de los servicios ciudadanos digitales deberá ser protegida y custodiadabajo los más estrictos esquemas de seguridad digital y privacidad con miras a garantizar la autenticidad, integridad, **disponibilidad**. confidencialidad, el acceso y circulación restringida de la información, de conformidad con lo estipulado en el habilitador transversal de seguridad de la información de la Política de Gobierno Digital. **(negrilla fuera de texto)**
>
> ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital. Los actores que traten información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y **continuidad de la prestación del servicio.** en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital. que incluya unaidentificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas. políticas. procedimientos. recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la

Información y las Comunicaciones. (**negrilla fuera de texto**)"

Modelo Integrado de planeación y gestión, 3ª. Dimensión: Gestión con valorespara resultados.

3.2.1.3 Política Gobierno Digital

Gobierno Digital es la política de MIPG que busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital. La política de Gobierno Digital contribuye a la Transformación Digital del sector público, la cual implica un cambio en los procesos, la cultura y el uso de la tecnología (principalmente tecnologías emergentes y de la Cuarta Revolución Industrial), para el mejoramiento de las relaciones externas de las entidades de Gobierno, a través de la prestación de servicios más eficientes.

3.2.1.4 Política de Seguridad Digital

En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivosa las entidades.

Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e **implementación de instrumentos de resiliencia, recuperación y respuesta nacional** en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y socialen el país. (**negrilla fuera de texto)**

Decreto 1072 de 2015, por medio del cual se expide el Decreto Único Reglamentariodel Sector Trabajo

Artículo 2.2.4.6.4. Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST). El Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG- SST) consiste en el desarrollo de un proceso lógico y por etapas, basado en la mejora continua y que incluye la política, la organización, la planificación,la aplicación, la evaluación, la auditoría y las acciones de mejora con el objetivo de **anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y la salud en el trabajo.** (**negrilla fuera de texto**)

Ley 1523 de 2012, Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres.

Artículo 2°. De la responsabilidad. La gestión del riesgo es responsabilidad de todas las autoridades y de los habitantes del territorio colombiano. **En cumplimiento de esta responsabilidad, las entidades públicas, privadas y comunitarias desarrollarán y ejecutarán los procesos de gestión del riesgo, entiéndase: conocimiento del riesgo, reducción del riesgo ymanejo de desastres**, en el marco de sus competencias, su ámbito de actuación y su jurisdicción, como componentes del Sistema Nacional de Gestión del Riesgo de Desastres.

Objetivos y Alcance del Plan de Continuidad

Objetivo General

Definir las actividades detectivas, preventivas, reactivas y correctivas para gestionar adecuadamente las situaciones que sean calificadas como emergencia y puedan comprometer la seguridad del personal, la prestación de servicio o la continuidad de las funciones misionales.

Objetivos específicos

- ✓ Asegurar la protección de las personas dentro de las instalaciones de la Entidaden caso de que se materialice una emergencia
- ✓ Mejorar el nivel de confianza de nuestros grupos de valor en las capacidades Institucionales de recuperación en caso de situaciones de emergencia.
- ✓ Disminuir el impacto para el cumplimiento de las actividades misionales en casode materialización de una situación de emergencia
- ✓ Identificar las actividades críticas, los recursos y los procedimientos necesariospara mantener en niveles aceptables las actividades misionales en caso ocurrencia de una emergencia
- ✓ Disminuir los tiempos de interrupción de las actividades misionales cuando se presenta una emergencia
- ✓ Asegurar una pronta recuperación de los servicios críticos en caso de una emergencia

Alcance

El plan de continuidad del negocio inicia con la identificación, socialización y aprobación de los escenarios de emergencia para los cuales la Entidad definirá, actividades, responsables y recursos en caso de materialización de la situación de emergencia, continua con la evaluación de impacto al negocio de los procesos institucionales para establecer orden de recuperación de los procesos afectados, sigue con la ejecución de pruebas y simulacros de las actividades de respuesta planificadasy termina con la evaluación de los resultados de las pruebas y formulación de planesde mejoramiento del plan de continuidad de negocio.

Glosario

Análisis de Impacto del Negocio: proceso de análisis del impacto a lo largo del tiempo de una interrupción en la organización

Continuidad del negocio: capacidad de una organización para continuar la entrega de productos y servicios dentro de marcos de tiempo aceptables a la capacidad predefinida durante una interrupción

Emergencia: ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata

Interrupción: incidente, anticipado o no anticipado, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de una organización

Plan de continuidad de negocio: información documentada que guía a una organizaciónpara responder a una interrupción y reanudar, recuperar y restaurar la entrega de productos y servicios de acuerdo con sus objetivos de continuidad del negocio.

Marco general trabajo del plan de continuidad de negocio

Con el fin de apoyar la implementación del modelo integrado de planeación y gestión institucional en lo referente a la 3ª. Dimensión: Gestión con valores para resultados y la Política de Seguridad Digital, El departamento administrativo de la función pública articula las acciones para dar respuesta emergencias que pongan en riesgo la continuidad de sus servicios institucionales, utilizando el plan de continuidad de negocio como que la herramienta de preparación para la respuesta que con base en unos escenarios posibles y priorizados (identificados en el proceso de conocimiento del riesgo), define los mecanismos de organización, coordinación, funciones, competencias, responsabilidades, así como recursos disponibles y necesarios para garantizar la atención efectiva de las emergencias que se puedan presentar: Igualmente precisa los procedimientos y protocolos de actuación para cada una de ellas minimizando el impacto en las personas, los bienes y el ambiente.

Componentes del plan de continuidad de negocio institucional

Componente de preparación para la respuesta a emergencias.

Es el conjunto de acciones principalmente de coordinación, sistemas de alerta, capacitación, equipamiento, centros de reserva, entrenamiento, entre otras,necesarios para optimizar la ejecución de la respuesta. La efectividad de la respuesta es proporcional a las medidas de preparación que se implementen.

Capacitación

Formación del personal, ya sea interno o externo, para la respuesta de las emergencias, con el fin de garantizar la idoneidad de los actores, estas acciones se articulan dentro del plan institucional de capacitación liderado por el proceso de gestión del talento humano.

Simulaciones y simulacros

Se lleva a cabo la revisión del plan de emergencias y contingencia mediante la prueba,que permite una evaluación y mejora continua, garantizando la efectividad de la respuesta ante una emergencia presentada. Estos ejercicios se deben realizar mínimouna vez al año en articulación con lo establecido en el sistema integra do de planeación y gestión institucional.

Equipamiento

Es el conjunto de herramientas, equipos, accesorios, sistema de alerta temprana de los procesos institucionales que garantizan de manera oportuna la primera respuesta,así mismo

con la disponibilidad de personal idóneo para atenderlo, teniendo en cuentalas capacidades de los actores externos que a través de figuras administrativas fortalecen el equipamiento en la preparación para la respuesta., esto se traduce en apoyo de organismos de manejo de emergencias como bomberos, sistema de salud, sistema nacional de gestión de riesgos y equipos especializados en respuesta a emergencias cibernéticas.

Planeación y organización

Compuesta por los protocolos y procedimientos y unos equipos de respuesta del plan de emergencia y contingencia, cuyas funciones y responsabilidades específicas, de acuerdo a cada escenario de riesgo identificado se describen en la sección roles y responsabilidades de este documento. Este equipo debe asumir la dirección y coordinación de las operaciones de respuesta ante emergencias.

Equipo de respuesta del plan de emergencia y contingencia

Es el enlace entre el comité directivo institucional, los jefes de cada dependencia y las instituciones y sectores administrativos públicos y privados para hacer efectiva la respuesta ante el desastre.

Principios de la gestión de emergencias

Los siguientes principios constituyen guía de acción para la toma de decisiones respecto a la gestión de emergencias

Ética: La gestión de incidentes debe respetar la prioridad de la vida y la dignidad humanas mediante la neutralidad y la imparcialidad en la toma de decisiones

Unidad de mando: La gestión de incidentes requiere que cada persona en cualquiermomento reporte a un solo líder.

Trabajando en equipo: La gestión de incidentes requiere que las organizaciones trabajen en equipo.

Enfoque de todos los peligros: La gestión de incidentes considera tanto los incidentes naturales como los inducidos por el hombre, incluidos los que la organización aún no ha experimentado.

Gestión de riesgos: La gestión de incidentes se basa en la gestión de riesgos.

Preparación: La gestión de incidentes requiere preparación.

Intercambio de información: La gestión de incidentes requiere compartir informacióny perspectivas.

Seguridad: La gestión de incidentes enfatiza la importancia de la seguridad tanto paralos socorristas como para los afectados.

Flexibilidad: La gestión de incidentes es flexible (por ejemplo, adaptabilidad, escalabilidad y subsidiariedad).

Factores humanos y culturales: La gestión de incidentes tiene en cuenta factores humanos y culturales.

Mejora continua: La gestión de incidentes enfatiza la mejora continua para mejorar el desempeño organizacional.

Gestión de incidentes y emergencias

La gestión de incidentes dentro del departamento administrativo de la función pública debe considerar una combinación de instalaciones, equipos, personal, estructura organizativa, procedimientos y comunicaciones.

La gestión de incidentes se basa en el entendimiento de que en todos y cada uno delos incidentes hay ciertas funciones de gestión que deben llevarse a cabo independientemente del número de personas que estén disponibles o involucradas enla respuesta al incidente.

Es de vital importancia para todos los involucrados en la gestión de incidentes entenderel valor del reaccionar a tiempo considerando:

a) Anticipar los efectos en cascada que puede generar un incidente
b) Tomar la iniciativa para actuar lo antes posible en lograr de esperar
c) Considerar las limitaciones de ttiempo que pueden afectar a la entidad en casode emergencia
d) Determinar los impactos de diferentes líneas de tiempo
e) Modificar la línea de tiempo de las acciones de acuerdo con la evaluación de impactos

Al realizar la evaluación de los incidentes el comité de emergencias debe considerar necesidades de recursos y efectos tanto a corto como a largo plazo de los eventos, esta evaluación debe considerar

- Como se está desarrollando el incidente
- En qué momento puede surgir nuevas necesidades
- Cuánto tiempo puede tomar resolver esas nuevas necesidades

Gestión proactiva de los incidentes

Cuando se detectan las señales tempranas de un posible escenario de emergencia los equipos de respuesta y líderes de respuesta de los diferentes escenarios deben tomarla iniciativa para:

1) Evaluar los riesgos y preparar las medidas de respuesta para aumenta la efectividad de las respuestas planificadas
2) Anticipar como pueden cambiar los incidentes y aprovechar en forma efectivalos recursos disponibles
3) Tomar decisiones sobre diversas medidas con la suficiente antelación paraque las decisiones sean efectivas cuando sean realmente necesarias.
4) Manejar lo más pronto posible el incidente
5) Iniciar una respuesta coordinada en lugar de esperar a que alguien más tomela iniciativa
6) Identificar qué información se requiere compartir
7) Informar y explicar a las partes involucradas sobre la necesidad de recursospara atender el incidente

Protocolos y Procedimientos de respuesta para cada tipo de emergencia:

La entidad estableció cinco (5) escenarios de emergencia que activan su plan de continuidad de negocio. Para cada escenario existe un protocolo general para el manejo de la respuesta ante la emergencia, para cada escenario se definen los objetivos de respuesta a la emergencia específica, las estrategias y tácticas que permitan planificar, coordinar la participación institucional, interinstitucional, sectorial, municipal, departamental, nacional o internacional, y optimizar las operaciones de respuesta de acuerdo con el panorama de daños y la disponibilidad de recursos para responder efectivamente a la emergencia.

Para los diferentes escenarios seleccionados se establecen:

Fase de detección

En esta fase se realiza la evaluación preliminar de la situación o el sitio de la emergencia y su área de influencia de probable afectación, esta fase busca identificar y evaluar las alertas tempranas que indiquen la posible materialización del escenario de emergencia, para recomendar la activación de los planes de contingencia.

Dentro de la misma fase de detección se describen el equipo responsable de liderar las primeras acciones de respuesta de la entidad y el escalamiento de la información sobre la situación de emergencia a la cadena de mando administrativa para el desarrollo de acciones.

Fase de activación

Para cada escenario identificado se relacionan los planes de contingencia o planes alternos de operación en donde se describen los recursos como: equipos, herramientas y los medios necesarios para garantizar la respuesta inmediata a la situación de emergencia.

Fase de operación alterna

En esta fase de describen las acciones a desarrollar, teniendo en cuenta la preparaciónante una emergencia y la ejecución de la misma, esta fase describe los protocolos de comunicación que deben seguir las diferentes dependencias para poner en funcionamiento los planes de trabajo alterno, canales de comunicación y acciones de evacuación según aplique.

Fase de resolución

En esta fase se describen las acciones de restablecimiento de los servicios una vez superada la emergencia.

Organización para la respuesta a emergencias

Comité de emergencia

El comité de emergencia es la instancia institucional responsable de coordinar el manejo de las emergencias, lo conforman: Director (a) , Subdirector (a), Secretaria General, Jefe de OTIC,

Jefe la Oficina Asesora Planeación, tienen bajo su responsabilidad centralizar la información de la emergencia, coordinar la solicitud y asignación de recursos, realizar seguimiento a la respuesta a la emergencia, ajustarla respuesta de acuerdo con las líneas de intervención y generar las decisiones que permiten el mejor desempeño para la respuesta a emergencias.

El comité de emergencias es el responsable de coordinar el desarrollo de estrategiasy tácticas de respuesta, asignación y liberación de recursos, en su rol de comité de emergencias, tiene la autoridad y la responsabilidad generales de administrar de manera ordenada la respuesta a los incidentes, así como la organización de los equipos de respuesta.

El comité de emergencias puede ser convocado por cualquiera de sus miembros mediante llamada telefónica, sistema de mensajería instantánea, correo electrónico uotros medios de comunicación que estén disponibles en el momento de la ocurrencia de la emergencia que se requiere evaluar. Los miembros del comité coordinarán el momento y modo en que se reunirán para evaluar la emergencia reportada, pueden reunirse de manera presencial o virtual empleando tecnología de información y comunicaciones para realizar el análisis de la información de diagnóstico, recomendaciones de respuesta o solicitudes de activación del plan de continuidad de negocio formuladas por cualquiera de sus miembros.

El comité de emergencias tiene como funciones específicas:

- Establecer los lineamientos para la implementación del Plan de continuidad de negociode la Entidad y tener pleno conocimiento sobre sus procedimientos y protocolos.
- Someter a aprobación del comité directivo el plan de continuidad de negocio institucional
- Reunirse para decidir las acciones a seguir frente a un evento o un riesgo, con el fin de mitigar, neutralizar o atender la situación.
- Promover y facilitar la participación de los servidores y colaboradores de la Entidad en las diferentes actividades de prevención de emergencias, tales como: campañas, eventos educativos y simulacros para la creación de cultura en la prevención de riesgos de emergencias.
- Participar activamente en las actividades de preparación y entrenamiento para el manejo de emergencias y simulacros.
- Dirigir a nivel estratégico todas las actividades relacionadas con la atención y control de emergencias y/o simulacros, de conformidad con el Plan de continuidad de negocio, así como decidir sobre la ejecución de otras acciones extraordinarias que puedan ser necesarias.
- Apoyar a las dependencias involucradas en la implementación del Plan de Continuidaddel Negocio, garantizando la integridad del personal en el punto de encuentro y apoyando las acciones necesarias para realizar el proceso para su reubicación.
- Verificar la disponibilidad de los recursos necesarios para la ejecución de todas las actividades de prevención y atención antes, durante y después de emergencias y/o simulacros.
- Mantener informados a los medios de comunicación sobre la evolución de las emergencias y desastres que afecten al departamento administrativo de la función pública.

- Direccionar y apoyar las acciones de los equipos de respuesta antes, durante y después de la emergencia y/o simulacro.
- Coordinar las reuniones de evaluación posteriores a cada emergencia o simulacro y elaborar un informe con las recomendaciones para el mejoramiento de los procedimientos contemplados en el Plan de Emergencias de la Entidad.
- Coordinar con los grupos de apoyo externo actividades relacionadas con la respuesta, control, entrenamiento y simulaciones de emergencia.

Vocero oficial en situación de emergencia

Es la persona responsable de interactuar con el público y los medios de comunicacióny / o con otros grupos de valor con necesidades de información relacionados con el incidente. El vocero oficial de la entidad en situación de emergencias es el Director Del Departamento Administrativo De La Función Pública con el apoyo y coordinación de la oficina asesora de comunicaciones el comité de emergencias debe contar con:

- Listado de medios de comunicación internos y externos con los cuales distribuirá la información oficial sobre el manejo de la emergencia.
- Base de datos de periodistas y medios de comunicaciones actualizada periódicamente.
- Base de Datos de contactos institucionales.
- La información de lo que se consideran “temas sensibles o delicados”.
- Identificación de los públicos afectados.
- Diseño de la estrategia de comunicación para enfrentar cada una de los escenarios de emergencia.
- Descripción general de la estrategia de comunicación del departamento administrativo de la función pública.
- Temas logísticos a tener en cuenta durante la crisis.
- Protocolo para comunicar a nivel interno y externo (incluye Formato de Comunicado de Prensa, Formato de Comunicación Oficial Interna y Externa, Modelo de respuesta para medios Virtuales como: Twitter, Facebook, YouTube, y otros en caso de tener cuentas en otras redes sociales).

Cuando se inicie la gestión de comunicaciones sobre la crisis el vocero debe tener en cuenta:

- Para enfrentar una crisis se debe actuar con tranquilidad, transparencia y prudencia.
- Frente a cualquier crisis, la entidad debe pronunciarse de manera responsable.
- No se deben dar declaraciones a ningún medio de comunicación, sin que pasepor el Comité de crisis.
- El o los voceros son los únicos que pueden dar declaraciones.
- Se debe decir la verdad ante cualquier situación de crisis.
- Se debe hablar de datos verdaderos y confirmados. Si existen dudas sobre losmismos, es mejor no mencionarlos.
- No se debe exagerar la situación o minimizar el problema.

Equipos de respuesta específicos

Cada escenario identificado de emergencia tiene un grupo especializado de respuesta.Estos grupos están conformados por servidores, contratistas o colabores institucionales

Son responsables de:

- Identificar las situaciones de alerta,
- evaluar inicialmente la situación,
- consolidar la información del evento identificado y remitir los datos al jefe de la dependencia que lidera el escenario de emergencia, con la información recolectada el jefe de la dependencia planifica una respuesta temprana
- Evalúar la efectividad de las acciones de respuesta inicial contra la emergencia
- Si las acciones de respuesta inicial no pueden mitigar los efectos negativos delevento, se comunica con un miembro del comité de emergencia para iniciar la posible activación del plan de continuidad de negocio.

Escenario de emergencias Función Pública:

Escenario	Grupo de respuesta específico
Emergencia social Agrupa todos los eventos asociados a la pérdidadel orden público, pérdida de orden constitucional o situaciones en donde diversos actores generan acciones fuera del orden legal como: Asonada, revuelta civil, retención arbitraria de personal (secuestro).	**Líder de respuesta:** Coordinador (a) de Gestión de Talento Humano **Equipo de respuesta:** Grupode Gestión de Talento Humano
Desastre natural y colapso de infraestructuras Agrupa todos los fenómenos naturales o causados por el hombre que generan daño estructural del edificio y que obliga a evacuación del personal con el objetivo primario de salvaguardar la vida (incendio, sismo, inundación, falla de servicios eléctricos, hidráulicos, sanitarios)	**Líder de respuesta:** Coordinador del Grupo de Gestión Administrativa **Equipo de respuesta:** Grupo de Gestión Administrativa
Tecnológico Falla de sistemas de información, pérdida de datos, fallas en sistemas de telecomunicaciones que interrumpen los procesos institucionales e inhabiliten el uso de servicios de tecnología de información y comunicaciones para el normal funcionamiento de la entidad.	**Líder de respuesta:** Jefe deOficina de Tecnologías de Información y Comunicaciones **Equipo de respuesta:** Oficinade Tecnologías de Información y Comunicaciones

Financiero Eventos que imposibilidad a la Entidad de contar con los recursos económicos para cumplir con compromisos misionales o con terceros como proveedores de servicios, estos eventos incluyen emergencia económica declarada por la rama ejecutiva, recortes presupuestales de emergencia o cambios económicos abruptos que desestabilizan el normal funcionamiento de la Entidad.	**Líder de respuesta:** Secretario (a) General **Equipo de respuesta:** Oficina Asesora de Planeación, Secretaria General y Direcciones técnicas.
Sanitario En esta categoría se agrupan los eventos causados por agentes biológicos que afectan ala salud de todos los seres vivos en particular la seguridad de los seres humanos, incluidos fenómenos como: pandemias, epidemias, crisis sanitaria que impide el funcionamiento de los procesos institucionales, entre otros.	**Líder de respuesta:** Coordinador (a) de Gestión de Talento Humano **Equipo de respuesta:** Grupode Gestión de Talento Humano

Equipos de respuesta Función Pública

Los equipos de respuesta de las dependencias son el conjunto especifico de servidores y colaboradores de cada dependencia, liderados por su respectivo jefe que tiene como responsabilidad activar los planes de contingencia específicos en caso de que el comité de crisis ordene la activación del plan de continuidad. En cada procedimiento de contingencia se describen las acciones y recursos necesarios para activar estos planes alternos en caso de que el comité de emergencias lo ordene.

- Oficina de tecnologías de información y las comunicaciones

Es un equipo de respuesta especial, conformado por especialistas en tecnología de información y las comunicaciones que pueden ser activados por el comité de emergencias y que, liderados por el Jefe de Oficina de tecnologías, ponen en funcionamiento el plan de recuperación ante desastres tecnológicos y apoyan el componente de servicios tecnológicos alternos requeridos por los grupos de respuestade cada dependencia mientras se reactivan los sistemas de información afectados.

- Otros grupos de apoyo

A juicio del comité de emergencias, se pueden activar otros grupos de apoyo especializados en labores como vigilancia, logística, comunicaciones externas y otraslabores de apoyo necesarias para gestionar apropiadamente la emergencia.

Documentación planes de contingencia:

El conjunto de planes de contingencia está conformado por los siguientes procedimientos que están documentados en el sistema integrado de planeación y gestión institucional.

- Plan de operación alterna servicio al ciudadano
- Plan de operación alterna gestión documental
- Plan de operación alterna gestión contractual
- Plan de operación alterna gestión financiera
- Plan de operación alterna gestión humana
- Plan de operación alterna gestión administrativa
- Plan de operación alterna OAC
- Plan de operación alterna OAP
- Plan de operación alterna Dirección DAFP
- Plan de operación alterna Subdirección DAFP

Roles y responsabilidades

Rol	Responsabilidad	Representantes	Mecanismos
Equipo de gestión de emergencias	Activación del Plan de continuidad o de emergencia y Plan de restablecimiento	Director (a) Subdirector (a) Secretaria GeneralJefe de OTIC Jefe la Oficina Asesora Planeación	Declaración formal de inicio de actividad de contingencia o continuidad
Líderes de proceso Estratégicos, Misionales y de Apoyo	Evaluar los riesgos e impactos de la perdida de continuidad	Líderes 15 procesos de acuerdo con sus responsabilidades definidas en el plan de continuidad	Evaluar los riesgos que puedan generar pérdida de continuidad Análisis impacto del negocio (BIA)

Jefe Oficina Asesora de Planeación Jefe de Oficinade TIC Secretaria General	Asesorar, coordinary documentar el Plan de continuidad de negocio	Jefe Oficina Asesora de Planeación y Coordinador OAP Jefe de Oficina de TIC, Asesor y Coordinadoresde grupo Secretaria General, Asesor y Coordinadores de Talento Humano, Administrativa, Contractual, Financiera y Documental	Aplicar las guías y metodologías institucionales Metodología de riesgos Análisis de la información Identificación de escenarios de continuidad Análisis y selecciónde la estrategia de continuidad Inclusión de los planes de respuesta en el plan de acción anual

Rol	Responsabilidad	Representantes	Mecanismos
Comité Institucional de Gestión y Desempeño	Aprobación del plan de continuidad	Miembros del Comité	Acta de Comité Institucional de Gestión y Desempeño Institucional Plan de continuidad aprobado Plan de Acción Anual Sesiones de inducción y reinducción-Simulacros
Jefe Oficina Asesora de Planeación Jefe de Oficinade TIC Secretaria General Oficina Asesorade comunicaciones	Socialización y pruebas del plan de continuidad	Líderes 15 procesos de acuerdo con sus responsabilidades definidas en el plan de continuidad	Talleres, Boletines, Resultados de las pruebas de continuidad Planes de mejoramiento
Líderes de procesos institucionales	Restablecer prestación de servicios a condiciones normales una vez superada la situación de emergencia	Líderes 15 procesos de acuerdo con sus responsabilidades definidas en el plan de continuidad	Notificaciones a los grupos de valor Reevaluación de riesgo Planes de mejoramiento

Generalidades del Plan de Continuidad

El Plan de Continuidad reúne un conjunto de actividades y procedimientos que mantienen en niveles aceptables el funcionamiento de la misionalidad de la Entidad y la prestación de sus servicios durante eventos que impidan de manera significativa susprocesos normales. El plan de Continuidad se establece en tres momentos:

Prevención y Detección

Dentro de este aspecto se involucran los recursos humanos, técnicos o administrativosquienes deben estar preparados en caso de presentarse un evento inesperado, las acciones y la preparación de las áreas para iniciar su contingencia, las cuales se puedan articular a la gestión institucional en los diferentes procesos. Incluye las acciones de monitorización de los indicadores de la ocurrencia potencial de una emergencia. Las acciones de prevención incluyen el fortalecer la difusión de las políticas internas, los canales de comunicación, las estrategias de activación de la respuesta a contingencias, la difusión de los planes de respuesta

Confirmación y Reacción

Este aspecto está orientado a las acciones necesarias para confirmar la materialización de un incidente que pondrá en riesgos la continuidad de la prestación de los servicios misionales, comunicar la emergencia identificada y la toma de decisión por parte del equipo de gestión de emergencias

Operar las contingencias y resolver emergencia

Cubre todas las tareas que se ejecutan para mantener la operación de los servicios institucionales en niveles aceptables mientras exista la emergencia que activo, en estafase de activan los planes de operación alterna y las acciones al alcance de la entidad para resolver las afectaciones sobre la Entidad que generó la situación de emergencia

Recuperación y restablecimiento

Esta etapa incluye todas las actividades necesarias para retomar las actividades en suestado normal de funcionamiento una vez se han superado las situaciones que generaron la emergencia, se han restablecido los sistemas afectados o se han reparado las estructuras afectadas.

Proceso de construcción/actualización del plan de continuidad

Análisis del entorno institucional

A partir de las funciones y obligaciones normativas delegadas al Departamento, de los

compromisos adquiridos con los diferentes grupos de valor y de los datos históricos dela operación institucional, anualmente se consolidan los factores que pueden afectar el desarrollo adecuado de las actividades de Función Pública, representadas así:

Contexto Externo

Económicos: Recorte presupuestal, demoras o dificultades para el traslado de recursos con los cooperantes, cambios de gobierno en la priorización y traslado de recursos.

Políticos: Cambio de gabinete, nuevas prioridades del gobierno nacional, jornada electoral, dificultad en la coordinación interinstitucional, cambio en las políticas aplicables a Función Pública.

Sociales: Manifestaciones y protestas frecuentes en el centro de la ciudad, dificultadde acceso para el ciudadano y los servidores, asonadas, paro armado, contaminación social, daños intencionados a la infraestructura de la Entidad.

Tecnológicos: Deficiencia en la interoperabilidad de los sistemas de gobierno, diferencia en las plataformas tecnológicas de los grupos de valor, ataques externos a la información y las herramientas tecnológicas.

Medio Ambientales: Ubicación de la entidad cerca a los cerros, incendios, terremotos, Inundaciones, desastres naturales, vulnerabilidades asociadas a factores como lluvia, tormenta eléctrica, sistemas hidráulicos y sanitarios.

Contexto Interno

Financieros: dificultad para la priorización de recursos, cambios frecuentes en el plan adquisiciones, comunicación inoportuna de los cambios, demoras en la apropiación de recursos, fallas en los sistemas de registro SIIF.

Personal: planta de personal insuficiente, nuevas exigencias de competencias del personal en el nuevo modelo de operación, tiempo insuficiente para el desarrollo de habilidades, falta de motivación e involucramiento del personal, alta rotación de personal, perdida de capital intelectual.

Procesos: nuevos procesos, desconocimiento de las características de los procesos, desconocimiento del nivel de responsabilidad y autoridad de los procesos, baja apropiación del nuevo modelo, baja asistencia a las capacitaciones de socialización y las mesas de creación de los procesos.

Tecnología: desconocimiento de un Plan estratégico de TI, desarticulación de las herramientas y aplicativos internos, fallas en la infraestructura tecnológica, fallas enel sistema de seguridad de la información, desconocimiento de los niveles de responsabilidad y autoridad frente a los sistemas.

Estratégicos: cambios en la gestión institucional sin planificación y comunicación oportuna, fallas en la comunicación y solicitud de información a las dependencias, ausencia de acuerdos de niveles de servicio concertados y socializados, fallas en la comunicación interna, solicitud de información múltiple, fallas en los sistemas de información.

Comunicación interna: Desconocimiento en los temas gestionados por parte de la Función Pública, saturación de los boletines internos y externos, Inapropiada distribución de canales internos, Inoportunidad en la entrega de información, falta de registros de información y contactos actualizados y protegidos.

Análisis de impacto al negocio

Anualmente el Departamento Administrativo de la función pública evalúa los impactosy las prioridades de recuperación de las actividades que apoyan a sus diferente productos y servicios. El análisis de impacto al negocio incluye la i identificación de todas las actividades que apoyan la provisión de productos y servicios, la evaluaciónen el tiempo de la imposibilidad de realizar dichas actividades, el establecimiento tiempos y priorización del orden de restablecimiento de las actividades a niveles mínimos aceptables.

Para el desarrollo del Análisis del impacto se siguen los siguientes pasos:

1. Listar todas las funciones del negocio
2. Determinar los criterios bajo los cuales se medirá la criticidad de cada función de negocio (Financiero, Reputacional, Legal / Regulatorio, Contractual, Misional)
3. Valorar la perdida de continuidad total o parcial de cada función de negocio deacuerdo con los criterios seleccionados
4. Priorizar las funciones de negocio de acuerdo con la valoración del impacto porperdida de continuidad
5. Determinar funciones y recursos que son esenciales para las funciones quefueron priorizadas como críticas
6. Presentar los resultados del análisis de impacto de negocio en el Comité Institucional de Gestión y Desempeño

Los resultados del análisis de impacto se utilizan para determinar los tiempos de respuesta de las diferentes etapas del BCP (Plan de continuidad de negocio por sus siglas en Ingles), en particular:

- ✓ Tiempo máximo tolerable que pueden una actividad permanecer suspendida antes de que los daños para la entidad sean totalmente irremediables
- ✓ Tiempo de necesario para el restablecimiento de los servicios y recursos indispensables para el funcionamiento normal de las actividades priorizadas
- ✓ Identificación del nivel máximo tolerable de pérdida de datos que obligue a su recuperación mediante procedimientos manual.

Riesgos asociados a la continuidad del negocio

Los riesgos asociados a la continuidad del negocio se analizan anualmente al mismo tiempo que se realiza la identificación de riesgos institucionales con cada proceso y se registra en el mapa de riesgos como “perdida de continuidad”, los riesgos de continuidad del negocio estarán implícitos en los riesgos institucionales asociados a cada proceso, se identifican siguiendo la misma metodología Institucional de Gestión de Riesgos.

Los riesgos de pérdida de continuidad se agrupan en escenarios de pérdida de continuidad cuando sus causas son comunes o que conducen a la interrupción del servicio total o parcial, de una o varias funciones calificadas como críticas

Función Pública contempla implícitamente en la gestión de sus procesos la identificación y administración de los riesgos como práctica para impedir que eventualidades internas o externas impidan cumplir sus objetivos institucionales.

Al desarrollar el plan de continuidad del negocio se integra la metodología de riesgosy los controles preventivos, detectivos y correctivos de los planes de tratamiento de riesgos, los cuales quedan asociados al mapa de riesgos institucional.

Definición de escenarios de pérdida de continuidad

Los riesgos identificados con mayor probabilidad de ocurrencia e impacto a nivel de continuidad se analizan y se determina si tienen entren si, causas comunes o correlaciones que permitan su análisis como un escenario factible de pérdida de continuidad. Este análisis se realiza para concentrar los esfuerzos en aquellos eventos que combinados tendrán una probabilidad razonable de impedir la continuidad de los servicios institucionales.

Como resultado del análisis de los riesgos se describen escenarios de pérdida de continuidad sobre los cuales se diseñará una estrategia de continuidad, paralelamentela documentación de los escenarios permite documentar los criterios que debe aplicarel comité de crisis para realizar la declaración de emergencia y autorizar la activación del plan de continuidad.

Aquellos riesgos que no se puedan correlacionar o consolidar en algún escenario, se deben revaluar para determinar si constituyen un escenario independiente que por su naturaleza obligan a la activación de la continuidad o simplemente se pueden tratar por los procedimientos ya definidos para manejo de eventos de riesgo con planes de tratamiento ya definidos.

Para cada actividad priorizada dentro de los escenarios de emergencia se establecenlos mínimos operativos que el Departamento Administrativo de la Función Pública se compromete a mantener durante la fase de operación en contingencia y el tiempo máximo que se puede mantener la operación en contingencia antes de que las afectaciones sean irremediables.

Definición de estrategia de continuidad

A partir de los escenarios de emergencia seleccionados se determina la estrategia específica que se debe aplicar en caso de que el escenario se materialice. Para cada caso específico se debe establecer:

- ✓ Cual o cuales son las formas para apropiadas para proteger las actividades priorizadas
- ✓ Determinar si las actividades afectadas se estabilizaran con los recursos disponibles, si se reanudaran las actividades con otros recursos propios a de terceros
- ✓ Determinando las dependencias de las actividades priorizadas frente a las actividades de apoyo
- ✓ Información vital que permita la continuidad de las actividades priorizada

Aunque la estrategia específica que se aplicará a cada escenario particular depende de la naturaleza de este, se deben considerar alternativas como:

- ✓ Recuperación de la actividad dentro de las mismas instalaciones de la entidad con recursos propios de la entidad
- ✓ Recuperación de la actividad en instalaciones de otra entidad usando recursos propios de la del Departamento Administrativo de la Función Pública
- ✓ Recuperación de la actividad en las instalaciones o con los recursos de un proveedor independiente, como por ejemplo centros de cómputo alternos o infraestructura de nube.
- ✓ Combinación de diferentes modelos de opciones de recuperación, utilizando recursos internos como externos

Identificación y selección de recursos

Usando los resultados del análisis de impacto y la selección de estrategia se determinar los recursos necesarios para implementar la estrategia de continuidad definida, estos recursos deben incluir, pero no limitarse a:

- ✓ Personas
- ✓ Información y datos
- ✓ Instalaciones físicas
- ✓ Equipos y elementos consumibles
- ✓ Tecnología de información
- ✓ Trasporte
- ✓ Recursos financieros
- ✓ Proveedores y contratistas

Documentación de procedimientos de continuidad

Todos los responsables de las actividades criticas incluidas en la estrategia de continuidad participan en el desarrollo de procedimientos e instrucciones claras e inequívocas para que permitan la gestión del evento que activo el plan de continuidad y dar continuidad a las actividades priorizadas dando cumplimiento los objetivos de recuperación que se hayan definido en durante el análisis de impacto, la gestión de riesgo y la identificación de escenarios. Los diferentes documentos que conformaran los procedimientos de continuidad incluyen, entre otros:

- ✓ Protocolo de comunicaciones durante la continuidad (quien reportara a quién y por qué medios)
- ✓ Pasos detallados y específicos para activar la estrategia seleccionada para operar los servicios en contingencia
- ✓ Pasos detallados que aplicaran los responsables de realizar la recuperación delos recursos afectados por el o los eventos que generaron la activación del plan de continuidad
- ✓ Pasos detallados que se deben aplicar para reactivar los servicios en la infraestructura una vez se ha superado el evento que genero la pérdida de continuidad
- ✓ Responsables de las diferentes actividades aplicar antes durante y después dela contingencia que activo la estrategia de continuidad.

Pruebas y revisión periódica del plan

En las sesiones de Comité Institucional de Desarrollo Administrativo se aprueba y monitoriza el plan de continuidad; las acciones preventivas se llevan a cabo en todala Entidad según la planificación de las dependencias de Talento Humano (relacionadas con las personas), de Administrativa (relacionadas con la infraestructura) y de Gestión Documental (relacionadas con la información), las cualesestarán coordinadas por la Secretaria General, la Oficina de Tecnologías de la Información y las Comunicaciones (lo relacionado con la infraestructura tecnológica y la seguridad de la información); Gestión financiera (lo relacionado con gestión de escenarios de crisis financiera) durante la definición de la planificación institucional sedefinen y autorizan las prueba y los simulacros, del plan de continuidad, según los recursos económicos con los que se cuente en cada vigencia, los cuales se harán de manera planificada y concertada con el Comité de Crisis; de igual manera los resultados y el seguimiento se realizará dos veces al año en los Comité Institucional de Desarrollo Administrativo y Directivos.

Gestionar el plan de continuidad

Una vez construido y aprobado el plan de continuidad, la Entidad emprende las acciones necesarias para socializarlo a los grupos de valor y de esta manera estar

someterlo a evaluación externa, mejoramiento y apropiación con el objetivo, preparados para enfrentar situaciones de emergencia y restablecer en el menor tiempoposible el servicio a los grupos de valor.

Escenarios de continuidad de negocio

Con el fin de adoptar un enfoque ordenado y metodológico para el manejo de los incidentes que puede afectar la continuidad de negocio, la entidad ha definido 5 escenarios que permiten agrupar los riesgos institucionales que por su naturaleza pueden conducir la pérdida de continuidad de las funciones esenciales:

Emergencia social

Agrupa todos los eventos asociados a la pérdida del orden público, pérdida de orden constitucional o situaciones en donde diversos actores generan acciones fuera del orden legal como: Asonada, revuelta civil, retención arbitraria de personal (secuestro).

Desastre natural y colapso de infraestructuras

Agrupa todos los fenómenos naturales o causados por el hombre que generan daño estructural del edificio y que obliga a evacuación del personal con el objetivo primario de salvaguardar la vida (incendio, sismo, inundación, falla de servicios eléctricos, hidráulicos, sanitarios)

Tecnológico

Falla de sistemas de información, pérdida de datos, fallas en sistemas de telecomunicaciones que interrumpen los procesos institucionales e inhabiliten el uso de servicios de tecnología de información y comunicaciones para el normal funcionamiento de la entidad.

Financiero

Eventos que imposibilidad a la Entidad de contar con los recursos económicos para cumplir con compromisos misionales o con terceros como proveedores de servicios, estos eventos incluyen emergencia económica declarada por la rama ejecutiva, recortes presupuestales de emergencia o cambios económicos abruptos que desestabilizan el normal funcionamiento de la Entidad.

Sanitario

En esta categoría se agrupan los eventos causados por agentes biológicos que afectana la salud de todos los seres vivos en particular la seguridad de los seres humanos, incluidos fenómenos como: pandemias, epidemias, crisis sanitaria que impide el funcionamiento de los procesos institucionales, entre otros.

De igual manera, durante el 2021 se definió la estrategia para cada uno de los escenarios así:

Escenario 1: Emergencia social

Escenario 1: Emergencia social	
Líder de respuesta:	**Coordinador (a) de Gestión de Talento Humano**
Equipo de respuesta:	Grupo de Gestión de Talento Humano

Fase 1: Detección

Identificación de alertas

1) La Oficina Asesora de Comunicaciones a través de la revisión de mensajes en redes sociales identifica mensajes de alerta asociados a convocatorias de manifestaciones y reuniones con el propósito de realizar protestas en la zona de trabajo de la Entidad
2) A través de revisión de los canales de comunicación oficial de la Secretaria de Gobierno o entidades de la Alcaldía responsables de la gestión del orden públicose identifica eventos como bloqueos, marchas o aglomeraciones de personal que pueden afectar el desplazamiento de servidores y contratistas
3) Mediante monitorización de los medios de comunicación se identifican situaciones de alerta de orden público confirmadas que afectan la zona de trabajode la Entidad

@Bogota Twitter de la alcaldía de Bogotá

@GobiernoBTA Twitter secretaria de Gobierno distrital

@SeguridadBOG Twitter secretaria de Seguridad y Justicia Gobierno distrital

@TransMilenio Twitter de sistema Transmilenio

@SectorMovilidad Twitter de sector Movilidad Bogotá

Confirmación

1) La Dirección, Subdirección o la Secretaría general a través de los canales oficiales de comunicación con Secretaria de Gobierno Distrital o la Alcaldía local (contacto telefónico, correo o electrónico, sitio web) confirman la situación de alerta por desórdenes y mediante mensaje instantáneo vía WhatsApp en el *Equipo de Gestión de Emergencias (Director (a) Subdirector (a), Secretario (a) General, Jefe de OTIC, o Jefe de la OAP)* (notifican al jefe del grupo de gestiónde talento humano que se debe activar el manejo de emergencias por crisis social.

Fase 2: Activación

1) Cuando el Coordinador (a) del Grupo de Gestión de Talento Humano recibe la confirmación sobre ocurrencia de crisis por emergencia social, recopila la

información de confirmación de la crisis y en llamada grupal con los miembros del *Equipo de Gestión de Emergencia* (Director, Subdirectora, Secretaria General, Jefe de OTIC y Jefe de OAP) expone la situación y somete a consideración la necesidad de iniciar la activación del plan de continuidad por la ocurrencia del escenario 1.

2) El *Equipo de Gestión de Emergencia* evalúa la información y decide si se debe activar o no el plan de evacuación, activación de manejo de crisis por emergencia social y autorización de hora cierre de las instalaciones y salida del personal.
3) Si se autoriza la activación del plan de continuidad, el Coordinador (a) del Grupo de Gestión de Talento Humano inicia la etapa plan de operación alterno
4) Si no se autoriza la activación del plan, el evento se gestiona mediante los planes definidos por la secretaria general

Fase 3: Plan de operación alterno

1) Coordinador (a) de Talento Humano comunica al Coordinador del Grupo de Gestión Administrativa vía telefónica o mediante mensaje instantáneo, que se deben cerrar las instalaciones y publicar mensaje en portería sobre suspensión de actividades por el día
2) Coordinador (a) del Grupo de Talento Humano coordina con la Oficina Asesora de Comunicaciones que se transmita el comunicado estandarizado de activación de plan de evacuación a través de: sistema de perifoneo, correo electrónico y grupos cerrados de mensajería instantánea de las diferentes dependencias.
3) Jefe de la Oficina Asesora de Comunicaciones ordena la publicación en sitio web institucional e intranet de banner de suspensión de servicio presencial.
4) Jefe del Grupo de Gestión Administrativa notifica al Coordinador del Grupo de Servicio al Ciudadano que se suspende la atención de ciudadanos y se debe coordinar la salida de visitantes de esa dependencia.
5) Los jefes de dependencia ordenan la activación del *trabajo en casa* utilizando las herramientas colaborativas TEAMS, Correo electrónico, grupos, se aplica el protocolo de trabajo remoto usando las herramientas colaborativas TEAMS, correo, redes virtuales
6) Los servidores públicos, contratistas y visitantes de la entidad deben abandonarla sede, dirigirse a sus casas y notificar a sus jefes inmediatos por los grupos internos de mensajería instantánea su llegada a casa.
7) Los jefes de cada dependencia comunican al Coordinador (a) del Grupo de Talento Humano el resultado del reporte de llegada a casa de sus subalternos

8) El Coordinador del Grupo de Talento Humano genera informe de resultado de evacuación de instalaciones al *Equipo de Gestión de Emergencia* vía correcto electrónico
9) Servidores y contratistas realizan sus actividades asignadas en modalidad de trabajo remoto hasta que los jefes de dependencia notifiquen el retorno a la sedenormal de trabajo
10) El trabajo remoto se debe mantener hasta que se reciba comunicación formal delEquipo de gestión de emergencias indicando la resolución de la emergencia.

Fase 4: Resolución del incidente

1) El *Equipo de Gestión de Emergencias (Director (a) Subdirector (a), Secretario (a) General, Jefe de OTIC, o Jefe de la OAP)* a través de canales oficiales de comunicación (Secretaria de Gobierno, Alcaldía) reciben confirmación de las autoridades de la finalización de la situación que obligo a la evacuación de las instalaciones y la posibilidad de retorno
2) El *Equipo de Gestión de Emergencias* define si se debe autorizar el reinicio de operaciones en la sede. En caso de autorizar el reingreso a la sede se comunicala decisión mediante mensaje instantáneo vía WhatsApp.
3) El Coordinador de grupo de Talento Humano gestiona con la Oficina Asesora de Comunicaciones la transmisión del mensaje de retorno a la sede principal a través de correo electrónico, mensajes instantáneos por grupos cerrados de WhatsAp p
4) Se publica en la intranet banner notificando la vuelta a normalidad de actividades.
5) Servidores y contratistas retornan a sus labores en la sede principal de la Entidad
6) Si se realizó movimiento de equipos de cómputo durante la activación del trabajo remoto el coordinador del Grupo de gestión administrativa organiza el reintegro de los equipos que salieron de las instalaciones nuevamente a la sede de la Entidad.

Escenario 2: Desastre natural y colapso de infraestructuras

Escenario 2: Desastre natural y colapso de infraestructuras
Líder de respuesta: Coordinador del Grupo de Gestión Administrativa
Equipo de respuesta: Grupo de Gestión Administrativa
Fase 1: Detección

Líder de respuesta: Coordinador del Grupo de Gestión Administrativa

Equipo de respuesta: Grupo de Gestión Administrativa

Identificación de alertas

En caso de sismo: se detectan movimientos súbitos en todo el edificio, se observa oscilaciones en objetos suspendidos.

En caso de fuego / incendio: Coordinador del Grupo de Gestión Administrativa identifica evento de riesgo asociado a fuego, la detección se puede realizar mediante el sistema de detección de humo, notificación de testigo o inspección directa de la escena.

En caso de fenómeno natural: vendaval, granizada, inundación por borrascao lluvia intensa: Grupo de Gestión Administrativa identifica evento de riesgo asociado a inundación, la detección se realiza por inspección directa de la escena.

Confirmación

En caso de sismo: la confirmación de sismo es inmediata, todo el personal dentro de las instalaciones percibe el fenómeno.

En caso de sismo personal dentro de edificio: buscan refugio bajo escritorios,mesas o estructuras fuertes, permanecen allí hasta que cese el movimiento, alejarse de ventanales, estantería alta, lámparas o cualquier otro elemento que esté suspendido o pueda caer protegerse la cabeza y cuello con las manos, prepárese para evacuar en caso de que se dé la señal de alarma; no debe devolverse por ningún motivo al edificio.

Nunca use ascensores para evacuar.

En caso de incendio, fuga de gases o líquidos peligrosos: Coordinador del Grupo de Gestión administrativa confirma el evento de fuego, evalúa nivel de riesgo y notifica necesidad o no de realizar evacuación de las instalaciones. Si el fuego esta fuera de control se deben ordenar la evacuación inmediata iniciando con el área afectada, las áreas próximas y luego las más alejadas. Se debe dar inicio la fase de activación del escenario de crisis 2 desastre natural, colapso de infraestructura. Se llama al cuerpo de bomberos 119. Si el fuego se puede controlar con la brigada de emergencia institucional, se realiza su control con los equipos disponibles y se notifica al cuerpo de bomberos. Se ejecuta la fase de activación del escenario de crisis 2 **[Desastre Natural y colapso de infraestructuras]**

En caso de fenómeno natural: vendaval, granizada, inundación por borrascao lluvia intensa: el Coordinador del Grupo de Gestión Administrativa confirma que el evento de inundación, borrasca o daño por inundación, evalúa nivel de riesgo y notifica necesidad o no de realizar evacuación de las instalaciones. Si la inundación imposibilita el desarrollo de las actividades institucionales convoca alEquipo de Gestión de Emergencia para evaluación de activación de escenario de crisis 2. **[Desastre Natural y colapso de infraestructuras]**

Fase 2: Activación

En caso de sismo, fuego, fuga de materiales peligrosos o gases, sismo;

- Coordinador de grupo de gestión administrativa activa la alarma sonora y notifica a los brigadistas de la orden de evacuación
- Coordinador de grupo de gestión administrativa alerta por radio al personal de vigilancia para realizar apertura de puertas y preparación para evacuación preventiva del edificio
- Jefe de la Brigada de emergencia determina momento adecuado para ordenar evacuación si es necesario.
- Brigadistas de piso inician protocolo de evacuación por dependencia, coordinan el proceso de evacuación hasta el punto de encuentro si es necesario.
- Cuando el personal haya sido evacuado en su totalidad el Coordinador de grupo de gestión administrativa evalúa por i inspección visual el detalle de daño a estructuras, presencia de víctimas o desarrollo particular de la emergencia en su sector.
- Si se detectan fallas en la estructura que hacen evidente que NO se puede reingresar:
- Coordinador de grupo de gestión administrativa, gestiona la interrupción inmediatamente suministros eléctrico, de gas, de combustibles **desde registros externos al edificio si es factible hacerlo,** en caso contrario deben esperar al personal de Bomberos o grupo de atención de emergencia
- Jefe de la Oficina de las Tecnologías de Información, define, de acuerdo con resultado de evaluación de daños en la estructura y por la naturaleza de la emergencia SI aún es viable apagar el centro de datos ordenadamente, en caso contrario los equipos tendrán apagado por el corte de energía preventivo
- Equipo de Gestión de Emergencias escala el manejo de la emergencia sobre la edificación en las autoridades competentes, Cuerpo de Bomberos
  Secretaria General coordina con jefe de la oficina asesora de comunicaciones la distribución de mensaje por grupos de mensajería instantánea la orden para que el personal se dirija a sus lugares de habitación y espere instruccionesde su jefe de dependencia
- Servidores y contratistas se dirigen a sus casas y reportan a su jefe inmediatosu llegada y estado de salud mediante los grupos cerrados de WhatsApp

- Los jefes de cada dependencia comunican al Coordinador (a) del grupo de talento humano el resultado del reporte de llegada a casa de sus subalternos
- El Coordinador (a) del Grupo de Gestión de Talento Humano genera informe de resultado de evacuación de instalaciones al Equipo de gestión de emergencia vía correcto electrónico
- Jefe de la Oficina de Tecnologías de Información y comunicaciones evalúa con su equipo de trabajo el estado de funcionamiento de los sistemas informáticos dentro del centro de cómputo y los servicios de información que estén en funcionamiento fuera del centro de cómputo.
- Jefe de la Oficina de TIC activa plan de recuperación antes tecnológico **[escenario de crisis Nro. 3], Desastre tecnológico**
- Cuando se cuente con servicios informáticos alternos, los jefes de dependencia ordenan la activación de trabajo en casa utilizando las herramientas colaborativas que disponga la OTIC
- Servidores y contratistas realizan sus actividades asignadas en modalidad detrabajo remoto hasta que los jefes de dependencia notifiquen el retorno a la sede normal de trabajo
- El trabajo remoto debe mantener hasta que se reciba comunicación formal delEquipo de gestión de emergencias del reportando l a resolución de la emergencia.
- Si se detecta que es viable volver a entrar al edificio, se debe esperar la autorización de los organismos de emergencia para el reingreso a las instalaciones. El coordinador del grupo de gestión administrativa debe comunicar el resultado de la evaluación que formule el organismo de emergencia e indicar a la Secretaria General la recomendación de reingresoo no al edificio.

7. En caso de **natural: vendaval, granizada, inundación por borrasca o lluvia intensa**
   a) Cuando el Coordinador del Grupo de Gestión Administrativa confirma la ocurrencia de crisis por fenómeno natural y la evaluación determina que no se pueden continuar operando en la sede, recopila la información de confirmación de la crisis y en llamada grupal con los miembros del *Equipo de Gestión de Emergencia* expone la situación y somete a consideración la necesidad de iniciar la activación del plan de continuidad por la ocurrencia del **escenario 2. [Desastre Natural y colapso de infraestructuras]**
   b) El *Equipo de Gestión de Emergencia* evalúa la información y decide si se debeactivar o no el plan de evacuación, activación de manejo de crisis por desastrenatural y colapso de infraestructuras, confirman la autorización de hora cierre de las instalaciones y salida del personal.
   c) Coordinador de Grupo de Gestión Administrativa activa la alarma sonora y notifica a los brigadistas de la orden de evacuación
   d) Coordinador de Grupo de Gestión Administrativa alerta por radio al personal de vigilancia para realizar apertura de puertas y preparación para evacuación preventiva del edificio

e) Jefe de la *Brigada de Emergencia* determina momento adecuado para ordenar evacuación si es necesario.
f) Brigadistas de piso inician protocolo de evacuación por dependencia, coordinan el proceso de evacuación hasta el punto de encuentro si es necesario.
g) Cuando el personal haya sido evacuado en su totalidad el Coordinador de grupo de gestión administrativa evalúa por inspección visual, el detalle de daño a estructuras, presencia de víctimas o desarrollo particular de la emergencia en su sector.
h) Brigadistas realizan la interrupción inmediatamente suministros eléctrico, degas, de combustibles desde registros externos al edificio si es factible hacerlo en caso contrario deben esperar al personal de Bomberos
i) Jefe de la Oficina de las Tecnologías de Información, define, de acuerdo con resultado de evaluación de daños en la estructura y por la naturaleza de la emergencia SI aún es viable apagar el dentro de datos ordenadamente, en caso contrario los equipos tendrán apagado por el corte de energía preventivo

8. Coordinador del Grupo de Gestión Administrativa comunica a la SecretariaGeneral que se completó la evacuación del edificio, estado de la edificación.
9. *Equipo de Gestión de Emergencias* evalúa si se debe realizar la activación delplan de operación alterno.
10. Si no se autoriza la activación del plan, el evento se gestiona mediante los planes definidos por la secretaria general
11. Si se acuerda activar el plan alterno se activa la fase 3 de la emergencia por eventos naturales

Fase 3: Plan de operación alterno

1) Jefe de la Oficina Asesora de Comunicaciones ordena la publicación en sitio web institucional e intranet de banner de suspensión de servicio presencial. Por grupos cerrados de WhatsApp se comunica a los servidores y contratistas que deben trabajar desde sus casas.
2) Coordinador del Grupo de Gestión Administrativa notifica al Coordinador de Grupo de Atención al Ciudadano que se suspende la atención presencial de ciudadanos y se fija cartel en la edificación
3) Los jefes de dependencia ordenan la activación de trabajo en casa utilizando las herramientas colaborativas TEAMS, Correo electrónico, grupos de mensajería.
4) Servidores y contratistas realizan sus actividades asignadas en modalidad de trabajo remoto hasta que los jefes de dependencia notifiquen el retorno a la sedenormal de trabajo
5) El trabajo remoto debe mantener hasta que se reciba comunicación formal del Equipo de gestión de emergencias del reportando la resolución de la emergencia.

Fase 4: Resolución del incidente

1) El *Equipo de Gestión de Emergencias* coordina con el jefe de servicios administrativos las actividades de reparación de las instalaciones físicas afectadas.
2) De acuerdo con la naturaleza de la emergencia puede llegar a ser necesario: reparar la sede por daños causados por agua o fuego. Limpieza de áreas con personal especializado en materiales peligrosos o en el peor escenario búsqueda de sedes alternas en caso de que la sede principal quede inutilizable.
3) El *Equipo de Gestión de Emergencias* define si se debe autorizar el reinicio de operaciones en la sede. En caso de autorizar el reingreso a la sede se comunicala decisión mediante mensaje instantáneo vía Whats App en el Equipo de gestión de emergencias
4) El Coordinador (a) del Grupo de Talento Humano coordina con el (la) Jefe de la Oficina Asesora de Comunicaciones la transmisión del mensaje de retorno a la sede principal a través de correo electrónico, mensajes i instantáneos por grupos cerrados de WhatsApp.
5) Se publica en la intranet banner notificando la vuelta a normalidad de actividades.

Escenario 3: Desastre tecnológico

Escenario 3: Desastre tecnológico	
Líder de respuesta:	**Jefe de Oficina de Tecnologías de Información y Comunicaciones**
Equipo de respuesta:	Oficina de Tecnologías de Información y Comunicaciones
Fase 1:Detección	

Identificación de alertas

El equipo de la Oficina de Tecnologías de Información y comunicaciones, el *oficial de seguridad de la información* o quien haga sus veces y el Grupo de Gestión Administrativa, monitorizan los componentes que soportan los sistemas de información, servicios informáticos y la infraestructura de servicio esenciales del centro de datos para identificar eventos no deseados que puedan generar fallas que conduzcan a pérdida de continuidad de servicio, los elementos que se monitorización continuamente incluyen:

Subsistemas de telecomunicaciones

- Router de acceso a Internet
- Canal de acceso a servicios de Internet
- Switches de core y switches de piso
- Equipos de seguridad perimetral como firewall y concentrador de VPN

Servicios de mensajería electrónica y sistema colaborativo Office 365

Servidores virtuales y físicos que soportan sistemas de información institucionales

- Sitio web Institucional
- Intranet institucional
- Sistema de gestión documental Orfeo
- Sistema de almacenamiento compartido de archivos Orfeo
- Sistema de información SIGEP
- Sistema de información SUIT
- Sistema de información FURAG
- Sistema CRM
- Sistema de información estratégica SIE
- Sistema Integrado de Planeación y Gestión
- Sistema de gestión institucional
- Sistema de gestión de mesa de ayuda Proactiva Net
- Canales virtuales de comunicación EVA

- Portales de divulgación de información: sirvo a mi país, banco de éxitos, banco de gerentes, reporte de conflicto de interés, declaración de bienes y rentas, gestor normativo, rendición de cuentas.

Sistemas de almacenamiento masivo SAN

Sistema de virtualización de servidores

Subsistemas de aire acondicionado

Sistema de energía eléctrica, sistema de UPS, bancos de baterías

Confirmación

A partir de los resultados de la revisión de los sistemas de información, monitorización de alertas, reportes de los usuarios y notificación de partes interesadas como el centrocibernético policial, centro de respuesta a incidentes informático del Min Defensa o el Min TIC se determina la ocurrencia de emergencias que suspenderán la prestación de servicios informáticos de la Entidad como:

- Ataques cibernéticos como denegación de servicios
- Secuestro de la información institucional por ataque de software malicioso (ransomware)
- Falla total de los subsistemas de energía o aire acondicionado del centro de computo
- Falla eléctrica por voltaje severamente reducido, depresión es, picos y sobrevoltajes
- Caída total del servicio de acceso a Internet o red local institucional
- Caída de canales de comunicación principales a cargo de los proveedores de acceso a Internet que alteren y/o interrumpan el normal funcionamiento de los equipos que se utiliza para los procesos misionales.
- Fuego o inundación del centro de datos que obliga al apagado de todo el centro de datos
- Falla total del sistema de almacenamiento masivo de datos compartidos
- Falla total del sistema de virtualización de serv idores
- Indisponibilidad total de bases de datos por corrupción de datos
- Pérdida acceso a sistemas críticos por finalización de licencia de uso
- Manipulación incorrecta de sistemas informáticos debido a: Actividad errónea de administración de base de datos, corrupción de la base de datos, acceso indebido a la base de datos para modificarla, errores en puestaen producción / regresión con impacto en base de datos y errores en generacióny restauración de respaldos que conlleven a la pérdida total o parcial de los servicios
- Por problemas y exposiciones en aplicación y componentes del sistema tales como código malicioso en el software, fuga de información de claves de usuarios, ataques externos para obtención indebida de claves, suplantación deusuarios externos al pedir cambio de clave, ataques externos para obtención/modificación indebida de información

Los profesionales responsables de la administración de los sistemas afectados realizan un diagnóstico sobre el incidente, teniendo en cuenta:

- Naturaleza e impacto del incidente.
- Estrategias definidas en el Plan de Recuperación ante desastres aplicables u otras soluciones potenciales definidas por la base de conocimientos de la mesade servicio.
- Tiempo estimado de solución del incidente.

De acuerdo con los protocolos y procedimientos de soporte para los diferentes sistemas de información y plataformas informáticas, la oficina de tecnologías de información aplica las acciones de remediación para resolver la contingencia, si el evento no se ha resuelto de acuerdo con el siguiente tiempo máximo tolerable de caída, el jefe de la oficina de tecnologías de información y las comunicaciones confirman la situación de alerta por falla de infraestructura tecnológica o ataque informático y mediante mensaje instantáneo vía WhatsApp notifica al equipo de gestión de emergencias la necesidad de activar el plan de continuidad para el escenario Nro. 3. Desastre tecnológico

Componente tecnológico/ Sistema de información	**Tiempo máximo tolerable de caída**
Suministro de energía eléctrica de negocio	Consultar tabla de análisis de impacto alcentro de datos
Servicio de acceso a internet	Consultar tabla de análisis de impacto alnegocio
Servicio de red local interna	Consultar tabla de análisis de impacto alnegocio
Sistema de almacenamiento de archivos compartidos	Consultar tabla de análisis de impacto alnegocio
Sistema de virtualización de servidores	Consultar tabla de análisis de impacto alnegocio
Sistema de información ORFEO	Consultar tabla de análisis de impacto alnegocio
Sistema de aire acondicionado de centro de datos	Consultar tabla de análisis de impacto alnegocio
Software colaborativo Office 365	Consultar tabla de análisis de impacto alnegocio

Fase 2: Activación

1) El Jefe de la Oficina de las Tecnologías de Información y Comunicaciones alerta al *Equipo de Gestión de Emergencias* de la necesidad de aplicar el plan de recuperación ante desastres de tecnología y la necesidad de activar los planes de operación alterna de cada una de las dependencias ante la caída de los servicios informáticos por un periodo superior al tiempo máximo tolerable definido en el análisis de impacto BIA. Dentro su comunicación incluye aspecto como:

- Sistemas y servicios afectados
- Resultados del diagnóstico sobre los sistemas afectados
- Acciones de recuperación realizadas hasta el momento
- Tiempo estimado para el restablecimiento de los servicios afectados
- Riesgos a los que está expuesta la entidad por el desastre presentado, y las alternativas disponibles
- Recomendación de activar el plan de continuidad institucional e iniciar la ejecución del plan recuperación ante desastres de tecnología

2) El Equipo de Gestión de Emergencias evalúa la información y decide si se debe activar el plan de continuidad y plan de operación alterno de cada una de las dependencias.

Si se aprueba la ejecución del plan de operación alterno por desastre tecnológico, el Jefe de la OTIC comunica por mensaje instantáneo al Jefe de la Oficina Asesora de Comunicaciones que se debe notificar a los jefes de dependencia la necesidad de aplicar sus respectivos planes de operación alterno por crisis de infraestructura tecnológica.

3) El equipo de gestión de emergencias define el mensaje oficial de respuesta que se comunicará a los grupos de valor que incluyen:

Centro de respuesta a incidentes informáticos de Gobierno -Csirtgob csirtgob@mintic.gov.co

Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT contacto@colcert.gov.co

Funcionarios y contratistas de la Entidad a través de los grupos de mensajería instantánea. Dentro de la comunicación a divulgar el equipo de gestión de emergencia define:

- ¿Qué información concreta se tiene sobre la crisis (incidente presentado, diagnóstico, tiempo de solución)?
- ¿Qué información está en proceso de verificación e investigación?
- ¿Qué información válida se puede comunicar inmediatamente (mensaje)?
- ¿Qué información se debe manejar al interior de la entidad?
- ¿Quiénes fueron afectados por la crisis (audiencia)?
- ¿Qué otras audiencias deberían saber sobre la crisis?
- ¿Cómo se comunicará la información a los interesados o afectados (medio)?

Fase 3: Plan de operación alterno

4) El Jefe de la Oficina de Tecnologías de Información y las Comunicaciones activael *plan de recuperación ante desastres* para restablecer los sistemas informáticos o sistemas de información afectados.
5) Los jefes de dependencia activan sus p lanes de operación alterno así:

- Plan de operación alterna servicio al ciudadano
- Plan de operación alterna gestión documental
- Plan de operación alterna gestión contractual
- Plan de operación alterna gestión financiera
- Plan de operación alterna gestión humana
- Plan de operación alterna gestión administrativa
- Plan de operación alterna OAC
- Plan de operación alterna OAP
- Plan de operación alterna Dirección DAFP
- Plan de operación alterna Subdirección DAFP

6) El equipo de gestión de emergencia activa su protocolo de comunicación a los grupos de valor considerando los siguientes lineamientos:

- Informar rápida y periódicamente a los grupos de valor ante una situación de emergencia tecnológica de alto impacto, la entidad se debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis para evitar malentendidos, especulaciones y rumores. Estos elementos le permitirán generar confianza y credibilidad con sus grupos de valor.
- Decir la verdad: ser honestos en los comunicados, sin embargo, no significa transmitir TODA la información, sólo aquella que es suficiente para generar confianza y tranquilidad a los grupos de valor.
- La información que esté calificada como clasificada o reservada solo se debe transmitir a los debidamente autorizados el Jefe de la Oficina de TIC determina con el apoyo en seguridad digital la sensibilidad de la información a publicar
- Emitir reportes lo más exactos posible: publicar la información que se tiene disponible, siempre y cuando ésta haya sido validada. Evitar toda clase de especulación o falsa expectativa.

7) La Oficina Asesora de Comunicaciones, realiza monitorización permanente de la información que circula en medios sobre la emergencia y formula recomendaciones al Equipo de Gestión de Emergencias sobre:

- ¿Qué información circula en los medios de comunicación y cómo reaccionar ante la misma?
- ¿Qué información circula a nivel interno de los chats de equipos transversales y cómo reaccionar ante la misma?
- ¿Qué impacto sobre la emergencia tiene la información que está circulando en los medios y cómo mitigar sus daños potenciales?
- Necesidad de nuevos comunicados

8) Siguiendo el plan de operación alterno de cada dependencia los jefes de dependencia imparten las ordenes correspondientes a los subalternos para mantener las actividades misionales críticas usando los recursos disponibles. Si paralelamente a la ocurrencia de la emergencia de desastre tecnológico se presentan los escenarios 1 Emergencia social y 2 Falla de infraestructura f física, el Equipo de Gestión de Emergencia sigue el protocolo de actuación de esos escenarios para determinar si el edificio se debe evacuar o no. Si no es necesaria la evacuación del edificio todas las actividades misionales continúan ejecutándose desde el edificio hasta que se supere la emergencia o el Equipo de gestión de emergencia determine lo contrario

Fase 4: Resolución del incidente

1) Cuando se realice el restablecimiento de los sistemas informáticos afectados El Jefe de la Oficina de Tecnologías de Información y Comunicaciones, notifica al Equipo de Gestión de Emergencias cuales servicios han sido restablecidos y que sistemas informáticos ha sido recuperados
2) Con la información de estado de funcionamiento de los sistemas informáticos, el Equipo de Gestión de Emergencias autoriza la reactivación de procesos a sus condiciones normales tomando en cuenta el orden de restablecimiento de servicios definido en el análisis de impacto al negocio BIA, para lo cual Consulta la tabla de análisis de impacto al negocio
3) El Jefe de la Oficina de Tecnologías de Información, siguiendo el or den de reanudación de procesos y la disponibilidad de servicios TIC requerido por cada proceso, notifica al jefe de la dependencia respectiva para que realice las actividades de vuelva a operación normal.
4) Los jefes de dependencia aplican las acciones definidas de vuelta a operación normal definidas en sus respectivos planes de operación alterna
5) El jefe de la Oficina de tecnologías de información y comunicaciones, informa al Equipo de Gestión de Emergencias el avance en la reactivación de procesos. Cuando todos los procesos hayan finalizado su plan de operación alterno, se prepara informe final de resolución de la emergencia para el Equipo de gestión de emergencias

   El Equipo de Gestión de Emergencias confirma que todos los procesos y dependencias se encuentran funcionando en condiciones normales y se prepara comunicado oficial de finalización de la emergencia para los grupos de valor.

Escenario 4: Crisis Financiera

Escenario 4: Crisis Financiera	
Líder de respuesta:	**Secretario (a) General**
Equipo de respuesta:	Oficina Asesora de Planeación, Secretaria General y Direcciones técnicas.

Fase 1: Detección

Identificación de alertas

Análisis del entorno interno

Mediante evaluación y seguimiento variables institucionales, se identifican signos de posibles restricciones financieras

1) Relevancia de las iniciativas del Plan de Gobierno asociadas a obligaciones institucionales
2) Análisis previo de las iniciativas consignadas en el plan sectorial
3) Ponderación de los compromisos del sector consignados en el Plan Nacional de Desarrollo
4) Prioridades de la Presidencia de la República frente a los compromisos planteados en el plan de gobierno
5) Existencia de indicadores para las iniciativas registrados en Sinergia, así comonivel de sensibilidad de la iniciativa.
6) Análisis de entorno país y variables macroeconómicas.
7) Tiempos destinados a la planeación sectorial vs los tiempos asignados a la planeación institucional.

Se identifican señales de alerta de escenario de crisis financiera a partir de:

1) Seguimiento a los resultados de la Comisión Sectorial de presupuesto
2) Seguimiento a la definición del marco de gasto de mediano plazo
3) Seguimiento a posibles recortes al presupuesto cuando se recomponen partidas
4) Distribución de presupuesto a las diferentes entidades públicas
5) Cambios de gobierno y ausencia de personal clave para la negociación del presupuesto

A través del seguimiento a la preparación del presupuesto de inversión se identifican síntomas de posibles problemas para la asignación del presupuesto con las entidades

1) Marco de Gasto con el Ministerio de Hacienda y Crédito Público, que genera un mensaje de techo presupuestal, con el cual se puede identificar si el monto definido en el techo presupuestal permitirá cubrir las necesidades de los proyectos de inversión
2) Presentación del proyecto de ley de presupuesto que implica negociaciones conel Departamento Nacional de Planeación, el Congreso de la República y el Ministerio de Hacienda, este es un segundo instante en donde se pueden identificar potenciales problemas de financiamiento debido a que dentro de la ley de presupuesto debe quedar consignado un artículo que faculte el traslado de recursos desde la ESAP hacia el DAFP
3) A través de comunicación y negociación con la ESAP también se pueden identificar señales de una potencial crisis financiera en la medida en que previoal ante proyecto de presupuesto se deben cruzar mensajes y comunicaciones con la ESAP para garantizar la transferencia de recursos.
4) Por último, se debe estar atentos a los mensajes del Ministerio de Hacienda y el Departamento Nacional de Planeación los cuales permiten identificar potenciales signos de alarma en la asignación de presupuesto.
5) Cuando se realiza la planeación (cuatrienal y anual) y se definen los productos a desarrollar para atender los compromisos definidos para la vigencia, se identifican las brechas de recursos para su debido cumplimiento.

Confirmación

Para lograr una identificación oportuna de posibles crisis financieras que afecten a la entidad se debe buscar la obtención de información real de la distribución del presupuesto a nivel de sector, lo que implica comunicación constante con instancias como la Alta dirección del DNP y el Ministerio de Hacienda.

Fase 2: Activación

Respecto a la activación del Plan de Continuidad, se identifica que, a partir del resultado de la asignación de presupuesto y la priorización de los proyectos misionales, la Alta dirección debe ser notificada acerca de la suficiencia de recursos para cumplir con las obligaciones del Plan Nacional de Desarrollo y las obligaciones misionales. En caso de detectar que el presupuesto asignado no será suficiente la Alta dirección debe activar las acciones de tratamiento de crisis financiera. Usando la información de resultados de la negociación del presupuesto y la priorización de proyectos, la alta dirección activa las acciones para contrarrestar los efectos de la eventual crisis financiera con acciones como:

1) Verificar la priorización de los diferentes proyectos de acuerdo con criterios quese diseñan en el mismo instante que se detecta la potencial emergencia.
2) Posibilidad de renegociar la asignación de presupuesto utilizando traslados dela ESAP

3) Búsqueda de fuentes alternativas para suplir recursos financieros para los proyectos
4) Sustentar la necesidad de obtener recursos de fuentes internacionales

Fase 3: Plan de operación alterno

Considerando la obligatoriedad de cumplir con los compromisos del Plan Nacional de Desarrollo y los objetivos institucionales, la alta dirección define estrategias para:

- Priorizar la ejecución de ciertas iniciativas de alto impacto en los compromisosy desarrollo de planes alternos para cumplir con los compromisos durante la vigencia

- Evaluar los parámetros de priorización de compromisos contra los criterios consignados en el Plan Nacional de Desarrollo (PND), documentos CONPES, compromisos de acuerdos nacionales (ej. Acuerdos de paz
- Nivel de prioridad de las necesidades versus el ante proyecto de presupuesto.
- Obtener recursos desde organizaciones internacionales o de cooperación.
- Recursos disponibles en la ESAP
- El ajuste de prioridades de ejecución de los proyectos de acuerdo con los recursos disponibles para la vigencia y prioridades misionales.
- Efectuar negociaciones complementarias con el Ministerio de Hacienda, Departamento Nacional de Planeación para lograr nuevos recursos.
- Fuentes alternas como convenios interinstitucionales

Las acciones de respuesta a la crisis financiera se mantienen para monitorizar el porcentaje de ejecución real de los compromisos versus la ejecución presupuestal planificada, lo que implica el uso de tableros de indicadores precisos.

Fase 4: Resolución del incidente

1. Cuando los compromisos de Gobierno están subsanados financieramentemediante la gestión de consecución de otras fuentes
2. Cuando el presupuesto de funcionamiento e inversión corresponde a lasnecesidades
3. Cuando las brechas de presupuesto (sin imprevistos) se han gestionadomediante recursos de cooperación nacional o internacionalmente.

Escenario 5: Pandemia - Epidemia

Escenario 5: Pandemia - Epidemia

Líder de respuesta:	**Coordinador (a) de Gestión de Talento Humano**
Equipo de respuesta:	Grupo de Gestión de Talento Humano

Fase 1: Detección

Identificación de alertas

A través de la monitorización de riesgos y alertas del sistema de gestión de seguridad y salud en trabajo, los reportes oficiales entidades y organizaciones de la salud, el Grupo de Gestión de Talento Humano se entera de brotes epidemiológicos a nivel Colombia o el continente:

Ministerio de Salud y la Protección Social (MinSalud), La Secretaria Distrital de Salud (sistema SIVIGILA),

Organización Panamericana de la Salud (OPS Alertas) Organización Mundial de la Salud (OMS Alertas)

@MinSaludCol twitter del Ministerio de salud de Colombia

@INSColombia twitter del instituto nacional de salud de Colombia @SectorSalud twitter del sector salud de Bogotá

@PositivaCol twitter ARL Positiva

Confirmación

1. La información sobre la evolución y recomendaciones para la prevención de brotes epidemiológicos de diferente naturaleza se consulta con la Administradora de Riesgos Laborales quienes generan recomendaciones a la Entidad.

2. El Grupo de Gestión de Talento Humano utiliza la información generada por la ARL y la información oficial del Ministerio de Salud, para alertar al Equipo de Gestión de Emergencias, sobre el nivel de alerta en Bogotá y otras ciudades del país

3. La información sobre niveles de alerta, medidas de mitigación y acciones que determine el gobierno nacional son evaluadas por el Equipo de Gestión de Emergencias para tomar la decisión de activar el plan de contingencia de trabajo remoto y otras medidas que determine la rama ejecutiva.

Fase 2: Activación

Con base en las ordenes de la rama ejecutiva, el Director del Departamento Administrativo de la Función Pública autoriza la activación del plan de contingencia para el escenario de pandemia / Epidemia siguiendo los protocolos que defina el gobierno nacional:

1) Seguir el protocolo de salud que defina el Ministerio de Salud y la Protección social. Ejemplo: decreto 666 de 2020 Protocolo general de Bioseguridad

   Normativa COVID-19

2) Coordinador (a) del Grupo de Gestión de Talento Humano se comunica con la Oficina Asesora de Comunicaciones para publicar en el sitio web institucional,

video pantallas, redes sociales de la Entidad e instalaciones de la Entidad, mensaje comunicando a todos los grupos de valor indicando las medidas adoptadas por la Entidad para la atención al público en caso de epidemia o pandemia

3) El Coordinador (a) del Grupo de Talento Humano se comunica con la Secretaria General para que se inicie la coordinación de los protocolos de trabajo remoto con todas las dependencias
4) La Secretaria General a través del Coordinador del Grupo de Gestión Administrativa remite correo electrónico a todos los jefes de dependencia para que coordinen internamente con sus equipos de trabajo la recolección de necesidades sobre traslado de equipos para permitir el trabajo remoto, la activación de conexiones remotas para acceso a la información institucional por red privada virtual
5) Los jefes de las dependencias coordinan con sus equipos de trabajo, el cargue de información vital o esencial para el trabajo remoto en los servicios de nube (office 365 / OneDrive), los coordinadores de grupo confirman con los servidoresy contratistas de sus dependencias, el cargue de información vital para iniciar el trabajo remoto. De acuerdo con las instrucciones del Director de la Entidad, el día y hora definidos por la Entidad, Los jefes de dependencia ordena n la activación del *trabajo en casa* utilizando las herramientas colaborativas TEAMS, Correo electrónico, grupo de mensajería instantánea a partir del día y hora definidos la entidad aplica sus protocolos de trabajo remoto.
6) Una vez se ha activado la modalidad de trabajo remoto para cada una de las dependencias, el Coordinador (a) del Grupo de Talento Humano genera un informe para el *Equipo de Gestión de Emergencias* sobre los resultados del iniciode la contingencia por Pandemia/Epidemia.
7) Servidores y contratistas realizan sus actividades asignadas en modalidad de trabajo remoto hasta que los jefes de dependencia notifiquen el retorno a la sede normal de trabajo
8) El trabajo remoto debe mantener hasta que se reciba comunicación formal del *Equipo de Gestión de Emergencias* indicando que se iniciará el retorno a trabajo dentro de la sede de la Entidad.

Fase 3: Plan de operación alterno

1) Durante la activación del trabajo remoto los servidores públicos y contratistas continuaran realizando sus labores desde sus casas de acuerdo con las instrucciones que para tal fin impartan los jefes de las diferentes dependencias y los supervisores de contrato.

2) Para aquellas dependencias con responsabilidad de atención presencial a grupos valor Los jefes de cada dependencia activan sus planes de operación alterno así:

- Plan de operación alterna servicio al ciudadano
- Plan de operación alterna gestión documental
- Plan de operación alterna gestión contractual
- Plan de operación alterna gestión financiera
- Plan de operación alterna gestión humana
- Plan de operación alterna gestión administrativa

3) Durante la ejecución de labores en la modalidad de trabajo remoto las siguientes actividades pueden llegar a ser actividades por el Equipo de gestión de emergencias:

a) Realizar capacitación virtual mediante infografías, videos, mensajes ocharlas virtuales a todos los servidores y trabajadores sobre prevención de las enfermedades que generaron la alerta de pandemia
b) Definir medidas que eviten la exposición de servidores y contratistas como flexibilización de turnos y horarios de trabajo.
c) Reporte de casos sospechosos por contagio de la Epidemia/ Pandemia antela ARL y la EPS
d) Establecer canales de comunicación para mantener informados a los servidores y contratistas sobre medidas de prevención sobre la prevención,propagación y atención de la enfermedad
e) Determinar en conjunto con al ARL los mecanismos para proveer a los servidores los elementos de protección personal en caso de que sean estos requeridos
f) Todos los servidores y contratistas deberán acatar las instrucciones determinen las autoridades en materia de salud para su cuidado personal.

Fase 4: Resolución del incidente

1) El Equipo de gestión de emergencias (Dirección, subdirección, secretaría general, jefe de OTIC, o jefe de la OAP) continuamente monitorizan las instrucciones del gobierno nacional como respuesta a la epidemia / pandemia.

@MinSaludCol twitter del Ministerio de salud de Colombia

@INSColombia twitter del instituto nacional de salud de Colombia

@SectorSalud twitter del sector salud de Bogotá

@PositivaCol twitter ARL Positiva

2) Cuando las autoridades en materia de salud así lo indiquen y siguiendo los protocolos de bioseguridad que para tal fin se definan, el *Equipo de Gestión de Emergencias* determina las condiciones de reactivación del trabajo en la sede del Departamento Administrativo de la Función Pública.
3) El *Equipo de Gestión de Emergencias* define si se debe autorizar el reinicio de operaciones en la sede. En caso de autorizar el reingreso a la sede se comunica la decisión mediante los canales oficiales establecidos
4) El Coordinador (a) del Grupo de Talento Humano coordina con la Jefe de la Oficina Asesora de Comunicaciones la transmisión del mensaje de retorno a la sede principal a través de correo electrónico, mensajes instantáneos por gruposcerrados de WhatsApp, comunicaciones en el sitio web institucional o los medios de comunicación formalmente adoptados por el Equipo de gestión de emergencias para este propósito.
5) La Oficina Asesora de Comunicaciones siguiendo la política de comunicaciones institucional informa a los grupos de valor la reactivación de la aten ción presencial, comunicando los protocolos de bioseguridad definidos por el Gobierno Nacional
6) Los jefes de dependencia coordinan con sus equipos de trabajo el retorno a trabajo presencial en sede siguiendo el protocolo que defina el *Equipo de Gestión de Emergencias*
7) El Grupo de Gestión Administrativa activa los protocolos para traslado de los equipos informáticos que hayan sido utilizados para la modalidad de trabajo remoto desde las casas de los servidores o contratistas hasta la sede principal de la Entidad
8) Siguiendo los protocolos de bioseguridad que la Entidad defina, servidores y contratistas reinician sus actividades en la sede principal

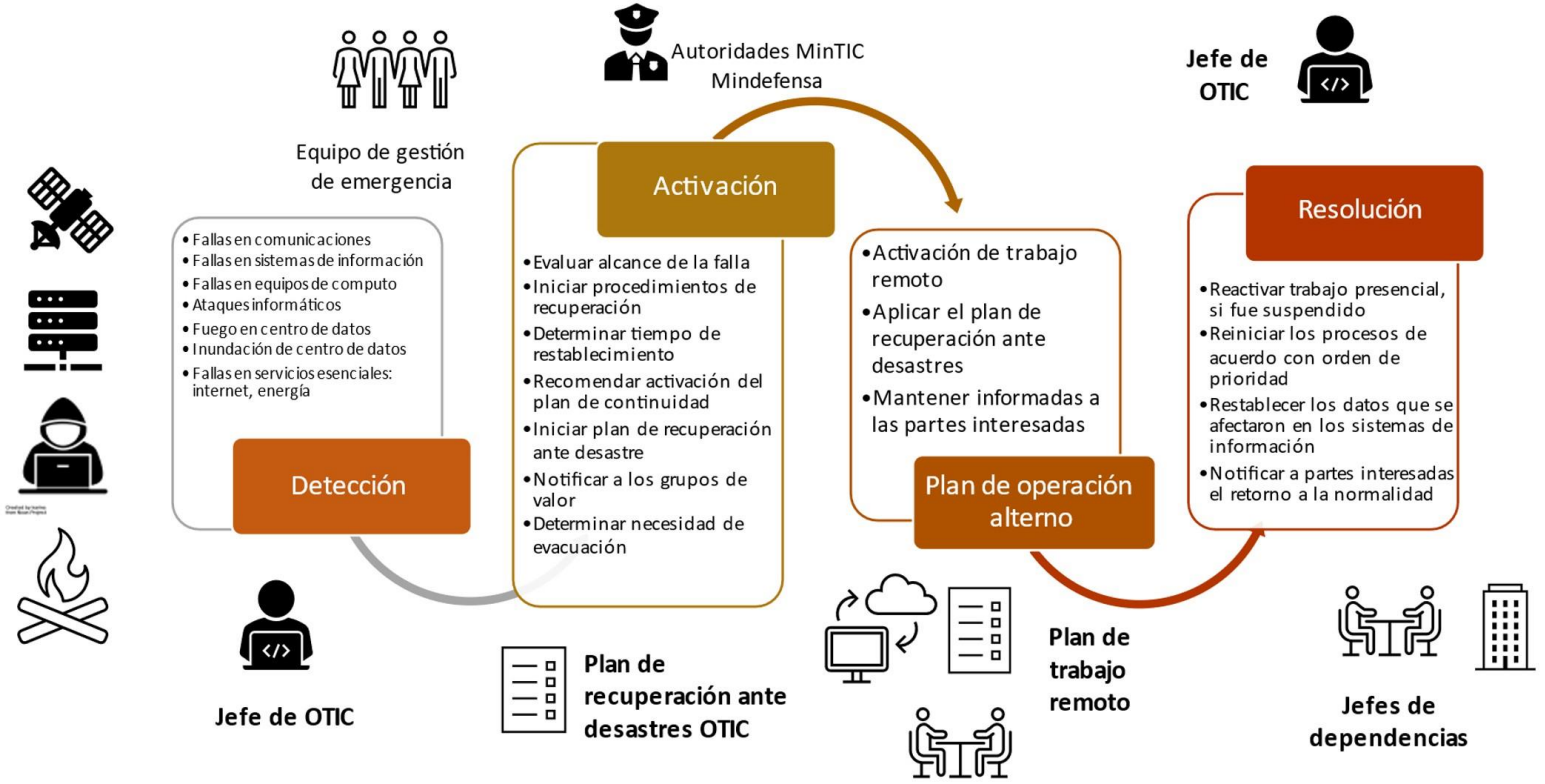
Fichas descriptivas de protocolo de acción por escenarios de emergencia

Escenario 2: Desastre natural y colapso de infraestructuras

Daño severo de nuestras instalaciones o el medio ambiente que impide laborar

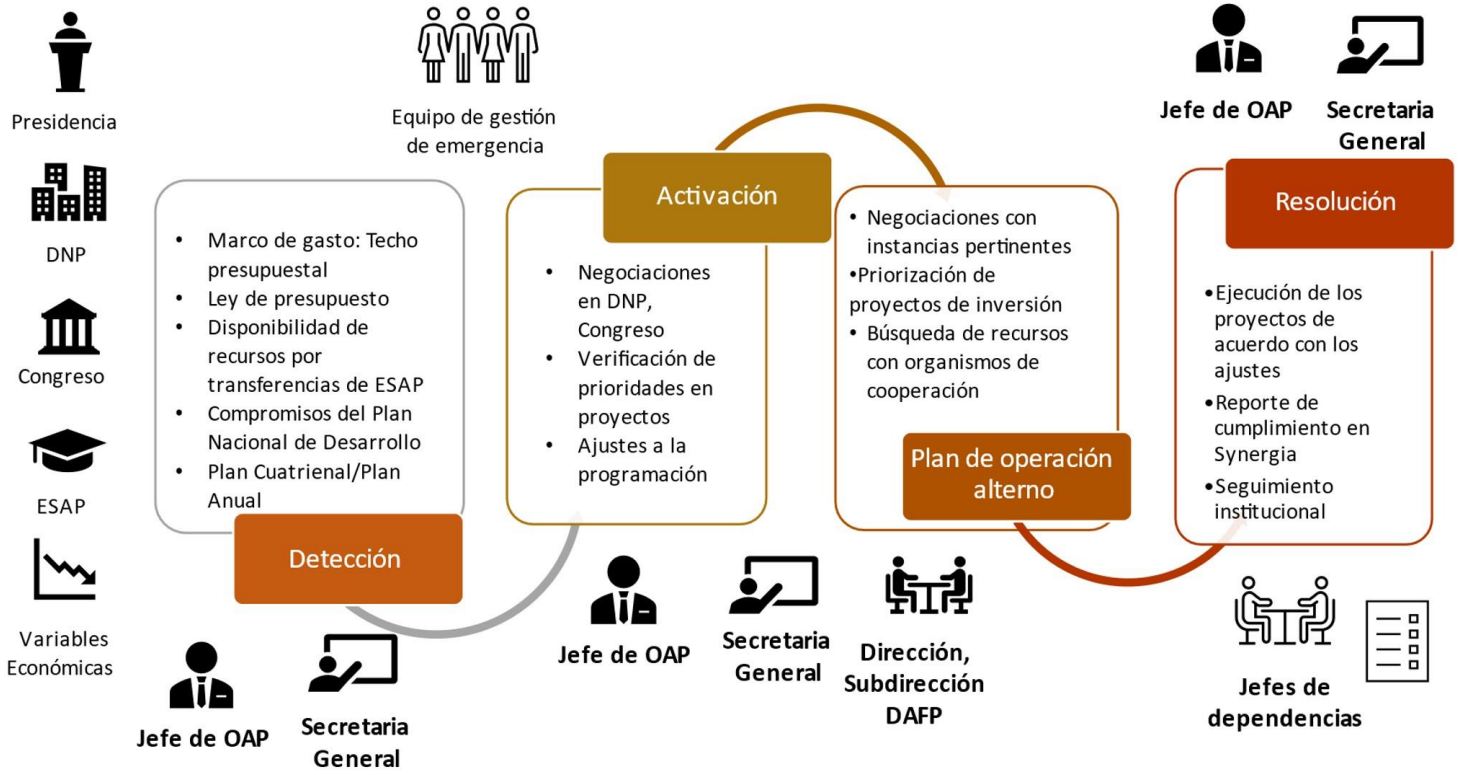
Escenario 3: Desastre Tecnológico

Daño severo en la infraestructura de servicios TIC o ataques informáticos como secuestro de datos



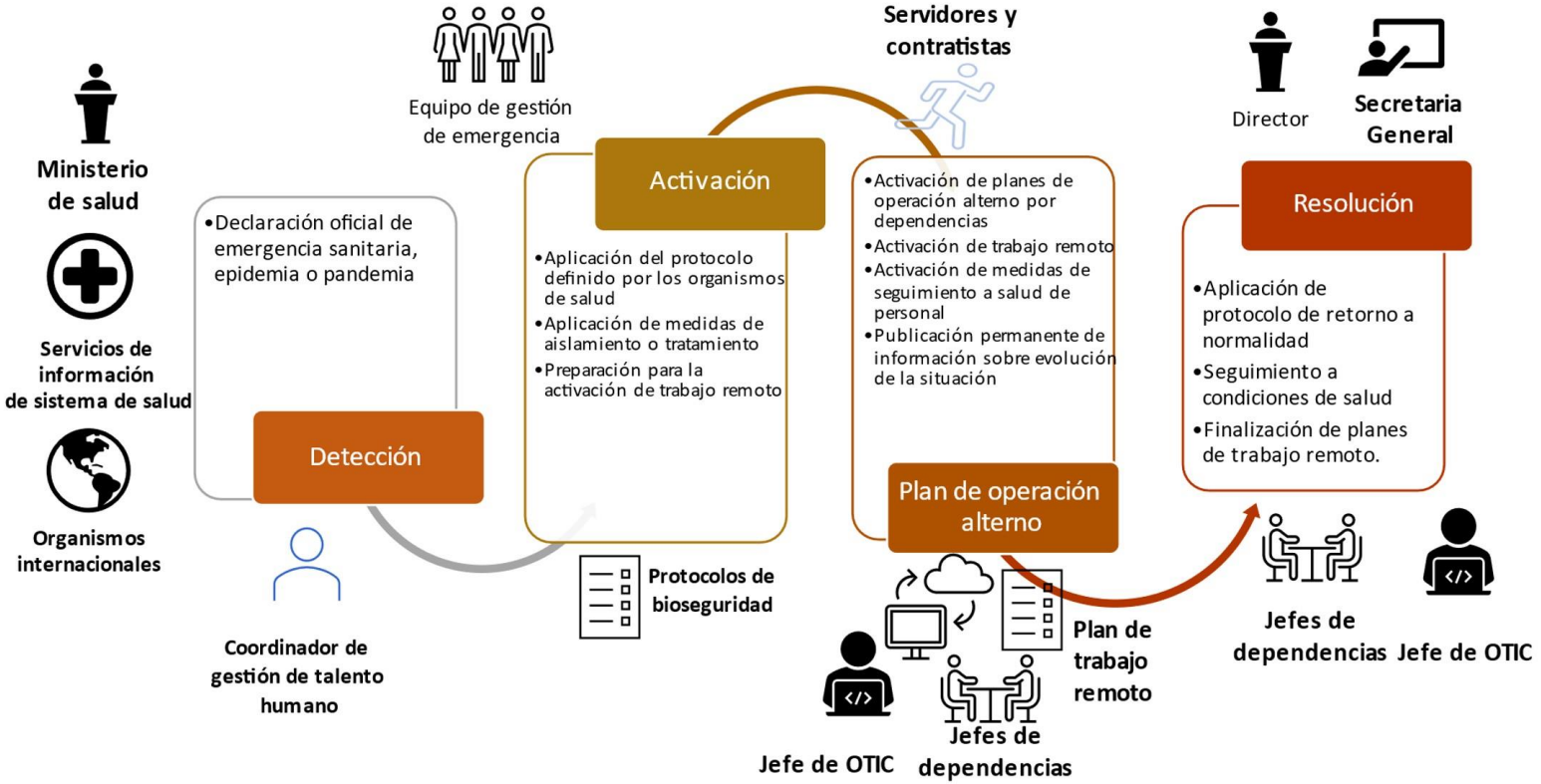
Escenario 4: Crisis financiera

Imposibilidad de contar con los recursos económicos para cumplir con compromisos misionales o con terceros proveedores de servicios



Escenario 5: Emergencia sanitaria

Pandemias, epidemias, crisis sanitaria que impide el funcionamiento de los procesos institucionales



Objetivo:

Definir las actividades detectivas, preventivas, reactivas y correctivas para gestionar adecuadamente las situaciones que sean calificadas como emergencia y puedan comprometer la seguridad del personal, la prestación de servicio o la continuidad de las funciones misionales.

No.	Actividades	Fecha inicio	Fecha fin	Responsable	Meta	Indicador
1	Publicar documentos asociados a las convocatorias de manifestaciones y reuniones de protesta en la zona de trabajo de la entidad.	1/02/2022	20/12/2022	Grupo de Mejoramiento Institucional	Documentos asociados a las convocatorias de manifestaciones y reuniones de protesta en la zona de trabajo de la entidad publicados y socializados	X=(Total documentos publicados/Total de documentos propuestos para publicación)*100% X=(Total documentos socializados/Total de documentos propuestos para socialización)*100%
2	Gestionar el envio de comunicaciones formales con estrategias para el manejo de la calma ante situaciones de emergencia.	1/02/2022	20/12/2022	Subdirección / Secretaria General / Dirección General	Comunicaciones con las estrategias para el manejo de la calma ante situaciones de emergencia diseñadas	
3	Desarrollar pruebas de Tecnología de Información para el control de la disponibilidad e integridad de la información ante desastres naturales y colapso de infraestructuras.	1/02/2022	20/12/2022	Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones	Pruebas de Tecnología de Información para el control de la disponibilidad e integridad de la información ante desastres naturales y colapso de infraestructuras diseñadas	
4	Definir estrategias para el desarrollo de las pruebas de Tecnologías de información para el control de la disponibilidad e integridad de la información ante cualquier emergencia de tipo social.	1/02/2022	20/12/2022	Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones	Estrategias para el desarrollo de las pruebas de Tecnologías de información para el control de la disponibilidad e integridad de la información ante cualquier emergencia de tipo social diseñadas	
5	Diseñar pruebas de tecnologías de información para el manejo de la confidencialidad, disponibilidad e integridad de la información financiera ante escenarios de continuidad del negocio.	1/02/2022	20/12/2022	Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones	Pruebas de tecnologías de información para el manejo de la confidencialidad, disponibilidad e integridad de la información financiera ante escenarios de continuidad del negocio diseñades	
6	Aplicar pruebas de tecnologías de información para el control de la disponibilidad de la información ante emergencias de orden sanitario como son las epidemias o pandemias.	1/02/2022	20/12/2022	Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones	Pruebas de tecnologías de información para el control de la disponibilidad de la información ante emergencias de orden sanitario como son las epidemias o pandemias diseñad s	
7	Desarrollar simulacros para el control de la confidencialidad, disponibilidad e integridad de la información ante un desastre tecnológico para garantizar la continuidad del negocio.	1/02/2022	20/12/2022	Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones	Simulacros para el control de la confidencialidad, disponibilidad e integridad de la información ante un desastre tecnológico para garantizar la continuidad del negocio diseñados	
8	Publicar informes de resultados de las pruebas realizadas en el área de OTIC ante eventualidades de fuerza mayor, desastres naturales y colapso de infraestructura.	1/02/2022	20/12/2022	Grupo de Mejoramiento Institucional	Informes de resultados de las pruebas realizadas en el área de OTIC	
9	Publicar documentos relativos a el plan de operación alterna de gestión financiera.	1/02/2022	20/12/2022	Grupo de Mejoramiento Institucional	Documentos relativos a el plan de operación alterna de gestión financiera publicados y socializados	
10	Realizar campañas de información sobre los diferentes elementos de bioseguridad necesarios en el área de trabajo.	1/02/2022	20/12/2022	Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones	Campañas de información sobre los diferentes elementos de bioseguridad necesarios en el área de trabajo desrrolladas	
11	Realizar campañas virtuales para el manejo y control de enfermedades.	1/02/2022	20/12/2022	Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones	Campañas virtuales para el manejo y control de enfermedades desarrolladas	
12	Actualizar las políticas de respaldo de información, planes de continuidad y disponibilidad y socializar al interior de la Entidad	1/02/2022	20/12/2022	Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones	Políticas de respaldo de información, planes de continuidad y disponibilidad publicados y socializados	

Documento Técnico del Plan de Continuidad del Negocio

VERSIÓN 6

Direccionamiento Estratégico

Enero de 2021

Departamento Administrativo de la Función Pública

Carrera 6 n.º 12-62, Bogotá, D.C., Colombia

Conmutador: 7395656 Fax: 7395657

Web: www.funcionpublica.gov.co

eva@funcionpublica.gov.co

Línea gratuita de atención al usuario: 018000 917770

Bogotá, D.C., Colombia.