IPES

PLAN DE CONTINGENCIA INSTITUCIONAL

SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO

PROCESO DE PLANEACIÓN ESTRATÉGICA Y TÁCTICA

BOGOTÁ, 2021

Elaboró:	Revisó:	Aprobó:
Edgar M Mera E CPS 53 de 2021 SDAE Sandra Florez CPS 825 de 2020	William Neil Vargas Contreras Subdirector De Diseño Y Análisis Estratégico (E) Gloria Castillo CPS 57 de 2021 SDAE	William Neil Vargas Contreras Subdirector de Diseño y Análisis Estratégico (E)

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. JUSTIFICACIÓN 3
3. OBJETIVOS 4
4. ALCANCE 4
5. RESPONSABLES 5
6. DEFINICIONES Y ABREVIATURAS 5
7. DESARROLLO 9
8 DOCUMENTOS ASOCIADOS 41
9 MARCO NORMATIVO 42
10 CONTROL DE CAMBIOS 50
11 REFERENCIAS BIBLIOGRÁFICAS 50
12 ANEXOS 54

1. INTRODUCCIÓN

El Instituto para la Economía Social -IPES- es una entidad con personería jurídica, autonomía administrativa y patrimonio propio; la cual está adscrita a la Secretaría Distrital de Desarrollo Económico.

El IPES dentro de los programas y proyectos que adelanta enfoca sus esfuerzos principalmente en el trabajo social con los vendedores informales, así como atiende poblaciones de alta vulnerabilidad desplazada y reincorporada en materia de emprendimiento.

Desde los esquemas de Seguridad de la Información, Gestión ambiental, Sistema de Gestión de Seguridad y Salud en el Trabajo, desde su gestión soportada en sus lineamientos y procedimientos, se especifican las directrices para la atención de situaciones y contingencias que se puedan presentar. Estas situaciones son de diferente origen a saber: **Naturales** (vendavales, inundaciones, sismos) **Tecnológicas** (incendios, derrames de combustible. Fallas eléctricas, fallas estructurales, etc) y **Sociales** (Atentados, vandalismo, terrorismo), estos eventos súbitos pueden afectar las personas, las instalaciones, el medio ambiente, y hasta ocasionar pérdidas económicas. Por lo anterior, la Entidad se prepara de manera previsiva para poder afrontar este tipo de adversidades y salir adelante frente a las emergencias y sus consecuencias.

Se resalta que a través de sus planes de acción se definen los lineamientos y establece las acciones, para que junto con las Entidades que conforman el Sistema Distrital de Atención y Prevención de Emergencias, se pueda responder de manera eficaz ante una situación de contingencias, en el marco de los objetivos estratégicos y la misión de cada Entidad, también incluye el sistema organizacional de acuerdo a los protocolos Distritales de Respuesta definidos en el Plan de Emergencia de Bogotá.

El presente Plan de Contingencia tiene la finalidad de establecer los lineamientos y acciones preventivas, orientados a incrementar la capacidad de respuesta ante cualquier contingencia de tipo natural y/o generada por el hombre, así mismo el contar con un plan de emergencias que contempla la integración de personal de la entidad en las brigadas aplicando acciones y procedimientos establecidos para casos de siniestros. La prevención de emergencias es una de las más importantes acciones de un sistema de gestión de seguridad y salud en el trabajo por ello implica la cooperación, el compromiso y el apoyo decidido de todos los niveles organizacionales de la entidad.

2. JUSTIFICACIÓN

Este documento se elabora para ser constituido como un instrumento que referencia los mecanismos que cada componente de gestión asociado a los esquemas de Seguridad de la Información, Gestión ambiental, Sistema de Gestión de Seguridad y Salud en el Trabajo y comunicaciones, contemplando las medidas técnicas, humanas y organizativas necesarias para brindar la continuidad del negocio y las operaciones de la entidad.

La Entidad procura por el bienestar de sus funcionarios y de la comunidad en general, teniendo en cuenta los efectos de alta severidad que las emergencias pueden ocasionar, aplicando el marco normativo y las necesidades específicas que se generen en las sede administrativa o unidades de negocio en territorio del Instituto Para la Economía Social el IPES. Es por esto que la Entidad en su constante interés de velar por la seguridad de todos los colaboradores, contratistas, visitantes, clientes y comunidad en general; hace parte de la estructuración de lineamientos y procedimientos que permitirán dar respuesta a situaciones de riesgo tales como: sismo, incendios, explosión, terrorismo, entre otros; los cuales serán dados a conocer a todos los involucrados, garantizando así que ante la materialización de una situación de emergencia, el personal en general tenga claro las acciones a seguir y la organización cuente con los planes, procedimientos, recursos, suministros y servicios necesarios para obtener un alto nivel de efectividad en la atención de una emergencia.

3. OBJETIVOS

Contemplar un esquema institucional de contingencia que sirva como instrumento de gestión para el funcionamiento normal de la entidad, ante posibles amenazas de tipo interna o externo como son: de origen natural, antrópicos, humanos, salud ocupacional, técnicos, informáticos, entre otros.

Igualmente, específicamente se busca:

- Identificar y evaluar los riesgos que puedan generar emergencias dentro y fuera de la organización.
- Preservar los bienes y activos de los daños que se puedan generar como consecuencia de accidentes y emergencias, teniendo en cuenta no solo lo económico, sino lo estratégico para la organización y la comunidad del instituto.
- Responder oportunamente ante caso de una atención de emergencia.
- Conformar brigadas que puedan reaccionar en caso de una emergencia, mientras llegan los entes especializados.
- Definir programación de actividades que lleven al fortalecimiento de brigadas en respuesta a emergencias.
- Disponer de documento guía en cómo actuar en diferentes situaciones de emergencias.
- Identificar y llevar control de los equipos y sistemas que permitirán dar respuesta a una emergencia.
- Definir el o los puntos de encuentro a donde se dirigirán los colaboradores y visitantes en caso de presentarse una emergencia.
- Calcular el tiempo teórico de evacuación que permitirá realizar una intervención inmediata y eficaz de la Brigada integral durante la atención de las Emergencias.
- Cumplir con los requerimientos legales sobre emergencias establecidos por las entidades gubernamentales.

4. ALCANCE

Este Plan de Contingencia de TI del Instituto Para La Economía Social IPES, aplica para los esquemas de Seguridad de la Información, Gestión ambiental, Sistema de Gestión de Seguridad y Salud en el Trabajo y da cubrimiento a la sede principal ubicada en el Edificio

Torre 73 Calle 73 No 11 – 66 y las unidades de servicio contemplados en las Plazas de mercado, puntos comerciales y puntos de encuentro; dado que allí se centraliza la gestión misionalidad del IPES.

Lo anterior permitirá no solo responder a una necesidad de la entidad, además permitirá estar alineados al marco estratégico dentro de la política de Talento humano, Fortalecimiento Organizacional y Simplificación de Procesos y Política de Seguridad Digital de SIGD-MIPG, al igual que soportar la estructura orgánica y operativa emitida por los entes gubernamentales como el Instituto Distrital de Gestión de Riesgos y Cambio Climático Bogotá (IDIGER) que busca encaminar sus lineamientos hacia una cultura de prevención para evitar o mitigar la atención de una situación de emergencia. El presente documento cubre la evaluación de Plan de Emergencia y Contingencia de la sede administrativa y todas las unidades de servicio que cumplen con la misionalidad del Instituto Para la Economía Social - IPES.

5. RESPONSABLES

El cumplimiento del presente plan involucra a todo el personal vinculado al IPES, ya que las funciones de la entidad dependen de una u otra forma de su talento humano y sin la activa participación de funcionarios y contratistas vinculados a la gestión de los esquemas de Seguridad de la Información, Gestión ambiental, Sistema de Gestión de Seguridad y Salud en el Trabajo y de comunicaciones: que inciden en la misión Institucional de la entidad.

Se documentan a continuación los principales roles y cargos tienen especiales responsabilidades dentro del plan.

- Director (a) General del IPES
- Subdirector (a) de Diseño y Análisis Estratégico
- Subdirector (a) Administrativo y Financiero
- Subdirector (a) Jurídica y de Contratación
- Subdirectores misionales
- Jefe de la Oficina de Comunicaciones.
- Funcionarios y contratistas

6. DEFINICIONES Y ABREVIATURAS

- **ACCIDENTE:** Evento o interrupción repentina no planeada de una actividad que da lugar a muerte, lesión, daño u otra pérdida a las personas, a la propiedad, al ambiente, a la calidad o perdida en el proceso.

- **ACTIVACIÓN:** Despliegue efectivo de los recursos destinados a un incidente.

- **ALERTA:** Estado o situación de vigilancia sobre la posibilidad de ocurrencia de un evento cualquiera. O acciones específicas de respuesta frente a una emergencia.

- **AMENAZA:** Condición latente derivada de la posible ocurrencia de un fenómeno físico de origen natural, socio natural o antrópico no intencional, que puede causar daño a la población y sus bienes, la infraestructura, el ambiente y la economía pública y privada. Es un factor de riesgo externo.

- **ANÁLISIS DEL IMPACTO AL NEGOCIO (BIA POR SUS SIGLAS EN INGLÉS):** Proceso del análisis de actividades las funciones operacionales y el efecto que una

interrupción del negocio podría tener sobre ellas. [Fuente: ISO 22300]

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

- **CIERRE OPERACIONAL**: desmovilización total de recursos.

- **CIERRE ADMINISTRATIVO:** realización de la reunión posterior al finalizar el ejercicio, la revisión y recopilación de los formularios correspondientes, la preparación y entrega del informe final a la gerencia.

- **COORDINADOR:** persona que dirige las acciones de dirección del Plan.

- **COMITÉ LOCAL DE EMERGENCIAS – CLE:** es el órgano de coordinación interinstitucional local, organizado para discutir, estudiar y emprender todas aquellas acciones encaminadas a la reducción de los riesgos específicos de la localidad y a la preparación para la atención de las situaciones de emergencia que se den en ésta y cuya magnitud y complejidad no supere sus capacidades. Sus funciones están determinadas en el artículo 32 del Decreto 332/2004.

- **DHCP:** protocolo de configuración dinámica de host

- **DNS:** sistema de nombres de dominio

- **ERP:** Planificación de Recursos Empresariales

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

- **INCIDENTE o EVENTO:** Suceso de causa natural o por actividad humana que requiere la acción de personal de servicios de emergencias para proteger vidas, bienes y ambiente.

- **IDIGER:** Instituto Distrital de Gestión de Riesgos y Cambio Climático.

- **MAPA:** Representación geográfica en una superficie de la tierra o de parte de ella en una superficie plana.

- **MEC:** Módulo de Estabilización y Clasificación de Heridos.

- **MEDIDAS DE SEGURIDAD:** Son aquellas acciones, para disminuir la probabilidad de un evento adverso.

- **MITIGACIÓN:** Toda acción que se refiere a reducir el riesgo existente.

- **MODO DE FALLA:** Manera forma en por la cual se observa una falla es observada. (Fuente: Guía No. 10, versión 1 – MSPI – MinTIC)

- **MTD:** En la columna MTD (Máximo tiempo tolerable de interrupción) se registra el tiempo máximo que se puede tolerar si servicio.

- **NIVEL DE CRITICIDAD:** Descripción cualitativa usada para enfatizar la importancia de unrecurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra. NOTA: Esta generalmente describe la manera en que la falla ocurre y su impacto para en la operación del sistema. (Fuente: Guía No. 10, versión 1 – MSPI – MinTIC)

- **OBJETIVO DE SEGURIDAD:** Es quién vigila las condiciones de seguridad e implementa medidas para garantizar la seguridad de todo el personal involucrado.

- **PAI:** Plan de Acción del Incidente, expresión de los objetivos, estrategias, recursos y organización a cumplir durante un periodo operacional para controlar un incidente.

- **PLAN DE EMERGENCIA:** El Plan de Emergencia y Contingencias es el instrumento principal que define las políticas, los sistemas de organización y los procedimientos generales aplicables para enfrentar de manera oportuna, eficiente y eficaz las situaciones de calamidad, desastre o emergencia, en sus distintas fases. Con el fin de mitigar o reducir los efectos negativos o lesivos de las situaciones que se presenten en la Organización.

- **PLANIFICAR:** Formular objetivos y determinar las actividades y los recursos para lograrlos.

- **PLANO:** Representación gráfica en una superficie y mediante procedimientos técnicos, de un terreno, de la planta de un edificio, entre otros.

- **PMU:** Puesto de Mando Unificado; Lugar donde se ejerce función de comando. Es una función prevista en el Sistema Comando de Incidentes (SCI) y esta se aplica cuando varias instituciones toman acuerdos conjuntos para manejar un incidente donde cada institución conserva su autoridad, responsabilidad y obligación de rendir cuentas.

- **PROCEDIMIENTO OPERATIVO NORMALIZADO:** Es la base para la realización de tareas necesarias y determinantes para el control de un tipo de emergencia. Define el objetivo particular y los Responsables de la ejecución de cada una de las acciones operativas en la respuesta a la Emergencia.

- **PREPARACIÓN:** Toda acción tendiente a fortalecer la capacidad de las comunidades de responder a una emergencia de manera eficaz y eficiente.

- **PREVENCIÓN:** Toda acción tendiente a evitar la generación de nuevos riesgos.

- **PUNTO DE ENCUENTRO:** Sitio seguro, definido para la llegada del personal en caso de evacuación.

- **PUNTO OBJETIVO DE RECUPERACIÓN (RPO):** Punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra. (Fuente: Guía No. 10, versión 1 – MSPI – MinTIC)

- **RECURSO:** Equipamiento y persona disponibles o potencialmente disponibles para su asignación táctica a un incidente.

- **RIESGO:** El daño potencial que, sobre la población y sus bienes, la infraestructura, el ambiente y la economía pública y privada, pueda causarse por la ocurrencia de amenazas de origen natural, socionatural o antrópico no intencional, que se extiende más allá de los espacios privados o actividades particulares de las personas y organizaciones y que por su magnitud, velocidad y contingencia hace necesario un proceso de gestión que involucre al Estado y a la sociedad.

- **SCI:** Sistema Comando de Incidentes. Es la combinación de instalaciones, equipamientos, personal, procedimientos y comunicaciones, operando en una estructura organizacional común, con la responsabilidad de administrar los recursos asignados para lograr efectivamente los objetivos pertinentes a un evento, incidente u operativo.

- **SDPAE:** Sistema Distrital de Prevención y Atención de Emergencias; el cual se adopta bajo el Decreto 332 del 11 de Octubre de 2004.

- **SERVICIOS:** Son todos aquellos servicios que satisfacen las necesidades básicas de la población.

- **SISTEMA DE ALARMA:** Medio audible y/o visual que permite avisar que ocurre un evento y pone en riesgo la integridad de personas, animales o propiedades.

- **RECUPERACIÓN DE DESASTRES DE TECNOLOGÍA Y TELECOMUNICACIONES (ITCTIC):** Habilidad Capacidad de los elementos de tecnología y telecomunicaciones (ITC) de las TIC de la organización para soportar sus funciones críticas a un nivel aceptable dentro de un periodo predeterminado de tiempo después de una interrupción. (Fuente: Guía No. 10, versión 1 – MSPI – MinTIC)

- **RTO:** Es el tiempo máximo disponible para la restauración de los sistemas que soportan el servicio antes de que se presenten impactos inaceptables para el IPES, el RTO no puede ser mayor al MTD.

- **SaaS:** Software como Servicio

- **SITIO ALTERNO:** Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción. (Fuente: Guía No. 10, versión 1 – MSPI – MinTIC)

7. DESARROLLO

7.1 INFORMACIÓN GENERAL DEL INSTITUTO

Razón Social: INSTITUTO PARA LA ECONOMIA SOCIAL – IPES.

La Reforma administrativa adelantada por el Distrito Capital y contenida en el Acuerdo No. 257 de 2006, que establece la estructura, organización y funcionamiento general de la Administración Distrital, transforma el Fondo de Ventas Populares FVP en Instituto para la Economía Social - IPES - , establecimiento público del orden distrital, con personería jurídica, autonomía administrativa y patrimonio propio, adscrito a la Secretaría Distrital de Desarrollo Económico.

El Artículo 79 del citado Acuerdo define las siguientes funciones del Instituto para la Economía Social IPES:

Definir, diseñar y ejecutar programas, en concordancia con los planes de desarrollo y las políticas trazadas por el Gobierno Distrital, dirigidos a otorgar alternativas para los sectores de la economía informal a través de la formación de capital humano, el acceso al crédito, la inserción en los mercados de bienes y servicios y la reubicación de las actividades comerciales o de servicios.

Gestionar la consecución de recursos con entidades públicas, empresas privadas, fundaciones u Organizaciones No Gubernamentales ONG- nacionales e internacionales para ampliar la capacidad de gestión de la entidad y fortalecer la ejecución de los programas y proyectos

Adelantar operaciones de ordenamiento y de relocalización de actividades informales que se desarrollen en el espacio público.

Administrar las plazas de mercado en coordinación con la política de abastecimiento de alimentos.

Adelantar operaciones de construcción y adecuación de espacios análogos y conexos con el espacio público con miras a su aprovechamiento económico regulado.

Ejecutar programas y proyectos para el apoyo a microempresas, famiempresas, empresas asociativas, e implementar el micro crédito, en los sectores de la economía popular.

PLAZAS DE MERCADO

No.	Plaza	Dirección Plaza
1	Quiriguá	Calle 90 No. 91 – 52
2	Doce de Octubre	Calle 72 No. 51 – 62
3	Fontibón	Calle 19 No. 103 - 26/10
4	Kennedy	Calle 42 No. 78M - 50 Sur
5	La Concordia	Calle 14 No. 1 – 40
6	La Perseverancia	Carrera 5 No. 30ª – 30
7	Las Cruces	Calle 1F No. 4 – 60
8	Las Ferias	Av. Rojas No. 74 – 52
9	Los Luceros	Carrera. 17F No. 69ª - 32 Sur

10	El Restrepo	Cra. 19 No. 18 - 51 sur
11	Samper Mendoza	Carrera 25 No. 22ª – 73
12	San Benito	Carrera 19C No. 50ª - 90 Sur
13	San Carlos	Carrera 17F No. 69 – 32 Sur
14	El Carmen	Dg. 49 sur No. 29ª – 07
15	Santander	Calle 26 sur No. 30 – 51
16	Siete de Agosto	Calle 66 No. 23 – 20
17	Trinidad Galán	Carrera 60 No. 5 – 00
18	Veinte de Julio	Carrera 6 No. 24 - 60 Sur

Adicionalmente el IPES cuenta con la Plaza BOYACÁ REAL (Carrera 68B No. 73ª – 45) que actualmente no tiene Servicios o infraestructura TI

Puntos Vive Digital: El IPES tiene a cargo Dos (2) Puntos Vive Digital (PVD) ubicados en los barrios de VERACRUZ situada en la localidad de Santa Fe de la ciudad de Bogotá y KENNEDY ubicada al suroccidente de la ciudad de Bogotá.

Bodega 38: Una (1) sede conocida como Bodega 38 la cual está ubicada en el sector conocido como San Andresito de la 38 en la ciudad de Bogotá.

7.2. ANÁLISIS DE IMPACTO AL NEGOCIO

Esta sección del plan de contingencia contiene el análisis de impacto al negocio para el proceso de gestión de seguridad de la información y recursos tecnológicos del IPES, esta sección del documento forma parte del proceso de planificación de la contingencia para los sistemas de información crítica del IPES.

7.3. PROPÓSITO Y ETAPAS DEL BIA (BUSINESS IMPACT ANALYSIS)

El propósito del BIA es identificar y priorizar los componentes de los sistemas de información, correlacionarlos con los procesos misionales que los soportan y de esta forma caracterizar el impacto que sobre estos procesos se presenta en caso de que no estén disponibles. El BIA está compuesto por:

- Identificación de los procesos misionales y criticidad de recuperación: En primera instancia se identifican los procesos misionales que son soportados por sistemas, el impacto que sobre los procesos genera la suspensión de los sistemas y el tiempo estimado de suspensión. El tiempo de suspensión debe reflejar el máximo tiempo que la entidad puede soportar la suspensión de servicios sin incumplir su función misional.

- Identificación de requerimientos de recursos: La identificación realista de los esfuerzos necesarios para recuperar los sistemas implica una evaluación detallada de los recursos necesarios para reactivar los procesos misionales y la identificación de las interdependencias entre recursos y sistemas. Algunos de los elementos que se deben considerar incluyen: personal, instalaciones, equipos, software, archivos de datos, componentes de los sistemas y registros vitales.

● Identificación de las prioridades de recuperación de recursos y sistemas: Basados en los resultados de la identificación de requerimientos se verifican las dependencias entre los sistemas y los procesos críticos de la entidad para determinar las prioridades de recuperación para establecer la secuencia de recuperación de las actividades y recursos.

Este documento se usa como entrada para construir el plan de contingencia de los procesos críticos. Este BIA puede ser usado como entrada a planes de recuperación ante desastres y los procedimientos de respuesta a incidentes de seguridad de la información.

7.4. IDENTIFICACIÓN DE PROCESOS Y SISTEMAS CRÍTICOS

Para formular el BIA del IPES se realizó un inventario de los procesos críticos y se determinaron los siguientes parámetros:

- Periodicidad de entrega: corresponde a la periodicidad en el tiempo de cómo cada proceso debe entregar resultados. Los parámetros de periodicidad definidos son: Diariamente, Semanalmente, Quincenalmente, Mensualmente, Bimensualmente, Trimestralmente, Semestralmente, Anualmente

- Evaluación de Tiempo de interrupción no programada: Este parámetro se utiliza para establecer cuál sería el tiempo máximo que un proceso crítico puede soportar una suspensión del sistema de información. Los posibles valores son:

  7: No se puede esperar, el proceso nunca se puede detenerse,

  6: Puede esperar, pero solo máximo 1 a 2 horas

  5: Puede esperar entre 3 y 5 horas

  4: Puede esperar hasta 1 día (8 horas)

  3: Puede esperar entre 2 y 3 días

  2: Puede esperar entre 4 y 5 días

  1: puede esperar más de 5 días

Tiempo de interrupción no programada tolerable servicios críticos

Nombre del servicio	Periodicidad de entrega (día, semanal, quincena, mes, bimensual, trimestral, semestral, anual)	Tiempo de interrupción no programa tolerable (Ver Evaluación de Tiempo de interrupción no programada)	Descripción del servicio
Sistema de información HEMI	El servicio se presta diariamente, el sistema de información HEMI funciona en modalidad 7x24	De acuerdo con la dinámica de utilización de los servicios de HEMI el tiempo máximo previsto para interrupción no programa de servicio HEMI está en 1 día (8 horas)	Sistema de información misional
GOOBI	El servicio se presta diariamente, el sistema de información GOOBI Se utiliza en modalidad 5 x 8 y en casos especiales sábado y domingos	El sistema de información GOOBI tiene fechas críticas de prestación de servicio que determinan diferentes tiempos de interrupción no programada entre 3 a 5 horas.	Sistema de información Financiero Administrativo

Almacenamiento compartido	El servicio se presta diariamente, la operación del servicio es 7x24 pero los usuarios solo tienen acceso al servicio desde las instalaciones de la red LAN de IPES	De acuerdo con la dinámica de utilización de los servicios el tiempo máximo previsto para interrupción no programa de servicio está en 3 a 5 horas	Permite el almacenamiento de archivos compartidos en drive compartido
Correo electrónico	El servicio se presta diariamente, la operación del servicio es los usuarios pueden tener acceso al servicio desde las instalaciones de la red LAN de IPES, el almacenamiento de los buzones de correo se realiza en la estación de trabajo de cada usuario.	El servicio de correo electrónico depende de la conectividad a Internet, ya sea interna o externa. tiempo máximo previsto para interrupción no programa de servicio está en 1 a 2 horas	Permite él envió y recepción de correos electrónicos.

Identificación de impactos y valoración de tiempo no disponible

Las siguientes categorías representan las áreas de mayor importancia que se deben evaluar por el impacto de incidentes en los procesos críticos.

- Impacto Financiero: Impactos relacionados con pérdida económica o multas. En el caso de las entidades del gobierno, el impacto financiero por pérdidas económicas siempre es severo.

- Impacto Operacional: Incumplimiento en los plazos para cumplir compromisos de la entidad. Capacidad para cumplir los compromisos misionales.

Criterios para cálculo de impactos de los eventos

Criterio	Impacto Severo (5)	Impacto Alto (3)	Impacto moderado (1)
Financiero	No es admisible ninguna clase de pérdida económica	No aplica	No aplica
Operacional (oportunidad para el cumplimiento de compromisos)	No se cumple el compromiso en ningún plazo. Es decir no se hace el trabajo	El compromiso no se cumple en la fecha establecida, se cumple en otra fecha y la entidad queda obligada a elaborar un plan de mejora para resolver el no cumplimiento	El compromiso no se cumple en la fecha definida, se cumple en fecha posterior pero no se requiere un plan de mejora para resolver el no cumplimiento
Satisfacción de interesados (ciudadano, otras entidades, entes de control	No se puede cumplir la misión institucional	Se cumple en forma parcial la misión institucional	Se cumple la misión institucional con variaciones que no afectan a los interesados

7.5. IDENTIFICACIÓN DE IMPACTOS POR SERVICIOS

El impacto a nivel de servicios permite determinar que puede ocurrir a nivel financiero e impacto operacional en caso de no disponibilidad de alguno de los servicios considerados como críticos para el cumplimiento de la función misional.

Impactos por servicios

Proceso	Impacto financiero	Impacto operacional		Impacto global
		Oportunidad (cumplir en los plazos)	Satisfacción (cumplir el alcance)	
HEMI	No aplica, HEMI no soporta obligaciones financieras en el IPES	(1) Impacto moderado. La entidad registra sus compromisos y tareas en el sistema HEMI, pero como el procesamiento se puede hacer fuera de línea con lo cual el cumplimiento de las obligaciones en cuanto a función misional se puede cumplir en caso de falla de HEMI	(3) Impacto Alto La entidad cumple con sus funciones de manera continua aún sin acceso a HEMI. A nivel de entes de control y partes interesadas en el cumplimiento de la función de IPES se necesita la entrega de información consistente por lo que el uso de HEMI en fundamental para presentar informes unificados de operación de la Entidad	(4)
(GOOBI) OPGET	(5) Impacto severo No es admisible ninguna clase de pérdida económica	(5) impacto severo No se cumple en compromiso en ningún plazo. Es decir no se hace el trabajo	(3) impacto alto Se cumple en forma parcial la misión institucional	13
(GOOBI) PREDIS	(5) No es admisible ninguna clase de pérdida económica	(5) impacto severo No se cumple en compromiso en ningún plazo. Es decir no se hace el trabajo	(5) impacto severo No se puede cumplir la misión institucional	15

Almacenamiento compartido	No aplica el almacenamiento compartido no soporta operaciones financieras	(5) impacto severo La disponibilidad de la información para toma de decisiones y presentación de informes es fundamental para el cumplimiento de la misión, cuando no existe acceso al drive compartido se debe recurrir a los archivos locales almacenados en las estaciones de trabajo, o archivos almacenados en las herramientas de la nube bajo G-SUITE	(5) impacto severo Los usuarios del servicio depende de su información almacenada para la realización de sus trabajos, pero puede operar con las réplicas de información que almacenan en sus estaciones de trabajo local o archivos almacenados en las herramientas de la nube bajo G-SUITE	10
Correo electrónico	No aplica el almacenamiento compartido no soporta operaciones financieras	(5) impacto severo La interrupción de los servicios de correo electrónico implica la ausencia de comunicación entre actividades y procesos de la entidad	(3) Impacto alto La comunicación con las partes interesadas se demora y se pueden presentar no cumplimientos en compromisos de entrega de información.	8

7.6. IDENTIFICACIÓN DE TIEMPOS Y OBJETIVOS DE RECUPERACIÓN

MTD: En la columna MTD (Máximo tiempo tolerable de interrupción) se registra el tiempo máximo que se puede tolerar sin servicio

RTO: Es el tiempo máximo disponible para la restauración de los sistemas que soportan el servicio antes de que se presenten impactos inaceptables para el IPES, el RTO no puede ser mayor al MTD.

RPO: Es la pérdida tangible de datos entre la copia de seguridad y un incidente

Identificación de tiempos y objetivos de recuperación

Nombre del Proceso	MTD Máximo tiempo tolerable de interrupción	RTO Tiempo objetivo de recuperación	RPO Punto Objetivo de recuperación
HEMI	1 día	2 horas	Diario
GOOBI	Hasta 1 día cuando no se está en fecha crítica o de entrega de información En fechas críticas de entrega de información el sistema el MTD no debe superar las 2 horas	1 día	Diario
Almacenamiento compartido	Hasta 1 día	1 día	Diario
Correo electrónico	Hasta 6 horas	2 horas	Diario

7.7. PRIORIDADES DE RECUPERACIÓN

La siguiente tabla registra las prioridades de recuperación de las funcionalidades del IPES en caso de un incidente mayor, los resultados se basan en los impactos financieros y operacionales derivados de una falla en los servicios analizados

Prioridades de recuperación – servicios de TI

Prioridad	COMPONENTE	DESCRIPCIÓN TÉCNICA
1	GOOBI	Sistema de información Financiero administrativo. En caso de falla mayor en los sistemas de información, la prioridad es recuperar este sistema debido a que su falla puede implicar sanciones para la entidad.
2	Correo electrónico	Debido a la dependencia de los servicios de correo para la comunicación misional el servicio de correo debe ser recuperado con segunda prioridad
3	Almacenamiento compartido	Tercera prioridad de recuperación, la no disponibilidad de la información afecta directamente la función misional de la Entidad. Prioridad Media
4	HEMI	La naturaleza del IPES implica el cumplimiento de estrategias que no son actividades de realización inmediata, el sistema de información HEMI permite el registro de las acciones para el cumplimiento de la Misión. En caso de fallas simultáneas en varios servicios críticos es prioritario recuperar los sistemas financieros, sistemas de almacenamiento de información, sistema de comunicación vía correo y finalmente el sistema HEMI que dada su infraestructura redundante tiene capacidad para recuperación inmediata.

7.8. ESCENARIOS DE RIESGO

La activación del plan de contingencia debe considerar los efectos que para los procesos misionales de la entidad tendrían la ocurrencia de riesgos cuyas consecuencias sean pérdida de disponibilidad en la prestación del servicio o pérdida de la integridad de la información que ponga en riesgo la capacidad operacional de la entidad para cumplir su función misional. Las combinaciones de amenazas (causas) y consecuencias (perdida de disponibilidad e integridad) generan los escenarios de riesgo bajo los cuales el comité de contingencia debe determinar si se autoriza o no la activación del plan de contingencia.

Dentro del análisis de riesgos de seguridad de la información se pueden encontrar información detallada sobre las estrategias para mitigar las vulnerabilidades y controles que se pueden aplicar para reducir el impacto o probabilidad de ocurrencia de los riesgos que activarían el plan de contingencia.

Todos los incidentes de seguridad de la información deben ser manejados inicialmente por el procedimiento de gestión de incidentes de seguridad de la información. En ese procedimiento se definen los parámetros iníciales para la atención de los incidentes.

En los casos en los que el incidente de seguridad ya no puede manejarse por los procedimientos normales de la mesa de ayuda, se debe proceder al escalamiento del incidente al coordinador del plan de contingencia quién debe seguir los pasos de notificación y evaluación del incidente para tramitar la autorización de activación del plan de contingencia ante la persona o personas responsables de esta acción.

Escenarios de riesgo generales

A partir de los resultados del análisis de impacto al negocio, se describen a continuación los escenarios de riesgos generales que pueden afectar al sistema y cuyas consecuencias generarían perdida de disponibilidad de servicios con la consecuente necesidad de activación del plan de contingencia.

- Debido a una ausencia o falta de mantenimiento en los equipos de energía o en los equipos activos de comunicaciones, los equipos dentro de los datacenter que soportan los sistemas de información del IPES pueden fallar.
- Debido a una ausencia o falta de mantenimiento en los servidores, los sistemas de información del IPES pueden funcionar mal o fallar.
- Cuando no se cuenta con sistemas centralizados de monitoreo y alarma, se presentan fallas en los equipos o en los servicios informáticos del IPES, por lo que no se tiene una respuesta rápida a los eventos y se presentan pérdidas en la efectividad para el cumplimiento de las funciones de la organización.

Escenarios de riesgo asociados a pérdida de disponibilidad

Dentro de las amenazas estudiadas en el análisis de riesgos del sistema de gestión de seguridad de la información del IPES que podrían generar perdida de disponibilidad de los servicios, se tienen los siguientes escenarios de riesgos:

- Cuando no se realizan análisis periódicos de riesgos o no están en constante supervisión y actualización las políticas de seguridad de los equipos de seguridad perimetral, se pueden tener ataques por denegación de servicios.
- Debido a una ausencia o falta de mantenimiento en los servidores y en las bases de datos de los sistemas de información del IPES, se puede presentar un mal funcionamiento en la base de datos.
- Se puede presentar robo de información debido a un acceso no autorizado a una aplicación, ya que no existe un procedimiento formal para desvinculación o eliminación de usuarios.
- Debido a la humedad, polución y otros factores, y ante la ausencia de espacios físicos adecuados para almacenamiento de documentos, se pueden perder o destruir registros o documentos importantes para la entidad.
- Debido al uso de tecnología ineficiente para gestión de archivos, y la no aplicación de procedimientos de gestión documental, se puede presentar daño o pérdida de registros y documentos.

- Puede haber un abuso de derechos o accesos no autorizados, debido a una inadecuada asignación de permisos en la información que se encuentra compartida con lo que se perdería la integridad, confidencialidad y disponibilidad de la información.
- Debido a que los usuarios no cuentan con una práctica adecuada para el uso de las herramientas colaborativas en la plataforma de Google Drive, Correo electrónico y demás bridadas por G-Suite

Escenarios de riesgo asociados a la pérdida de integridad

Las amenazas asociadas a la pérdida de integridad de los sistemas de información pueden derivar en los siguientes escenarios de riesgos:

- Se puede presentar un tratamiento deficiente de la información por falta de disponibilidad de personal debido a la alta rotación de funcionarios.
- Puede haber un abuso de derechos o accesos no autorizados, debido a una inadecuada asignación de permisos en la información que se encuentra compartida con lo que se perdería la integridad, confidencialidad y disponibilidad de la información.
- Hay un error en el uso de los sistemas y los procesos debido a un procedimiento inadecuado de inducción del personal, con lo que se puede presentar una manipulación o procesamiento inadecuado de la información, lo que puede derivar en una corrupción de datos no intencional.

7.9. CONTROLES PREVENTIVOS

En esta sección se describirán los mecanismos de control que se tienen implementados en el IPES para mitigar los impactos de incidentes que afecten la disponibilidad de los servicios de información y tecnología identificados como críticos.

Capacidad de Planta Eléctrica y UPS:

El IPES cuenta con UPS, una para los servidores y otra para los computadores conectados al circuito regulado del cableado estructurado. En caso de una falla de energía, los UPS suministraran potencia por un período de tiempo limitado por la autonomía de las UPS dependiendo de la capacidad de las baterías.

En caso de un corte de energía mayor al 30% del tiempo de autonomía real del UPS de servidores y equipos activos deberían iniciarse las labores de bajado de servicios y apagado sincronizado, labor que en lo posible debe hacerse de forma automática ya que el corte se puede presentar en horario donde no hay personal de atención de equipos. En el caso de los Computadores personales el personal del IPES debería iniciar de inmediato el proceso de apagado de los equipos.

De acuerdo a lo anterior, en los mantenimientos preventivos de las UPS, deben hacerse pruebas de funcionamiento de UPS y medición de autonomía de baterías para conocer la capacidad real de tiempo con que se cuenta en caso de falla de energía comercial. Para las baterías las pruebas mínimas de autonomía deben realizarse por lo menos una vez por semestre.

Otra de las tareas a ejecutar es la de realizar un estudio de cargas teórico y real de los equipos que son alimentados por las UPS y actualizarlo de acuerdo a los cambios como instalación de nuevos equipos, retiro de equipos o potenciación de equipos o cambio de partes, esto con el fin de mantener actualizado los requerimientos de potencia de equipos informáticos.

Capacidad de los sistemas de refrigeración.

El Datacenter del IPES, cuenta con un aire acondicionado, que brinda la sensación térmica es suficiente para el correcto funcionamiento de los equipos.

Considerando que a la fecha no se cuenta con registros de mediciones de temperatura y humedad del aire por medio de termómetros e higrómetros que permitan alarmar el sistema y dar orden de apagado de servidores en caso que se presenten temperaturas perjudiciales para los equipos. Es necesario realizar verificaciones diarias de las condiciones ambientales del data center.

De acuerdo a lo anterior se debe formular un proyecto para la instalación equipos medidores de temperatura y humedad integrados al monitoreo del sistema, así mismo se debe hacer un estudio de cargas de temperaturas de equipos y mantenerlo actualizado de acuerdo a la instalación o retiro de equipos.

Sistema de extinción de incendio

El IPES no cuenta con un sistema de extinción de incendios. En la actualidad solo se cuenta con extintores manuales los cuales son de utilidad en el momento que haya personal de brigadas en caso de que se presente un incidente de fuego y no cuando están desatendidos como es en las noches. Es necesario realizar verificaciones periódicas de las condiciones ambientales del data center y formular un proyecto de implementación de un sistema de protección contra incendios en el Datacenter.

Por lo anterior se debe implementar un sistema de extinción de incendio automático con supervisión integrada al sistema de monitoreo general, con un programa de mantenimiento periódico.

Sistemas de monitoreo de capacidad de servidor.

Las herramientas de monitoreo de los recursos de tecnología (incluidas variables fundamentales del servidor y ancho de banda de canales), son necesarias para establecer comportamientos de los recursos de tecnología y predecir incidentes. El Monitoreo de la capacidad de servidores es una medida preventiva frente a incidentes de seguridad de la información. Sin embargo, en la actualidad el monitoreo se realiza manualmente a través de los profesionales a cargo de la infraestructura de TI, y se encuentra en proceso de implementación de la herramienta NAGIOS para automatizar el monitoreo

Sistemas de monitoreo de aplicación

En la actualidad no se cuenta con herramientas centralizadas de monitoreo de las aplicaciones. Una de las oportunidades de mejora para el plan de contingencia incluye la implantación de

herramientas de supervisión que permitan identificar comportamientos anómalos en las aplicaciones y así prevenir incidentes

Sistemas de monitoreo de base de datos

En la actualidad no se cuenta con herramientas centralizadas de monitoreo base de datos. Una de las oportunidades de mejora para el plan de contingencia incluye la implantación de herramientas de supervisión de bases de datos que permitan identificar comportamientos anómalos y así prevenir incidentes. La segunda estrategia que es prioritaria para mejorar los tiempos de recuperación es fortalecer las capacidades internas para la administración de bases de datos (DBA) que permitan realizar actividades de afinamiento, supervisión y recuperación de bases de datos.

Sistemas de almacenamiento de copias de respaldo

La infraestructura actual cuenta con un servidor dedicado de BackUP, el cual tiene tareas automáticas de respaldo sobre:

- La información digital que reposa en los servidores físicos y virtuales institucionales.
- Respaldo sobre el S.O. y la configuración de las máquinas virtuales que soportan el 90% de la operación institucional.
- De acuerdo con el resultado del BIA, la periodicidad del respaldo de datos para los diferentes sistemas de información críticos del IPES se realiza de acuerdo a lo estipulado por el procedimiento BACKUP GENERACIÓN Y RECUPERACIÓN.
- A través del servidor BACKUP se realiza de manera automática y conforme a la criticidad de la información – tareas de respaldo.

Respecto al Servicio de Correo Electrónico, el IPES cuenta con los servicios brindados por un proveedor, mediante el cual se adquirieron cuentas de nivel Business de la plataforma GSUITE, de tal forma que el correo electrónico y demás funcionales como Drive, Calendario, Formularios, entre otros, cuentan con respaldo en la nube de internet, esto de acuerdo a la categoría Business ofrecida por GOOGLE.

Destacando de lo anterior, que al interior del IPES se adoptó el uso de FileStream – Google Drive, como herramienta para el almacenamiento digital de la información de cada usuario, y como herramienta colaborativa, las áreas y procesos hacen el uso de carpetas compartidas a través de Google Drive.

Sistemas de protección de la seguridad de la información

Los resultados del análisis de brecha del sistema de gestión de seguridad de la información del IPES indican que los puntos de vulnerabilidad más delicados de los sistemas son:

- Debilidades en la toma de conciencia en seguridad de la información: Para mitigar incidentes generados por amenazas externas como denegación de servicio e infiltración es necesario promover la cultura de uso seguro de los sistemas de información.
- Análisis de Vulnerabilidades: Pruebas técnicas para identificar debilidades y tomar las medidas necesarias.

- Almacenamiento de código de fuente: Siguiendo las recomendaciones de la norma de gestión de seguridad de la información, el código fuente de las aplicaciones de misión crítica debe ser respaldado siguiendo las buenas prácticas de la industria.
- Controles de auditoría: Todas las aplicaciones misionales deben ser sometidas al menos una vez al año a auditorias de sistemas y auditorias de seguridad de la información siguiendo las recomendaciones del sistema de gestión de seguridad de la información y el área de control interno.
- Cuando falla un sistema de información o un servicio informático, y no se tiene un sistema centralizado de monitoreo que alerte a una persona de contacto de la falla, puede pasar bastante tiempo hasta que la persona que administra el servicio se entere de la falla y la repare.
- Se presente un evento o incidente de seguridad de la información y no existe un procedimiento formal para comunicarlo o reportarlo, puede pasar que se acumulen eventos que degraden la seguridad de la información de la entidad.
- Si no se tiene un procedimiento documentado de control de cambios y se tenga que hacer un mantenimiento o un cambio que involucre algún activo de seguridad de la información, puede pasar que la actividad no culmine con los resultados esperados y pueda comprometer la seguridad de otros activos.
- Por un daño en el disco duro o un malware que contamino un PC, el usuario puede perder los datos.
- Se puede presentar robo de información debido a un acceso no autorizado a una aplicación, ya que no existe un procedimiento formal para desvinculación o eliminación de usuarios.

La implementación de las acciones de mitigación de estas vulnerabilidades reduciría la posibilidad de ocurrencia de incidentes de seguridad de la información que impliquen la activación del plan de contingencia.

7.9. DEFINICIÓN DE LAS ESTRATEGIAS DE CONTINGENCIA

Uso de site alterno

- Escenario: No se puede usar la sede principal del IPES y el centro de cómputo no es apto para correr las aplicaciones.
- Alternativa: Centro alterno en instalaciones del IPES diferente a la sede principal

Debido a que el BIA identificó que los tiempos máximos de restablecimiento de los servicios en fecha crítica son de 2 días, la estrategia de contingencia en caso de falla del centro de cómputo principal es:

Estrategia de Site Alterno

Nombre del servicio	Estrategia de Site Alterno
Sistema de información HEMI	La entidad determinará emplear una de sus sedes para instalar un servidor de contingencia, de tal forma que se realice la puesta en operación del mismo y se realice la publicación de su servicio web.
GOOBI	El establecimiento de un acuerdo con la Secretaría de Hacienda para desplazar a dos funcionarios responsables de registrar la información vital de GOOBI directamente en la secretaría de Hacienda. La estrategia se activaría sólo en fallas que se presenten en fechas críticas de entrega de información.
Almacenamiento compartido	Aunque es factible la reinstalación del servidor en donde se almacenaban los datos del Drive U antes de la instalación de la NAS, los usuarios cuentan con copias de su datos en los computadores personales, la relación de Beneficio/Complejidad de la estrategia no viabiliza el plan
Correo electrónico	La afectación de la Sede Principal no generaría consecuencias sobre la disponibilidad del servicio de correo electrónico, ya que tanto este servicio como los archivos almacenados en Google Drive, están alojados en la nube de internet. Y su disponibilidad está sujeta al canal de internet al cual se conecte el usuario que requiera su uso.

Centro alterno en acuerdo con otra entidad

Esta estrategia se aplicaría en caso de que el IPES establezca acuerdo para reubicación de sus sistemas de información en el centro de cómputo de otra entidad, la estrategia depende de los acuerdos establecidos. Para los efectos del presente plan de contingencia no se cuenta con acuerdos con otra entidad.

Centro alterno contratado

Esta estrategia se aplicaría en caso de que el IPES contará con un contrato para uso de site alterno con un proveedor de servicios de tecnología. Para los efectos del presente plan de contingencia no se cuenta con acuerdos con proveedor externo a excepción del correo electrónico tal como se ha mencionado en ítems anteriores.

Identificación de equipos

Los siguientes equipos son esenciales para la operación del plan de contingencia. Los equipos se aprovisionan de acuerdo con la evaluación que se realice durante la fase de evaluación y activación del plan de contingencia.

- Servidor de BackUP
- Servidores de sistemas de información
- Switches y firewall
- Fuentes de GOOBI
- Fuentes de sistema operacional
- Copias de respaldo de imágenes de los servidores virtuales
- Fuentes de motor de base de datos
- Copia de respaldo de base de datos de GOOBI
- Copia de respaldo de base de datos de HEMI
- Estaciones de trabajo de usuario final

Acuerdos con proveedores

Los siguientes acuerdos para apoyo son esenciales para la correcta operación del plan de contingencia.

- Soporte del servidor de backup
- Soporte de hardware y sistemas operacionales de servidores
- Soporte de aplicación GOOBI
- Soporte de hardware y software de Switches y Firewall
- Soporte de hardware y software de NAS
- Acuerdos para cargue de datos en secretaria de hacienda
- Acuerdos con proveedor de acceso a Internet (ETB)

Fase de notificación y activación

A continuación, se relacionan las fechas críticas dentro del año en las que los procesos misionales del IPES requieren disponibilidad de los sistemas de información. Durante esas fechas se debe reforzar la aplicación de los controles preventivos, verificación del correcto funcionamiento de aplicaciones e infraestructura de Información y Tecnología. Uno de los criterios fundamentales para activar el plan de contingencia es la ocurrencia de incidentes durante esas fechas.

Daños en componentes de tecnología

Sistema o Servicio de Información y tecnología	Fechas críticas dentro del año
HEMI	Diario - días hábiles
GOOBI	7 hábiles antes del fin de cada mes- Todo el mes de diciembre
Almacenamiento compartido	Diario - días hábiles
Correo electrónico	Diario - días hábiles

7.10. IDENTIFICACIÓN DE INCIDENTES

El grupo de sistemas del IPES debe seguir los procedimientos de gestión de incidentes de tecnología y gestión de incidentes de seguridad. En el caso del procedimiento de gestión de incidentes cuando se realice un escalamiento de segundo nivel al grupo de especialistas y no se obtenga solución al incidente se debe iniciar un proceso de evaluación de activación del plan de contingencia.

La evaluación de la necesidad de activar el plan de contingencia estará a cargo del responsable de iniciar el plan de contingencia, en este caso el líder de Sistemas. En la sección Criterios de activación del plan de contingencia se describen los parámetros mínimos a evaluar para determinar que se debería activar el plan de contingencia.

En el caso de los incidentes de seguridad de la información, la evaluación de la necesidad de activar el plan de contingencia se debe realizar tan pronto como se identifica la ocurrencia de un incidente de seguridad de la información que genera no disponibilidad de servicios de misión crítica. El procedimiento de gestión de incidentes de seguridad de la información establece los mecanismos para iniciar las actividades de recuperación y restablecimiento de servicios.

7.11. CRITERIOS PARA ACTIVACIÓN DEL PLAN DE CONTINGENCIA

El responsable de activación del plan de contingencia debe considerar los siguientes parámetros para ordenar la activación del plan de contingencia.

En caso de que algunas de las siguientes condiciones se presenten se debería activar el plan de contingencia sobre el sistema afectado.

Daños en componentes de tecnología: Se activa el plan de contingencia cuando se presenten eventos en los componentes de tecnología si:

Daños en componentes de tecnología

Evento	Descripción
Indisponibilidad total de componentes de tecnología que soportan las aplicaciones críticas	El diagnóstico del procedimiento de gestión de incidentes o el procedimiento de gestión de incidentes de seguridad de la información demuestra un daño total o parcial físico en uno o varios de los componentes de tecnología de información y comunicaciones que soportan uno o varios de los sistemas de información críticos y que impide la prestación de servicios misionales.

Criticidad del sistema afectado: Se activa el plan de contingencia cuando se presenten eventos en los componentes de tecnología si:

Criticidad del sistema afectado

Evento	Descripción
Ocurrencia de incidente sobre un sistema de información crítico en fecha crítica	Cuando se identifique un incidente de seguridad de la información o incidente de tecnología que afecta un sistema de información crítico y además el incidente se presenta en una de las fechas críticas para el sistema.

Duración del incidente: Se activa el plan de contingencia cuando se presenten eventos en los componentes de tecnología si:

Duración del incidente

Evento	Descripción
La duración del incidente supera el tiempo disponible para restablecer los servicios y se entra en fecha crítica de operación de los servicios.	Cuando se esté atendiendo un incidente de tecnología o de seguridad de la información y el tiempo empleado para resolver el incidente empiece a consumir tiempo de las fechas críticas de operación de los sistemas críticos

Procedimientos de notificación

Para efectos de notificación de la ocurrencia de un incidente de tecnología o un incidente de seguridad de la información, se generan reportes que deben ser remitidos al coordinador del plan de contingencia para que se diligencie el formato de reporte de incidente y valoración de

incidente.

- Notificación telefónica: La primera notificación del incidente se debe realizar vía teléfono en caso de que no se pueda hacer personalmente. A continuación, se tiene la lista de contactos para notificación

Notificación telefónica

Contacto	Celular	Teléfono Casa	Debe realizar notificación a:
líder de sistemas			Subdirector de la SDAE y Director IPES
Administrador LAN			Líder de sistemas IPES (coordinador de plan de contingencia)
Administradores sistemas de información			Líder de sistemas IPES (coordinador de plan de contingencia)
Administrador de sistema de Almacenamiento y Servidores			Líder de sistemas IPES (coordinador de plan de contingencia)

- Notificación vía correo electrónico: Una vez se complete la notificación telefónica y si existe servicio de correo electrónico, se debe proceder a remitir el formato de reporte y valoración de incidente al personal que forma parte del plan de contingencia.

Notificación vía correo electrónico

Contacto	Email	Debe continuar notificación con:
Líder de sistemas		Director IPES y Comité de plan de contingencia
Administrador LAN		Líder de sistemas IPES (coordinador de plan de contingencia)
Administradores sistemas de información		Líder de sistemas IPES (coordinador de plan de contingencia)
Administrador de sistema de Almacenamiento y Servidores		Líder de sistemas IPES (coordinador de plan de contingencia)

Fase de recuperación

La fase de recuperación de servicios en la infraestructura de contingencia depende del resultado de la valoración del incidente por parte del grupo de contingencia. A continuación se detalla una secuencia de recuperación que supone una pérdida total de disponibilidad de servicios de infraestructura. El coordinador del plan de contingencia y los líderes de infraestructura deben valorar la extensión del incidente para identificar qué grupos de actividades se deben aplicar para recuperar los servicios de misión crítica en situación de contingencia.

Recuperación en sitio alterno

Si el incidente afecta el centro de cómputo principal pero es viable seguir trabajando desde la sede misma se debe proceder reubicar los servidores que sean factibles de mover a un sitio predefinido dentro de la sede principal de IPES, la prioridad de recuperación en estos casos es el sistema de almacenamiento, la operación de GOOBI debe trasladarse a las instalaciones de la Secretaria de Hacienda mediante el desplazamiento de los funcionarios responsables de las funciones críticas de GOOBI, los archivos vitales y los certificados digitales asignados al IPES.

Los servicios de Correo y HEMI serán las prioridades subsecuentes y su restauración en sitio alterno dentro del IPES dependerá de la disponibilidad de energía eléctrica y espacio físico.

Si el incidente afecta todo el edificio principal del IPES es necesario definir un plan de recuperación ante desastres[1]

Aprovisionamiento de servicios de energía

Si el incidente afecta el suministro de energía eléctrica del centro de cómputo, y ha sido necesaria la activación del plan de contingencia dentro del edificio del IPES se debe hace uso de los servicios de la Planta Eléctrica y las UPS mientras que la afectación no ponga en riesgo la operación de los equipos y sea necesario apagar las máquinas y esperar al retorno del fluido eléctrico.

Aprovisionamiento de servicios de conectividad LAN

En los casos en los que el incidente afecta solo los equipos de conectividad de los servidores:

- Switch para conexión de servidores o Switch de Core/distribución: Se debe verificar el resultado de la valoración de incidente y si el resultado indica que no están disponibles los switches, la solución de contingencia implica reemplazar Switch afectado por un Switch de contingencia que debe ser configurado con una copia de respaldo de la configuración del Switch que falló en el caso de ser de iguales características.

- Firewall: La no disponibilidad del firewall impide la conexión entre el sistema GOOBI del IPES y la secretaría de hacienda, la navegación y consulta de correo electrónico desde la LAN hacia el exterior, y la publicación del portal de HEMI. Para mitigar este impacto,

la entidad cuenta actualmente con un sistema de seguridad perimetral en alta disponibilidad, mediante la cual ante la falla del firewall de producción, entra en operación el firewall de respaldo, así como se escala el evento ante el proveedor quien bajo los términos vinculantes entrará a dar soporte y respaldo de la operación.

- Canal de internet: Al igual que el Firewall la no disponibilidad del firewall impide la conexión entre el sistema GOOBI del IPES y la secretaría de hacienda, la navegación y consulta de correo electrónico desde la LAN hacia el exterior, y la publicación del portal de HEMI. Para mitigar este impacto, la entidad cuenta con un canal alterno el cual entra en operación ante una falla del primario.

Aprovisionamiento de servidor

Si el incidente implica falla de un servidor o servidores que soportan los procesos misionales críticos del IPES se debe informar a los responsables de los procesos misionales para que activen sus planes de continuidad de negocio en forma manual, mientras que se configura un nuevo servidor virtual y se restablece el servicio. Para el caso del sistema de información HEMI se cuenta con configuración redundante que mitiga la afectación en caso de falla de alguno de los servidores (Aplicación o Base de datos). En el caso del servidor GOOBI si el daño es físico es necesario el reemplazo del servidor por un equipo diferente lo que implicaría tiempos de restablecimiento de servicios superiores a los admitidos por el BIA y es necesario activar la contingencia mediante operación en puesto de trabajo gestionado con la secretaria de Hacienda Distrital.

Aprovisionamiento de sistema operacional

Cuando la valoración del incidente indique que se ha presentado una falla que implica la no disponibilidad total del sistema operacional del servidor o servidores que soportan las aplicaciones misionales se debe notificar a los dueños de los procesos misionales para que inicien sus procedimientos de continuidad de negocio en forma manual. Una vez notificada la necesidad de plan de continuidad manual se debe iniciar las tareas de restauración de las imágenes de los servidores virtuales afectados. En el caso de GOOBI se debe proceder a la reinstalación del sistema operacional y restablecimiento de la base de datos, situación que implicaría tiempos de restablecimiento de servicios superiores a los admitidos por el BIA y es necesario activar la contingencia mediante operación en puesto de trabajo gestionado con la secretaria de Hacienda Distrital.

Aprovisionamiento de canales de comunicaciones

En la eventualidad en que falle el acceso con la secretaria de hacienda o con Internet, se puede activar el uso de un canal alterno disponible con el proveedor de internet. la prioridad será el restablecimiento de servicios fundamentales sobre el sistema GOOBI. Ante falla de la contingencia, se debe proceder a generar los datos misionales críticos de GOOBI, grabar los datos o transacciones en un medio removible (esta operación implica apoyo del administrador de GOOBI para apoyar a los usuarios de los procesos misionales) y desplazarse físicamente a la sede de la secretaría de hacienda para cargar los datos.

En el caso de los servicios de correo electrónico las fallas en los canales de comunicación deben ser escalada al proveedor del acceso a Internet, los tiempos máximos tolerables de no disponibilidad del servicio de acceso a Internet permiten que se haga uso del escalamiento al proveedor de servicios

Aprovisionamiento de motor de base de datos

Cuando el resultado de la valoración del incidente indique que el binario del motor de la base de datos que soporta las aplicaciones misionales no está disponible y no puede ser recuperado por los procedimientos de gestión de incidentes o problemas, se debe proceder a la recuperación del binario mediante reinstalación del motor de la base de datos y la recuperación de la copia más reciente del BackUP de base de datos. En el caso de GOOBI la actividad implica el apoyo del proveedor de servicios de soporte a la base de datos Oracle. En el caso de HEMI, el esquema de contingencia permite dar continuidad a los servicios en caso de falla de una de las maquinas mediante la activación de la máquina de contingencia. El tiempo de restablecimiento del servicio de HEMI está dentro de los tiempos del BIA.

Recuperación de BackUP más reciente de base de datos y aplicaciones

El restablecimiento del BackUP de base de datos se ordena cuando la valoración del incidente determina que se existe una falla en los datos de la base de datos que no se puede recuperar mediante los procedimientos de gestión de incidentes o problemas, o que el tiempo de recuperación de los datos mediante estos procedimientos excede los tiempos máximos tolerables de no disponibilidad definidos en el BIA.

Verificación de funcionamiento de aplicaciones críticas

Una vez aplicado el procedimiento de contingencia para el componente o componentes que fallen se debe seguir el protocolo de verificación de correcto funcionamiento de aplicaciones.

Aprovisionamiento de puestos de trabajo para personal de misión crítica

En caso de requerirse estaciones de trabajo para los líderes de los procesos misionales críticos, la prioridad de selección de estaciones se ajustará la disponibilidad a los siguientes criterios:

- En primera instancia la estación de trabajo asignada al usuario.
- En segunda instancia una estación de trabajo portátil de la misma área del usuario líder.
- En tercera instancia una estación de trabajo portátil de otra área del IPES.
- En última instancia una estación de trabajo alquilada o aprovisionada por un proveedor externo.

Verificación de funcionamiento de puestos de trabajo

Una vez aplicado el procedimiento de contingencia para las estaciones de trabajo se debe seguir el protocolo de verificación de correcto funcionamiento de estaciones de trabajo.

Aprovisionamiento de servicio de impresión de contingencia

En caso de activación del plan de contingencia, el aprovisionamiento de servicios de impresión tiene baja prioridad, bajo circunstancias de fuerza mayor que impliquen la generación de informes, el servicio se aprovisionará mediante impresoras departamentales habilitadas específicamente para tal fin. La impresión se coordinará con el apoyo de los administradores de las aplicaciones y se prestará únicamente a los procesos misionales críticos.

Aprovisionamiento de servicio telefónico de contingencia

En caso de activación del plan de contingencia, el aprovisionamiento de servicios de telefonía tiene baja prioridad, los líderes de proceso crítico se comunicarán mediante medios como teléfono celular o correo electrónico si está disponible.

Criterios para finalizar las acciones de contingencia

De acuerdo con las estimaciones del análisis de impacto, los sistemas críticos identificados podrían operar bajo la infraestructura de contingencia durante un plazo no superior a dos (2) semanas, pasado ese tiempo es necesario contar con la infraestructura completa de información y tecnología del IPES. Los pasos que se describen a continuación detallan las actividades que se deben ejecutar para retornar la operación normal de sistemas de información después de la activación del plan de contingencia. Las condiciones para el restablecimiento de los servicios a condición normal deben ser evaluadas por el responsable de contingencia del IPES, en este caso particular se trata del Líder de sistemas del IPES quien determinara la viabilidad para reactivar los sistemas de información después de la contingencia teniendo en consideración los siguientes aspectos:

Condiciones a considerar para finalizar el plan de contingencia y volver a la operación normal de servicios y sistemas de información

1. El incidente que obligó a la activación del plan de contingencia haya sido completamente controlado
2. Los sistemas de información afectados se haya restablecido exitosamente
3. El comité de contingencia apruebe el retorno a condiciones normales de operación

Ejecución de procesos concurrentes entre infraestructura de contingencia e infraestructura normal de tecnología

Debido a que la estrategia de contingencia definida para los sistemas de información de naturaleza crítica consiste en el uso de instalaciones propias del IPES y equipos de contingencia, la ejecución concurrente de dos versiones o dos instancias de los sistemas de información (el de contingencia y el oficial) se descarta por las siguientes consideraciones

1. Los tiempos de restablecimiento de los sistemas de información críticos a lo sumó tomarían 1 días y el tiempo máximo MTD para los procesos es superior a 1 día, con lo cual el tiempo se cuenta con holgura para recuperación de servicios.
2. En caso de ejecutarse más de una copia de los sistemas de información críticos, el proceso de sincronización de las bases de datos y los registros entre los dos sistemas es más complejo que simplemente tomar un respaldo a las bases de datos del sistema de contingencia y restablecer los datos (se excluyen binarios y aplicaciones), en el sistema oficial
3. Bajo las condiciones más críticas de ausencia total de los sistemas de información, los sistemas que soportan los procesos misionales críticos tienen la posibilidad de operación manual, por lo que intentar correr simultáneamente dos versiones de los

sistemas es innecesario y haría que los tiempos de restablecimiento a operación normal se prolonguen innecesariamente.

Restablecimiento de sistemas críticos

El proceso de restablecimiento de sistemas a condiciones normales se debe realizar siguiendo las etapas que se describen a continuación:

1. Confirmar con el coordinador de plan de contingencia que el incidente que afectó a los sistemas de información ha sido resuelto, que se ha corrido las pruebas de correcto funcionamiento de los sistemas de información y todo funciona de acuerdo con los parámetros de operación normal.
2. Informar al personal de contingencia que los sistemas de información ya fueron restablecidos y que la infraestructura de contingencia se va a deshabilitar, para realizar respaldo de los datos registrados en contingencia y restaurar los datos en los sistemas de información normales.
3. Cuando se confirme con el personal de contingencia que ha cerrado las operaciones o transacciones que realizaron en la plataforma de contingencia, se debe proceder a realizar un respaldo de datos y cerrar los sistemas de contingencia

Advertencia: Para preservar la consistencia de bases de datos y registros, NO se deben tener simultáneamente activos a los usuarios el sistema de contingencia y el sistema normal. El sistema normal, solamente se debe activar a todos los usuarios cuando se restaure el BackUP en los sistemas normales y los líderes de proceso haya verificado que las transacciones que se aplicaron en contingencia están disponibles en el sistema normal. Los sistemas de contingencia no se desmontan hasta que se corran las pruebas de correcto funcionamiento de los sistemas de información normales

Prueba de sistemas restablecidos

Pruebas previas al restablecimiento de BackUP: Los líderes de cada plataforma, debe ejecutar pruebas internas de correcto funcionamiento de los componentes de sistemas de información, las pruebas y sus resultados se deben registrar.

Pruebas de sistemas de información después de restaurar BackUP

Una vez que los líderes técnicos hayan verificado el correcto funcionamiento de los componentes de IT (servidor, bases de datos, comunicaciones), se debe proceder a restaurar el BackUP de datos del sistema de contingencia y llamar a los líderes de proceso para que corran pruebas de correcto funcionamiento de los sistemas de información (GOOBI, HEMI). Las pruebas y resultados deben ser registrados.

Cuando los líderes de proceso, certifiquen que la aplicación y los datos funcionan de acuerdo con las condiciones normales de operación, se puede autorizar el apagado de la infraestructura

de contingencia e iniciar los procesos de restablecimiento de servicios en condición normal.

Notificaciones

Cuando los sistemas de información críticos hayan sido restablecidos, se debe informar al responsable de contingencia (Líder de sistemas) para que se proceda a la notificación oficial a las diferentes áreas del IPES para que puedan volver a utilizar los sistemas de información. El esquema de notificación de usuarios se realizará empleando los medios de comunicación disponibles después de la contingencia: notificación personal, teléfono, mensajes SMS, Correo electrónico.

Limpieza y desmonte de la infraestructura de contingencia

Al finalizar la contingencia y cuando el responsable de contingencia, (Líder de sistemas) autorice el desmonte de la infraestructura de contingencia, se debe proceder a desmontar los equipos empleados en la contingencia. En caso de haber usado equipos en préstamo o convenio se procede a su embalaje y coordinación de devolución a sus dueños. Todo equipo de contingencia debe ser inventariado para generar un acta de devolución. El acta de devolución debe describir el estado en que se devuelven los equipos. Incluso en los casos en que sean equipos de reserva del IPES se debe documentar su estado final.

Documentación

Una vez se restablezcan los sistemas de información a sus condiciones normales, se debe iniciar el proceso de documentación formal del incidente. La documentación del incidente se realiza siguiendo las actividades descritas en el procedimiento de gestión de incidentes de seguridad de la información y la guía para atención de incidentes de seguridad de la información.

Pruebas y entrenamiento

Pruebas

Con el fin de velar por el correcto funcionamiento del plan de contingencia, se deben realizar pruebas regulares del mismo. Los mecanismos que se deben emplear para la prueba del plan de contingencia. Estas incluyen..

- Divulgación y sensibilización del plan, se realizará mínimo una vez al año o cuando se presenten cambios que afecten el entorno o condiciones bajo las cuales fue planificado el plan de contingencia.

- Revisión de escritorio: Revisión anual de los procedimientos, formatos y documentos del Plan de contingencia. La revisión debe ser realizada por los responsables de cada una de las secciones del plan de contingencia. Se debe revisar la documentación de procedimientos que acompañan el plan de contingencia.

- Pruebas de restauración: Realizar pruebas de restauración a partir de la herramienta de backup. y de conformidad con lo establecido en el PR-033-BACKUP GENERACIÓN Y RECUPERACIÓN aislado del ambiente de producción para certificar que las copias de respaldo operan correctamente

- Documentación: Documentar las acciones realizadas bajo el entorno de pruebas, donde se relacionen los casos de pruebas, y se determinen las acciones de mejora que den lugar.

Entrenamiento de personal de TI

El éxito en la operación y funcionamiento del plan de contingencia del IPES depende de que el personal con funciones asignadas en el plan participe en un programa de sensibilización y capacitación en los procedimientos del plan de contingencia. A continuación, se describen los aspectos generales de capacitación en el plan de contingencia, las capacitaciones deberán abarcar conceptos dentro de los cuales se podrá contemplar:

- Conceptos relacionados con continuidad de negocio: BCP, DRP, Plan de contingencia.
- Razones para la implementación de un plan de continuidad.
- Concepto de BIA: Análisis de impacto al negocio.
- Análisis y gestión de riesgos.
- Formatos, procedimientos y políticas asociadas al plan de contingencia.
- Restauración de copias de respaldo, o configuración o reinstalación de equipos de conectividad, servidores, bases de datos.

7.12. ESQUEMA DE CONTINGENCIA SEGURIDAD Y SALUD EN EL TRABAJO

Identificación de amenazas

Dado que las amenazas se encuentran relacionadas con el peligro que significa la posible ocurrencia de un fenómeno físico de origen natural, tecnológico o social y pueden manifestarse en un sitio específico y en un tiempo determinado, el Instituto para la Economía Social a través del DE-031 Plan de Prevención, Preparación y Respuesta ante Emergencias, establece la metodología para la identificación de las Amenazas y la calificación de las mismas a través de colores según sea posible, probable o inminente.
Con el fin de identificar peligros valorar los riesgos y determinar controles, la entidad se basa en la metodología de la Norma Técnica Colombiana 45, y establece en el PR-091 Identificación de Peligros, Valoración de riesgos y determinación de controles SG-SST, las matrices de peligros que se presentan a continuación:

- MP- 001 – 018. Matriz de Peligros plazas de mercado (18 matrices)
- MP -019. Matriz de peligros Sede Administrativa (1 matriz)
- MP- 020 – 051. Matriz de Peligros puntos comerciales (32 matrices)
- MP- 052 Matriz de peligros Puntos de encuentro (22 matrices)

- MR-014 MAPA RIESGOS SG-SST.

De otra parte, para mitigar el riesgo de contagio y propagación del virus ocasionado por el COVID-19, se elaboró el IN-096 Esquema de Prevención y Manejo del Coronavirus COVID-19, el cual contempla todos los lineamientos de bioseguridad para todos los actores de la Entidad.

Determinación de la vulnerabilidad

Una vez identificadas las amenazas, se procede a realizar el análisis de vulnerabilidad, entendido como la predisposición o susceptibilidad que tienen las personas, los recursos, los sistemas y procesos a ser afectados o sufrir una pérdida ante una amenaza específica, el documento DE-031 Plan de Prevención, Preparación y Respuesta ante Emergencias para el Instituto de la Economía Social, contempla cómo se determina el nivel de vulnerabilidad según el criterio a calificar, para luego realizar la valoración de la misma.

Clasificación del nivel de riesgo

Una vez identificada, descrita y analizada las amenazas, como resultado del análisis de vulnerabilidad a personas, recursos, sistemas y procesos, se procede a determinar el nivel de riesgo. En el documento DE-031 Plan de Prevención, Preparación y Respuesta ante Emergencias para el Instituto de la Economía Social, se contempla la metodología que combina la amenaza y la vulnerabilidad utilizando la teoría del Diamante de riesgo, para cada amenaza identificada, cada uno de los rombos tiene un color que fue asignado de acuerdo con los análisis desarrollados.

Priorización de amenazas y medidas de intervención

Una vez priorizada las amenazas, organizándolas desde calificación “Alta”, hasta las de calificación “Baja”, se definen las medidas de intervención ya sea de prevención, mitigación o ambas. Para el caso del Instituto para la Economía Social a través del DE-031 Plan de Prevención, Preparación y Respuesta ante Emergencias se contempla: Movimientos sísmicos, cortos circuitos, falla estructural, asonadas, robos, derrames químicos.

Plan de prevención, preparación y respuesta ante emergencias

El plan de Prevención, Preparación y respuesta ante emergencias contempla un sistema de alerta que son actos declaratorios de la situación de inminencia de presentación de eventos constitutivos de desastre, calamidad o emergencia a fin de que se proceda oportunamente a activar los planes de acción en la Entidad, en el DE-031 Plan de Prevención, Preparación y Respuesta ante Emergencias, se contemplan los niveles de alerta utilizados en la Entidad, siendo estos de Nivel I-Alerta Verde, Nivel II- Alerta Amarilla, Nivel III- Alerta Roja.
Al igual establece un Centro de Comando el cual es un lugar destinado para el manejo de la Emergencia, el cual se establece como la Recepción interna que hace parte de la Entidad, puesto que es el sitio más cercano a las salidas de emergencia en caso de ser necesario evacuar).
Dentro del documento DE-031 se establecen las matrices de amenazas que evidencian la causa, consecuencia, recursos, medidas de prevención, mitigación y respuesta de: movimientos sísmicos, tormentas eléctricas, explosiones, incendios, incidentes con materiales peligrosos, falla en la red de alcantarillado, terrorismo, riesgo público.
Así mismo, el IPES cuenta con los planes de emergencia para cada uno de los espacios de su administración, tal y como se presenta a continuación:

- PE-01 Enlace a plan de emergencia Sede Administrativa.
- PE-02 Enlace a plan de emergencias puntos de encuentro.
- PE-03-27 Enlace a plan de emergencias puntos comerciales.
- Los PE-30-48 tienen el enlace a plan de emergencias de Plazas de Mercado.

La Entidad de igual manera contempla el PR-50 procedimiento operativo normalizado de emergencias, como documento anexo al DE-031 Plan de Prevención, Preparación y Respuesta ante Emergencias, el cual contiene el mecanismo de reporte, mecanismo de evaluación, activación de la emergencia, junto con la especificidad en el procedimiento de la actuación antes, durante y después de la emergencia con relación a colaboradores, visitantes, Comité de Emergencias, Coordinadores de Brigada, Jefe de Brigada, Brigadistas en caso de ocurrencia de: disturbios que generen riesgo público, incendio, sismo, inundación, acción terrorista, evacuación general, robo o asalto.

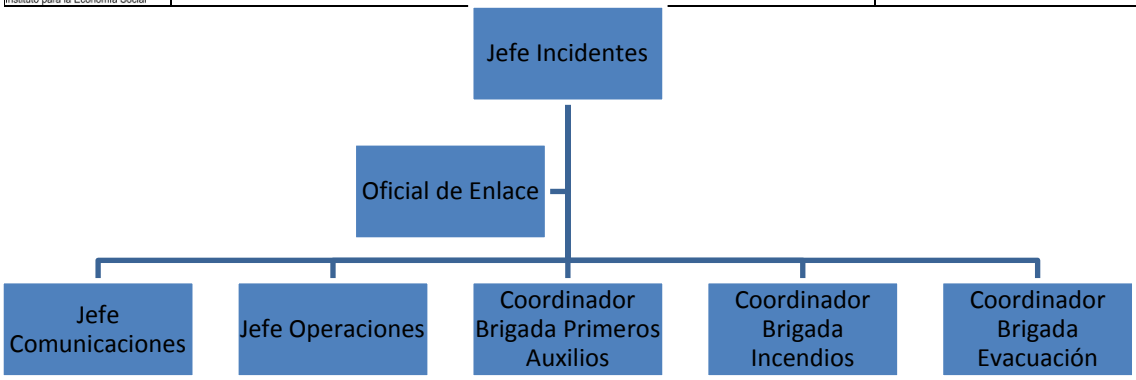
En cuanto a presencia de Emergencias Médicas, el DE-031 Plan de Prevención, Preparación y Respuesta ante Emergencias, contempla el plan PAEMED BASICO, el cual contempla aspectos como clasificación, responsabilidades del Jefe Brigada, Brigadistas, Coordinador de primeros auxilios, Jefe Brigadas, Coordinador Primeros Auxilios y Profesional SST, al igual se enuncia el directorio de los centros médicos de servicios especializados, servicios de apoyo de salud dónde se puede recibir la atención y traslado de pacientes.
Por último, contempla los contactos de la red de apoyos como: número único de seguridad y emergencias, cuerpo de bomberos, policía nacional, Administradora de Riesgos Laborales y el Centro de Información de Seguridad de Productos Químicos de Derrames fugas de sustancias químicas.
Un aspecto fundamental con relación a la preparación ante las Emergencias incluye los simulacros, los cuales permiten detectar los puntos débiles o fallas en la puesta en marcha de la implementación de los planes de emergencia a fin de afrontar una emergencia.
De todo lo expuesto anteriormente, se evidencia el esfuerzo administrativo del Instituto para la Economía Social IPES para identificar y gestionar las amenazas y riesgos que puedan presentarse en el desarrollo cotidiano de sus actividades, así como determinar las actividades y los planes que le permiten realizar una contingencia ante la ocurrencia o materialización de alguna de las amenazas.

Organización del talento humano en la entidad para las emergencias

Describe la estructura orgánica de los colaboradores que atienden directamente las emergencias, contempla cargos, roles y responsabilidades, las cuales son vitales para responder de manera efectiva ante las novedades presentadas, está conformado por:

a. ***Comité Emergencias***:

Conformado en el Instituto para la Economía Social a través de la Resolución 182 de 2018, cuya función principal es la de organizar y dirigir los recursos humanos y materiales disponibles para ejecutar y evaluar las acciones encaminadas a la prevención y control de situaciones de emergencia y desastre. Su estructura está conformada de la siguiente manera:



Dentro de las actuaciones del Comité de Emergencia están:

Jefe Incidentes: Es la máxima autoridad de la Organización en todo lo relacionado con el esquema de atención de emergencias y es el responsable de dirigir las acciones durante la emergencia en la Entidad asumiendo el control de la Emergencia. Sus deberes son:

Antes de la Emergencia	Durante la Emergencia	Después de la Emergencia
- Desarrollar y aprobar plan de acción de incidentes - Divulgar el plan de acción - Actualización del plan de acción - Evaluar el riesgo para los respondientes con respecto del propósito y potenciales resultados de sus acciones en cada situación - Dirigir las reuniones del Comité de Emergencias - Capacitarse y asegurar la capacitación de los respondientes	- Asegurar que se tomen las medidas adecuadas de seguridad en el sitio - Establecer un puesto de comando estacionario - Evaluar permanentemente la situación - Considerar los principios de administración de riesgos para la toma de decisiones - Evaluar y comunicar la necesidad de: Intervención de apoyo interno (Respondientes, Comité Emergencias). Apoyo externo (Bomberos, Cruz Roja, IDIGER, Antiexplosivos, Defensa Civil), Evacuación - Ordenar la movilización y desmovilización de recursos (Humanos, financieros, tecnológicos, físicos) - Proveer el control de acceso a la escena del incidente - Autorizar la liberación de la información a los medios de noticias - Aprobar los comunicados que emitirá el Jefe de Comunicaciones	- Autorizar regreso a la normalidad o la suspensión temporal o indefinida de las actividades - Dirigir la revisión de los lugares evacuados y verificar que no se presenten peligros, antes de dar la orden de retorno - Revisar tanto el informe del incidente como el reporte de daños y pérdidas a presentar a la Dirección

Oficial de Enlace: El oficial de Enlace debe ser el contacto para el personal asignado al incidente por agencias de asistencia o cooperación. (Bomberos, Cruz Roja, IDIGER, Antiexplosivos, Defensa Civil, Corposéptima etc)

Jefe Comunicaciones: El Jefe de Comunicaciones es la única persona autorizada para emitir comunicados en representación de la Entidad, bien sea dirigidos a los medios de comunicación o a las familias de las personas que sufran alguna lesión o se vean

involucrados en una situación de Emergencia.

Jefe Operaciones: El Jefe de Operaciones aprueba la liberación de recursos, aporta los recursos adicionales que considere necesarios al jefe de incidentes, registra monitorea la asignación de recursos durante un incidente, asiste al Jefe de Incidentes, verifica el estado de los elementos utilizados durante el control de la emergencia, elabora el informe del incidente a presentar al jefe de incidentes, elabora reporte de daños y pérdidas a presentar a la Dirección, provee de vestuario y equipo de protección total al Comité de Emergencias.

b. Brigadas de Emergencia

Constituida por un grupo de colaboradores organizados, con conocimiento, entrenamiento y práctica, que apoyan el plan de emergencias, a través de la prevención y control de las situaciones de riesgo que pueden generar una emergencia dentro de las instalaciones de la Entidad, buscan salvaguardar el bienestar de todas las personas. Aunque la brigada es integral, al interior se conforman grupos que realizan actividades focalizadas en la atención de emergencias a saber: Grupo de Control de Incendios quienes están encargados de la inspección de extintores (FO-586), Evacuación y primeros Auxilios, esta último es el encargado de realizar el manejo de botiquines (PR-084), inspección a los mismos a través de los Formatos establecidos para este fin. De igual manera dentro del Documento Estratégico DE-031 Plan de Prevención, Preparación y Respuesta ante Emergencias, se estipula el accionar antes, durante y después de presentada la Emergencia.

c. Comité Paritario de Seguridad y Salud en el Trabajo (COPASST)

Es un equipo de personas encargados de promover y vigilar las normas de Seguridad y Salud en el Trabajo de la Entidad, colaboran con el análisis de los accidentes de trabajo los cuales se basan en lo establecido en el PR-056 Reporte e Investigación de Accidentes de Trabajo, y en el PR-138 Reporte de Investigación de Enfermedad Profesional. Como también el COPASST, realiza las inspecciones las cuales están contempladas en el DE-029 Programa de Inspecciones a lugares de trabajo (ambientes, máquinas, equipos, aparatos etc), y respecto al plan de emergencias apoya en su promoción y divulgación.

Identificación de riesgos o peligros

Desde el Sistema Integrado de Gestión en el proceso de Planeación Estratégica y táctica y el Sistema de Gestión Ambiental, se cuenta con la matriz MR-011 Matriz riesgos gestión ambiental en cuyo documento se identifican los riesgos, estos están relacionados directamente con objetivos estratégicos y de proceso. Los riesgos identificados se describen a continuación:

a. Los Residuos Peligrosos generados en la entidad tales como: luminarias, aceites usados, toners, RAEES, envases contaminados, etc., son gestionados inadecuadamente, razón por la cual pueden ocasionar afectaciones por su exposición directa e indirecta.

b. Al no realizarse un adecuado aprovechamiento de los residuos ordinarios generados en las sedes a cargo de la entidad, se contribuye a una sobre saturación del Relleno Sanitario, afectando negativamente los recursos naturales y así mismo se ocasionan afectaciones a la salud humana.

c. Durante el desarrollo de las actividades de cárnicos, en algunos de los locales asignados a los comerciantes de los equipamientos a cargo de la entidad, se vierten a la

red pública de alcantarillado, vertimientos con contenidos de sangre, piel, pelos y demás residuos de animales, lo cual constituye una descarga de aguas residuales no permitidas por parte de la autoridad ambiental.

d. Durante el desarrollo de su misionalidad, el IPES puede generar Residuos Especiales tales como Residuos de Construcción y Demolición (RCD's), Aceite de Cocina Usado y Llantas, los cuales al ser gestionados inadecuadamente, pueden ocasionar afectaciones al medio ambiente.

e. El IPES contrata los servicios de Fumigación y Control de Plagas y Palomas , para los equipamientos a cargo de la entidad; para la ejecución de dichas actividades se utilizan sustancias químicas que contienen características de peligrosidad, y de no tomarse las medidas necesarias, relacionadas con la protección de los alimentos que se expenden en las alternativas comerciales a cargo de la entidad, se puede afectar la salud humana de los consumidores.

f. Con el funcionamiento de los vehículos a cargo de la entidad, se generan en el proceso de combustión, gases contaminantes como el monóxido de carbono (CO), los cuales pueden ocasionar afectaciones a la salud y aportar Gases Efecto Invernadero que contribuyen al calentamiento global.

g. En los equipamientos a cargo de la entidad se evidencian consumos de agua que pueden ser minimizados, con el fin de no afectar este recurso natural.

h. En los equipamientos a cargo de la entidad se evidencian consumos de energía que pueden ser optimizados de una manera más eficiente, con el fin de disminuir la emisión de gases efecto invernadero, los cuales contribuyen al cambio climático y calentamiento global.

i. Con el fin de posicionar la imagen institucional de la entidad y de los equipamientos a cargo del IPES, se instalan avisos en fachada con Publicidad Exterior Visual, sin haberse realizado los trámites ambientales previos requeridos.

Es importante precisar que cada riesgo está asociado con mínimo un control, presentando la respectiva evidencia de ejecución del control.

7.13. ESQUEMA DE PLAN DE CONTINGENCIAS AMBIENTALES

Investigación de incidente y/o accidentes ambientales

Previo a la investigación del incidente y/o accidentes ambientales es importante precisar que se realiza la identificación y valoración de los aspectos e impactos ambientales significativos mediante el procedimiento PR – 055 con el objetivo de identificar y valorar los aspectos e impactos ambientales significativos que se generan con el desarrollo de las actividades y servicios por parte de la entidad y la respectiva Matriz de identificación de aspectos y valoración de impactos ambientales esta identificación y valoración se realiza con base en los lineamientos de la Secretaría Distrital de Ambiente, en el marco de los Planes Institucionales de Gestión Ambiental PIGA.

En la etapa de la identificación del impacto ambiental que se genera como resultado parcial o total del aspecto ambiental, se realiza a partir algunos impactos ambientales en el formato de matriz listados por la Secretaría Distrital de Ambiente y en la etapa de valoración de los impactos ambientales definidos se estima el impacto ambiental a través de una interpretación cuantitativa, identificando sus atributos así como el cumplimiento normativo en relación con el aspecto y/o el impacto ambiental. La importancia del impacto se cuantifica de acuerdo a la influencia, posibilidad de ocurrencia, tiempo de permanencia del efecto, afectación o riesgo sobre el recurso generado por el impacto y por el cumplimiento de la normatividad asociada al impacto y/o al aspecto ambiental de forma específica.

En consecuencia, para definir los lineamientos para la realización de la investigación de accidentes e incidentes ambientales en los equipamientos administrados por la entidad y establecer las medidas de intervención para prevenir y controlar las condiciones de riesgo y establecer las acciones en caso de que el riesgo se materialice la entidad, se formula el procedimiento PR-063 Investigación de incidente y/o accidentes ambientales. Dentro de los documentos asociados al procedimiento PR-063 se encuentran el formato FO-007 Formato Acciones correctivas, preventivas y/o de mejora permitiendo realizar de forma secuencial las actividades establecidas el procedimiento de Acciones Correctivas, Preventivas o de Mejora (PR-055) para la consolidación, análisis de no conformidades y formulación de acciones correctivas, preventivas o de mejora en su proceso, el formato FO-307 Plan de Mejoramiento Institucional en el cual se realiza el seguimiento a las acciones correctivas por proceso y dependencia responsable entre otros categorías de análisis para el respectivo seguimiento cada tres (3) meses.

Con el fin de establecer el procedimiento interno para la identificación y valoración de riesgos ambientales la entidad establece el procedimiento PR-129 Identificación y valoración de riesgos ambientales para mediante el formato FO-016 MAPAS DE RIESGOS, esta herramienta del mapa de riesgos permite la identificación del riesgo que se realiza determinando las causas, con base en el contexto interno y/o externo analizado. Para identificar las causas es útil dar respuesta a la pregunta ¿por qué puede pasar?; de esta forma se analizan las situaciones encontradas y se identifican los riesgos ambientales en Puntos y plazas de mercado y a nivel administrativo. Para identificar las consecuencias se debe resolver la pregunta ¿Si ocurre el riesgo, que pérdida se puede generar? Estas pueden ser: pérdida de vidas, pérdida de capital, pérdida de mercado, costos de reposición o reconstrucción de datos, pérdida de ingresos, gastos por sanciones, gastos por indemnizaciones, sanciones disciplinarias, pérdida de imagen, pérdida de confianza, entre otras.

Esta actividad igualmente hace referencia al diligenciamiento para la documentación de toda la información recopilada anteriormente en la herramienta facultativa cumpliendo así con las exigencias del DAFP y para la cual se establece el Instructivo IN- 004 Matriz de Riesgos, todo lo anterior integrado en la matriz MR-011 MATRIZ RIESGOS DE GESTIÓN AMBIENTAL.

Una vez identificadas las causas que generan el riesgo y sus consecuencias, se realiza un análisis y evaluación de los riesgos generados, finalizando con la definición del control operacional para mitigar los riesgos ambientales, derivados del desarrollo de las actividades y servicios por parte de la entidad, los siguientes son los controles operacionales definidos:

Gestión inadecuada de los RESPEL generados por la entidad.

- Informar, instruir y capacitar al personal encargado de la gestión y manejo de residuos peligrosos con el fin de divulgar el riesgo que estos residuos representan para la salud y el ambiente., mediante la socialización del Plan de Gestión Integral de Residuos Peligrosos - PGIRESPEL.
- La Entidad contrata los servicios de almacenamiento, aprovechamiento, recuperación, tratamiento y/o disposición final, con instalaciones que cuenten con licencias, permisos o autorizaciones de control ambiental que haya lugar, de conformidad con la normatividad vigente, especialmente en lo que se refiere con la entrega de tóner a gestores autorizados por las autoridades competentes.
- Se garantiza el almacenamiento de residuos peligrosos en la sede administrativa y se adoptan medidas tendientes a prevenir cualquier afectación a la salud humana y al ambiente, teniendo en cuenta las mínimas condiciones locativas y operativas de almacenamiento de los RESPEL, contando con kit de derrame, dispositivo detección de fuego, entre otros.
- La entidad cuenta con el documento estratégico DE-033 Plan de Gestión de Residuos Peligrosos conforme a los lineamientos técnicos establecidos por la autoridad ambiental, actualizado con la información del año inmediatamente anterior (2020) y da cobertura a la totalidad de los equipamientos administrados por la entidad.

Gestión inadecuada de los Residuos Sólidos ordinarios generados en las sedes de la entidad.

- La entidad hace entrega del material aprovechable a organizaciones o grupos de recicladores con cobertura en todos los equipamientos administrados por el Ipes, mediante acuerdo de corresponsabilidad con las asociaciones recicladoras de oficio.
- La entidad garantiza la correcta segregación en la fuente mediante el fortalecimiento de capacitaciones dirigidas a comerciantes de plazas de mercado, beneficiarios de puntos comerciales y colaboradores de la sede administrativa en relación a la correcta segregación de residuos sólidos.
- La entidad dispone de los elementos necesarios para la separación de residuos (Puntos Ecológicos) en las plazas de mercado, puntos comerciales y la sede administrativa para dar cumplimiento a satisfacción se solicita las necesidades de nuevos puntos ecológicos en cada uno de los equipamientos y posterior a ello se realiza la contratación para la adquisición e instalación de este tipo de elementos, además de contar con un cuarto de almacenamiento de residuos de manera temporal que cumple con las especificaciones técnicas requeridas según la normatividad vigente.
- Descarga de vertimientos no permitidos a la red pública de alcantarillado.

7.14. ESTRUCTURA ORGÁNICA INSTITUCIONAL PARA GESTIONAR PLANES DE CONTINGENCIAS.

Fuente. SAF 2020

- El director/a General del IPES, es el responsable de revisar de manera periódica los resultados de la investigación de incidentes y accidentes ambientales y la efectividad de las acciones implementadas, como de proponer acciones que permitan mejorar el desempeño de la gestión ambiental al respecto y asignar los recursos requeridos para tal fin.
- El gestor ambiental de la entidad, es el responsable de coordinar que la emergencia ambiental sea atendida oportunamente, aprobar y hacer seguimiento a las acciones establecidas desde el inicio hasta el cierre de la emergencia, como la validación de los diferentes informes resultados de la misma.
- El profesional responsable del sistema de gestión ambiental de la entidad, es el encargado de verificar que la emergencia se haya controlado definitivamente, realizar la investigación del incidente o accidente ambiental, coordinar el establecimiento e implementación de acciones preventivas, correctivas y de mejora y rendir los diferentes informes.
- El profesional responsable del equipamiento y el comité de emergencias son los encargados de: atender en primera instancia la emergencia ambiental, controlarla si es posible e informar sobre su ocurrencia al gestor ambiental.

7.15. ESQUEMA DE COMUNICACIONES PARA PLAN DE CONTINGENCIAS

Los sucesos y mecanismos de contingencia se comunican asertivamente con todos sus públicos en situaciones de crisis organizacional, o cuando se presenten impactos externos directos e indirectos, para facilitar el direccionamiento de las acciones comunicativas orientadas a blindar su imagen corporativa y a mitigar los efectos negativos que puedan derivarse de la situación.

Contempla como objetivos:

- Identificar asuntos y situaciones que pueden convertirse en temas críticos

- para el IPES y establecer rutas básicas para actuar frente a momentos de
- crisis relacionada con ellos.
- Establecer mensajes claves y respuestas estandarizadas que le faciliten a
- los voceros del IPES, responder asertivamente ante la opinión pública en la
- eventualidad de una crisis.
- Fortalecer la capacidad de respuesta de los funcionarios y servidores del
- IPES para formar parte de la solución ante la probabilidad de una crisis.
- Conformar un Comité directivo de Comunicaciones que lidere las
- alternativas de solución para salir de la crisis.

Para ello se contempla un manual de crisis el cual es de conocimiento de todas las dependencias, dado que una crisis se puede presentar en cualquier área.

8 DOCUMENTOS ASOCIADOS

Mantenimiento:

- MS-018 Mantenimiento plazas distritales de mercado
- Manual mantenimiento puntos comerciales
- Planes de saneamiento básico
- PR 095 Trabajo en alturas
- DE-029 Programa inspecciones

Planes de emergencia y contingencia

- PR 093 Procedimiento para la atención de emergencias
- DE-043. Plan de saneamiento básico plazas de mercado
- MS-024. Manual de saneamiento básico de pm la concordia
- DE-024 Plan institucional de respuesta emergencias - PIRE
- DE-31 Plan maestro de emergencia 2017
- PE-30 - 48 Enlace a plan de emergencia Plazas de mercado
- PE-01 Enlace a plan de emergencia Sede Administrativa
- PE-02 -27 Enlace a plan de emergencia puntos comerciales
- PE-02 Enlace a plan de emergencia puntos de encuentro
- R 050 Procedimientos operativos normalizados en caso de emergencias
- PR-040 Valoración afectación hábitat urbano por catástrofes
- PR-056 Reporte accidentes de trabajo
- PR-059 Investigación de accidentes trabajo
- PR-084 Manejo botiquín de primeros auxilios
- PR-085 Investigación incidentes de trabajo
- PR-091 Peligros y riesgos SG-SST
- PR-138 Reporte e investigación de enfermedad profesional
-

Tecnología de la información

- PR-033- Backup generación y recuperación V3
- PR-123 Gestión de incidentes de seguridad V3
- MS-013 Manual seguridad de la información
- FO-319 Solicitud recuperación de información
- FO-625 Documentación incidentes
- FO-626 Lecciones aprendidas respuesta incidentes

9 MARCO NORMATIVO

LEY 9 /79 CÓDIGO SANITARIO NACIONAL	Título III - Salud Ocupacional Título VIII - Desastres. Artículo 501. Cada Comité de Emergencias, deberá elaborar un plan de contingencia para su respectiva jurisdicción con los resultados obtenidos en los análisis de vulnerabilidad. Además, deberán considerarse los diferentes tipos de desastre que puedan presentarse en la comunidad respectiva. El Comité Nacional de Emergencias elaborará, para aprobación del Ministerio de Salud, un modelo con instrucciones que aparecerá en los planes de contingencia. Artículo 502. El Ministerio de Salud coordinará los programas de entrenamiento y capacitación para planes de contingencia en los aspectos sanitarios vinculados a urgencias o desastres. Parágrafo. El Comité Nacional de Emergencias, deberá vigilar y controlar las labores de capacitación y de entrenamiento que se realicen para el correcto funcionamiento de los planes de contingencia.
CONPES 3146/01.	Estrategia para consolidar la ejecución del Plan Nacional para la Prevención y Atención de Desastres – PNPAD, en el corto y mediano plazo
RESOLUCIÓN 2400/79 ESTATUTO DE SEGURIDAD INDUSTRIAL	“Por el cual se establecen disposiciones sobre vivienda, higiene y seguridad industrial en los establecimientos de trabajo” Artículo 2. Todos los empleadores están obligados a Organizar y desarrollar programas permanentes de Medicina Preventiva, Higiene y Seguridad Industrial”
DECRETO 614/84	“Por el cual se determinan las bases para la organización de administración de salud ocupacional en el país” Artículo 24. Los empleadores tendrán las siguientes responsabilidades: - Responder por la ejecución del programa de Salud Ocupacional
RESOLUCIÓN 1016 /89	“Por la cual se reglamenta la organización, funcionamiento y forma de los programas de Salud Ocupacional que deben desarrollar los patronos o empleadores en el país” Artículo 11. Numeral 18. Organizar y desarrollar un plan de emergencias teniendo en cuenta las siguientes ramas: a) Rama Preventiva: Aplicación de las normas legales y técnicas sobre combustibles, equipos eléctricos, fuentes de calor y sustancias peligrosas propias de la actividad económica de la empresa. b) Rama Pasiva o Estructural: Diseño y construcción de edificaciones con materiales resistentes, vías de salida suficientes y adecuadas para la evacuación, de acuerdo con los riesgos existentes y el número de trabajadores. c) Rama Activa o Control de las Emergencias: Conformación y organización de Brigadas (selección, capacitación, planes de emergencias y evacuación), Sistema de

	detección, alarma, comunicación, inspección, señalización y mantenimiento de los sistemas de control. Artículo 14. El programa de Salud Ocupacional, deberá mantener actualizados los siguientes registros mínimos: Planes específicos de emergencias y actas de simulacro en las empresas cuyos procesos, condiciones locativas o almacenamiento de materiales riesgosos, puedan convertirse en fuente de peligro para los trabajadores, la comunidad o el ambiente.
LEY 1523/12	"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 y se dictan otras disposiciones".
DIRECTIVA MINISTERIAL No. 13 /92	“Responsabilidades del Sistema Educativo como integrante del Sistema Nacional para la Prevención y Atención de Desastres” 2a. Planes de Prevención de Desastres en establecimientos educativos 3. Planes de Emergencias en escenarios deportivos.
LEY 100 /93	“Por la cual se crea el Sistema de Seguridad Social Integral “Libro III: Sistema General de Riesgos Profesionales.
DECRETO 1295/94	“Por el cual se determina la organización y administración del Sistema General de Riesgos Profesionales” Artículo 2. Objetivos del Sistema General de Riesgos Profesionales a) Establecer las actividades de promoción y prevención tendientes a mejorar las condiciones de trabajo y salud de la población trabajadora, protegiéndola contra los riesgos derivados de la organización del trabajo que puedan afectar la salud individual o colectiva en los lugares de trabajo tales como los físicos, químicos, biológicos, ergonómicos, de saneamiento y de seguridad.
RESOLUCIÓN 7550 DE 1994	"Por la cual se regulan las actuaciones del Sistema Educativo Nacional en la prevención de emergencias y desastres". Artículo 3. Solicitar a los establecimientos educativos, la creación y desarrollo de un proyecto de prevención y atención de emergencias y desastres, de acuerdo con los lineamientos emanados por el Ministerio de Educación Nacional, el cual hará parte integral del proyecto educativo institucional. Este contemplará como mínimo los siguientes aspectos: a) Creación del comité escolar de prevención y atención de emergencias y desastres como también brigadas escolares b) Análisis escolar de riesgos c) Plan de acción d) Simulacro escolar ante una posible amenaza.
LEY 400 /1997	“Por el cual se adoptan normas sobre construcciones sismo resistentes”
DECRETO 321 DE 1999	"Por el cual se adopta el Plan Nacional de Contingencia contra derrames de Hidrocarburos, Derivados y Sustancias Nocivas”. Artículo 1. Adoptase el Plan Nacional de Contingencia contra derrames de Hidrocarburos, Derivados y Sustancias Nocivas en aguas marinas, fluviales y lacustres, aprobado mediante Acta número 009 del 5 de junio de 1998 del Comité Nacional para la Prevención y Atención de Desastres, y por el Consejo Nacional Ambiental, cuyo texto se integra como anexo del presente decreto. Artículo 2. El objeto general del Plan Nacional de Contingencia contra derrames de Hidrocarburos, Derivados y Sustancias Nocivas en aguas marinas, fluviales y lacustres que será conocido con las siglas -PNC- es servir de instrumento rector del diseño y realización de actividades dirigidas a prevenir, mitigar y corregir los daños que éstos puedan ocasionar, y dotar al Sistema Nacional para la Prevención y Atención de Desastres de una herramienta estratégica, operativa e informática

	que permita coordinar la prevención, el control y el combate por parte de los sectores público y privado nacional, de los efectos nocivos provenientes de derrames de hidrocarburos, derivados y sustancias nocivas en el territorio nacional, buscando que estas emergencias se atiendan bajo criterios unificados y coordinados.
DECRETO No. 3888 /07	"Por el cual se adopta el Plan Nacional de Emergencias y Contingencia para Eventos de Afluencia Masiva de Público y se conforma la Comisión Nacional Asesora de Programas Masivos y se dictan otras disposiciones" Artículo 2. El objetivo del Plan Nacional de Emergencias y Contingencia para Eventos de Afluencia Masiva de Público es servir como instrumento rector para el diseño y realización de actividades dirigidas a prevenir, mitigar y dotar al Sistema Nacional para la Prevención y Atención de Desastres de una herramienta que permita coordinar y planear el control y atención de riesgos y sus efectos asociados sobre las personas, el ambiente y las instalaciones en esta clase de eventos. Este Plan se complementará con las disposiciones regionales y locales existentes. Artículo 5. Actualización del Plan. Cuando las circunstancias lo ameriten, el Plan Nacional de Emergencias y Contingencia para Eventos de Afluencia Masiva de Público deberá ser actualizado por el Comité Nacional para la Prevención y Atención de Desastres o por el Comité Técnico Nacional, por delegación que haya recibido de aquél, en todo caso, con la asesoría de la Comisión Nacional Asesora de Programas Masivos creada por este decreto. Artículo 20. Planes institucionales. Los organismos operativos del Sistema Nacional para la Prevención y Atención de Desastres elaborarán sus propios planes institucionales para la atención de los eventos de afluencia masiva de público, los cuales se articularán con los Planes Locales de Emergencias y Contingencia para Eventos de Afluencia Masiva de Público.
Decreto 926 de 2010	Por el cual se establecen los requisitos de carácter técnico y científico para construcciones sismo resistentes NSR-10
Ley 769 de 2002	Código Nacional de Tránsito. Artículo 1. Ámbito de aplicación y principios. Las normas del presente código rigen en todo el territorio nacional y regulan la circulación de los peatones, usuarios, pasajeros, conductores, motociclistas, ciclistas, agentes de tránsito y vehículos por las vías públicas o privadas que estén abiertas al público, o en las vías privadas, que internamente circulen vehículos; así como la actuación y procedimientos en las autoridades de tránsito.
Ley 322 de 1996	Sistema Nacional de Bomberos. Artículo 1. La prevención de incendios es responsabilidad de todas las autoridades y los habitantes del territorio colombiano. En cumplimiento de esta responsabilidad los organismos públicos y privados deberán contemplar la contingencia de este riesgo en los bienes inmuebles tales como parques naturales, construcciones, programas y proyectos tendientes a disminuir su vulnerabilidad.
Decreto 1072 de 2015	Por medio del cual se expide el decreto único reglamentario del sector trabajo.
RETIE 180398 de 2004	Resolución Min. Minas y Energía.
Resolución 256	Por medio de la cual se reglamenta la conformación, capacitación y

	entrenamiento para las brigadas contraincendios de los sectores energético, industrial, petrolero, minero, portuario, comercial y similar en Colombia.

Legislación Distrital

RESOLUCIÓN 3459 DE 1994	“Por la cual se regulan las actuaciones del Sistema Educativo de Bogotá D.C. en la prevención y atención de emergencias”
ACUERDO 20/95	“Por el cual se adopta el Código de Construcción del Distrito Capital de Bogotá, se fijan sus políticas generales y su alcance, se establecen los mecanismos para su aplicación, se fijan plazos para su reglamentación prioritaria y se señalan mecanismos para su actualización y vigilancia.”
RESOLUCIÓN 1428 DE 2002	"Por la cual se adoptan los Planes Tipo de Emergencias en seis escenarios Distritales, se modifica y adiciona la Resolución 0151 del 06 de febrero de 2002".
ACUERDO 79/03	CÓDIGO DE POLICÍA
DECRETO 350/03	“Por el cual se regulan las rifas, juegos, concursos, espectáculos públicos y eventos masivos en el Distrito Capital” Capítulo VI. De los espectáculos públicos y eventos masivos Artículo 17. Parágrafo Segundo Los eventos masivos deberán contar con las medidas de prevención y seguridad contempladas en el modelo de Plan de Emergencias General y Planes Tipo, que para tal efecto sea aprobado por la Dirección de Prevención y Atención de Emergencias de la Secretaria de Gobierno.
DECRETO 332/04	“Por el cual se organiza el régimen y el Sistema para la Prevención y Atención de Emergencias en Bogotá Distrito Capital y se dictan otras disposiciones” Artículo 7- Planes de Emergencias Se adoptarán para cada una de las entidades y comités sectoriales, y establecerán con claridad cuáles son las funciones de respuesta, autoridades responsables de cumplirlos y los recursos que se pueden y deben utilizar. Parágrafo. La adopción de los planes corresponderá por comités sectoriales, al tenor del Decreto 87/03 y a los representantes legales de las entidades en los demás casos. Artículo 8 – Planes de Contingencia Son aquellos que deben adoptarse para el Distrito Capital en su conjunto, sus entidades y sectores, por las mismas autoridades señaladas en el parágrafo del artículo 7 precedente, para responder específicamente a un tipo determinado de situación de calamidad, desastre o emergencia.
DECRETO 423/06	“Por el cual se adopta el Plan Distrital para la prevención y Atención de Emergencias para Bogotá D.C”. Artículo 18 - Planes de Emergencias. En armonía con el artículo 7º del decreto 332 de 2004 los Planes de Emergencias son instrumentos para la coordinación general y actuación frente a situaciones de calamidad, desastre o emergencia. Definen las funciones y actividades, responsables, procedimientos, organización y recursos aplicables para la atención de las emergencias independientemente de su origen o naturaleza. Artículo 19 – Planes de Contingencia. En armonía con el artículo 8º del Decreto 332 de 2004, los Planes de Contingencia son instrumentos Complementarios a los planes de emergencias, que proveen información específica para la atención de desastres o emergencias derivadas de un riesgo o territorio en particular. Un plan de contingencia desarrolla en detalle aspectos pertinentes para la respuesta que solo son propios del riesgo y el territorio al que este

	referido. Los planes de contingencia se organizan por tipo de riesgo, tales como deslizamientos, inundaciones, incendios forestales, materiales peligrosos y aglomeraciones de público, entre otros. Los planes de continencia pueden ser desarrollados por la Administración Distrital en sus diferentes niveles (central, institucional o local), por el sector privado y por la comunidad.
RESOLUCIÓN No. 375 /06	"Por la cual se establecen las condiciones básicas para las empresas que prestan el servicio de logística en las aglomeraciones de público en el Distrito Capital". Artículo 2. Numeral 3. Capacitación mínima del personal.
DECRETO 633/07	"Por el cual se dictan disposiciones en materia de prevención de riesgos en los lugares donde se presenten aglomeraciones de público y se deroga el Decreto 043 de 2006 el cual regulaba antes la materia". Artículo 5- Planes de Contingencia De conformidad con lo previsto en los artículos 8º y 9º del Decreto Extraordinario 919 /89 y en el artículo 15 del Decreto Distrital 332 /04, todas las entidades o personas públicas o privadas responsables de edificaciones, instalaciones o espacios en los cuales se realicen aglomeraciones de público, deberán preparar y observar planes de contingencia que incluyan los análisis de riesgos y las medidas de prevención, preparación y mitigación, en forma y condiciones que establezca la DPAE (hoy FOPAE).
ACUERDO DISTRITAL 341 /08	"Por el cual se adiciona el acuerdo No. 30 de 2001 y se establece la relación de un simulacro de actuación en caso de un evento de calamidad pública de gran magnitud con la participación de todos los habitantes de la ciudad". Artículo 4. La Administración Distrital promoverá acciones para que todos los patrones con carácter de empresa y domicilio en la ciudad de Bogotá, de acuerdo con las normas en materia de riesgos profesionales y salud ocupacional, y en especial la Resolución 1016 de 1989 del Ministerio de la Protección Social, informe a la Dirección de Prevención y Atención de Emergencias –DPAE (hoy FOPAE)- sobre la implementación de sus planes de emergencia, para ello contará con un plazo de cuatro meses contados a partir de la aprobación del presente Acuerdo, a través del formulario electrónico que para este fin elabore esta entidad.
RESOLUCIÓN No. 004/09	"Por la cual se adopta la versión actualizada del Plan de Emergencias de Bogotá, el cual establece los parámetros e instrucciones y se definen políticas, sistemas de organización y procedimientos Interinstitucionales para la administración de emergencias en Bogotá D.C". Deroga las Resoluciones 137/07, 195 y 196 del 2008. Capítulo 2.2. Fortalecimiento de las operaciones de emergencias.

Normas técnicas colombianas

NTC-5254	Gestión de Riesgo.
Guía Técnica Colombiana 202/06	Sistema de Gestión de Continuidad del Negocio.
NTC-1700	Higiene y Seguridad. Medidas de Seguridad en Edificaciones. Medios

	de Evacuación y Código NFPA 101. Código de Seguridad Humana. Establece cuales son los requerimientos que debe cumplir las edificaciones en cuanto a salidas de evacuación, escaleras de emergencia, iluminación de evacuación, sistema de protección especiales, número de personas máximo por unidad de área, entre otros requerimientos; parámetros que son analizados con base en el uso de los edificios es decir comercial, instituciones educativas, hospitales, industrias, entre otros.
NTC-2885	Higiene y Seguridad. Extintores Portátiles. Establece en uno de sus apartes los requisitos para la inspección y mantenimiento de portátiles, igualmente el código 25 de la NFPA Standard for the inspection, testing and maintenance of Water – Based fire protection systems USA: 2002. Establece la periodicidad y pruebas que se deben realizar sobre cada una de las partes componentes de un sistema hidráulico contra incendio.
NTC-4764	Cruces peatonales a nivel y elevados o puentes peatonales.
NTC-4140	Edificios. Pasillos y corredores.
NTC-4143	Edificios. Rampas fijas.
NTC-4144	Edificios. Señalización.
NTC-4145	Edificios. Escaleras.
NTC-4201	Edificios. Equipamientos, bordillos, pasamanos y agarraderas.
NTC-4279	Vías de circulación peatonal planas
NTC-4695	Señalización para tránsito peatonal en el espacio público urbano.
NTC-2388	Símbolos para la información del público.
NTC-1867	Sistemas de señales contra incendio, instalaciones, mantenimiento y usos.

Normatividad seguridad digital

Decreto 1499 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto ÚnicoReglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de laLey 1753 de 2015
Circular 02 de 2019	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valorpúblico en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
Conpes 3292 de 2004	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites),enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicosque permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
Conpes 3701 2011	Lineamientos de política para la Ciberseguridad y Ciberdefensa
Conpes 3854 2017	Aborda las incertidumbres, los riesgos, las amenazas, las vulnerabilidades ylos incidentes digitales Documento
Conpes 3920 2018	Política nacional de explotación de datos (Big Data).

Conpes 3975 2019	Define la Política Nacional de Transformación Digital e Inteligencia Artificial,estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
Decreto 1008 2018	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones
Decreto 103 2015	Reglamenta parcialmente la Ley 1712 de 2014 (Gestión de la informaciónpública)
Decreto 1078 2015	Expide el Decreto Único Reglamentario del Sector de las TIC
Decreto 1151 de 2008	Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y sedictan otras disposiciones
Decreto 1413 de 2017	Actualiza el Decreto Único Reglamentario del sector de las TIC, estableciendo lineamientos generales en el uso y operación de los serviciosciudadanos digitales
Decreto 2573 2014	Establece los lineamientos generales de la Estrategia de Gobierno en línea,se reglamenta parcialmente la Ley 1341 de 2009
Decreto 2693 2012	Establece los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de2009, 1450 de 2011
Decreto 415 2016	Adiciona al Decreto Único Reglamentario del sector de la Función Pública (Decreto Número 1083 de 2015), en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías dela información y las comunicaciones (PETI)
Decreto 619 2007	Se establece la estrategia de gobierno electrónico de los organismos y de lasentidades de Bogotá, distrito capital y se dictan otras disposiciones
Decreto 728 201	Actualiza el Decreto 1078 de 2015 con la implementación de zonas deacceso público a Internet inalámbrico
Directiva 02 2019	Establece los lineamientos generales de la política de Gobierno Digital yactualizando el Decreto Único Reglamentario del sector de las TIC
Directiva 05 2005	Por medio de la cual se adoptan las políticas generales de tecnología de información y comunicaciones aplicables al Distrito Capital.
Directiva 22 2011	Estandarización de la información de identificación, caracterización, ubicacióny contacto de los ciudadanos y ciudadanas que capturan las entidades del Distrito Capital.
Ley 1266 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regulael manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

Ley 1273 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologíasde la información y las comunicaciones, entre otras disposiciones
Ley 1341 2009	Define principios y conceptos sobre la sociedad de la información y laorganización de las TIC, se crea la Agencia Nacional de Espectro
Ley 1581 2012	Por la cual se dictan disposiciones generales para la protección de datospersonales
Ley 1618 2013	Establece las disposiciones para garantizar el pleno ejercicio de los derechosde las personas con discapacidad
Ley 1680 2013	Garantiza a las personas ciegas y con baja visión, el acceso a la información,a las comunicaciones, al conocimiento y a las TIC
Ley 1712 2014	Crea la Ley de Transparencia y del Derecho de Acceso a la InformaciónPública Nacional
Ley 1834 2017	Por medio de la cual se fomenta la economía creativa (ley economía naranja)
Ley 1955 2019	Plan de desarrollo 2018-2022. "pacto por Colombia, pacto por la equidad¨
Ley 1978 del 2019	Simplificación de interacción digital los ciudadanos y el Estado
Resolución 184 2014	Por la Cual se adopta el manual del Subsistema de Gestión de Seguridad dela Información y el Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Instituto para la Economía Social - IPES

Otras normas

NFPA 101/06	Life Satefy Code. (Código de Seguridad Humana).
NFPA 1600/07	Standard en Disaster/Emergency Management and Business Continuity Programs. (Norma sobre manejo de Desastres, Emergencias y Programas para la Continuidad del Negocio).
Convención sobre los Derechos de las Personas con Discapacidad y el Protocolo Facultativo	Naciones Unidas en el cual está la convención sobre los Derechos de las Personas con Discapacidad y el Protocolo Facultativo, a la cual le deben dar cumplimiento los estados partes (Colombia firmo en mayo de 2011).

10 CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
01	30/01/2021		Elaboración del documento.

11 REFERENCIAS BIBLIOGRÁFICAS

- Ministerio de las Tecnologías de la Información y las comunicaciones - MINTIC. Modelo de Seguridad y Privacidad de la Información. https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/. Fecha de consulta 27-ene-2021
- Icontec internacional, Norma técnica NTC-ISO-IEC Colombiana 27001, 11dic2013