Documento Técnico del Plan de Continuidad del Negocio

Entendimiento Función Pública

Secretaria General

Oficina de la Tecnologías y las comunicaciones – OTIC

Oficina Asesora de Planeación

Grupo de Gestión Humana

Grupo de Gestión Administrativa

Marzo de 2017

Versión 2

Presentación

Con el fin de contar con una herramienta que nos permita prevenir o reaccionar adecuadamente ante posibles incidentes que pongan en riesgo a los *Servidores Públicos*, afectar el debido *desarrollo de las actividades* propias de Función Pública, impedir *la prestación y continuidad del servicio* a los Grupos de Valor o el *cumplimiento de los compromisos* establecidos en la planeación estratégica, la Entidad consolidó una serie de acciones a emprender en el *Plan de continuidad del negocio* que, diseñadas y ejecutadas de forma planificada, permitirían responder de manera eficiente ante una eventualidad, restablecer en menor tiempo la prestación de los servicios y mitigar el impacto negativo de la pérdida de recursos.

El plan de continuidad del negocio tiene en cuenta las obligaciones legales aplicables a la Función Pública que establece la Ley de Seguridad y Salud en el Trabajo, la Ley de Control Interno (análisis del entorno y manejo de riesgos), la Ley de Seguridad de la Información, la Ley de Calidad, la Ley de archivos, y se encuentra diseñado en diferentes actividades detectives, preventivas, reactivas y correctivas, articuladas a la planeación estratégica y operativa de cada vigencia según la función y responsabilidad de cada proceso.

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

El plan de continuidad adquiere mayor relevancia una vez sea apropiado por todos los Servidores Públicos de manera anticipada y será actualizado y comunicado en cada vigencia según las necesidades de la Entidad.

1. Objetivos y Alcance del Plan de Continuidad

Objetivo General

Definir las actividades preventivas, defectivas y correctivas para reaccionar de manera eficiente ante una eventualidad que comprometa el desarrollo de las actividades cotidianas, la seguridad del personal o la prestación del servicio.

Objetivos específicos

- Asignar responsabilidades al personal designado
- Asegurar la protección de los Servidores Públicos
- Identificar las actividades críticas, los recursos y los procedimientos necesarios para llevar a cabo las operaciones durante las interrupciones prolongadas del servicio
- Asegurar una pronta recuperación en los servicios críticos para los Grupos de Valor
- Disminuir los tiempos de interrupción de la operación de los procesos
- Proteger los bienes de la Función Pública de manera adecuada.

Alcance

El plan de continuidad del negocio inicia con la identificación y socialización de los elementos críticos en Función Pública que puedan definirse como incidente o desastre que impidan continuar la operación y finaliza con el análisis y acciones de mejora identificadas de la reacción ante la situación presentada mínimo una vez al año (simulacro o realidad)

2. Roles, mecanismos y responsabilidades

Rol	Responsable	Representantes	Mecanismos
Asesor , coordinador y documentador del Plan de continuidad	• Jefe Oficina Asesora de Planeación • Jefe de Oficina de TIC • Secretaria General	• Jefe Oficina Asesora de Planeación y Coordinador OAP • Jefe de Oficina de TIC, Asesor y Coordinadores de grupo • Secretaria General, Asesor y Coordinadores de Talento Humano, Administrativa, Contractual y Documental	Para crear y documentar el plan: • Mesas de trabajo • Análisis de la información • Metodología de riesgos • Inclusión en el plan de acción anual de las actividades

Aprobación, socialización y pruebas del plan de continuidad,	• Comité Institucional de Desarrollo Administrativo • Grupo de Comunicaciones • Grupo de Gestión Humana	• Miembros del Comité • Coordinador de Comunicaciones • Coordinador del Grupo de talento humano	• Sesiones ordinarias y extraordinarias del Comité • Boletín de noticias/intranet • Sesiones de inducción y reinducción-Simulacros
Activación del Plan de emergencia y Plan de restablecimiento	• Comité de Crisis	• Secretaria General • Jefe de OTIC • Jefe la Oficina Asesora Planeación	• Declaración escrita • Comunicación telefónica • Reuniones extraordinarias
Restablecer prestación de servicio /información	• Subdirector (a) • Secretaria General • Jefe de OTIC • Jefe de Oficina Asesora de Planeación-Coordinadores de grupo	• Subdirector y Asesor • Secretaria, Asesor , Coordinadores de Grupo, grupo de administrativa, talento humano y servicio al ciudadano • Jefe OTIC, Asesor, Coordinadores de Grupo. Grupo de infraestructura • Jefe y Coordinador	• Mesas de trabajo • Análisis y pruebas • Inspección y verificación • Comunicación con los grupos de valor

3. Generalidades del Plan de Continuidad

El Plan de Continuidad reúne un conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento de la misionalidad de la entidad y la prestación de sus servicios se establece en tres momentos:

- Preventivo: Dentro de este aspecto se involucran los recursos humanos, quienes deben estar preparados en caso de presentarse un evento inesperado, y las acciones anticipadas que se puedan articular a la gestión institucional en los diferentes procesos
  .
- Reactivo**:** Este aspecto va dirigido a fortalecer las políticas internas y comunicarlas oportunamente para ponerlas en marcha una vez detectada la contingencia.

- Recuperación: Este aspecto está enfocado en las actividades a desarrollar en el momento de atender una contingencia.

La descripción consecutiva de las actividades en los diferentes momentos estará definida en el documento denominado "*plan de continuidad*" anexo a este documento técnico.

4. Análisis del entorno institucional

A partir de las funciones y obligaciones normativas delegadas al Departamento, de los compromisos adquiridos con los diferentes grupos de valor y de los datos históricos de la operación institucional, se consolidan las situaciones que pueden presentarse en Función Pública y que ocasionarían un inadecuado desarrollo en la planificación y prestación de los servicios, las cuales se pretenden mitigar con un plan de continuidad formalizado y comunicado, representadas así:

Contexto Externo:

- Económicos: Recorte presupuestal, demoras o dificultades para el traslado de recursos con los cooperantes, cambios de gobierno en la priorización y traslado de recursos.
- Políticos: Cambio de gabinete, nuevas prioridades del gobierno nacional, jornada electoral, dificultad en la coordinación interinstitucional, cambio en las políticas aplicables a Función Pública.
- Sociales: Manifestaciones y protestas frecuentes en el centro de la ciudad, dificultad de acceso para el ciudadano y los servidores, Indigencia, contaminación social, daños intencionados a la infraestructura de la Entidad.
- Tecnológicos: Deficiencia en la interoperabilidad de los sistemas de gobierno, diferencia en las plataformas tecnológicas de los socios de negocio, ataques externos a la información y las herramientas tecnológicas.
- Medio Ambientales: Ubicación de la entidad cerca a los cerros, incendios, terremotos, Inundaciones, desastres naturales.

Contexto Interno:

- Financieros: Dificultad para la priorización de recursos, cambios frecuentes en el plan adquisiciones, comunicación inoportuna de los cambios, demoras en la apropiación de recursos, fallas en los sistemas de registro SIIF.
- Personal: Planta de personal insuficiente, nuevas exigencias de competencias del personal en el nuevo modelo de operación, tiempo insuficiente para el desarrollo de habilidades, falta de motivación e involucramiento del personal, alta rotación de personal

- Procesos: nuevos procesos, desconocimiento de las características de los procesos, desconocimiento del nivel de responsabilidad y autoridad de los procesos, baja apropiación del nuevo modelo, baja asistencia a las capacitaciones de socialización y las mesas de creación de los procesos.
- Tecnología: desconocimiento de un Plan estratégico de TI, desarticulación de las herramientas y aplicativos internos, fallas en la infraestructura tecnológica, fallas en el sistema de seguridad de la información, desconocimiento de los niveles de responsabilidad y autoridad frente a los sistemas.
- Estratégicos: Cambios en la gestión institucional sin planificación y comunicación oportuna, fallas en la comunicación y solicitud de información a las dependencias, ausencia de ANS concertados, fallas en la comunicación interna, solicitud de información múltiple, fallas en los sistemas de información.
- Comunicación interna: Desconocimiento en los temas gestionados por parte de la Función Pública, saturación de los boletines internos y externos, Inapropiada distribución de canales internos, Inoportunidad en la entrega de información, falta de registros de información y contactos actualizados y protegidos.

5. Riesgos asociados a la continuidad del negocio

Función Pública contempla implícitamente en la gestión de sus procesos la identificación y administración de los riesgos como práctica para impedir que eventualidades internas o externas impidan cumplir sus objetivos institucionales, por lo cual, al desarrollar el plan de continuidad del negocio se integra la metodología de riesgos aplicada y el control preventivo, detectivo y correctivo de dicho plan queda asociado al mapa de riesgos institucional.

A continuación se definen los criterios para los riesgos asociados a la continuidad del servicio aclarando que se atenderán y hará parte del mapa de riesgos institucional los de la dimensión 5 x 5 y se identifiquen con nivel extremos y altos:

Tabla 1: Criterios Matriz de Riesgos

		IMPACTO				
		NIVEL1	NIVEL2	NIVEL3	NIVEL4	NIVEL5
PROBABILIDAD	NIVEL5	5	10	15	20	25
	NIVEL4	4	8	12	16	20
	NIVEL3	3	6	9	12	15
	NIVEL2	2	4	6	8	10
	NIVEL1	1	2	3	4	5

Nivel 5 - Extremo. Es un riesgo que puede representar pérdidas para la organización si se materializa con un impacto crítico o grave, y se debe mitigar por medio de planes de acción.

Nivel 4 - Alto. Es un riesgo que puede representar pérdidas para la organización si se materializa con un impacto alto y se debe mitigar por medio de planes de acción.

Nivel 3 - Medio. Es un riesgo que representa un nivel moderado y se debe controlar para que no aumente.

Nivel 2 - Bajo. es un riesgo que se debe monitorear pero está dentro de los riesgo para la entidad

Nivel 1 – Muy Bajo. es un riesgo que se debe monitorear pero está dentro de los riesgo para la entidad

Para el monitoreo preventivo del ejercicio de continuidad del negocio y del servicio la Entidad cuenta con los siguientes riesgos existentes:

Clasificación del Riesgo	Nombre del Riesgo	Descripción del Riesgo
Comunicación	Uso inadecuado de los canales de comunicación.	Comprende el empleo o selección inadecuada del canal de comunicación para difundir un mensaje o reportar datos, estadísticas o información.
Cumplimiento	Incumplimiento legal.	Contempla el incumplimiento de la normativa vigente, de las obligaciones contraídas por la Entidad y/o de requisitos legales exigibles.
Imagen	Pérdida de credibilidad y confianza en la entidad.	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la Entidad.
Información	Pérdida de información.	Se asocia con la pérdida de información física y/o digital de los archivos, bases de datos, servidores y/o Sistemas de Información de la Entidad.
Información	Uso indebido de la información.	Se asocia con el inadecuado empleo o tratamiento de la información que reposa en los archivos físicos, bases de datos, servidores o sistemas de información.

Operativo	Daño o deterioro de los activos tangibles.	Comprende el daño o deterioro de los bienes muebles o inmuebles de la Entidad.
Operativo	Inexistencia de los bienes y servicios necesarios para el normal funcionamiento de la entidad.	Comprende la carencia de bienes y/o servicios requeridos en la Entidad para el normal funcionamiento de la Entidad.
Tecnológico	Accesos no autorizados.	Se asocia con el acceso a los sistemas de información, aplicativos, bases de datos o servidores sin autorización previa.
Tecnológico	Afectación de la infraestructura tecnológica.	Está relacionado con el daño, pérdida o deterioro a nivel de hardware y comunicaciones.
Tecnológico	Inadecuados servicios de Tecnologías de la Información.	Contempla la pertinencia, calidad y oportunidad de los servicios de tecnología y las deficiencias en la prestación de los mismos.

Y se crean los siguientes riesgos de categoría Tecnológicos y operativos para su prevención:

Clasificación del Riesgo	Nombre del Riesgo	Descripción del Riesgo
Operativo	Afectación de los servicios por error humano	Ausencia del personal, rotación, errores involuntarios, mala ejecución de los procedimientos internos.

Estos riesgos se integrarán a la administración de riesgos del proceso y serán monitoreados a través del sistema de seguimiento a la planeación institucional según su periodicidad.

6. Pruebas y revisión periódica del plan

En las sesiones de Comité Institucional de Desarrollo Administrativo se aprobará y monitoreará el plan de continuidad; las acciones preventivas se llevarán a cabo en toda la entidad según la planificación de las dependencias de *Talento Humano* (relacionadas con las personas), de *Administrativa* (relacionadas con la infraestructura) y de Gestión Documental (relacionadas con la información), las cuales estarán coordinadas por la Secretaria General, la *Oficina de Tecnologías de la Información y las Comunic*aciones (lo

relacionado con la infraestructura tecnológica y la seguridad de la información); durante la definición de la planificación institucional se definirán y aprobarán los simulacros, interrupción del servicio, evacuación de emergencia o pruebas aleatorias del plan de continuidad, según los recursos económicos con los que se cuente en cada vigencia, los cuales se harán de manera planificada y concertada con el Comité de Crisis; de igual manera los resultados y el seguimiento se realizará dos veces al año en los Comité Institucional de Desarrollo Administrativo y Directivos.

7. Pasos a seguir para gestionar el plan

Una vez construido y aprobado el plan de continuidad la Entidad deberá emprender las acciones necesarias para comunicarlo a todos los servidores públicos de la entidad y de esta manera estar preparados para enfrentar situaciones de emergencia y restablecer en el menor tiempo posible el servicio a los grupos de valor, para lo cual se seguirá el siguiente protocolo:

Paso 1 - Declaración manifiesta de la emergencia – miembro del comité
Paso 2 - Convocar comité de crisis –Secretaria general
Paso 3 - Contactar centro de operación (propio o alterno)– realizar reunión
Paso 4 - Analizar daños (lista de chequeo) – Comité de crisis
Paso 5 - Contacto con sedes alternas y visita de alistamiento – Secretaria General
Paso 6 - Llamado al equipo de restablecimiento – Comité de crisis
Paso 7 - Llamado al personal interno y comunicación de acciones a seguir –Comité crisis
Paso 8 - Restablecimiento de los sistemas de información según plan – Jefe TIC
Paso 9 - Activación de protocolo con usuarios – Servicio al Ciudadano
Paso 10 - Restablecimiento gradual de la información – Jefe de OTIC
Paso 11 - Análisis de la situación – Comité de crisis
Paso 12 - Establecer plan de mejoramiento a partir del análisis

8. Normatividad asociada al Plan

NTC 5722: Gestión de Continuidad del negocio: Esta norma específica los requisitos para planificar, establecer, implementar, operar, supervisar, mantener y mejorar continuamente un sistema de gestión documentado para protegerse, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de los incidentes perjudiciales que puedan surgir.

SO 31000:2009: norma internacional para la Gestión de Riesgos. Proporciona principios y guías para que las organizaciones lleven a cabo su análisis y evaluación de riesgos.

ISO 17799:2000: estándar para la administración de la seguridad de la información, publicado por la International Organization for Standardization (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad. Esta norma internacional ofrece

recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

COBIT: Control Objectives for Information and related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC

ITIL: "Information Technology Infraestructura Library", es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es la Office of Jovenmente Commerce, una entidad independiente de la tesorería del gobierno británico.

ISO Serie 27000: es una serie de estándares, que incluye, definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información), (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoria y certificación de SGSI (ISO 27006), una guía de auditoria de SGSI (ISO 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), y una guía de seguridad de la información en el sector sanitario

Departamento Administrativo de la Función Pública

Marzo de 2017