ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

PLAN DE CONTINUIDAD DEL NEGOCIO

2021

Titulo	PLAN DE CONTINUIDAD DE NEGOCIO.				
Fecha actualización:	Agosto de 2021				
Sumario	Este documento presenta una Guía de procedimientos de para mantener la funcionalidad del AGN a un nivel mínimo aceptable durante una contingencia y contempla las medidas preventivas y de recuperación para cuando se produzca un evento que afecte la operatividad en cuanto a la Infraestructura de IT de la entidad.				
Palabras claves:	Riesgos, Infraestructura, Plan de acción, impacto, buenas prácticas				
Formato:	PDF		Lenguaje:	Español	
Código:	GIT-M-02	Versión:	2	Estado:	
Categoría:	Documento Técnico Interno				
Autores:	Daniel Eduardo Arciniegas Herrera Jaime Alberto Duarte Hoyos				
Revisó:	Omar Villareal Osorio				

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

TABLA DE CONTENIDO

INTRODUCCIÓN

El Archivo General de la Nación , con el único fin de contar con un instrumento que le permita prevenir y/o reaccionar adecuadamente ante incidentes que pongan en riesgo la vida de los funcionarios, contratistas, pasantes y terceros, afectar el desarrollo de las actividades propias de su misión; consolidó una serie de acciones a emprender en el Plan de Continuidad del Negocio, que diseñadas y ejecutadas de manera planificada le permitirán responder de manera eficiente ante una eventualidad, restablecer en el menor tiempo posible la prestación de sus servicios, mitigar el impacto negativo de la pérdida de recursos.

El Plan de Continuidad del Negocio, tiene en cuenta las obligaciones legales que establece la Ley de Seguridad y Salud en el Trabajo, la Ley de Control Interno, la Ley de Archivo y se encuentra diseñado en diferentes actividades detectivas, preventivas, reactivas y correctivas articuladas con la planeación estratégica y operativa de cada vigencia según la función y responsabilidad de cada proceso.

El plan incluye una elaboración de la guía de trabajo: la primera la compone un documento que define los elementos críticos a controlar a partir de los riesgos asociados, los responsables, etapas, definiciones y generalidades.

La segunda está compuesta por las actividades específicas y secuenciales a desarrollarse, fechas de ejecución, recursos requeridos y análisis de brechas de cada una de ellas, teniendo las restricciones económicas del AGN

El Plan de Continuidad del Negocio, adquiere mayor relevancia una vez sea apropiado por todos los funcionarios, contratistas y pasantes, de manera anticipada y será actualizado y comunicado en cada vigencia según las necesidades del AGN

1. POLÍTICA DE CONTINUIDAD

Objetivos

Los principales objetivos son:

- Garantizar la continuidad de los procesos críticos del AGN en escenarios de contingencia
- Respaldar y proteger la información confidencial del AGN
- Integración de los siguientes elementos:

  - Minimizar las interrupciones en las operaciones normales
  - Limitar la extensión de perturbaciones y daños
  - Minimizar el impacto económico de las interrupciones
  - Establecer medios alternativos de operación con antelación
  - Proporcionar la restauración rápida y sin problemas del servicio
  - Capacitar al personal de soporte de infraestructura, con los procedimientos de emergencia.
  - Preservar la seguridad de la información durante las fases de activación, de desarrollo y planes para la continuidad de negocio y de vuelta a la normalidad.
  - Integrar en los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, operaciones, personal, servicios e instalaciones para que estén dispuestos de un modo distinto a la operativa habitual
  - Asignar responsabilidades al personal designado
  - Asignar la protección de los funcionarios, contratistas, pasantes y/o terceros
  - Identificar las actividades críticas, los recursos y procedimientos necesarios para llevar a cabo las operaciones durante las interrupciones prolongadas del servicio
  - Asegurar una pronta recuperación en los servicios críticos.
  - Disminuir los tiempos de interrupción en las operaciones del proceso o procesos detenidos.
  - Proteger los bienes del AGN de manera adecuada.

2. ALCANCE

El Plan de Continuidad del Negocio, inicia con la identificación y socialización de los elementos críticos en el Archivo General de la Nación, que puedan definirse como incidente o desastre que impidan dar continuidad con las operaciones normales del negocio y finaliza con el análisis y acciones de mejora identificadas de la reacción de los funcionarios, contratistas, pasantes y/o terceros mínimos una vez al año (simulacro o realidad).

Se contemplaron las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio, con el objeto de desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las

consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos

3. DEFINICIONES

Se adopta para este plan de contingencia y continuidad del negocio, el glosario del Guía para la preparación de las TIC para la continuidad del negocio, del MINTIC el cual hace parte de la política de gobierno digital según el decreto 1008 de 2018, publicado en el portal oficial:
https://www.mintic.gov.co/gestionti/615/articles 5482_G10_Continuidad_Negocio.pdf

4. MARCO NORMATIVO

La normatividad aplicable para este documento se encuentra referenciada en la Matriz de Determinación y Evaluación de Requisitos legales y otros Requisitos AGN

5. ROLES, MECANISMOS Y RESPONSABILIDADES

ROL	RESPONSABLE	REPRESENTANTES	MECANISMOS
Coordinador y documentador del plan de continuidad	Jefe Oficina Asesora de Planeación Coordinador Grupo de Sistemas Secretaria General Servicios Administrativos	Jefe Oficina asesora de Planeación, Coordinador Grupo de Sistemas, Oficial de Seguridad de la Información, Secretaria General, Coordinador de Gestión Humana Coordinador Servicios Administrativos	Para crear y documentar el plan: Mesas de trabajo Análisis de la información Metodología de Riesgo Inclusión en el PEI
Aprobación, socialización y pruebas del Plan de Continuidad	Comité Desarrollo Administrativo, Oficina de Comunicaciones Grupo de Gestión Humana	Miembros del Comité Desarrollo Administrativo, Delegado Oficina de Comunicaciones Coordinador Grupo de Gestión Humana	Secciones Ordinarias y extraordinarias del Comité Boletín de noticias intranet Sesiones de Inducción y reinducción Simulacros
Actividades del Plan de Emergencia y plan de restablecimiento	Comité Desarrollo Administrativo (funciones comité de crisis)	Miembros del Comité Desarrol Administrativo	Declaración escrita Comunicación telefónica Reuniones extraordinarias

Reestablecer prestación de servicio/información	Director Subdirectores Secretaria General Coordinador Grupo de Sistemas Coordinador Servicios Administrativos Jefe de Planeación Oficial de Seguridad de la Información Oficina de Comunicaciones	Director Subdirectores Secretaria General Coordinador GSIR Coordinador Servicios Administrativos Jefe de Planeación Oficial de seguridad de Información Delegado Oficina d Comunicaciones	Mesas de Trabajo Análisis y pruebas Inspección y verificación Comunicación al AGN

6. GENERALIDADES DEL PLAN DE CONTINUIDAD

6.1. ANÁLISIS DE IMPACTO DEL NEGOCIO

En el Análisis de Impacto de Negocio (Business Impact Analisys **- BIA)** se pretende presentar la relación de los componentes específicos del AGN (sistema, procesos y las interdependencias), con sus servicios esenciales; y en base a esta información determinamos las necesidades y prioridades de contingencia.

6.1.1. Identificación de Procesos Críticos

- Los Procesos críticos para la prestación de servicios en el AGN:
- Herramientas de Gestión de Servicios y la Infraestructura que la soporta (Servidores, Redes y Telecomunicaciones)
- Todos los procesos de Finanzas y Recursos Humanos que dependen de las herramientas corporativas localizadas en los Proveedores locales y en consecuencia, los recursos TI críticos que soportan dichos procesos.
- Seguridad de la información, que involucra la creación de políticas y la estructura de seguridad de la información, y la gestión de incidentes de seguridad de la información.

6.1.2. Identificación de Impacto y tiempos de interrupción permitidos.

Las funciones de negocio de del AGN se clasifican en:

a) **Funciones Críticas:**

- Personal para la prestación del servicio de mesa de servicios
- Centro de Cómputo
- Disponibilidad de la infraestructura de los centros de cómputo (Servidores, almacenamiento y conectividad)
- Conectividad
  - Disponibilidad de infraestructura de telefonía IP
  - Disponibilidad de acceso a Internet
  - Disponibilidad de canales de comunicación entre el ESC y los clientes

b) Funciones Esenciales:

- Disponibilidad de las herramientas de gestión de servicios para los grupos solucionadores de los clientes
- Disponibilidad de correo electrónico
- Disponibilidad de Chat, Portales de Servicio

c) Funciones Necesarias:

- Disponibilidad de acceso a Intranet

Basado en estas necesidades de recuperación, los puntos de tiempo máximo para recuperación son:

- Funciones Criticas: <= 4 horas,
- Funciones Esenciales: <= 2 días,
- Funciones Necesarias: <= 4 días,

6.1.3. Prioridades de Recuperación

De acuerdo a la clasificación de funciones del AGN y los puntos máximos de recuperación, las prioridades de recuperación durante el plan de contingencia son:

6.1.3.1. Prioridad Alta

- Infraestructura de Red Local
- Canales de comunicación
- Infraestructura de apoyo (Telefonía/telecomunicaciones y aplicaciones)
- Herramientas de Gestión de Servicios y su infraestructura de apoyo (Servidores y Bases de Datos)
- Correo electrónico
- Canal de Internet Local y servidor PROXY.

6.1.3.2. Prioridad Media

- Aplicaciones de negocio

6.1.3.3. Prioridad Baja

- Ambientes de prueba y desarrollo.

6.2. RIESGOS ASOCIADOS A LA CONTINUIDAD DEL NEGOCIO

El AGN contempla implícitamente en la gestión de sus procesos la identificación y administración de los riesgos como practica 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 del AGN

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 del AGN 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 el AGN 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 el canal de comunicación para difundir un mensaje o reportar datos estadísticos o información
Cumplimiento	Incumplimiento legal	Contempla el incumplimiento de la normativa vigente de las obligaciones contratadas por el AGN y/o de requisitos legales exigibles
Imagen	Pérdida de credibilidad y confianza en el AGN	Está relacionado con la percepción y la confianza por parte de los ciudadanos hacia el AGN
Información	Perdida de información	Se asocia con la perdida de información física y/o digital

Operativo	Daño o deterioro de los activos tangibles	Comprende el daño o deterioro de los bienes muebles del AGN
Operativo	Inexistencia de los bienes y servicios necesarios para el funcionamiento normal del AGN	Carencia de bienes y/o servicios requeridos en el AGN para su funcionamiento normal
Tecnológico	Acceso no autorizado	Se asocia con el acceso a los sistemas de información, aplicativos, bases de datos o servidores si autorización previa
Tecnológico	afectación de la infraestructura tecnológica	Está relacionado con en el daño, pérdida o deterioro a nivel hardware y comunicaciones
Técnico	Servicios inadecuados de tecnología de la información	Contempla la pertinencia, calidad y oportunidad de los servicios de tecnología y las deficiencias en la prestación de los mismos

6.3. PRUEBAS Y REVISIÓN PERIÓDICA DEL PLAN

En las sesiones de Comité Desarrollo Administrativo se aprobará y monitoreará el plan de continuidad; las acciones preventivas se llevarán a cabo en todo el AGN según la planificación 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, el Grupo de Sistemas, Comunicaciones y el Oficial de seguridad de la Información. (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 Desarrollo Administrativo; de igual manera los resultados y el seguimiento se realizará dos veces al año.

6.4. PASO A PASO PARA SEGUIR EL PLAN

Una vez construido y aprobado el plan de continuidad el AGN deberá emprender las acciones necesarias para comunicarlo a todos los funcionarios , contratistas y pasantes , de esta manera estar preparados para enfrentar situaciones de emergencia y restablecer en el menor tiempo posible el servicio, para lo cual se seguirá el siguiente protocolo:

- Declaración manifiesta de la emergencia – Comité Desarrollo Administrativo
- Convocar el Comité Desarrollo Administrativo – Secretario General
- Contactar centro de operaciones (propio y externo (UNGD))- Realizar Reunión
- Analizar daños (elaborar lista de chequeo) Comité Desarrollo Administrativo) (grupo de crisis creado por el Grupo de Gestión Humana)
- Llamado al equipo de restablecimiento (el cual se creará y hará parte del grupo de crisis)
- Llamado al personal interno y comunicación de acción a seguir - Grupo de Crisis
- Restablecimiento de los sistemas de información según el plan –Coordinador Grupo de Sistemas
- Re establecimiento gradual de la información - Coordinador Grupo de Sistemas
- Análisis de situación - Grupo de Crisis
- Establecer plan de mejoramiento a partir del análisis.

6.4.1. Notificación de información hacia los empleados

Dependiendo de la posición del empleado dentro del AGN, se le pondrá en contacto a través del coordinador de área, sub director o secretario general; debe contener:

• Naturaleza de la emergencia que se ha producido
• Estimaciones de daños que se conozcan
• Punto de encuentro

Cada coordinador de área o subdirector, será el punto de contacto con su equipo de apoyo, hará llegar la información necesaria y las instrucciones a su equipo y será responsable de un informe sobre la situación correcta de los progresos en su equipo.

6.4.2. Coordinación con sitios fuera de la organización

La notificación a los terceros que se encuentren en las instalaciones del AGN debe ser implementada en máximo 15 minutos después de tomada la decisión de activar el BCP.

6.4.3. Plan de criterios para la activación

Los criterios de activación se basan en la evaluación de los siguientes parámetros:

- Seguridad del personal y/o magnitud de los daños de las instalaciones
- Magnitud del daño de la infraestructura (Física, Operacional, otra)
- Estimativo del tiempo de interrupción

Si la notificación inicial es clara y evidente, se puede activar el plan de continuidad asignando un código de color:

Morado: Perdida total del centro de operación ESC

Rojo: Incidentes graves en curso que afectan los procesos críticos del AGN

Amarillo: Incidentes graves en progreso, pero bajo control.

Verde: El incidente ya no está en progreso o el incidente se realiza bajo procedimientos operativos normales.

En los demás casos, la notificación se iniciará como código de color amarillo. Así mismo, después de la evaluación de los daños, el código se puede cambiar a rojo o verde, dependiendo del resultado.

6.4.3.1. **Criterio para código Morado**

Incidente grave que afecte, debido a causas de desastre naturales o evento de fuerza mayor; así mismo se considera la ausencia masiva de personal que impida la operación normal.

Instrucciones:

a. Activar Lugar Alterno de Operación ESC. (definido con anterioridad por el Comité Desarrollo Administrativo)
b. Activar Plan de Continuidad del Grupo de Gestión Humana solo si es necesario.

6.4.3.2. **Criterio para código Rojo**

Un incidente que tiene efectos severos o catastróficos para las operaciones, activos o personas del AGN, algunos escenarios son:

• Incidentes en las facilidades del Centro de cómputo. (Falla de Suministro Eléctrico, Aire Acondicionado o presencia de alarma de detección de incendios), al no existir un centro alterno se corre el riesgo de quedar el AGN sin comunicaciones o en el peor de los casos, una pérdida total de la información
• Perdida de infraestructura crítica: Enlaces de Red, Telefonía o Directorio Activo.
• Epidemia de enfermedades humanas.

Instrucciones:
a. Activar Plan de Contingencia Infraestructura de acuerdo al Escenario.
b. Activar Plan de Continuidad HSE solo si es necesario.

6.4.3.3. **Criterio para código Amarillo**

Progreso de un riesgo o incidente grave, pero bajo control:

- Perdida de aplicaciones críticas: Financieras, Talento Humano, Hora Legal Premium
- Ataque de virus informáticos.

Instrucciones:

- ❖ Solicitar al Administrador del Centro de cómputo, ejecutar los procedimientos de restauración de servicios de acuerdo al Incidente
- ❖ Plan de retorno a la normalidad (Recuperación y Restauración)

La meta de la recuperación y restauración es recobrar la operatividad de la organización manteniendo la entrega de productos y servicios críticos. En esta etapa se incluyen las siguientes actividades:

6.5. Decidir donde reiniciar operaciones

Es necesario establecer si las facilidades estropeadas se pueden reparar, dependiendo del daño y al no existir un centro alterno el Comité Desarrollo Administrativo debe tomar acciones del caso.

Lo anterior deberá decidirse entre el Coordinador del BCP (que para este caso es el mismo Coordinador de Grupo de Sistemas).

6.6. Regreso del personal a las instalaciones

Una vez se realicen los trabajos de reparación de las facilidades estropeadas, el Coordinador del BCP y el Gestor de incidentes (que para el AGN será el Secretario General) notificarán al personal el momento a partir del cual el personal pueda regresar a las instalaciones para reanudar la entrega del servicio.

6.7. Restablecer las operaciones normales de la organización.

Con el personal operando en las instalaciones recuperadas, el coordinador del BCP con el apoyo del Gestor de Incidentes, procederán a evaluar y monitorear la entrega de los servicios afectados con el objetivo de en el menor tiempo posible, llegar a los niveles de entrega anteriores a la interrupción

6.8. Reanudación de las operaciones en los niveles anteriores a la interrupción

Al conseguir operar a los niveles previos a la interrupción el coordinador del BCP y el Gestor de Incidentes notificarán al COE el retorno a normalidad en la entrega de los servicios afectados vía correo electrónico y por este mismo medio se procederá con la notificación a los clientes afectados por la interrupción.

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

CONTROL DE CAMBIOS

VERSIÓN	FECHA APROBACIÓN	RESPONSABLE	DESCRIPCIÓN
1.0	25-05-2018	Manuel Gómez	Versión inicial
2.0	30/03/2021	Omar Villareal	Actualización