****

La recuperación ante desastres se ha definido tradicionalmente como la recuperación de los sistemas de TI después de eventos catastróficos que generan una interrupción en los sistemas. ISACA (2020)

**PLAN RECUPERACIÓN DE DESASTRES**

**Superintendencia de Industria y Comercio**

Bogotá, 2022

**CONTENIDO**

[1. OBJETIVO 2](#_Toc117512019)

[2. DESTINATARIOS 2](#_Toc117512020)

[3. ALCANCE 2](#_Toc117512021)

[4. ALCANCE 2](#_Toc117512022)

[5. REFERENCIAS 3](#_Toc117512023)

[6. GENERALIDADES 4](#_Toc117512024)

[7. SUPUESTOS Y RESTRICCIONES 5](#_Toc117512025)

[8. ANÁLISIS DE IMPACTO EN EL NEGOCIO - BIA 5](#_Toc117512026)

[9. RIESGOS DE CONTINUIDAD DE TI 2](#_Toc117512027)

[13. HOJA DE RUTA 17](#_Toc117512028)

[14. DOCUMENTOS RELACIONADOS 18](#_Toc117512032)

# **OBJETIVO**

Planear las estrategias para apoyar la continuidad de la prestación de los trámites y servicios de la Entidad a los ciudadanos, grupos de valor y partes interesadas; a través de la recuperación de los sistemas de información que ante la materialización de escenarios de desastre puedan causar interrupción total o parcial de los servicios misionales.

1. **DESTINATARIOS**

El presente documento está dirigido a todos los funcionarios y contratistas de la Oficina de Tecnología e Informática y líderes de los procesos misionales que se encuentren relacionados con la continuidad de los servicios de TI.

1. **ALCANCE**

El Plan de Recuperación de Desastres cubre exclusivamente las estrategias de recuperación de la infraestructura tecnológica para la recuperación de los trámites y servicios misionales críticos de acuerdo con el Análisis de Impacto al Negocio -BIA.

1. **GLOSARIO**

ANÁLISIS DE IMPACTO AL NEGOCIO (BIA): Proceso en el que se analiza el impacto de una interrupción conforme avanza el tiempo.

CONTINUIDAD DE NEGOCIO: Capacidad de una organización de continuar la oferta de productos y servicios dentro de un período de tiempo aceptable a una capacidad predefinida durante una interrupción.

DESASTRE: Es un evento nocivo, inesperado o imprevisible, que afecta seriamente el funcionamiento normal de los trámites y servicios de TI.

INTERRUPCIÓN: Incidente bien sea esperado o no, que causa una alteración negativa y no planeada de la oferta esperada de los productos y servicios de acuerdo con los objetivos de la organización.

LIF: Laboratorio de Informática Forense.

MTPD: Periodo de tiempo dentro del cual el impacto de no reanudar las actividades sería inaceptable para la organización.

OPERACIÓN ALTERNA: La operación Alterna se da en el momento que se activa el sitio de contingencia como soporte para la prestación de los servicios de TI, en la operación Alterna se debe tener en cuenta que la capacidad de los recursos podría no ser la misma de la operación normal, por lo cual algunos procesos podrían tomar más tiempo en su ejecución, o podría no haber capacidad de atención del 100% de la operación.

OPERACIÓN INTERRUMPIDA: Es el periodo de tiempo transcurrido entre el evento de un desastre que causa indisponibilidad de los servicios y la recuperación de la operación, ya sea en sitio principal o alterno.

OPERACIÓN NORMAL: Es la operación de los trámites y servicios tal como funcionan actualmente, esto es, cada servicio es soportado en la sede en la que fue definida originalmente.

OPERACIÓN RESTABLECIDA: Este estado se alcanza cuando se ha retornado la operación de todos los servicios a su estado normal, esto es, todos los servicios y componentes de aplicación se encuentran ejecutando correctamente y bajo las mismas condiciones que presentaba antes del desastre.

PLAN DE CONTINUIDAD DE NEGOCIO: Información documentada que orienta a una organización para responder una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad de negocio.

RPO: Corresponde al punto en el cual se retoma la información en caso de recuperación. Se asocia al último backup generado en las aplicaciones

RTO: Período de tiempo dentro del MTPD, para reanudar las actividades interrumpidas en una capacidad aceptable mínima especificada.

TRÁMITE: Conjunto de requisitos, pasos, o acciones reguladas por el Estado, dentro de un proceso misional, que deben efectuar los ciudadanos, usuarios o grupos de interés ante una Entidad u organismo de la administración pública o particular que ejerce funciones administrativas, para acceder a un derecho, ejercer una actividad o cumplir con una obligación, prevista o autorizada por la ley.

1. **REFERENCIAS**

| **JERARQUÍA DE LA NORMA**  | **NÚMERO/ FECHA**  | **TÍTULO** | **ARTÍCULO** | **APLICACIÓN ESPECÍFICA**  |
| --- | --- | --- | --- | --- |
| Decreto Nacional | 1008 del 14 de junio de 2018 | Política de Gobierno Digital | Artículo 2.2.9.1.1.1 al 2.2.9.1.4.2 | Aplicación total |
| Norma Técnica Colombiana | ISO 27001 | Tecnología de Información, Técnicas de seguridad Sistemas de gestión de la seguridad de la información | Ítem A.17 | Aspectos de seguridad de la información, de la Gestión de Continuidad de Negocio. |
| Norma Técnica Colombiana | ISO 22301 | Seguridad y resiliencia. Sistema de gestión de continuidad de negocio. Requisitos | Aplicación total | Aplicación total |

1. **GENERALIDADES**

El propósito de un Plan de Continuidad de Negocio (BCP) es prepararse para, brindar y mantener los controles y las capacidades para gestionar el total de una organización para seguir operando durante una interrupción.

La relación entre un BCP y un DRP (Plan de Recuperación de Desastres), es tal que el DRP un subconjunto del BCP. Específicamente mientras que las metas del BCP incluyen la prevención y mitigación del incidente, el DRP está centrado en lo que debe hacerse para restablecer las operaciones después de que ya ha ocurrido un incidente. Un BCP puede verse como un proceso continuo que está siendo implementado activamente en los escenarios habituales, mientras que el DRP es reactivo por naturaleza y se ejecuta solo cuando se cumple con una serie específica de condiciones, es decir, la entidad ha incurrido en un incidente catastrófico.

La recuperación ante desastres se ha definido tradicionalmente como la recuperación de los sistemas de TI después de eventos de interrupción que causan fallas en los sistemas, tales como huracanes e inundaciones que tiene como resultado la falta de acceso o interrupciones prolongadas de energía y comunicación. La recuperación del negocio se define como el restablecimiento de todos los procesos de misionales críticos que son necesarios para continuar o restablecer las operaciones. La recuperación incluye: la recuperación ante desastres, gestión de crisis, gestión de emergencias y plan de comunicaciones. En la gráfica No. 1 se ilustra lo enunciado.