LINEAMIENTOS PARA LA RECUPERACIÓN DEL SERVICIO ANTE UN EVENTO ADVERSO

Agencia Nacional de Tierras

DIRECCIÓN DE GESTIÓN DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD
SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

Octubre 2021

Contenido

1.INTRODUCCIÓN 3
2.OBJETIVO 3
3.DEFINICIONES 4
4.GENERALIDADES..... 4
4.1 Efectuar el análisis del impacto del negocio BIA 4
4.2 Identificación y valoración de los riesgos informáticos 5
4.3 Definir las estrategias generales de recuperación 5
5.CAUSAS DE INTERRUPCION Y ACCIONES A EJECUTAR 6
6.SUPUESTOS 7
7.ESCENARIOS 7

1. INTRODUCCIÓN

Teniendo en cuenta la importancia que representa los activos de información para la Agencia Nacional de Tierras (ANT), es necesario disponer de unos lineamientos que permitan identificar las principales acciones y actividades que se deben desarrollar ante un evento critico que afecte la prestación de un servicio tecnológico que ofrezca la entidad o que active el plan de recuperación ante desastres, esto teniendo las variables y afectaciones que pueden llegarse a presentar y las consecuencias, las cuales se tendrán en cuenta a través de un análisis de impacto del negocio (BIA).

2. OBJETIVO

Establecer los lineamientos que se deben cumplir en el caso que se llegase a presentar un evento o incidencia que afecte la prestación de alguno de los servicios tecnológicos que ofrece la ANT, teniendo en cuenta la criticidad de cada uno de estos.

3. DEFINICIONES

Acciones prioritarias: Actividades que deben contemplarse de prioridad ante la materialización de un evento o incidente.

Amenaza: Posible hecho que puede afectar el desarrollo de un proceso.

Continuidad del Negocio: Son los planes en donde se organizan y definen las acciones, riesgos y evaluaciones correspondientes a actividades, con el objetivo de recuperar y restaurar las funciones criticas interrumpidas por un evento o incidente catastrófico.

Catastrófico: Suceso fatídico que altera el orden regular de las cosas que causa daño o perdida no aceptable de una organización.

Incidente: Suceso que ocurre generando una interrupción, o alteración de las actividades gestionadas en un proceso.

BIA: (Business Impact Analysis) por sus siglas en inglés, es el informe que permite identificar los procesos críticos de una entidad, analizando los impactos con relación a la gestión del negocio.

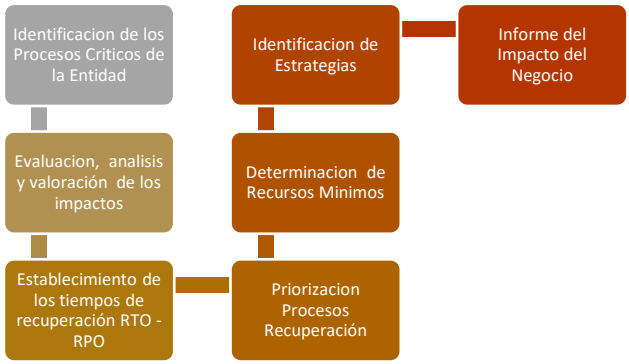
Riesgo: Posible efecto sobre los objetivos de una actividad.

4. GENERALIDADES

Teniendo en cuenta las buenas prácticas que se deben efectuar en cuanto a temas de plan de continuidad del negocio, o plan de recuperación ante desastres, es necesario contar con información que será la base general para la toma de decisiones y priorizaciones como son:

4.1 Efectuar el análisis del impacto del negocio BIA

El objetivo de este insumo es el de identificar los principales procesos críticos de la entidad y determinar las principales actividades de impacto a la ocurrencia de un incidente que afecta la operación de los servicios que sean determinados fundamentales para la operación del negocio en el cual se deberá llevar a cabo las siguientes actividades:



4.2 Identificación y valoración de los riesgos informáticos

Durante esta etapa se debe realizar la actualización de los riesgos digitales que se han identificado en la entidad, analizando los factores que potencialmente podrían afectar la normal operación, dentro de estos factores se encuentran los siguientes:

- Las actividades que realiza la entidad para la obtención del servicio.
- Las herramientas y aplicaciones que soportan la operación del servicio del SIT.
- Equipos e infraestructura técnica que soporta la operación del servicio.
- La relación del recurso humano y las actividades que realizan cada uno de sus integrantes dentro de la operación del SIT.
- Procesos Críticos, determinados por (2) valoraciones:
    - valoración cualitativa.
    - valoración cuantitativa.

4.3 Definir las estrategias generales de recuperación

Dentro de los temas más importantes que se deben definir en temas de continuidad del negocio está la definición de las estrategias que se deben analizar e implementar en la Entidad, siendo acordes a los dimensionamientos determinados según las necesidades en cumplimiento de su misionalidad, por lo tanto, se deberá tener en cuenta los siguientes aspectos:

- Análisis y evaluación de los daños.
- Evaluación de los tiempos estimados para la recuperación de los servicios.
- Evaluación de las acciones que se deberán tomar conforme al tipo de incidente.

Incidente menor: Son los incidentes que pueden ser remediados de una manera más rápida por su nivel de criticidad, en donde a través de herramientas de diagnóstico y reparación de fallas puedan ser intervenidas.

Indecente mayor: Este tipo de incidencias son la que son clasificadas de alto impacto donde se afecta la infraestructura tecnológica principal de la Entidad impidiendo el cumplimiento de las funciones y prestación de los servicios, este tipo de incidentes deben ser identificados y remediados con un tiempo de afectación mínimo y a su vez se tomará la decisión de la necesidad de activación del Plan de Recuperación ante Desastres (DRP sus siglas en ingles).

Incidente catastrófico: Este tipo de incidentes son los que afectarían el 100% de la totalidad de las operaciones de la entidad declarando de manera inmediata la contingencia y la activación del DRP.

Adicionalmente, en la estrategia se deben contemplar temas como:

- Los equipos necesarios para el desarrollo, para la recuperación de los servicios.
- Las responsabilidades y funciones de cada uno de los equipos que intervienen.
- El desarrollo de los procedimientos de alerta y protocolos de acción ante eventos o incidente.
- La estrategia de vuelta a la normalidad.

Asimismo, es necesario proponer estrategias de mitigación de eventos como son:

- Entrenamiento del personal.
- Disponibilidad de personal competente.
- Procesos de gestión y monitoreo.
- Procesos de administración.
- Disponibilidad de políticas y procedimientos.
- Disponibilidad de planes de respuesta a incidentes.
- Definición de niveles de soporte y escalamiento.
- Redundancia local en componentes críticos de la infraestructura.
- Ambientes controlados de operación.
- Disponibilidad de medios de respaldo de información.
- Pruebas y ejercicios de los procedimientos de recuperación.
- Disponibilidad de esquemas organizacionales de respuesta.

5. CAUSAS DE INTERRUPCION Y ACCIONES A EJECUTAR

A continuación, se detallan las posibles interrupciones y las acciones a seguir en caso de que las mismas se materialicen de la siguiente manera:

5.1 No acceso al sitio normal de trabajo:

Se presenta cuando por algún evento como desastre natural, enfermedad contagiosa, actividad terrorista, problemas de transporte, huelgas, entre otros, el personal no puede acceder a su lugar de trabajo para desarrollar las actividades propias de su cargo.

5.2 Caída de los sistemas tecnológicos:

Se presenta cuando el hardware o software no pueden ser accedidos para la prestación del servicio de la infraestructura tecnológica.

5.3 Ausencia de personal:

Se presenta cuando más del 85% de los colaboradores que ejecutan los procesos no pueden asistir a trabajar para desarrollar las actividades propias de su cargo.

5.4 Escenarios de falla:

Corresponden a los escenarios de falla que se han dispuesto para los simulacros en ambientes controlados y a los que está expuesto el servicio de infraestructura tecnológica.

6. SUPUESTOS

- Se contará con todos los recursos o permisos, en caso de ser necesarios, para acceso a infraestructura y servicios de la infraestructura tecnológica por parte de los terceros que sean necesarios.

- Se contará con todos los protocolos de eventos de riesgo no informático que afecten a la prestación de los servicios de la ANT.

- Se deberá promover la elaboración de los siguientes planes, los cuales serán parte fundamental para la recuperación de los servicios:

    - Plan de respuesta a emergencias.
    - Plan de evaluación de daños.
    - Plan de salvamento.
    - Plan de registros vitales.
    - Plan de relaciones públicas y gestión de crisis.
    - Plan de servicios y alojamiento.
    - Plan de seguridad.
    - Plan de personal.
    - Plan de comunicación.
    - Plan de administración y finanzas.

7. ESCENARIOS

A continuación, se relacionan los escenarios identificados y las estrategias de recuperación previstas:

Escenario	Descripción	Sistemas y/o Componentes Localmente Redundantes.	Disponibilidad de Procedimientos de Atención a Incidentes y Problemas.	Disponibilidad de Procedimientos de Recuperación Tecnológica.	Disponibilidad de Copias de Respaldo.	Replicación de Datos y Transacciones a Sistemas Geográficamente Redundantes	Disponibilidad de Data Center Alterno	Contratos con Cláusulas y/o Acuerdos de Servicio que incluyen requerimientos de Continuidad de las Operaciones
E1	El evento genera una falla "total" en los sistemas de información del ambiente de producción del SIT, localizadas en el Data Center Principal[1].			■		■	■	■
E2	Evento que inhabilita el Data Center Principal.			■		■	■	■
E3	Evento de falla en los enlaces de comunicación de las oficinas de la sede principal, o del Data Center Principal.	■	■					■
E4	Evento de falla que afecta la disponibilidad del SIT o sistemas conexos que soportan los procesos críticos del negocio.	■	■		■			■
E5	Evento de falla que afecta la disponibilidad de servicios de tecnología y/o sus derivados que han sido subcontratados con terceros.							■

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
25-10-2021	01	Primera versión del documento.

Elaboró: Basco German Ricaurte G.	**Revisó:** Duberly Eduardo Murillo Barona **Cargo:** Subdirector - SSIT	**Aprobó:** William Gabriel Reina Tous

[1] Un Data Center es el espacio donde se concentran los recursos tecnológicos para el procesamiento de información de una organización

	Firma: ORIGINAL FIRMADO	
Cargo: Contratista – Subdirección de Sistemas de Información de Tierras	**Revisó:** Eduard Fabian Álvarez Pacheco **Cargo:** Contratista – Subdirección de Sistemas de Información de Tierras	**Cargo**: Director - DGOSP
Firma: ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO	
	Revisó: Jenifer Andrea Álvarez Hernández **Cargo:** Contratista - DGOSP **Firma:** ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO