AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

GUÍA DE GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

BOGOTÁ D.C. SEPTIEMBRE DE 2021

Contenido

1. OBJETIVO

Describir la Gestión de Continuidad de los Servicios TI críticos, identificando los riesgos que pueden llegar a afectar los acuerdos de niveles de servicio (SLA) predefinidos como aceptables tras incidentes de interrupción de la actividad definidos por la Oficina de Tecnologías de la Información-OTI.

1.1. OBJETIVOS ESPECIFICOS

- Elaborar los documentos de Plan de Continuidad de cada servicio crítico de TI y mantenerlos actualizados.
- Mantener de manera eficiente la operación de la organización y los servicios prestados por la OTI después de una interrupción del servicio imprevisible o indeseada, reduciendo el impacto negativo en los usuarios.

2. ALCANCE

El contenido de este documento aplica para la Agencia de Reincorporación y la Normalización - ARN y la prestación de los servicios TI críticos de la Oficina de Tecnologías de la información - OTI.

3. DEFINICIONES

ACUERDOS DE NIVELES DE SERVICIO (SLA): Acuerdo documentado entre la organización y el cliente que identifica los servicios y su rendimiento acordado.

ANS: Acuerdos de Niveles de Servicio.

AMENAZA: Cualquier elemento que pueda aprovechar una vulnerabilidad. Cualquier causa potencial de un Incidente puede ser considerada una amenaza.

BIA: Business impact analysis – Bia

DISPONIBILIDAD: Capacidad de un servicio, o componente de un servicio, de realizar la función requerida en un momento acordado o durante un periodo de tiempo acordado.

DRP: Disaster Recovery Plan (Plan de Recuperación de Desastres)

INCIDENTE: Una interrupción inesperada de un servicio, una reducción en la calidad de un servicio o un evento que todavía no ha tenido impacto en el servicio para el cliente o para el usuario. En la herramienta de gestión se usa este término

para los incidentes que han sido escalados por el primer nivel de atención y son identificados con la letra IM.

INCIDENTE MAYOR: Cualquier evento identificado con prioridad y urgencia alta de acuerdo a la matriz de impacto definida por la ARN.

IMPACTO: Determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.

MTD: Tiempo de inactividad máximo tolerable

OTI: Oficina de Tecnología de la información

PROBLEMA: Causa de una o más incidencias reales o potenciales. En el momento en el que se crea el registro del problema, no es frecuente conocer su causa, por lo que es necesario realizar su investigación mediante el proceso de Gestión de Problemas.

PUNTO OBJETIVO DE RECUPERACIÓN (RECOVERY POINT OBJETIVE – RPO): Es un nivel de tolerancia permitida que está definido por la cantidad máxima de información que puede ser perdida cuando el servicio es restaurado tras una interrupción. El RPO se expresa como una longitud de tiempo antes de una falla.

PLAN DE CONTINUIDAD DE LOS SERVICIOS DE TI: Plan que define los pasos necesarios para recuperar uno o más servicios de TI. El Plan además identificará los disparadores de la Invocación del plan, las personas que han de ser involucradas, las comunicaciones necesarias etc.

PLAN DE RECUPERACIÓN DE DESASTRES (DRP): Un plan de recuperación ante desastres (del inglés Disaster Recovery Plan) es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

RECUPERACIÓN GRADUAL: Opción de recuperación que también es conocida como reserva fría. Normalmente la recuperación de recuperación del servicio de TIC se extiende a un periodo de tiempo superior a 72 horas. La recuperación gradual normalmente emplea recursos portátiles que pueden soportar el entorno, sin embargo, no contienen aplicaciones.

RECUPERACIÓN INMEDIATA: Opción de Recuperación también conocida como reserva medio. Normalmente la recuperación de recuperación del servicio de TI se

da en un periodo de tiempo entre 24 y 72 horas. La recuperación media emplea normalmente recursos fijos o portátiles compartidas que contienen sistemas de información informáticos y componentes de red. El hardware y software necesita ser configurado y los datos deben ser restaurados como parte integrante del Plan de Continuidad del Servicio de TI.

RPO: Recovery point objetive

RTO: Recovery time objetive

TIEMPO OBJETIVO DE RECUPERACIÓN (RECOVERY TIME OBJETIVE – RTO): El tiempo máximo permitido para la recuperación de una interrupción de un servicio TI. El nivel de servicio a ser provisto debe ser inferior a los definidos por los ONS (objetivos de nivel de servicio) para asegurar que estos no sean desvirtuados. Los RTO para cada servicio de TIC deberían ser negociados, acordados y documentados.

TI: Tecnologías de la Información

URGENCIA: Depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente y/o el nivel de servicios acordados.

4. CONSIDERACIONES GENERALES

- Las estrategias del plan de recuperación de servicios de TI son acordadas entre los líderes funcionales y técnicos responsables de cada servicio.

- La OTI ha definido los lineamientos de continuidad de servicios de TI, los cuales deben ser comunicados a todos los involucrados, de manera que cada uno pueda identificar y ejercer su rol en caso de una interrupción o activación del servicio.

- Cada vez que surjan oportunidades de mejora provenientes de la ejecución de las pruebas de continuidad de servicios tecnológicos de forma periódicas, se debe actualizar la documentación relacionada con el servicio, así como informar a la gestión de mejora continua.

- La ejecución de las pruebas de continuidad de servicios de TI debe realizarse de acuerdo con lo descrito en el documento TI-G-09 Guía de Gestión de Cambios de Tecnologías de la Información

- Articular acciones con el Proyecto de implementación del Sistema de Gestión de Continuidad del Negocio.

- Si se presentan cambios significativos en el entorno del servicio, se deben ejecutar las pruebas definidas en el plan de continuidad de cada servicio.

- Se debe identificar riesgos de continuidad de manera periódica para los servicios TI e infraestructuras críticas.

5. PASOS GENERALES GESTIÓN DE CONTINUIDAD

Para el desarrollo de la Gestión de Continuidad se deben considerar las siguientes fases y actividades descritas, con el fin de establecer un diseño efectivo frente a las necesidades de continuidad de negocio en el marco de los servicios tecnológicos críticos de la ARN de los servicios prestados por la OTI.

- **Análisis de impacto de Servicios TI**

  Su objetivo es analizar los activos, infraestructuras y tiempos de recuperación óptimos de los sistemas críticos, de acuerdo con los servicios TI establecidos teniendo en cuenta los siguientes aspectos:

  - Identificar la infraestructura física críticas por cada servicio TI.
  - Determinar el RTO, RPO y MTD de cada servicio TI: se debe estimar el tiempo de recuperación objetivo, el punto de recuperación objetivo y el tiempo máximo tolerable fuera de servicio para cada proceso en cada instalación con el fin de ayudar en la definición de las estrategias de recuperación.

- **Análisis de riesgos (AR)**

  Para la identificación, valoración, medidas de control y seguimiento de los riesgos de continuidad de los servicios de TI prestados por la ARN, se tendrá como referencia las disposiciones de la ARN para la gestión de riesgos.

- **Plan de Continuidad de Servicios TI**

  Establecer las necesidades y/o requisitos sobre los planes de continuidad, que se vayan a implementar por servicio TI.

  Los documentos del plan de continuidad de servicios TI se puede consultar en el repositorio del proyecto en la siguiente ruta:

\\ruttman\GESTION_TI\Gestion Oficina TI\

6. DESCRIPCIÓN DE ACTIVIDADES DE LA CONTINUIDAD

No	Actividad	Descripción
1	Identificar Requerimientos de Continuidad	El líder de servicio establece los requerimientos de Continuidad de Negocio para los servicios de TI, de acuerdo con el análisis de riesgos e impacto de negocio de la ARN.
2	Actualizar estrategias de Continuidad de Negocio de Servicios de TI	Los gestores de continuidad revisarán las estrategias de continuidad, con base a los cambios de tecnologías. La información enviada por los líderes de los servicios se almacenará en la ruta: \\ruttman\GESTION_TI\Gestion Oficina TI\
3	Validar / solicitar aprobación de estrategia	El líder de servicio y los gestores de continuidad validarán la estrategia de continuidad y recuperación del servicio de TI en caso de presentarse un desastre.
4	¿Estrategia aprobada?	Si después de definir la estrategia, se tienen observaciones por las partes interesadas se pasa al punto 5. Si no se tienen observaciones se pasa a la actividad 6
5	Proponer Ajustes a la estrategia	El líder de servicio debe proponer los ajustes correspondientes al Plan de Continuidad del Servicio de TI.
6	Actualizar Plan de Continuidad de Servicios de TI	Los Gestores de Continuidad realizará los ajustes al Plan de Continuidad de Servicios de TI de acuerdo con las observaciones. Se deben realizar los ajustes a las observaciones de la estrategia, con el objetivo de ser aprobado por las partes interesadas.
7	Realizar Divulgación a los involucrados	Los gestores de continuidad luego de definir el Plan de Continuidad de Servicios de TI deben divulgar a las partes interesadas.

6.1. ENTRADAS

Proveedor	Entrada
Gestión de la Disponibilidad	Estrategias de Disponibilidad
Gestión de Eventos	Alarmas Críticas en los elementos de configuración
Gestión de Incidentes	Incidentes mayores que afectan la operación de los servicios TI
Gestión de la Configuración	Información de los Elementos de Configuración
Gestión de la Capacidad	Reportes de capacidad
Gestión de Cambios	Solicitudes de Cambios
Gestión de la Seguridad	Lineamientos de seguridad
Gestión de Mejora Continua	Reporte sobre planes de mejora de periodos anteriores a los cuales se debe revisar su cumplimiento
Gestión del Conocimiento	Conocimiento de los servicios
Todos los Servicio TI	Procedimientos de recuperación documentadas, listado de riesgos asociados a la continuidad del servicio y definición de RTO y RPO de acuerdo a los ANS de disponibilidad del servicio.

6.2. SALIDAS

Salida	Cliente
Gestión de la Seguridad	Plan de Continuidad del Servicio
Gestión de Mejora Continua	Acciones de mejora, acciones correctivas y preventivas del proceso
Gestión del Conocimiento	Informe de las pruebas DRP realizada sobre los servicios TI.
Todos los Servicios TI	Informe de resultados de las pruebas DRP.

6.3. RELACIONES

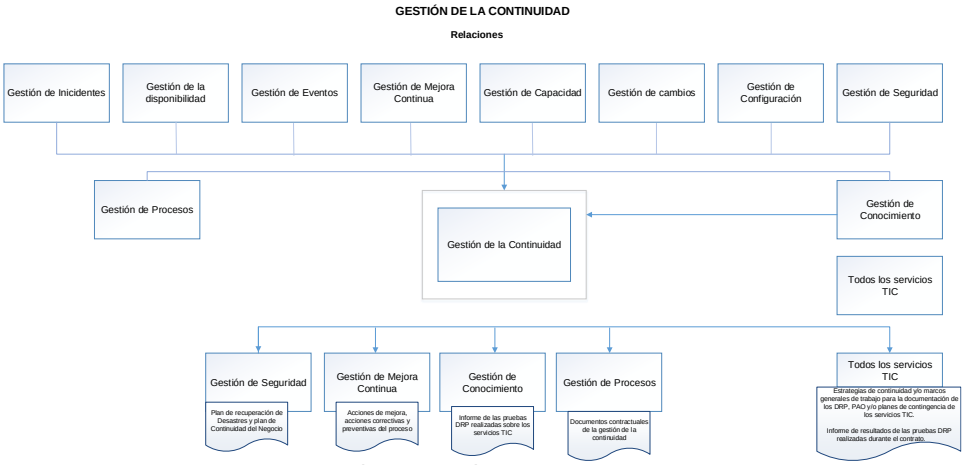

Ilustración 1: Relación con otras gestiones

7. INFORMES PERIÓDICOS (ENTREGABLES)

Nombre	Descripción	Periodicidad	Responsable
Informe de Gestión	Informe con los detalles de la gestión del proceso para el periodo incluyendo Informe con las acciones de mejora que se ejecutarán al proceso y los planes de acción del periodo.	Anual	Gestores de Continuidad
Informe de pruebas realizadas al plan de recuperación de desastres	Informe con detalle de pruebas realizadas al plan de recuperación de desastres	Por demanda	Líder de servicio

8. RESPONSABILIDADES

Rol	Responsabilidades
Gestor de Continuidad.	• Dar a conocer los lineamientos de las actividades de análisis de riesgos, estrategias de la continuidad y plan de recuperación de desastres en los servicios de TI. • Apoyar la gestión para la ejecución de los planes de pruebas a nivel de DRP. • Apoyar la actualización de los procesos de la continuidad, e identificación y aplicación de las oportunidades que permitan mejorar el desempeño de estos. • Acompañar en las pruebas DRP realizadas a los servicios TI. • Llevar a cabo las revisiones regulares de los planes de gestión de continuidad. • Informar el fin del plan de continuidad y realizar informe y recomendaciones de continuidad.
Líderes de Servicios	• Evaluar impacto de la afectación a los servicios en el evento de materialización de un desastre y la aplicación del presente documento en caso de afectación a su servicio. • Cumplir los planes de continuidad y las políticas de continuidad necesarios para proteger la continuidad de los servicios de TI que administra en caso de un eventual desastre. • Ejecutar las actividades de los planes y procedimientos del DRP. • Realizar seguimiento a la ejecución, y validar la viabilidad de retornar a la operación normal. • Mantener informados internamente los avances y cierres de los planes de recuperación, retorno y cierre del DRP. • Coordinar la ejecución de los planes de recuperación y restauración para los respectivos servicios. • Coordinar la realización de los procedimientos de retorno a la operación normal.

9. MATRIZ RACI

La definición de la matriz de responsabilidades se constituye como una herramienta práctica y útil cuando se establecen las obligaciones que tiene cada uno de los actores del flujo.
Cuando se diseña un servicio es imperativa la definición clara de los roles que hacen parte de estos y las responsabilidades que cada uno tiene en su ciclo de vida, por esto se hace necesaria la conformación de una matriz RACI que represente la asignación de estas responsabilidades. RACI es el acrónimo empleado para las cuatro funciones principales de:

- **Responsible (Ejecutor):** La persona o personas responsables por la ejecución de la actividad.
- **Accountable (Dueño):** Este es el rol encargado de aprobar el trabajo realizado y a partir de este momento es quien responde a las directivas o instancias superiores por el trabajo.
- **Consulted (Consultado):** Son las personas que son consultadas y en quienes se busca una opinión.
- **Informed (Informado):** Son los grupos de personas a quienes se informa sobre el progreso y resultados del trabajo.

En la siguiente matriz se asignan las responsabilidades de cada rol dentro del proceso Gestión de la Continuidad de Tecnologías de la Información:

ROL / Actividad	Gestor de Continuidad	Líder de servicio
Identificar Requerimientos de Continuidad	CI	RA
Actualizar estrategias de Continuidad de Negocio de Servicios de TI	RA	CI
Validar / solicitar aprobación de estrategia	CI	RA
Proponer Ajustes a la estrategia	CI	RA
Actualizar Plan de Continuidad de Servicios de TI	RA	CI
Realizar Divulgación a los involucrados	RA	CI

10. ANEXOS

ANEXO 1 LINEAMIENTOS DE CONTINUIDAD DE TI

La Oficina de Tecnologías de información (OTI) responsable de la operación y administración de los recursos tecnológicos que soportan los procesos de la Agencia para la Reincorporación y la Normalización (ARN) y conociendo la importancia que tienen los servicios de TI para la operación y continuidad de los procesos de la Entidad, se asegurará de implementar estrategias o planes de continuidad que permitan reducir el riesgo y aumentar la capacidad de recuperación de los servicios, en caso interrupción o contingencias en los mismos.

la OTI ha establecido un conjunto de lineamientos articulados con los objetivos estratégicos de la ARN, para garantizar que los procesos requeridos para la continuidad de los servicios se gestionen dentro del marco de referencia de las mejores prácticas[1] y bajo los niveles de calidad y servicio acordados con las partes interesadas.

Ámbito de Aplicación

Los planes y estrategias de continuidad de TI apoyan el Plan de Continuidad del Negocio ARN, y permitirán a la OTI responder de forma oportuna a incidentes e interrupciones en la prestación de críticos de la Entidad.

Los lineamientos de continuidad deben ser aplicados por los diferentes equipos de trabajo de la OTI.

Enunciado

Los lineamientos de continuidad y recuperación se sustentan en un conjunto de principios que han sido formulados basándose en las necesidades de la ARN y el entendimiento de los riesgos asociados:

1. La OTI garantizará que se desarrolle e implemente un Plan de Continuidad de servicios de TI y recuperación de desastres, para asegurar que los servicios, puedan ser restaurados dentro de una escala de tiempo razonable y bajo los niveles de calidad acordados con los responsables de los servicios de la Entidad.

[1] ITIL® 2011 Conjunto de publicaciones de mejores prácticas para la gestión de servicios de TI.
COBIT 5 – Un marco de negocio para el gobierno y la gestión de TI de la Empresa.

2. El Plan de Continuidad de servicios de TI, debe estar alineado con los objetivos y actividades propuestas en el Plan de Continuidad del Negocio ARN.

3. El Plan de Continuidad de servicios de TI debe contener la asignación de roles, este se realiza a alto nivel dentro de la definición de los procesos de Gobierno y Gestión de TI.

4. El Plan de Continuidad de servicios de TI debe contener un análisis del impacto en la Entidad por la interrupción de los servicios de TI, identificación de los riesgos a los cuales está expuesta la infraestructura y un plan de respuesta para los riesgos identificados.

5. Los propietarios y administradores de la información en cada una de las dependencias deben identificar, clasificar y priorizar la información crítica de sus procesos.

6. Los propietarios y administradores de los sistemas de información deben identificar y priorizar aplicaciones de software, que se encuentren operando.

7. Se debe establecer el tiempo aceptable para recuperar los datos que tiene la Entidad en caso de una interrupción o desastre (RPO), y garantizar una recuperación eficaz.

8. Se debe establecer el tiempo para retornar a las actividades normales después de la interrupción o desastre (RTO), y garantizar que los procesos críticos son recuperados.

9. Se debe contar con equipos servidores alternos que permitan tener disponibles versiones de sistema operativo, plataformas de base de datos, de servicios Web y configuraciones necesarias que estén compatibles y sincronizados con los servidores principales.

10. Se debe disponer de energía eléctrica a través de Sistemas de Alimentación Ininterrumpida y plantas eléctricas para suministrar energía a los equipos de cómputo, principalmente a equipos servidores.

11. Se debe garantizar la divulgación y concientización del plan de Continuidad de servicios de TI y recuperación de desastres dentro de la ARN.

12. Se debe contar con una ubicación física desde la cual el plan de recuperación de desastres pueda ser ejecutado; es decir, un centro de procesamiento alterno con capacidad para el respaldo de las operaciones críticas de la Entidad.

13. Se deberá establecer un protocolo de activación del plan y notificación oficial en la ARN ante la ocurrencia de un desastre. Una vez que la notificación se ha hecho, los responsables deberán activar al personal apropiado para realizar las actividades de verificación y evaluación.

14. Se deberá establecer un procedimiento de verificación del desastre y de evaluación de daños. Una vez que la evaluación se ha hecho, los responsables deberán activar al personal apropiado para realizar las actividades de soporte y recuperación.

15. Se debe realizar copia de seguridad (Backup) de las aplicaciones, bases de datos y bodegas de archivos alojados en servidores, con el propósito de salvaguardar la información. Estas se deben realizar periódicamente por profesionales de la OTI de acuerdo con las indicaciones establecidas en el plan de continuidad y se deberán almacenar en un sitio alterno fuera del edificio donde se encuentra en centro de procesamiento principal.

16. Se debe almacenar copias de seguridad de archivos relevantes de las dependencias, organizadas en archivos electrónicos de documentos, incluyendo sus metadatos a través de Tablas de Retención Documental (TRD) y preservar los documentos según se indique en la TRD de cada dependencia.

17. Se debe etiquetar los medios de almacenamiento con el propósito de identificar las características de las copias de seguridad, de acuerdo con las indicaciones definidas en el plan de continuidad de servicios de TI y recuperación de desastres

18. Los proveedores de TI deben tener capacidad para brindar soporte a requerimientos que se deriven después del desastre.

19. Los planes de contingencia o respuesta deben ser sometidos a prueba, con el objetivo de identificar debilidades u oportunidades de mejora en la formulación de estos.

20. La OTI debe garantizar el continuo seguimiento y evaluación de los planes de recuperación, para su adecuación a las necesidades reales de la Entidad.

21. La OTI debe asegurar la formación específica a los empleados públicos de TI involucrados, sobre los diferentes procedimientos de prevención y recuperación.

22. La OTI debe asegurar la elaboración periódica de informes sobre la gestión de los diferentes planes de continuidad.

23. La OTI velará por la implantación de las medidas relativas al Plan de Continuidad de TI y actividades necesarias para el mantenimiento de estas medidas.

24. La OTI gestionará la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con el plan de continuidad de los servicios de TI.

25. La OTI debe asegurar que se ejecuten revisiones periódicas de los procesos de Continuidad del Servicio (por lo menos una al año), asegurando que sus técnicas y métodos asociados sean regularmente revisados y auditados, con el objetivo de mejorar la calidad de los servicios de TI.