Objetivo:

El presente documento pretende establecer el procedimiento que permita la recuperación de las actividades normales en el menor lapso de tiempo de la información y servicios informáticos.

Alcance:

La presente metodología definida en el presente documento aplica para los recursos informáticos del proceso de gestión tecnología Instituto distrital de las artes - IDARTES.

Fecha de Aprobación	Responsable del Documento	Ubicación
16/01/2019	Área de TIC	Página Intranet: http://comunicarte.idartes.gov.co/idartes

HISTÓRICO DE CAMBIOS		
Versión	**Fecha de Emisión**	**Cambios realizados**
01	Enero 2019	Emisión Inicial de acuerdo con la actualización del mapa de procesos de la entidad, en LMD anterior corresponde al código: 3AP-GTI-PCONT
Oficinas Participantes		
Subdirección Administrativa y Financiera Área de TIC		

Elaboró:	Aprobó:	Validó	Aprobó
Luis Albeiro Cortés Contratista Área de TIC	**Juan Carlos Cubillos** Profesional Universitario Área de TIC		
Néstor Ruiz Contratista Área de TIC	**Liliana Valencia Mejía** Subdirectora Administrativa y Financiera	**Camila Crespo Murillo** Contratista Oficina Asesora de Planeación	**Luis Fernando Mejía Castro** Jefe Oficina Asesora de Planeación

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

Es responsabilidad del Instituto Distrital de las Artes, implementar medidas que permitan mitigar los riesgos y principalmente la restauración de los servicios y recuperación de la información en caso de presentarse situaciones de contingencia.

Presentamos el plan de contingencia en tecnología de la información, el cual reúne los aspectos a tener en cuenta en caso de presentarse acontecimientos que impidan el normal funcionamiento de la plataforma tecnológica de la entidad.

1. OBJETIVO DEL DOCUMENTO

El objetivo es diseñar un plan de contingencia con las herramientas y procedimientos necesarios que permitan la recuperación de las actividades normales en el menor lapso de la información y servicios informáticos tales como los sistemas de información, los equipos, la infraestructura y el personal, ante eventuales sucesos internos o externos que produzcan su pérdida total o parcial, en el Instituto Distrital de la Artes.

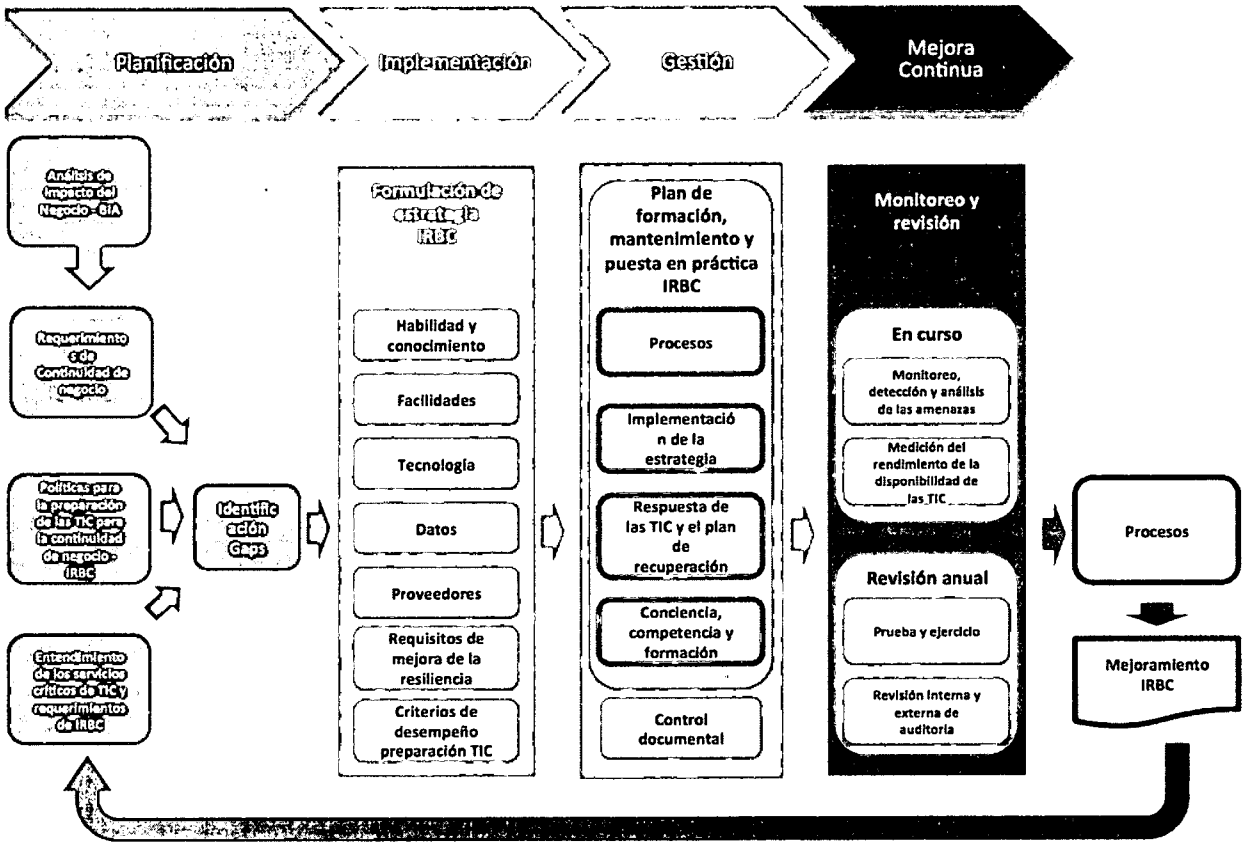
2. ALCANCE

El plan de contingencia está limitado solo a los activos de información que tienen una clasificación como ALTA dentro del inventario de activos de información.

3. METODOLOGÍA

El ciclo de funcionamiento del modelo de operación de continuidad del negocio y su funcionamiento dentro del modelo de operación seguridad y privacidad de la información y la descripción detallada de cada una de las fases. Las cuatro (4) fases que comprenden el modelo de operación contienen objetivos, metas y herramientas que permiten que la continuidad del negocio sea un sistema de sostenible dentro de las entidades.

Figura 1. Etapas en el IRBC – Marco continuidad del Negocio para MSPI



Fuente: GTC-ISO/ IEC 27031 – Guía Continuidad del negocio – MINTIC

Figura 2. Proceso de continuidad de Negocios

Fuente: Autor

4. FASE I. IDENTIFICACIÓN DE RIESGOS

El objetivo de la identificación de riesgos es determinar que podría suceder que cause una perdida potencial y llegar a comprender el cómo, dónde y por qué podría ocurrir pérdida. Las causas pueden ser internas o externas, según lo que haya identificado la Entidad a través del Contexto estratégico.

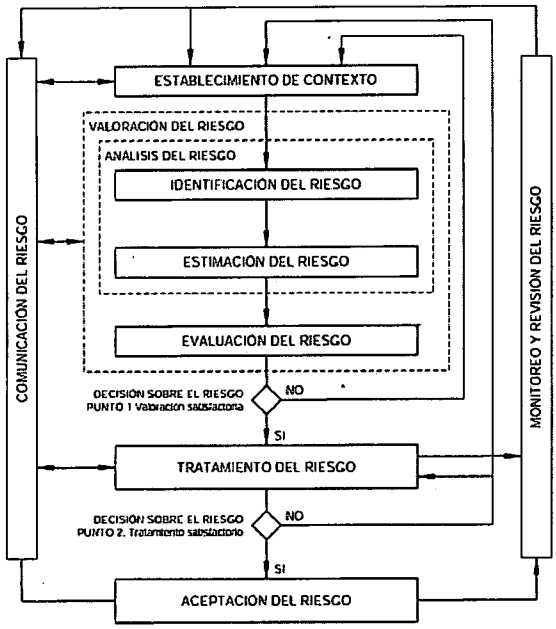
Es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible y revisar los procesos según la clasificación.

Ver: Matriz de riesgos de SGSI

Metodología de gestión de riesgos - SGSI

Plan de tratamiento de Riesgos

Figura 3. Proceso de gestión del riesgo de la seguridad de la información



Fuente: NTC-ISO/ IEC 27005

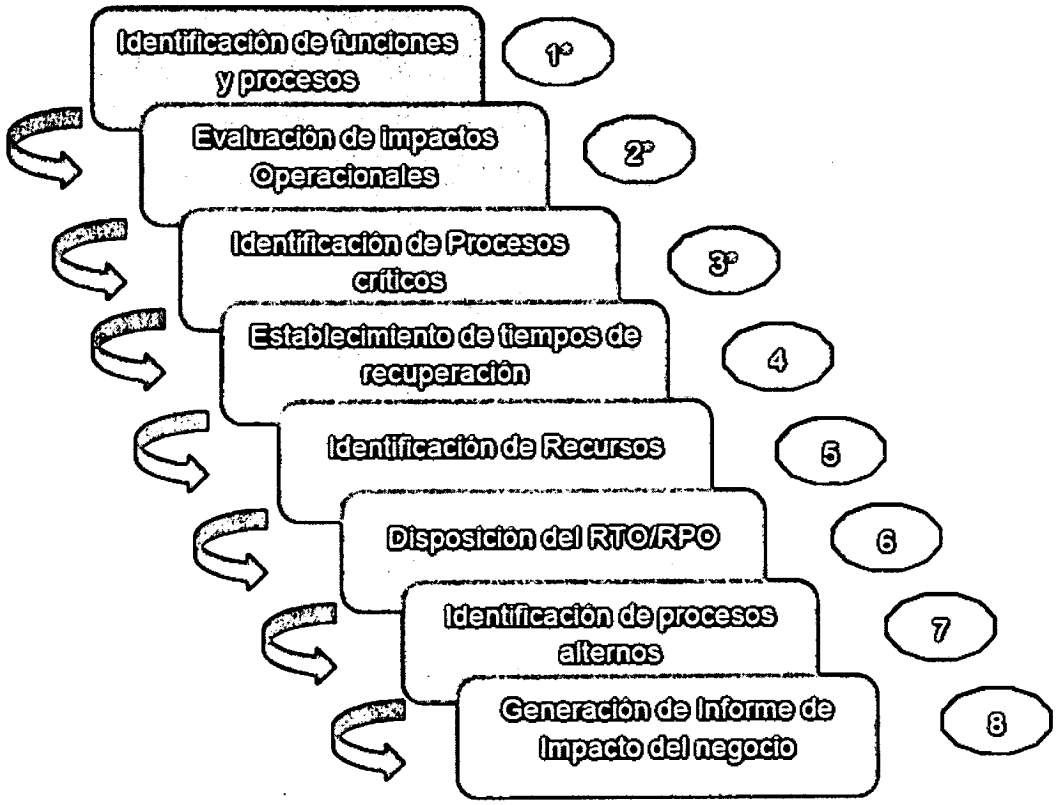
5. FASE II. ANÁLISIS DEL IMPACTO DE NEGOCIO

5.1 Metodología del Análisis de Impacto del Negocio (BIA)

La metodología del Análisis de Impacto del Negocio (BIA), consiste en definir una serie de pasos interactivos con el objeto de identificar claramente los impactos de las interrupciones y tomar decisiones respecto a aquellos procesos que se consideran críticos para la organización y que afectan directamente el negocio ante la ocurrencia de un desastre.

El proceso de gestión de riesgo en la seguridad de la información está basado en las normas NTC-ISO/IEC 27005 y la NTC-ISO 31000.

Figura 4. Metodología del Análisis de Impacto del Negocio



Fuente: Guía Análisis de impacto - MINTIC

5.2 Identificación de Funciones y Procesos

Se identifican las funciones del negocio útiles para apoyar la misión y los objetivos a alcanzar en el Sistema de Gestión de Seguridad de Información de la Entidad.

Tabla. 1. Procesos críticos del negocio

Categoría (Función del Negocio)	Proceso (Servicios)
Sistemas de información	Sistema de Planificación de Recursos Empresariales - ERP - SICAPITAL
	SIF – Sistema de Sistema Integrado de formación, nidos y crea
	Sistema de Gestión Documental - SGDA - ORFEO
Servicios	Servidor de correo electrónico - GOOGLE APPS
	Sitios Web Oficiales de la Entidad - IDARTES:GOV:CO
	Intranet de la Entidad - COMUNICARTE.IDARTES.GOV.CO
Infraestructura Tecnológica Centro de datos principal	Servidor BLADE
	Servidor IBM
	Firewall
	Servidor Proliant - Servicios
	Servidor BD SICAPITAL
	Servidor IBM - ELASTIX
	Sistemas de almacenamiento NAS
	Switch Core
	Switch Conexión fibra entre pisos
	Switch Voz
Recurso Humano	Personal Interno
	Contratistas y proveedores Externos

Fuente: Estructura guía análisis de impacto de Negocios BIA

5.3 Evaluación de Impactos Operacionales

El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles:

Nivel A: La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.

Nivel B: La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.

Nivel C: La operación no es una parte integral del negocio.

Se debe tener en cuenta la tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema.

5.4 Identificación de Procesos Críticos

Con base en la clasificación y evaluación de los impactos operacionales de las organizaciones para lo cual se contempla:

Tabla. 2. Valores de procesos críticos del negocio

Valor	Interpretación del proceso crítico
A	Crítico para el Negocio, la función del negocio no puede realizarse
B	No es crítico para el negocio, pero la operación es una parte integral del mismo.
C	La operación no es parte integral del negocio.

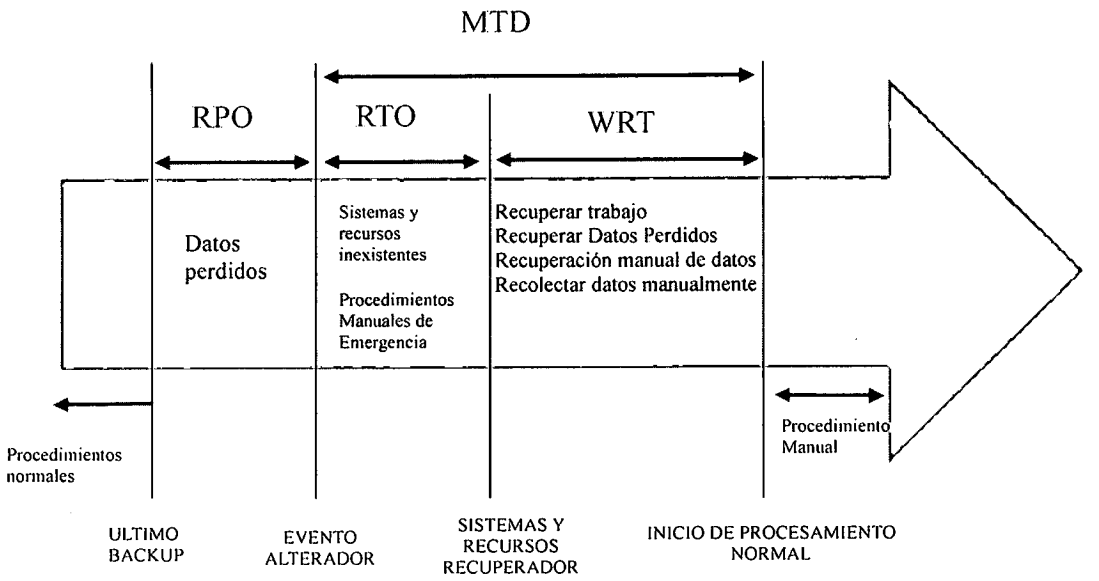
Fuente: Estructura guía análisis de impacto de Negocios BIA

5.5 Establecimiento de Tiempos de Recuperación

Tabla. 3. Descripción de tiempos de recuperación

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Figura 5. Mapa de tiempo para la recuperación de un desastre



***Fuente**: Backtrack Academy – implementación ISO 27001*

Maximium Tolerable Downtime (MTD) (Tiempo de inactividad máxima tolerable): Representa el máximo tiempo de inactividad que puede tolerar la organización.

Recovery time Objetive (RTO) (Tiempo de recuperación Objetivo): Indica el tiempo disponible para recuperar sistemas/recursos que han sufrido una alteración.

Recovery Point Objetive (RPO) (Punto de Recuperación Objetivo): Se refiere a la magnitud de perdida de datos en términos de un periodo de tiempo que puede ser tolerado por un proceso de negocios.

Work Recovery Time (WRT) (Recuperación de trabajo): Es el tiempo disponible para recuperar datos perdidos una vez que los sistemas están separados, dentro del MTPD

5.6 Identificación de Recursos

La identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomas acciones para medir el impacto del negocio de las Entidades.

5.7 Disposición de los RTO/RPO (RECOVERY TIME OBJECTIVE / RECOVERY POINT OBJECTIVE)

Se debe tener en cuenta el Tiempo de Recuperación Objetivo (RTO): Asociado con la restauración de los recursos que han sido alterados de las Tecnologías de la Información; comprende el tiempo disponible para recuperar recursos alterados. Igualmente, Punto de Recuperación Objetivo (RPO): Este punto es importante para determinar por cada uno de los procesos críticos (servicios), el rango de tolerancia que una Entidad puede tener sobre la pérdida de información y el evento de desastre.

5.8 Identificación de Procesos Alternos

Hace posible que los procesos del negocio puedan continuar operando en caso de presentarse una interrupción; para ello es oportuno que las Entidades tengan métodos alternativos de manera temporal que ayuden a superar la crisis que ha generado una interrupción.

5.9 Generación de Informe de Impacto del Negocio

Matriz de impacto de negocio BIA

6. FASE III. ESTRATEGIA DE RESPALDO

6.1 Centro Alterno para Contingencias

Ante eventuales daños catalogados como "Pérdida Total" y que además no pueden ser restaurados en el mismo "Data Center", es necesario contar con uno alterno, en el cual se pueda llevar a cabo las siguientes actividades:

- Disposición de servidores virtuales con el espacio en disco suficiente para operar durante cierto tiempo.
- Espacio físico y conexiones suficientes para instalar servidores de cómputo físicos.
- Disposición de mínimo dos (2) puestos de trabajo para que los profesionales de Tecnologías de la Información y las Comunicaciones puedan operar.
- Disposición de conexión a internet con suficiente ancho de banda para realizar conexiones remotas y para publicar los servicios restaurados.
- Espacio de almacenamiento suficiente para ir alojando periódicamente copias de seguridad, antes de presentarse cualquier tipo de contingencia.
- Se realizarán las gestiones necesarias para llevar a cabo convenios interadministrativos con el objeto de hacer uso de sus instalaciones mientras se mitiga la situación presentada.

7. FASE IV. DESARROLLO DEL PLAN DE CONTINUIDAD

7.1 Responsabilidades del Plan de Contingencia

El plan de contingencia involucra a todas las personas de IDARTES, sin embargo, para responder de manera eficiente a las eventuales contingencias, se conforman los siguientes grupos de respuesta para su elaboración, validación y mantenimiento.

Equipo de seguridad de la información

Es un equipo transversal de trabajo, encargado de validar y aprobar las actividades del presente plan como lo son:

- Proponer actualizaciones o modificaciones al "Plan de Contingencia".
- Aprobar o rechazar actualizaciones o modificaciones al Plan de Contingencia Presentadas al comité.
- Verificar que el personal esté capacitado en la ejecución del plan de contingencia.
- Aprobar los informes presentados por el Coordinador de Sistemas de la entidad en cuanto a Contingencias TIC.
- Coordinar la ejecución y validación de las actividades de pruebas a realizar.
- Determinar las prioridades de recuperación de los diferentes servicios que pudieran verse afectados.
- Coordinar los recursos internos o con proveedores externos requeridos para soportar y restaurar los servicios afectados por una contingencia.
- Verificar que se realice, documente y actualice el plan de contingencia a partir de la experiencia de los simulacros, eventualidades o incidencias presentadas.

Coordinador de tecnología TIC

Es el encargado de activar el plan de emergencias y coordinar todas las actividades y personal involucrado, conforme a los protocolos definidos.

Administrador de infraestructura

Profesional con experiencia y conocimiento de la infraestructura tecnológica de los centros de cómputo de la entidad.

Administrador de Bases de datos

Se designará un profesional para base de datos, es decir quien conoce y tiene la experiencia en su instalación, configuración, parametrización, mantenimiento y soporte de alto nivel.

Profesional de Conectividad

Es aquel profesional encargado de garantizar la conectividad de los canales y de los elementos que conforman la red de la entidad.

7.2 Despliegue del Plan de Contingencia

Figura 6. Gestión de incidencias – Plan de contingencia

Fuente: *Fuente: GTC-ISO/ IEC 27035*

Ante una eventual emergencia, que comprometa la plataforma tecnológica y sistemas de información del Instituto Distrital de las Artes, se debe seguir el siguiente procedimiento:

El "líder de emergencias TIC" evaluará el impacto del evento y activará el plan de contingencia.

Declarar la emergencia como Parcial o Total:

7.3 Contingencia para Pérdida Parcial

Se solicita al responsable del área o servicio afectado que realice el procedimiento técnico que permita restaurarlo en el menor tiempo posible. El directorio de emergencias contiene el nombre y datos de contacto de cada uno de los responsables.

7.4 Contingencia para Pérdida Total

- El Líder de emergencias TIC, convoca el comité.
- El comité define un punto de encuentro u operaciones, según el evento.
- Se designa un vocero o encargado de las comunicaciones, quien mantendrá informado a todos los funcionarios de los avances, tiempos y paso a seguir. Junto a esta actividad, se debe definir el sitio o medio a través del cual se mantendrá informado a los usuarios y directivos de la entidad.
- Se autoriza la fase de restauración de la plataforma tecnológica y servicios de los sistemas de información.
- Convocar las personas responsables para la solución.

7.5 Directorio de Emergencias:

Tabla. 4. Directorio Personal de emergencias

Nombre	Responsabilidad	Contacto
Juan Carlos Cubillos	Coordinador de Tecnología	Personal: Institucional: 3795750 Ext 4300, Mail Institucional: juan.cubillos@idartes.gov.co
Néstor Albeiro Ruiz Barragán	Administrador de Infraestructura	Personal: Institucional: 3795750 Ext 4301 Mail Institucional: nestor.ruiz@idartes.gov.co
Nelson Andrés Maldonado	Profesional de conectividad	Personal: Institucional: 3795750 Ext 4303, Mail Institucional: Nelson.maldonado@idartes.gov.co

Nombre	Responsabilidad	Contacto
Arquitecto	Reparaciones Físicas - Mantenimiento	Personal: Institucional: 3795750 Ext 4001,
Idelber Sánchez	Sistema de Gestión documental ORFEO	Personal: Institucional: 3795750 Ext 4302, Mail Institucional: Idelber.sanchez@idartes.gov.co
Luis Cortes	SGSI	Personal: Institucional: 3795750 Ext 4304, Mail Institucional: Luis.cortes@idartes.gov.co
Jorge Alvarado	Webmaster	Personal: Institucional: 3795750 Ext 1405 Mail Institucional: Jorge.alvarado@idartes.gov.co
Grupo Desarrollo CREA	Si CREA	Personal: Diego Forero Institucional: 3795750 Ext Mail Institucional: diego.foreroposada@idartes.gov.co
ETB	Proveedor ISP	Móvil: 3057066068 Línea gratuita 018000123737 opción 2 Correo: helpdesketb@etb.com.co
CODENSA	Proveedor	Línea gratuita: 115 Fijo: 7115115
Centro Cibernético Policial de la Policía Nacional	Atención respuesta a incidentes Informáticos.	Teléfono 4266900 ext.104092

8. PROCESO DE RESTAURACIÓN

Una vez reunido el equipo técnico de trabajo en el punto o centro de operaciones definido, se inician las actividades de restauración de los servidores y servicios informáticos en el siguiente orden:

- Con el fin de determinar cuáles son los servicios más críticos e importantes restaurar, se debe definir prioridad sobre los mismos.

- Se inicia los procedimientos técnicos de restauración de los servidores y sistemas de información. El procedimiento a seguir será un documento técnico que debe reposar en la documentación del Área de Tecnología.
- Una vez restaurado cada servicio, se realizarán las pruebas de estrés y de funcionamiento normal con un grupo de usuarios limitado.
- Cuando las pruebas sean satisfactorias, el líder de comunicaciones informará a todos los usuarios para que hagan uso del servicio.

8.1 Controles existentes

Los controles existentes para infraestructura tecnológica:

- Aplicar Políticas de seguridad de información - TIC
- Mantenimiento preventivo de los servidores
- Mantenimiento de los aires acondicionados.
- Mantenimiento de UPS
- Garantías con proveedores.
- Restricción de acceso al centro de cómputo.
- Actualización permanente del antivirus
- Restricción de acceso a las oficinas y áreas de la sede administrativa.
- Acceso privilegiado a las configuraciones del firewall
- Copia de seguridad de la Información
- Contrato de custodia de medios externos y enviar periódicamente la información

Los controles existentes para los sistemas de información:

- Aplicar Políticas de seguridad de información - TIC
- Mantenimiento preventivo a los servidores de los sistemas de información.
- Actualización permanente del antivirus
- Realizar la Copia de seguridad de la Información de las bases de datos e información de los sistemas de información.
- Aplicar las Políticas de Firewall.
- Mantener Niveles de autorización a las bases de datos para evitar accesos no autorizados
- Tener Procesos Documentados
- Revisión permanente de la consola de red y Firewall de eventos de los sistemas de información.

- Mantener Registros logs de los diferentes sistemas.
- Mantener el contrato de mantenimiento del sistema de los sistemas de información.
- Se tiene establecido servidores independientes para pruebas y producción.
- Capacitación a los usuarios en el manejo del aplicativo.
- Revisión Documentos de perfiles del personal de la administración de la base de datos y de los sistemas de información.

8.2 Plan maestro de recuperación

8.2.1 Infraestructura Tecnológica - Centro de datos

➢ **Desastres Naturales Incendio / inundación**

- Activar Plan de Emergencia Institucional.
- Apagar de manera inmediata todos los breakers asociados al centro de Cómputo y centros de cableado.
- Hacer uso de los extintores en caso de incendio.
- Para los pisos inferiores bloquear fuente de activación de inundación y cerrar registros para limitar propagación del agua.
- Revisar y notificar al jefe de área la última fecha de copia de seguridad de las bases de datos de los sistemas de información críticos (Sicapital y ORFEO) y su última fecha de sincronización con el servidor remoto.
- En caso de no ser posible la recuperación de servicio a corto plazo, se debe activar el plan de contingencia de servicios de información sobre el servidor alterno ubicado en el datacenter del Planetario de Bogotá.
- Una vez estabilizada la zona, realizar la recuperación y levantamiento de información de los equipos afectados para su inventario.
- Reportar novedad a la aseguradora.

8.2.2 Perdida de Equipos Tecnológicos

- Tomar las pruebas necesarias para la identificación de los presuntos responsables.
- Notificar a la oficina de Control Disciplinario
- Notificar a la aseguradora
- Verificar la existencia de Backups del equipo sustraído
- Adecuar equipo temporal mientras se gestiona la reposición

8.2.3 Servidores fuera de servicio

- Realizar el diagnóstico del servidor fuera de servicio.
- Notificar de manera inmediata al proveedor del servidor afectado en caso de garantía
- Notificar de manera inmediata a la empresa de mantenimiento de servidores para que atienda la falla.
- Notificar a los usuarios de la situación detectada e informar del tiempo aproximado en que se estará fuera de servicio.
- El coordinador de tecnología debe solicitar al operador de centro de Cómputo que inicie las actividades de configuración y/o activación de un servidor alterno o imagen para que entre en operación de manera temporal mientras se da solución al servidor principal.
- Realizar las pruebas al servidor antes de liberarlo en operación alterna.
- En el evento de contar con centro alterno, coordinar con el proveedor de T.I. las acciones y/o protocolos de activación contingentes y establecer tiempos de activación real de los servicios.

8.2.4 Acceso/borrado no autorizado a información confidencial

- Identificar nombre el nombre y ruta de las carpetas o archivos que fueron borrados.
- Hacer uso de las herramientas de recuperación de información.
- Aplicar procedimiento de Copia y Restauración de la Información.
- Informar al jefe superior de las acciones adelantadas y de los resultados.

8.2.5 Perdida de conectividad, red e internet

- Verificar si el punto de fallo se encuentra en la infraestructura de IDARTES o si por el contrario es generado en los equipos de conectividad o red del proveedor.
- Verificar funcionamiento de los dos (2) canales de internet para definir si el fallo implica también al canal secundario de contingencia.
- En caso de que los dos canales hayan sido afectados, se debe notificar al proveedor de servicios de conectividad ETB sobre las fallas detectadas.
- Ejecutar las acciones contingentes acordadas con el proveedor de servicios de canales dedicados y de internet. Notificar de manera inmediata a los usuarios de áreas críticas sobre la situación detectada y temporalidad de la misma, para reactivar los servicios principales.
- Monitorear las actividades que realicen los usuarios de áreas críticas a través de medios alternos.
- Llevar registro y documentar acciones contingentes.
- Recursos de Contingencia como Routers, switches, firewall, Herramientas de internet.

8.2.6 Sistemas de información SICAPITAL, ORFEO

- Restringir el acceso al ambiente de producción a los usuarios durante el proceso de recuperación de la información.
- Informar a los usuarios internos y externos por diferentes medios (correo electrónico, web, o telefónico) de la activación del servidor temporal de Sistemas de Información.
- Tener las copias de seguridad disponibles y sincronizadas con el servidor alterno ubicado en el Planetario de Bogotá al día hábil anterior, o contactar empresa de responsable de la custodia de las copias.
- Con el encargado de infraestructura y redes realizar la verificación de servicios básicos del servidor alterno (Sistema operativos, conexión base de datos, copias de seguridad y red)
- Activar protocolo de servidor alterno de recuperación de información de bases de datos y aplicaciones para SICAPITAL y ORFEO
- Los administradores de los sistemas de información SiCapital y ORFEO deben verificar la integridad de la información contenida en las que las copias de bases de datos realizadas desde el datacenter principal.
- Los administradores de los sistemas de información SiCapital y ORFEO deben subir los servicios y restaurar las bases de datos desde las copias encontradas en el servidor de respaldo.
- Realizar el paso a paso para recuperar los sistemas de información de contingencia y ponerlos a disposición de los usuarios de acuerdo con los instructivos correspondientes.
- Informar a los usuarios del restablecimiento del servicio.
- Documentar las correcciones y reportarlas al encargado del Área de Tecnología.

8.3 Documentos anexos contingencias de TI

Adicional del plan maestro de recuperación se cuenta con manuales específicos para la contingencia y/o restauración de la infraestructura tecnología:

- Matriz Análisis de Impacto al negocio - BIA
- Manual de plan de contingencia hosting interno
- Manual de plan de contingencia para las páginas web del IDARTES
- Manual de plan de contingencia B.D ORACLE
- Manual de plan de contingencia para restauración ORFEO
- Contingencia y restauración SIF

La anterior información (manuales) es de índole confidencial por lo tanto es solo de uso del personal encargado de cada sistema o infraestructura.

9. DOCUMENTACIÓN DE LA CONTINGENCIA

Durante el tiempo que dure la emergencia de la contingencia hasta que se haya restaurado todos los servicios y superado todos los problemas, designará una persona responsable de documentar todo el proceso, el cual será insumo importante para mitigar futuros eventos y para identificar las fallas que se hayan presentado, con el fin de no cometer los mismos errores en futuras emergencias.

9.1 Inventario de Daños

Cuando todos los servicios funcionen normalmente, se realizará una evaluación e inventario de los daños, a partir del siguiente cuestionario.

- ¿Cuál fue la causa de la emergencia y/o incidente?
- ¿Se pudo evitar los daños causados?
- ¿La entidad se encontraba preparada para atender de manera eficiente este tipo de problemas?
- ¿Cuáles fueron los equipos que sufrieron mayor daño? Realizar inventario de equipos afectados.
- ¿Si la restauración se realizó en el mismo "¿Data Center", persisten daños que pueden ser reparados paralelamente con los equipos en producción?

10. SIMULACRO CONTINGENCIA TIC

Sólo en situaciones reales de una emergencia, es posible evidenciar las debilidades y ciertas variables no contempladas en el imaginario de una contingencia, por lo tanto, es de gran importancia simular un posible ambiente o emergencia de pérdida total y poner en marcha el plan de contingencia, para así identificar los ajustes que se deben realizar y estar mejor preparados ante una eventual situación.

Son muchos los factores que impactan una contingencia TIC y que obligan a realizar cambios permanentemente, entre los más comunes están:

- El hardware se actualiza o cambia constantemente.
- Las personas cambian de trabajo o se integran nuevas.
- Los sistemas de información están en permanente evolución.
- Se implementan nuevos sistemas de información en la entidad.
- Se adoptan nuevas políticas en materia de tecnologías de la información y las comunicaciones.
- Se cambia de lugar físico el hardware o se abren nuevas sedes.
- Permanente cambio de proveedores de servicios.

- El formato de las copias de seguridad puede cambiar.

Por lo anterior, se debe programar al menos una vez al año un simulacro de contingencia TIC.

11. NORMATIVA

Guía de gestión de Riesgos (MSPI-MinTIC).

Décimo segundo lineamiento – Gestión del Riesgo (Sistema Integrado de Gestión Distrital).

Norma Técnica Distrital NTD-SIG 001-2011

NTC-ISO-IEC27001:2013: Sistemas de Gestión de la Seguridad de la información.

NTC-ISO-IEC27002:2013: Código de Buenas Prácticas en Gestión de la Seguridad de la Información

ISO 22301:2012, Sistemas de Gestión y Continuidad del Negocio.

ISO 27031 – DE198-13, Tecnología de la Información, Técnica de Seguridad, Directrices para la continuidad del negocio.

12. DEFINICIONES

Análisis del impacto al negocio (BIA por sus siglas en inglés): Proceso del análisis de actividades las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas.

MTD (Maximun Tolerable Downtime) o Tiempo Máximo de Inactividad Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.

RTO (Recovery Time Objective) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

RPO (Recovery Point Objective) o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.

SITIO ALTERNO: Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha

producido una interrupción.

WRT (Work Recovery Time): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

(Fuente ISO 27000)