ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA RECREACION Y DEPORTE
Instituto Distrital de las Artes

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

DE CONTINUIDAD DE TI

GTI-P-06

V.2

2024-09-13

Instituto Distrital de las Artes -IDARTES-
Carrera 8 No. 15 - 46 - Bogotá
+57 (601) 379 5750
Código postal: 111711

BOGOTÁ

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA, RECREACIÓN Y DEPORTE
Instituto Distrital de las Artes

PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

BOGOTÁ | INSTITUTO DISTRITAL DE LAS ARTES IDARTES

HISTÓRICO DE CAMBIOS		
Versión	**Fecha de Emisión**	**Cambios realizados**
01	30/12/2022	Emisión Inicial.
02	16/09/2024	Actualización de las fases de implementación del Plan de Continuidad.

Elaboró:	**Revisó:**	**Validó:**	**Aprobó:**
Jorge Enrique Ramírez Rodríguez Contratista de la Oficina Asesora de Planeación y Tecnologías de la información **Martha Mateus** Contratista de la Oficina Asesora de Planeación y Tecnologías de la información	**Jonathan González Bolaños** Profesional Universitario Oficina Asesora de Planeación y Tecnologías de la Información **María Cristina Herrera Calderón** Contratista Oficina Asesora de Planeación y Tecnologías de la Información	**Daniel Sánchez Rojas** Jefe de la Oficina Asesora de Planeación y Tecnologías de la información	**Daniel Sánchez Rojas** Jefe de la Oficina Asesora de Planeación y Tecnologías de la información

TABLA DE CONTENIDO

Tabla de ilustraciones

Tabla de Tablas

1. Introducción

Teniendo en cuenta lo establecido en la Política de Gobierno Digital, liderado por el Ministerio de las Tecnologías de la Información y las Comunicaciones, en cuanto a la infraestructura, los servicios, las aplicaciones y los usuarios en el marco de un ecosistema digital; las recomendaciones brindadas en cuanto a la necesidad de reconocer la seguridad y privacidad de la información, como un factor primordial para la apropiación de las TIC; la constante evolución de las nuevas tecnologías; y la dinámica de las entidades, plantea un marco de seguridad de la información para la prestación de servicios a los ciudadanos a través de las tecnologías de la información, el cual deberá ser respaldado por una gestión, unas políticas y unos procedimientos adecuados, que resaltan el papel de las personas como el primer eslabón de una compleja cadena de responsabilidades y que esté orientado a preservar los pilares fundamentales de la seguridad y privacidad de la información.

La implementación de un plan de gestión y preservación de la información pública ante situaciones disruptivas, permite minimizar el impacto y recuperación por pérdida de activos de información del IDARTES, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación. En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, recursos, transporte e instalaciones.

Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, pérdida del servicio y disponibilidad del servicio) se deberían someter a un análisis del impacto del negocio (BIA). Por ello se plantea el desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales. La correcta implementación de la gestión de la continuidad del negocio disminuirá la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, la organización estará preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por de ese incidente.

Es por la importancia de la información, que el Instituto Distrital de las Artes – IDARTES, a través del presente documento establece la inclusión de un plan de continuidad TI que fortalezca la planificación, implementación, evaluación y mejora del Modelo de Seguridad y Privacidad de la Información, determinado por las necesidades, objetivos, estructura organizacional, los procesos misionales y tamaño de la Entidad, así como requisitos legales y exigencias de seguridad de la información dadas por MINTIC establecido en el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 en el artículo 2.2.9.1.1.3 Principios, que define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 que define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital; así como la Resolución 00500 de 2021 y sus anexos que incorporan lineamientos en materia de Seguridad Digital en las entidades del estado.

La política de gobierno digital tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo por el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Además establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las Entidades públicas de orden nacional y territorial, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura crítica, los riesgos e incidentes de seguridad y privacidad de la información

y así evitar la interrupción en la prestación de los servicios de la Entidad enmarcados en su modelo de operación por procesos.

Teniendo en cuenta la creciente participación de ciudadanos en el entorno digital, la alta dependencia de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) traen consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital, lo cual exige que el país cuente con suficientes capacidades para su gestión adecuada y oportuna, las amenazas, los ataques e incidentes de seguridad digital cada día son más sofisticados y complejos e implican graves consecuencias de tipo económico o social, esto conlleva al deterioro de la confianza digital y la desaceleración del desarrollo de los países en el futuro digital y debido a lo anterior, los gobiernos alrededor del mundo han venido atendiendo los nuevos retos para la detección y manejo de amenazas, ataques e incidentes cibernéticos mediante la formulación y actualización de estrategias o políticas relacionadas con la seguridad digital en el marco de la pandemia y la apropiación de estrategias TI.

En atención a esto la Oficina Asesora De Planeación y Tecnologías de la Información el firme propósito de avanzar en su transformación digital incluyó en su Plan Estratégico Institucional 2024 los lineamientos de la Política de Gobierno Digital, a través de diversas iniciativas estratégicas de fortalecimiento institucional, participación y empoderamiento de ciudadano, arquitectura empresarial y seguridad de la información.

2. Objetivo

Desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales. La correcta implementación de la gestión de la continuidad del negocio disminuirá la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, la Entidad estará preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por de ese incidente.

3. Alcance

Establecer, implementar y mantener un plan de continuidad TI al Modelo de Seguridad y Privacidad de la Información en el IDARTES, con este documento y su alineación con el Plan Estratégico de Tecnologías de la Información, en adelante PETI, se referencia la estrategia TI y aporta línea de acción en caso de contingencia ante eventos disruptivos, apoyando la ejecución de los proyectos, contemplando actualizaciones, para lograr los objetivos estratégicos engranados al Plan Estratégico Institucional y el marco de Referencia de arquitectura Empresarial del comprender, analizar, construir y presentar, con el enfoque de la estructuración del modelo de gestión Estrategia, Gobierno, Información, Sistemas de Información, Infraestructura de TI, Uso y Apropiación y Seguridad.

4. Responsables

Oficina Asesora de Planeación y Tecnologías de la Información-OAPTI

5. Definiciones y Abreviaturas

Conforme a la estructura de la presente caracterización se tomará como referencia el normograma del Plan Estratégico de Tecnologías de la Información - PETI; en el entendido de la referencia normativa como una herramienta que permite al Instituto distrital de las artes – Idartes, delimitar las normas que regulan sus actuaciones en desarrollo con su objeto misional. El normograma del PETI contiene las

normas externas como leyes, decretos, acuerdos, circulares y resoluciones que regulan la gestión TI de la entidad y las normas internas como reglamentos, estatutos, manuales y, en general, todos los actos administrativos de interés para el Idartes que permiten identificar las competencias, responsabilidades y funciones de las dependencias de la Entidad.

- **Activo:** cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO 27000).
- **Ataque:** Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo. (ISO 27000).
- **BIA:** (Bussiness Impact Analysis), permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio. (MinTic).
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO 27000).
- **Continuidad de la seguridad de la información:** Procesos y procedimientos para garantizar la continuidad de las operaciones de seguridad de la información. (ISO 27000)
- **Disponibilidad:** Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada. (ISO 27000).
- **Instalaciones de procesamiento de información:** Cualquier sistema de procesamiento de información, servicio o infraestructura, o la ubicación física que lo alberga. (ISO 27000).
- **Integridad:** Propiedad de la exactitud y la integridad. (ISO 27000).
- **IT:** Infraestructura Tecnológica.
- **PETI:** Plan Estratégico de la Tecnología de Información.
- **PCN:** Plan de Continuidad del Negocio.
- **Riesgo:** riesgo la probabilidad de que ocurra un evento. (ISO 9001).
- **Sistema de información:** Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información. (ISO 27000).

6. Condiciones Generales

La seguridad de la información constituye una parte fundamental del Plan, para el diseño y planificación del Modelo de Seguridad y Privacidad de la Información el cual debe ser conocido por todo el Instituto, así como tener en cuenta los compromisos y normatividad establecida por el Ministerio de las Tecnologías de la Información y Comunicaciones MINTIC y la Alta Consejería Distrital de TIC - ACDTIC para las entidades gubernamentales; como lineamientos, políticas y directrices establecidas, según la De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", la Política de Gobierno Digital será definida por MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Por otra parte, el resumen ejecutivo técnico y administrativo del Instituto, los instrumentos y guías diseñados por MINTIC, se tomaron como base para establecer la implementación del Modelo de Seguridad de la Información - MSPI, mediante la formulación de iniciativas, estrategias que garanticen el apoyo y cumplimiento de sus objetivos y funciones, que soporte adecuadamente los procesos misionales, estratégicos, transversales, de evaluación y mejora; entendiendo que a través de la Oficina

asesora de planeación y tecnologías de la información es quien liderar la política de MIPG Seguridad Digital y Gobierno Digital alineado con el Plan estratégico institucional IDARTES 2024.

Es importante mencionar en esta instancia, que la Oficina asesora de planeación y tecnologías de la información tiene como función formular y liderar el diseño, planeación, implementación y control de las actividades y productos asociados a la seguridad y privacidad de la Información, garantizando la integridad y debida custodia de la información, en línea con la normatividad y legislación vigente y la Política de Gobierno Digital y Seguridad Digital, abordando los siguientes aspectos:

- Formulación, actualización y divulgación de líneas específicas referentes a Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.
- Fortalecer el Modelo de Seguridad y Privacidad de la Información del Idartes.
- Salvaguarda de la información institucional
- Administrar, controlar y gestionar los incidentes de la seguridad de la información.
- Apoyar a las unidades de gestión en diligenciar los formularios y autodiagnósticos que emitan las entidades cabeza de sector para verificar la correcta implementación de las políticas y lineamientos establecidos MINTIC, ACDTIC y DAFP.
- Optimización de sistemas de apoyo a la infraestructura tecnológica Idartes

6.2 Normatividad

Conforme a la estructura de la presente caracterización se tomará como referencia el normograma del Plan estratégico de tecnologías de la información – PETI; en el entendido de la referencia normativa como una herramienta que permite al Instituto distrital de las artes – Idartes, delimitar las normas que regulan sus actuaciones en desarrollo con su objeto misional. El normograma del PETI contiene las normas externas como leyes, decretos, acuerdos, circulares y resoluciones que regulan la gestión TI de la entidad y las normas internas como reglamentos, estatutos, manuales y, en general, todos los actos administrativos de interés para el Idartes que permiten identificar las competencias, responsabilidades y funciones de las dependencias de la Entidad.

7. Desarrollo documento

El Idartes, como entidad distrital, debe cumplir con las metas establecidas por el MINTIC en materia de Seguridad de la Información, un componente crucial de la Política de Gobierno Digital (anteriormente conocida como el componente de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea – GEL). Para estructurar el contexto, realizar el análisis y llevar a cabo la implementación, se han utilizado herramientas de diagnóstico definidas por los entes rectores que orientan la estrategia de apropiación de Gobierno Digital y Seguridad Digital.

En términos generales, se identifican tres tipos de planes según su alcance:

Plan de Continuidad de Negocio (PCN): Establece la continuidad de una organización desde múltiples perspectivas, como infraestructura TIC, recursos humanos, mobiliario, sistemas de

comunicación, logística, sistemas industriales e infraestructuras físicas. Cada uno de estos ámbitos requiere un plan de continuidad específico.

Plan de Continuidad TIC (PCTIC): Es un componente del PCN, centrado exclusivamente en el ámbito tecnológico. Mientras que el PCN abarca todos los aspectos de la continuidad de negocio, el PCTIC se limita a los aspectos tecnológicos. Por ejemplo, en el caso de un incendio en un almacén, se activarán los planes de continuidad relacionados con los procesos afectados, con un enfoque específico en la tecnología.

Plan de Recuperación ante Desastres (PRD): Se enfoca en el ámbito técnico con un análisis menos profundo y es reactivo ante posibles catástrofes.

Los planes de continuidad de negocio pueden ayudarnos a:

Ilustración 1 Fuente Incibe

7.2 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 sostenible dentro de la entidad.

Ilustración 2 Ilustración 1 - Modelo de operación de seguridad

La ilustración 1, muestra el modelo de operación de seguridad y privacidad de la información, del cual solo tendremos en cuenta las fases de planificación, implementación, gestión y mejora continua.

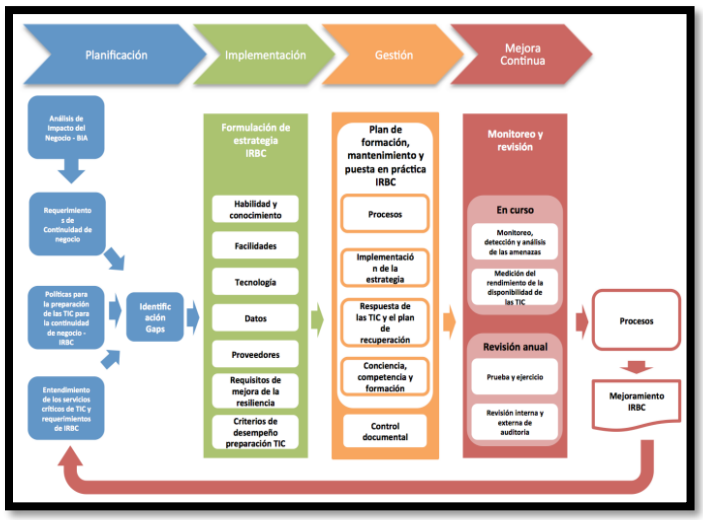

Ilustración 3 Ilustración 2 - Marco Continuidad del Negocio para Seguridad

Como parte del proceso de continuidad del negocio, la preparación de las TIC para la continuidad del negocio (IRBC), hace referencia a un sistema de gestión que complementa y soporta la continuidad del negocio de la Entidad y los programas de Sistemas de Gestión de Seguridad de la Información (SGSI), para mejorar la preparación de la Entidad que le permita:

a) Responder al cambiante ambiente de riesgos.
b) Asegurar la continuidad de las operaciones críticas del negocio soportadas por servicios de TIC.
c) Estar preparado para responder antes de que una disrupción de los servicios de TIC ocurra, identificar los eventos o las series de eventos relacionados provenientes de incidentes.
d) Responder y recuperarse de incidentes y/o desastres y fallas.

7.2.1 FASE I – IDENTIFICACIÓN DE RIESGOS

El objetivo de la identificación de riesgos es determinar qué podría suceder que cause una pérdida potencial y llegar a comprender el cómo, dónde y por qué podría ocurrir la 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.

Conforme a lo anterior, teniendo en cuenta que la entidad cuenta con un Plan de tratamiento de riesgos de seguridad y privacidad de la información, en el cual se identificaron los riesgos a abordar para la vigencia 2024, el cual define el proceso de gestión del riesgo de la seguridad de la información adoptado por la entidad.

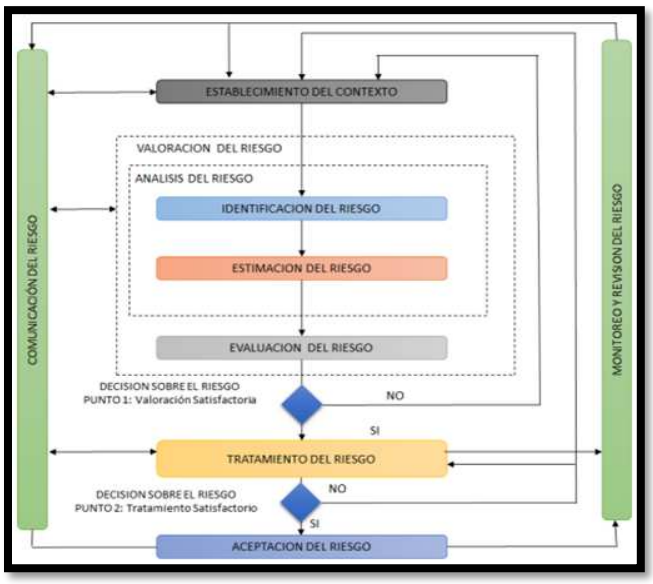

Ilustración 4 Ilustración 3 Proceso de gestión del riesgo de la seguridad de la información

7.2.2 Riesgo 1: Pérdida de disponibilidad TI

Análisis: En IDARTES se puede presentar amenazas materializando vulnerabilidades como la pérdida o daño total o parcial de los equipos de cómputo, servidores y equipos activos causando pérdida de integridad y disponibilidad de la información, dado que la información no se encuentra disponible en el momento que se necesita para cumplir la operación o funciones propias en la Entidad debido a que la información como un activo vital para la gestión institucional no se encuentra disponible por ausencia o falla en los activos de información que hacen parte de los procesos u operaciones, y por fallas en los equipos tecnológicos o redes de comunicación debido a agentes externos, ambientales, intencionales o no intencionales afectan la disponibilidad de la información para el desarrollo de las funciones y operaciones, así como por el extravío o no disponibilidad de equipos o información debido a un inadecuado tratamiento en el almacenamiento, disposición final, custodia o destrucción segura de los mismos. En este sentido se contempla este riesgo teniendo en cuenta que la administración de la continuidad de los servicios TI y las operaciones de la entidad no puede concebirse como una disciplina

exclusiva de la Oficina asesora de planeación y tecnologías de la información, sino que debe formar parte integral de la disciplina de continuidad del negocio y debe estar coordinada a nivel institucional.

7.2.3 Riesgo 2: Posible afectación de la confidencialidad, integridad y disponibilidad de la información

Análisis: En las unidades de gestión existen vulnerabilidades en la seguridad de la información dado que no se realiza un seguimiento a las bitácoras de control de acceso y los seguimientos a actividades para evitar que la información pueda ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas de información o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente, y contemplando que la información no se encuentra disponible por ausencia o falla en los sistemas de información y servicios tecnológicos que hacen parte de los procesos u operaciones de las diferentes áreas de gestión, se puede afectar la operación de la entidad con amenazas de acceso indebido a los sistemas y a la información de los mismos aprovechando las vulnerabilidades tecnológicas, ambientales y del recurso humano. Así mismo, se ha evidenciado que en el marco de la seguridad de la información que se utiliza en IDARTES para proteger los datos que tiene, maneja y dispone, se deben contemplar vulnerabilidades como las generadas por las nuevas tecnologías del teletrabajo en casa a raíz de la pandemia y la adopción de nuevas tecnologías que han modificado la forma de utilizar la seguridad de la información a gran velocidad.

7.2.4 Riesgo 3: Fallas en la infraestructura tecnológica hardware/software que respalda y apoya los servicios tecnológicos de la entidad

Análisis: Conforme a la operación de los servicios y sistemas TI y el propósito de garantizar el correcto funcionamiento y la disponibilidad, se evidencian amenazas que se aprovechan de las vulnerabilidades generadas en el uso indebido de los equipos y herramientas de la plataforma tecnológica, lo cual puede estar derivado de un tratamiento inadecuado de la información e incorrecto uso por desconocimiento de políticas, controles y buenas prácticas que son causa directa de las fallas en el hardware y software que soporta la infraestructura tecnológica de IDARTES. Aunado a lo anterior permitir en cierto momento que se presenten errores en el control y mantenimiento que evite una posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de la misma accidental o intencionalmente. Resulta complejo contar con la infraestructura tecnológica perfecta para garantizar al recurso tecnológico de las unidades de gestión un funcionamiento libre de fallas, pero es posible tener procesos organizados y herramientas con fortaleza para asegurar respuestas frente a diferentes vulnerabilidades, y tomar las medidas para que no se repitan o se materialicen aprovechando el uso con falta de controles de la interacción de la información que se hace actualmente a través de dispositivos móviles y ordenadores portátiles de Idartes y personales, y por lo anterior, se han reforzados desde la estrategia TI, herramientas y servicios que están interconectadas con herramientas web, aplicativos, plataformas y otras interfaces tecnológicas, con el fin de que sean lo más efectivas y funcionales evitando amenazas y contratiempos.

7.2.5 Riesgo 4: Afectación por accesos no permitidos a información crítica de la Entidad

Análisis: La información debe ser protegida apropiadamente contra el acceso no autorizado, modificación, divulgación, pérdida o destrucción, sin importar la fuente en donde esté almacenada (computadores, librerías, portátiles, medios extraíbles como discos duros externos, USB, DVD, cintas Backups, etc), contratos, documentos, comunicaciones, etc.). Desde este punto de vista, es importante determinar el papel que cumplen las unidades de gestión, partes internas o externas y funcionarios que por diversos motivos están involucrados en el tratamiento de la información del IDARTES.

7.3 Fase II - ANÁLISIS DEL IMPACTO DE NEGOCIO

7.3.1 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 Entidad 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.

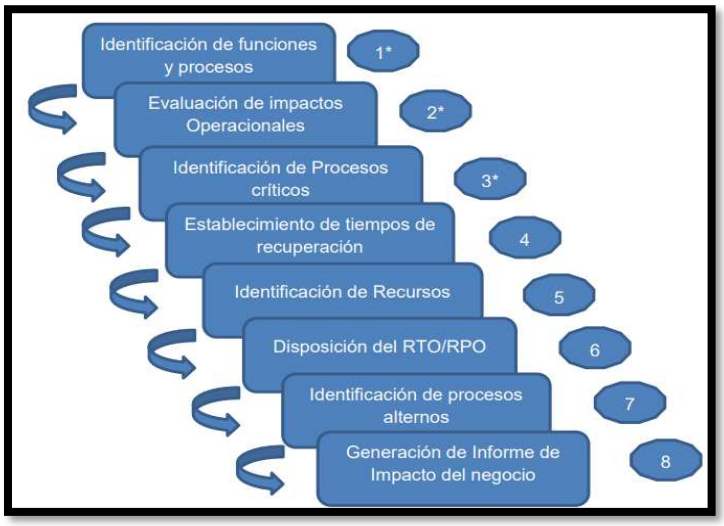

Ilustración 5 Ilustración 4 Metodología del Análisis de Impacto del Negocio

7.3.2 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.

Entornos tecnológicos del negocio		
1	Sistemas de Información	Orfeo Pandora SUMA+ (Plataforma de DADEP) PUFA SIF KOHA Contratación SICapital Caja Menor IRIS Convocatoria Planta Temporal Planeador GLPI Gestión de proyectos Geoclick Libroalviento

Entornos tecnológicos del negocio		
		Equipamientos Huella de carbono
2	Servicios TI	Internet SSO Visor GLPI Red LAN Red Wifi Conexión VPN Intranet Correo Institucional Almacenamiento Institucional Mesa de Ayuda Atención PQRSD Control de dominio Seguridad Perimetral Video Vigilancia Protección Antivirus Chatbot
3	Infraestructura Tecnológica Centro de datos principal	Chasis principal servidores Sistemas de almacenamiento SAN Switch de Core Switch de cabecera Swich secundarios Firewall Bases de datos Copias de seguridad Sistema de almacenamiento NAS
4	Recurso Humano	Ingeniero de conectividad Ingeniero de bases de datos Ingeniera de gobierno digital Arquitecto de software Ingeniero de seguridad de la información Director de tecnología Profesional universitario Profesional especializado Personal técnico
5	Procesos impactados con gestión TI	Procesos estratégicos Procesos misionales Procesos de apoyo Procesos de evaluación y control

Tabla 1 Entorno crítico del negocio

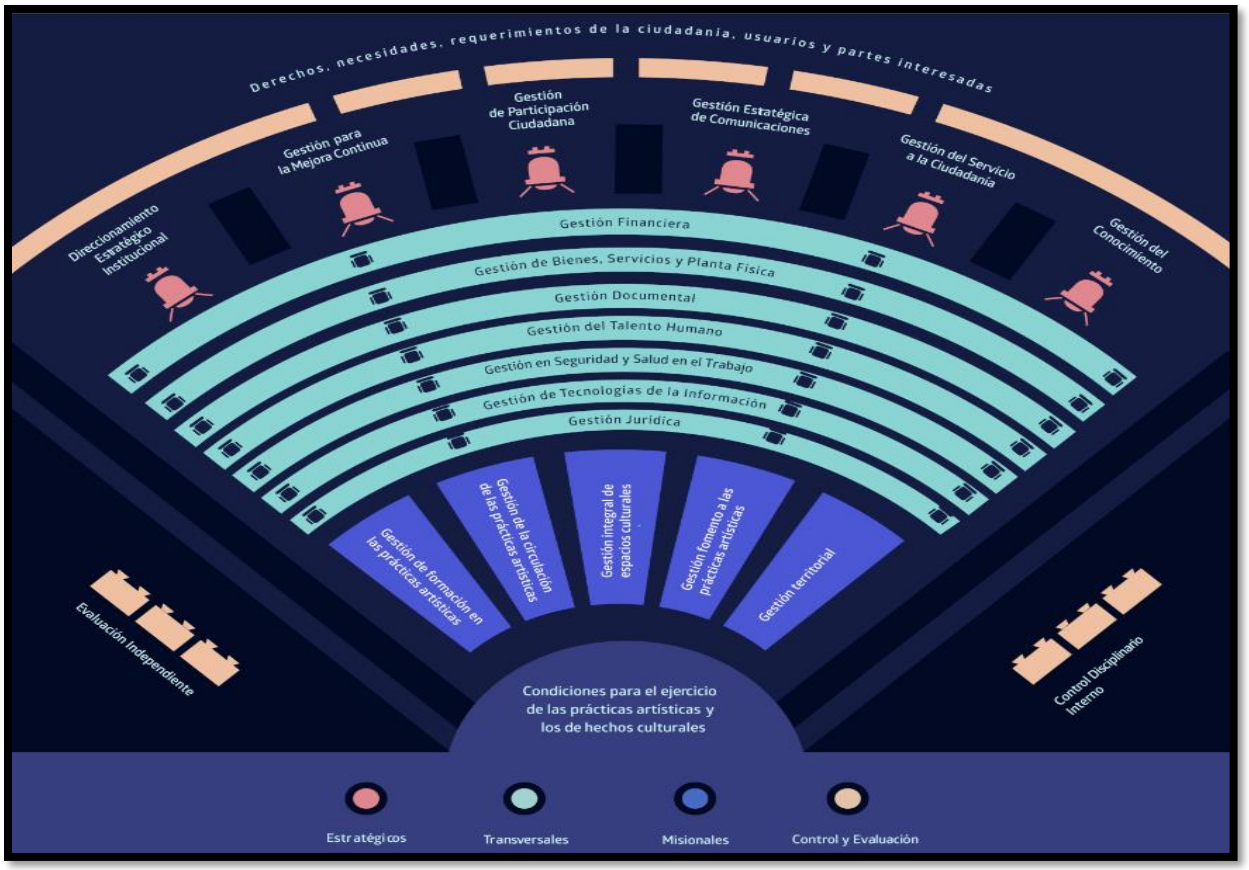

Ilustración 6 Mapa De Procesos Idartes

PROCESOS ESTRATÉGICOS	
Proceso	**Objetivo del proceso**
Direccionamiento estratégico institucional	Proporcionar la dirección que guía la entidad frente a los escenarios presentes y futuros, a través de instrumentos de programación, seguimiento, evaluación y realimentación de la gestión institucional, facilitando el desarrollo articulado de sus planes, programas y proyectos propuestos para el cumplimiento misional, con el fin de generar el impacto social esperado.
Gestión de tecnologías de la información y las comunicaciones - TIC	Gestionar integralmente los servicios de tecnologías de la información y comunicaciones - TIC, garantizando la implementación, administración, desarrollo e innovación a partir de la prestación de los servicios acorde a las necesidades de la entidad para contribuir en el desarrollo de los procesos estratégicos, misionales y de apoyo en el fortalecimiento de la Entidad.
Apoyo - Gestión Comunicaciones	Generar estrategias de difusión, promoción y divulgación efectiva de la oferta cultural y artística del Idartes dirigidas a los ciudadanos y al sector artístico, consolidando las comunicaciones como un medio vital para el logro de la coherencia organizacional, los objetivos misionales y el posicionamiento de la entidad.
Gestión del servicio a la ciudadanía	Garantizar a los usuarios y demás partes interesadas el acceso oportuno. eficaz y eficiente a la información. trámites y servicios que ofrece el Idartes, a través de los canales de atención a la ciudadanía, asegurando que se brinde en los términos previstos por la normatividad vigente. bajo los principios de oportunidad, calidad y calidez.

Gestión del conocimiento	Fomentar procesos de Investigación y gestión del conocimiento a partir de la producción, sistematización, análisis y evaluación de la información, que permita Innovar, generar y fortalecer las reflexiones en tomo a la interacción de las prácticas artísticas, sirviendo como referente para los diferentes agentes del sector y soporten la toma de decisiones de la entidad con relación a su quehacer.

Tabla 2 Procesos estratégicos

Procesos misionales	
Gestión de formación en las prácticas artísticas	Contribuir a la generación de capacidades de los ciudadanos a través del desarrollo de actividades de apropiación y transmisión de los saberes en torno a las prácticas artísticas, bajo enfoques multidisciplinares e interdisciplinares con criterios de accesibilidad, articulación intersectorial y territorial
Gestión de circulación de las prácticas artísticas	Potenciar el papel de las prácticas artísticas en la transformación de la ciudad y el ejercicio de la libertad creativa de los ciudadanos, a través de la puesta en escena de los procesos artísticos, para lograr su apreciación, significación, re-significación y apropiación.
Gestión integral de los espacios culturales	Garantizar las condiciones óptimas para la operación integral de los espacios culturales a cargo de la entidad, logrando su sostenibilidad física, económica y cultural, a través de la generación de oferta artística y cultural diversa, permanente y de calidad, que sea articulada con los territorios y otros sectores, con criterios de eficiencia y eficacia.
Gestión fomento a las prácticas artísticas	Promover el desarrollo de las prácticas de los campos de las artes, por medio de la entrega de recursos financieros, técnicos y en especie necesarios para su ejecución y generación de productos culturales y artísticos, con el fin de lograr visibilizar gestión, fortalecimiento y proyección de las prácticas artísticas en la ciudad y su interrelación con otros campos del saber.
Gestión de participación y organización del sector artístico	Propiciar escenarios de encuentro, diálogo, interacción y concertación entre los agentes artísticos y la entidad, para la consolidación de las organizaciones artísticas, la formalización del sector, en el marco de un ejercicio democrático e intercultural.

Tabla 3 Procesos misionales

Procesos de apoyo	
Transversal - Gestión Financiera	Garantizar el óptimo registro, administración y control de los recursos financieros de la entidad, atendiendo al cumplimiento de las disposiciones legales vigentes, buscando el cumplimiento de las metas y objetivos institucionales, con principios de integralidad, veracidad, oportunidad y transparencia de la información.
Transversal - Gestión de bienes servicios y planta física	Administrar, custodiar, mantener, adecuar y suministrar los bienes, planta física e infraestructura, servicios y recursos físicos que requiera la entidad de manera oportuna para asegurar su adecuado funcionamiento.

Transversal - Gestión Documental	Garantizar la administración y conservación del acervo documental de Idartes para el acceso y consulta con el propósito de satisfacer las necesidades y expectativas de los usuarios internos y externos que sirva como apoyo a la investigación, formación, creación, circulación, apropiación de las prácticas artísticas y a la gestión administrativa de la entidad.
Transversal - Gestión Talento Humano	Propender por el establecimiento de relaciones laborales y contractuales amónicas, colaborativas y constructivas en el equipo de trabajo que refuercen su compromiso. identidad y convicción frente a la labor desarrollada en la entidad.
Transversal - Gestión Jurídica	Orientar todas las actuaciones de la entidad en el cumplimiento del marco normativo y los principios que rigen la función pública, al igual que apoyar el desarrollo de los procesos contractuales requeridos para la adquisición de los bienes y/o servicios necesarios para su operación.

Tabla 4 Procesos de apoyo

Procesos de evaluación y control	
Control evaluación y seguimiento	Medir la efectividad del Sistema de Control Interno, la eficiencia, eficacia y efectividad de los procesos, el nivel de ejecución de los planes, programas y proyectos, los resultados de la gestión y realizar actividades tendientes a reducir las faltas disciplinarias, a través de la función preventiva y/o conectiva, generando recomendaciones en pro del mejoramiento y fortalecimiento de la institucionalidad.
Gestión integral para la mejora continua	Mejorar continuamente la eficiencia, eficacia y efectividad de la gestión de la entidad, a partir de los instrumentos de contingencia, seguimiento y retroalimentación que conllevan a llevar un modelo de interacción e interrelación entre los diferentes procesos, respondiendo a las dinámicas cambiantes que enfrente la entidad

Tabla 5 Procesos de evaluación y control

7.3.3 Establecimiento 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.

Tabla 6 Descripción de tiempos de recuperación

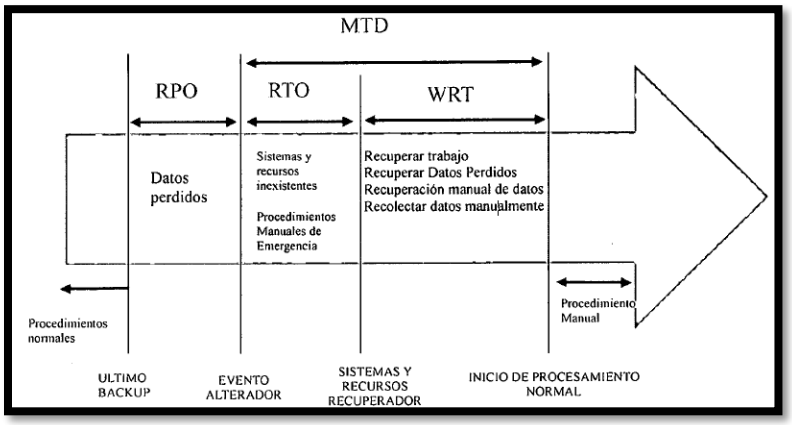

Ilustración 7 Mapa de tiempo para la recuperación de un desastre

7.3.4 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.

7.3.5 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.

7.3.6 Tipos de Impactos

- En este sentido, se definen los diversos tipos de impacto que una disrupción puede causar en el negocio, dependerá de la naturaleza que tiene el negocio, posiblemente los factores que más se pueden ver impactados son los que abarcan el rubro financiero por multas y daños o serán los que puedan afectar a una misionalidad de la entidad del sector gobierno. A continuación, se indican algunos de los principales tipos de impacto que pueden ser utilizados en el BIA:

- Costos involucrados. Uno de los principales impactos que produce una disrupción en un negocio

es la pérdida monetaria, dicha pérdida puede ser de manera directa (costo asociado a la recuperación de la operación, en horas hombre, equipamientos y otros) o indirecta (dinero no percibido por la interrupción de las actividades del Idartes). Para determinar estas pérdidas indirectas, se puede recurrir a datos estadísticos que permitan proyectar el ingreso generado por el proceso, dependiendo de la hora y fecha en la cual dicha disrupción ocurra.

- Efecto en la imagen. Otro impacto que puede ocasionarse debido a una disrupción es el daño en la imagen corporativa del Idartes, el cual puede traducirse en pérdida de usuarios actuales o alejamiento de potenciales usuarios de esta. En este sentido, el auge de las redes sociales y los medios de denuncia masivos hacen de que dicho factor pueda transformarse en relevante a la hora de determinar un RTO.

- Impacto normativo. En las organizaciones del estado que están sujetas a entes reguladores, el impacto de una disrupción a nivel normativo puede traducirse en observaciones, sanciones e incluso restricciones para la operación de la Entidad cuando se ve afectada por una disrupción.

- Impacto a nivel operacional. Como bien es sabido, rara vez un proceso de negocio será totalmente independiente del resto de los procesos del Idartes, en este sentido, un proceso de disrupción que afecte un proceso de negocio puede terminar afectando otros procesos a nivel institucional.

- Masividad. El impacto que una interrupción de un proceso de negocio produce puede medirse con base a la cantidad de transacciones que se ven interrumpidas o la cantidad de clientes que se pueden ver afectados.

Una vez que se definen los factores que serán medidos para determinar el RTO, se debe crear una matriz que permita determinar el nivel de impacto en base a una escala.

7.3.7 Generación de Informe de Impacto del Negocio

Matriz de factores de impacto de negocio					
	Factor económico	*Factor Imagen*	*Factor Normativo*	*Factor Operacional*	*Factor Transaccional*
Insignificante	0 a 1.000.000	No afecta la imagen del Idartes	No afecta la reputación del Idartes	No afecta la operación de la Entidad	Afecta hasta 100 transacciones mensuales de la Entidad
Menor	1.000.000 a 10.000.000	Afecta a un grupo reducido de personas	La situación no provoca impacto normativo	Interrumpe la operación o proceso de control para la gestión interna de la organización	Afecta entre 100 a 500 transacciones mensuales de la Entidad
Moderado	10.000.000 a 100.000.000	La información trasciende y se divulga en comunicaciones o medios externos	La situación provoca sanaciones y/o observaciones de entes regulatorios	Interrumpe la operación de un proceso de gestión interna del Idartes	Afecta entre 500 a 1.000 transacciones mensuales de la Entidad

Mayor	100.000.000 a 1.000.000.000	la situación trasciende a medios específicos de denuncia y redes sociales	La situación provoca multas de los entes regulatorios, pero no trae sanciones	Interrumpe la operación de un proceso crítico de gestión y afecta a los usuarios del Idartes	Afecta entre 1.000 a 10.000 transacciones mensuales de la Entidad
Catastrófico	Mayor a 1.000.000.000	La situación trasciende y se divulga en medios masivos	La situación provoca multas y sanciones al Idartes y requiere un pronunciamiento público para conocimiento de la ciudadanía	Interrumpe procesos críticos y afecta al usuario y los tiempos de respuesta establecidos.	Afecta a más de 10.000 transacciones mensuales de la Entidad

Tabla 7 Matriz de factores de impacto de negocio

Matriz de impacto cualitativo de negocio						
	1-5 Horas	**5-10 Horas**	**10-15 Horas**	**15-24 Horas**	**24-36 Horas**	**Más de 36 Horas**
Económico	Insignificante	Menor	Menor	Moderado	Mayor	Mayor
Imagen	Menor	Moderada	Mayor	Mayor	Catastrófica	Catastrófica
Reputación	Insignificante	Insignificante	Menor	Menor	Moderado	Moderado
Operación	Insignificante	Insignificante	Menor	Menor	Moderado	Moderado
Transacciones	Menor	Moderada	Mayor	Mayor	Catastrófica	Catastrófica

Tabla 8 Matriz de factores de impacto de negocio

7.3.8 Identificación de Recursos

Se realizó la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomar acciones para medir el impacto del negocio de la Entidad. Para lo cual se estableció una tabla de valores de procesos críticos que se aplica a la tala de sistemas de información que requieres aplicar a la continuidad y conforme a los factores de impacto de negocio. Para esta actividad se contempla un recurso de infraestructura tecnológica y un recurso humano que estará soportando la gestión de continuidad TI.

7.3.9 Identificación de Sistemas y Servicios TI Críticos

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

Valores de procesos críticos del negocio - análisis de impacto de Negocios BIA	
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

Tabla 9 Valores de procesos críticos del negocio

Sistemas para continuidad del TI	
A: Crítico para el Negocio, la función del negocio no puede realizarse	SIF SUMA+ SSO PUFA Librealviento Equipamientos culturales
B: No es crítico para el negocio, pero la operación es una parte integral del mismo.	Pandora KOHA Geoclick Planeador Glpi - Visor Glpi SI CAPITAL ORFEO Sistema de Información de Contratación
C: La operación no es parte integral del negocio	Sistema de gestión de proyectos Sistema de Caja Menor Sistema de Atención Al Usuario - Iris Sistema de Convocatorias para Planta Temporal Sistema de Gestión de Proyectos

Tabla 10 Sistemas para continuidad del TI

7.3.10 Identificación de sistemas alternos

Hace posible que los procesos del negocio puedan continuar operando en caso de presentarse una interrupción; para esto, se definirá conforme al incidente de interrupción presentado, métodos alternativos de manera temporal que ayuden a superar la crisis que ha generado una interrupción.

7.4 FASE III - ESTRATEGIA DE RESPALDO

7.4.1 Centro Alterno para Contingencias

Ante eventuales daños, ataques a la seguridad de la información o ciberataques 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:

- Respaldo en una infraestructura en premisa fuera de las instalaciones del Idartes.
- Datacenter Alterno

7.5 FASE IV - DESARROLLO DEL PLAN DE CONTINUIDAD

7.5.1 Roles y 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.

7.5.2 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 Profesional Universitario De La Oficina Asesora De Planeación y Tecnologías 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.

Profesional Universitario de la OAP - TI	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.
Administrador de Conectividad	Es aquel profesional encargado de garantizar la conectividad de los canales y de los elementos que conforman la red de la entidad.
Oficial de Seguridad de la Información	Es el profesional encargado de velar por la gestión de incidentes que afecten la disponibilidad, integridad y accesibilidad de la información y validar la gestión realizada para atender a la recuperación ante eventos que generen indisponibilidad de servicios vitales para el funcionamiento de la entidad.

Tabla 11 Roles y responsabilidades PCN

7.5.3 Despliegue del Plan de Contingencia

Ante una eventual emergencia, que comprometa la plataforma tecnológica y sistemas de información del Instituto Distrital de las Artes, se debe seguir el *Procedimiento de atención a incidentes de seguridad de la información* publicado en la intranet del Idartes, contemplando el *Plan de Modelo de Seguridad y Privacidad de la Información.*

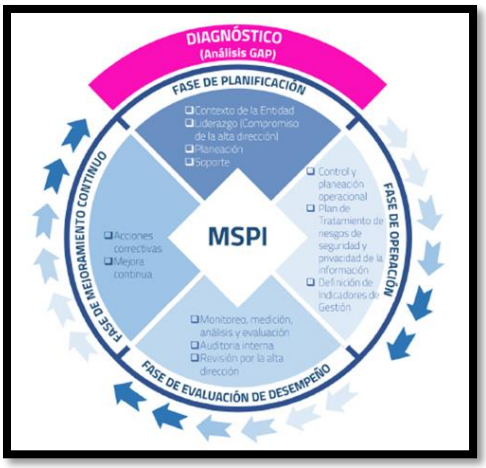

Ilustración 8 Ciclo del Modelo de Seguridad y Privacidad de la Información

El Profesional Universitario de la OAP - TI, evaluará el impacto del evento y activará el plan de contingencia conforme a lo informado en el análisis realizado por el oficial de seguridad de la información para declarar la emergencia como Parcial o Total asa:

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.

Contingencia para Pérdida Total: Profesional Universitario de la OAP - TI, convoca el comité para atender los siguientes aspectos.

7 El comité define un punto de encuentro u operaciones, según el evento.
8 Se designa un vocero o encargado de las comunicaciones, quien mantendrá informado a todos los funcionarios de los avances, tiempos y pasos a seguir.
9 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.
10 Se autoriza la fase de restauración de la plataforma tecnológica y servicios de los sistemas de información.
11 Convocar a las personas responsables para la solución.

7.5.4 Directorio de emergencias

En caso de presentarse un incidente que impacte la continuidad de los servicios TI afectando la gestión de funcionamiento normal de la entidad se tiene los siguientes enlaces de comunicación.

Nombre	Rol de Responsabilidad	Contacto
Jonathan González	Profesional Universitario	Jonathan.gonzalez@idartes.gov.co
Jorge Ramírez	Administrador de Infraestructura	jorge.ramirez@idartes.gov.co
Jorge Ramírez	Administrador de conectividad	jorge.ramirez@idartes.gov.co
Juan Bacca	Adecuaciones y mantenimiento	Juan.bacca@idartes.gov.co
Martha Mateus	Oficial SGSI	martha.mateus@idartes.gov.co

Miguel Acuña	Web Master	Sidney.acuna@idartes.gov.co
Miguel Acuña	Redes Sociales	Sidney.acuna@idartes.gov.co
Luis Jiménez	DBA	Luis,jimenez@idartes.gov.co
ETB	ISP conectividad	Helpdesketb@etb.com.co
Codensa	Energía eléctrica	
Acueducto	Proveedor acueducto	
Csirt	Centro Cibernético – Apoyo en atención respuesta a incidentes Informáticos.	

Tabla 12 Directorio Contingencia

7.5.5 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 iniciaron los procedimientos técnicos de restauración de los servidores y sistemas de información. El procedimiento para seguir será un documento técnico que debe reposar en la documentación del Área de Tecnología.
- Una vez restaurado cada servicio, se realizan 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.

7.5.6 Controles existentes

Actualmente el Instituto Distrital de las Artes – Idartes cuenta con el instrumento documental de gestión de tecnologías de la información y las comunicaciones denominado Política de Seguridad y Privacidad de la Información, aprobado y publicado, con el cual se incorporan controles a la infraestructura tecnológica del Idartes y la gestión de seguridad de la información.

- Controles de infraestructura de conectividad
- Gestión de activos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de los incidentes de la seguridad de la información
- Gestión de la continuidad del negocio

- Cumplimiento de los requisitos legales
- Monitoreo y seguimiento

7.6 Plan maestro de recuperación

7.6.1 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 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.

7.6.2 Pérdida 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

7.6.3 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 profesional universitario de la OAP- TI 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.

7.6.3.1 Acceso/borrado no autorizado a información confidencial

- Identificar 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

7.6.3.2 Pérdida 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 el 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

7.6.3.3 Sistema de información SICAPITAL

- 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 la cinemateca de Bogotá al día hábil anterior, o contactar con la empresa 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

- Los administradores de los sistemas de información SiCapital 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 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.

7.6.3.4 Sistema de información PANDORA

- Restringir el acceso al entorno de producción para los usuarios durante el proceso de recuperación de la información.
- Informar a los usuarios internos y externos sobre la activación del servidor temporal de Sistemas de Información utilizando diferentes canales de comunicación, como correo electrónico, sitio web o teléfono.
- Asegurar que las copias de seguridad estén disponibles y sincronizadas con el servidor alterno ubicado en la Cinemateca de Bogotá hasta el último día hábil anterior. En caso contrario, contactar a la empresa encargada de la custodia de las copias.
- Verificar con el encargado de infraestructura y redes los servicios básicos del servidor alterno, incluyendo el sistema operativo, conexión a la base de datos, copias de seguridad y red.
- Activar el protocolo de recuperación del servidor alterno para la restauración de bases de datos y aplicaciones en PANDORA.
- Los administradores de los sistemas de información de PANDORA deben verificar la integridad de la información contenida en las copias de bases de datos realizadas desde el datacenter principal.
- Los administradores de los sistemas de información de PANDORA deben reiniciar los servicios y restaurar las bases de datos utilizando las copias disponibles en el servidor de respaldo.
- Seguir el procedimiento detallado 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 sobre el restablecimiento del servicio.
- Documentar todas las correcciones realizadas y reportarlas al encargado del Área de Tecnología.

7.7 DOCUMENTACIÓN DE LA CONTINGENCIA

7.7.1 Documentos requeridos para contingencias de TI

Adicional del plan maestro de recuperación se debe contar con los siguientes documentos específicos para la contingencia y/o restauración de la infraestructura tecnología:

1. Matriz Análisis de Impacto al Negocio – BIA.
2. Contingencia para las páginas web del Idartes.
3. Contingencia B.D ORACLE.
4. Contingencia para restauración ORFEO.
5. Contingencia y restauración SIF.
6. Contingencia y restauración PANDORA.

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

Durante el tiempo que dure la emergencia de la contingencia, y 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.

7.7.2 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?

7.7.3 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:

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

7.8 APLICABILIDAD

La Declaración de Aplicabilidad SoA referenciado en el numeral 6.1.3d de la norma ISO-27001:2013, es un documento que lista los objetivos y controles que se van a implementar en la Entidad, el cual se encuentra publicado en el sitio web de la entidad comunicarte en el proceso de Gestión de tecnologías de la información con el formato Código: GTI-F-21 en este entendido y conforme al análisis realizado para establecer los controles del presente plan, este tipo de análisis se hace evaluando el cumplimiento de la norma ISO27001:2013, para cada uno de los controles establecidos en los 14 dominios o temas relacionados con la gestión de la seguridad de la información que este estándar.

7.9 CONTROL Y SEGUIMIENTO

Es importante conocer de manera permanente los avances en la gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de éstos en el comité de gestión institucional y desempeño, como lo establece el MIPG. La Oficina Asesora de Planeación y Tecnologías de la Información debe realizar el seguimiento y control a la implementación y/o mantenimiento de la Seguridad de la Información.

Se debe revisar periódicamente por cada responsable de los procesos al interior de las entidades, junto con su equipo los siguientes aspectos:

Ajustes y modificaciones:

Después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el plan de seguridad y privacidad de la información, en este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

Monitoreo:

En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizan monitoreo y evaluación permanente a la gestión de seguridad y privacidad de la información.

Seguimiento:

- El jefe de control interno, o quien haga sus veces, debe adelantar seguimiento a la gestión de seguridad y privacidad de la información, en este sentido, es necesario que en sus procesos de seguimiento interno analicen las causas, los riesgos y la efectividad de los controles incorporados en el documento.

- Es importante que las Entidades conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de éstos en el comité de gestión institucional y desempeño, como lo establece el MIPG.

- Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política de seguridad de la información y el Plan de Seguridad y Privacidad de la Información deben ser

tratados y aprobados en el comité institucional de gestión y desempeño de ser necesario para su óptimo cumplimiento.

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
1	2023-02-28	Emisión inicial
2	2024-09-13	Actualización de las fases de implementación del Plan de Continuidad.

CONTROL DE APROBACIÓN

ESTADO	FECHA	NOMBRE	CARGO
ELABORÓ	2024-09-13	MARYURY FORERO BOHORQUEZ	ENLACE MIPG
REVISÓ	2024-09-13	MARIA CRISTINA HERRERA CALDERON	REFERENTE MIPG
APROBÓ	2024-09-13	DANIEL SANCHEZ ROJAS	LIDER DE PROCESO
AVALÓ	2024-09-13	DANIEL SANCHEZ ROJAS	JEFE DE LA OFICINA ASESORA DE PLANEACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN

COLABORADORES

NOMBRE
JONATHAN GONZALEZ BOLANOS
MARTHA PATRICIA MATEUS GONZALEZ