OBJETIVO

Definir un procedimiento para asegurar la información contenida en la infraestructura donde se salvaguarda información, sistemas de información, Bases de Datos, archivos a través de la generación de copias de seguridad y respaldo, garantizando la integridad y disponibilidad en la continuidad de los procesos, además de su recuperación ante posibles eventos de desastre.

ALCANCE

El procedimiento inicia con el aseguramiento del área y del equipo por parte de los usuarios que detectaron el incidente de seguridad de la información, que luego será tratado por el personal de operativo quienes se encargaran de recolectar y salvaguardar la evidencia en cadena de custodia, la actividad termina con la evaluación y monitoreo del administrador de seguridad informática.

Este procedimiento aplica para todos los procesos de la entidad.

RESPONSABILIDADES

RESPONSABLES	RESPONSABILIDADES
CIO y/o Coordinador / líder de Gestión de las Tecnologías de la Información	Realizar la aprobación de solicitud por parte de los servidores públicos y/o contratistas para la autorización y aprobación de la creación de la cuenta de usuario
Profesionales de infraestructura	Garantiza la prestación de los servicios de TI, identificando las capacidades actuales de los Servicios Tecnológicos y proyectando las capacidades futuras requeridas para un óptimo funcionamiento y prestación de capacidad para los backup
Profesionales de mesa de servicio	Es el responsable de recibir la solicitud del servicio de resguardar información en la plataforma de mesa de servicio - Aplicar las medidas de protección de la información
Profesional de seguridad	Velara por la realización oportuna de las copias de seguridad en el área de infraestructura y su cumplimiento con el procedimiento
Asesores, Subdirectores, Servidor Público y/o Contratista	Realizar uso adecuado de las cuentas asignadas y velar por el cumplimiento de las políticas de seguridad de la información definidas por la entidad.

DEFINICIONES	
TÉRMINO	**DEFINICIÓN**
Activos de Información	Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc. https://www.secretariajuridica.gov.co/sites/default/files/2022-03/Gu%C3%ADa%20para%20el%20Registro%20y%20la%20Clasificaci%C3%B3n%20de%20Activos%20de%20Informaci%C3%B3n%20V5_copia_controlada.pdf
Almacenamiento	Es la propiedad o capacidad de guardar datos que tiene un dispositivo electrónico. Computadoras, y demás dispositivos electrónicos se utiliza no sólo para guardar datos sino también para procesarlos. https://sites.google.com/view/gerardo-isaias-espinoza-leal/unidad-3/3-5-almacenamiento-direccionamiento-y-representaci%C3%B3n-en-memoria
Backup	El backup o copia de seguridad (de respaldo), es la copia total o parcial de información importante como respaldo frente a eventualidades. https://es.wikipedia.org/wiki/Copia_de_seguridad
Cifrar	El cifrado es la práctica de codificar y decodificar datos, aplicándoles un algoritmo para codificarlos, de manera que dejan de estar en su formato original y, por consiguiente, no se pueden leer. Los datos solo se pueden decodificar a su forma original aplicando una determinada clave de descifrado. https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)
Confidencialidad	Acceso a la información por parte de únicamente de quienes estén autorizados. Característica o propiedad por la cual la información no está disponible o revelada a individuos, entidades o procesos no autorizados. https://www.vecol.com.co/politica-de-seguridad-de-la-informacion/#:~:text=Confidencialidad%20de%20la%20Informaci%C3%B3n%3A%20Acceso,empresas%2C%20o%20procesos%20no%20autorizados.
Copias de seguridad	se utilizan ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas. https://es.wikipedia.org/wiki/Copia_de_seguridad#:~:text=Las%20copias%20de%20seguridad%20son,virus%20inform%C3%A1tico%20u%20otras%20causas%3B
Disponibilidad	Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Característica o propiedad de la información de permanecer asequible y disponible para su uso cuando lo requiera una entidad autorizada. (propia a partir de información en la red)

DEFINICIONES	
TÉRMINO	**DEFINICIÓN**
Fiabilidad	La fiabilidad de un sistema es la probabilidad de que ese sistema funcione o desarrolle una cierta función, bajo condiciones fijadas y durante un período determinado. https://es.wikipedia.org/wiki/Fiabilidad_de_sistemas#:~:text=La%20fiabilidad%20se%20define%20como,el%C3%A9ctrica%2C%20nivel%20de%20vibraciones).
Hash:	Son algoritmos que logran crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado. (propia a partir de información en la red)
Infraestructura	Conjunto de todos los elementos tecnológicos hardware y software: servidores, computadores, portátiles, impresoras, switches, routers, firewall, escáneres, cableado estructurado, CPU's, software informático, sistemas de información, equipos de comunicación, internet, red LAN. https://www.participacionbogota.gov.co/sites/idpac/files/informacion-de-la-entidad/2024-07/1513625358-idpac-gti-pr-20-analisis-adquisicion-infraestructura-tecnologica.pdf
Integridad	Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Propiedad/característica de salvaguardar la exactitud y completitud de los activos. https://www.iso27000.es/sgsi.html
Respaldo	Se refiere al resguardo que se realiza de ciertos datos, suele emplearse con relación a los datos digitales (que están alojados en el disco duro de una computadora u ordenador), aunque también puede vincularse a la protección de documentos físicos. https://steemit.com/spanish/@smilefalse/respaldo-en-un-sistema-de-informacion-y-telecomunicacion
Usuario	Persona que tiene el derecho de usar de una cosa ajena con unas limitaciones determinadas. (propia a partir de información en la red)

MARCO LEGAL

I. **Ley 2294 de 2023** por el cual se expide el plan nacional de desarrollo 2022-2026 "Colombia potencia mundial de la vida"
II. **Ley 1712 de 2014** "Ley de transparencia y del derecho de acceso a la información pública nacional"
III. **Ley 1672 de 2013** - política Pública de Gestión Integral de Residuos de Aparatos eléctricos y electrónicos (RAEE).
IV. **Ley 1618 de 2013** - Ley de Acceso y Accesibilidad (Derecho a la Información y Comunicación de las Personas con Discapacidad.

MARCO LEGAL	
V.	**Ley 1581 de 2012**. "Por la cual se dictan disposiciones generales para la protección de datos personales".
VI.	**Ley 1266 de 2008** - Ley de Habeas Data y Manejo de BD de información.
VII.	**Ley 1273 de 2009** - Ley de la Protección de la Información y de los Datos.
VIII.	**Ley 1341 de 2009**: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones
IX.	**Ley 527 de 1999.** "Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las Entidades de certificación y se dictan otras disposiciones".
X.	**Decreto 767 de 2022**, para la implementación de la Política de Gobierno Digital, se han definido los cinco elementos: Gobernanza, Innovación Pública Digital, Habilitadores, Líneas de acción e iniciativas dinamizadoras.
XI.	**Decreto 338 de 2022:** Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"
XII.	**Decreto 088 de 2022:** "Por el cual se adiciona el Titulo 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea".
XIII.	**Decreto 620 de 2020:** Por el cual se establecen los lineamientos generales en el uso y operación de los servicios ciudadanos digitales
XIV.	**Decreto Ley 2106 de 2019:** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
XV.	**Decreto 612 del 2018** - Integración de los Planes Institucionales y estratégicos al Plan de Acción.
XVI.	**Decreto 1008 del 2018** – Política de Gobierno Digital.
XVII.	**Decreto 1413 de 2017**- Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones,
XVIII.	**Decreto 1078 de 2015**, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
XIX.	**Decreto 2573 de 2014** Lineamientos Generales de Gobierno en línea
XX.	**Decreto 1377 de 2013** - Reglamentación de protección de Datos Personales.
XXI.	**Decreto 2609 de 2012** – preservación y Gestión de Documentos en Ambientes electrónicos.
XXII.	**Decreto 235 de 2010** – Intercambio de Información Entre Entidades Públicas.

MARCO LEGAL	
XXIII.	**Decreto 1078 de 2015**: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
XXIV.	**Resolución MINTIC 1951 de 2022**: Por la cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital.
XXV.	**Resolución MinTIC 1117 de 2022:** "Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital
XXVI.	**Resolución MinTIC 746 de 2022** Por la cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales de la Resolución 500 de 2022
XVII.	**Resolución 500 de 2021** – "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"
XVIII.	**Resolución MinTIC 2160 de 2020**: Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos.
XXIX.	**Resolución 1519 de 2020** de MinTic "Reglamentación de aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública"
XXX.	**Resolución UNP 1767 de 2024** - Por la cual se organiza el modelo integrado de Planeación y Gestión y deroga Resolución 1023 de 2022 de la UNP
XXXI.	**Resolución UNP 0649 de 2024** - Se adopta la Política del Modelo Integrado de Planeación y Gestión - Sistema Integrado de Gestión de la UNP
XXII.	**Resolución UNP 0054 de 2024** - Actualización Plataforma Estratégica de la UNP para el periodo 2023 - 2026 y se deroga la Resolución 0199 de 2020.
XXIII.	**ISO/IEC 27001:2022**, Sistemas de Gestión de la Seguridad de la Información esta referencia al Anexo A puede entenderse como una lista de posibles controles de seguridad de la información más abierta y, por tanto, de aplicación más flexible.
XXIV.	Norma Técnica Colombiana NTC-ISO/IEC 27002 Tecnología de la Información. Técnica de Seguridad. Código de Práctica para Controles de Seguridad de la Información
XXV.	**Documento CONPES 3975-2019** política Nacional para la Transformación Digital e Inteligencia Artificial.
XXVI.	**Documento CONPES 3854-2016** - política Nacional de Seguridad Digital.

MARCO LEGAL
XVII. **Documento CONPES 3920-2018** – Política Nacional de Explotación de Datos (BIG DATA)

DOCUMENTOS RELACIONADOS
• GTE-MA-02 Manual de Políticas Específicas de seguridad y privacidad de la información. • GTE-FT-51 Formato de copia de seguridad y restauración • GTE-FT-34 Formato acuerdo de confidencialidad para Servidores públicos, contratistas y/o terceros • ISO/IEC 27001: (Information technology - Security techniques - Information security management systems - Requirements) Estándar para la seguridad de la información. • Ley 1581 de 2012 Ley de Protección de Datos Personales. • Decreto 1078 de 2015 de MINTIC – Modelo de Seguridad y Privacidad de la Información.

CONSIDERACIONES GENERALES

1. En este procedimiento se tiene el compromiso de la salvaguarda de la información que se tienen en los servidores que se encuentran en el data center buscando cumplir los objetivos estratégicos institucionales,
2. Este procedimiento requiere del acompañamiento de los dueños de la información y las actividades de restauración que se requieren para mejorar los procesos y las oportunidades estratégicas de TI y no es una actividad que se pueda delegar en terceros,
3. Se tendrá como marco de referencia para el desarrollo del procedimiento Planeación y Lineamientos de
4. Tecnologías de la Información
5. Los responsables de los sistemas de información deben aplicar las buenas prácticas para la protección de la información y la administración de las bases de datos
6. Plataforma de La mesa de servicio es el principal y único punto de contacto entre los servidores públicos y los contratistas, Centraliza las demandas e incidentes relacionados con TI en un solo lugar. Registra y monitorea todas las actividades con el objetivo de solucionarlas y evitar que se repitan.

DESCRIPCIÓN DEL PROCEDIMIENTO

N° ACTIVIDAD	RESPONSABLE	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	REGISTRO
1	Jefe oficina asesora de planeación Coordinador / líder de GGT Equipo de infraestructura	Identificar Datos a Incluir en la Copia de Respaldo	Se realiza la identificación del alcance de acuerdo con las necesidades, el inventario de activos de información y su nivel de criticidad, obligaciones de ley, acuerdos contractuales y lo necesario para respaldar las funciones desarrolladas por la UNP	Políticas de copias de respaldo Bases de Datos
2	Coordinador de GGT	Definir las Copias de Respaldo	Se elabora el Formato de copias de respaldo teniendo en cuenta: • Frecuencia de la copia de respaldo.	

DESCRIPCIÓN DEL PROCEDIMIENTO				
N° ACTIVIDAD	**RESPONSABLE**	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**REGISTRO**

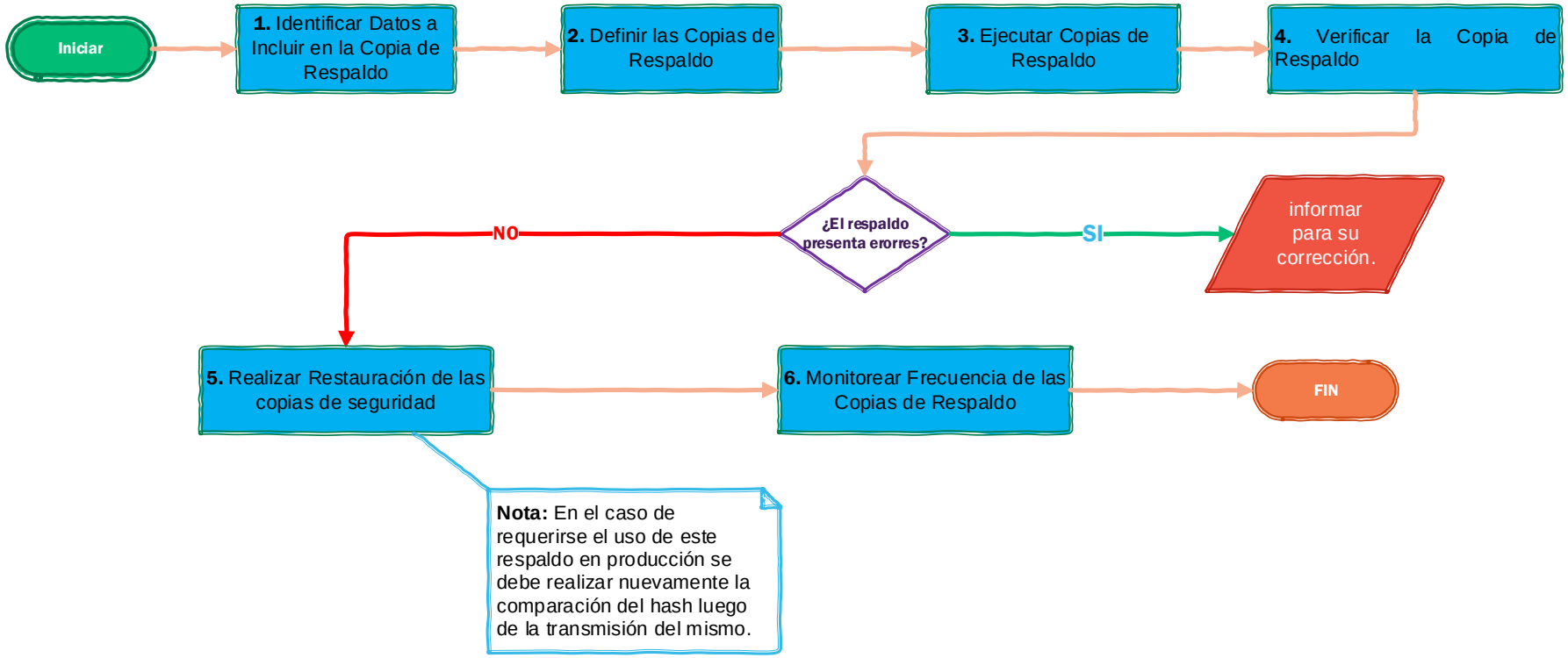
	Equipo de infraestructura		• Responsable.
			• Tipo de información
			• Tipo de Copia
			  ○ Completa
			  ○ Incremental
			  ○ Diferencial
			• Procesos involucrados.
			• Vigencia de las copias en función de su
			• Cifrar la información confidencial.
			• Localización del almacenamiento.
			• Acuerdos de nivel de servicio garantizando
			• Clasificación de las copias de respaldo.
			• disponibilidad, integridad, confidencialidad y control de
			
			En caso de que algún servidor público necesite copias de sus activos de información almacenados, realizará la solicitud requerida con su respectiva justificación, para evaluar las necesidades particulares.
				GTE-FT-51 Formato de copia de seguridad y restauración

3	Coordinador/ lider de GGT Equipo de Infraestructura	Ejecutar Copias de Respaldo	Para realizar las copias de respaldo se realizan las siguientes instrucciones: Acceder a la solución de respaldo, crear las tareas programadas de copia de Respaldo Indicando el recurso al cual se va a realizar el backup y la configuración de las rutas, el tipo de backup, la frecuencia y el horario de la ejecución de la tarea.	Solución de Backup Hash de Bases de Datos Configuraciones Registros Por medio de la plataforma de mesa de servicios

DESCRIPCIÓN DEL PROCEDIMIENTO				
N° ACTIVIDAD	**RESPONSABLE**	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**REGISTRO**
			Ejecutar las tareas programadas – tarea ejecutada automáticamente por el software de backup. Generar Hash del estado del Backup, con el fin de que al momento de restaurar la información se pueda realizar la respectiva comparación de integridad en la copia de respaldo.	GTE-FT-51 Formato de copia de seguridad y restauración
4	Coordinador / líder de GGT Equipo de Infraestructura	Verificar la Copia de Respaldo	Se realiza la verificación de los datos al finalizar la copia, debido a que estos pueden presentar errores, para esto se debe ingresar al software de copias de respaldo y verificar la operación realizada, en dado caso de que alguna copia de respaldo haya presentado errores se debe informar para su corrección.	GTE-FT-51 Formato de copia de seguridad y restauración
5	Coordinador/ líder de GGT Equipo de Infraestructura	Realizar Restauración de las copias de seguridad	Se verifica el estado final del proceso de la restauración documentando de la siguiente manera: • Fecha de la restauración. • ID Backup (nombre • Servidor • Ruta del directorio o Nombre De Recurso A Restaurar • Tipo • Responsable de Infraestructura • Responsable de la información • hash Base de datos producción • hash Base de datos del respaldo • Se procederá a realizar la comparación de la siguiente manera: ○ En el momento exacto de realizar el respaldo se debe comparar: Hash de la base de datos en producción con el hash que queda almacenado del respaldo, este	GTE-FT-51 Formato de copia de seguridad y restauración

DESCRIPCIÓN DEL PROCEDIMIENTO				
N° ACTIVIDAD	**RESPONSABLE**	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**REGISTRO**
			debe coincidir asegurando que no hubo alteración de la integridad de la información. Observaciones **Nota:** En el caso de requerirse el uso de este respaldo en producción se debe realizar nuevamente la comparación del hash luego de la transmisión del mismo. La frecuencia es cada seis meses o cuando lo requiera el dueño de la información	
6	Coordinador de GGT Equipo de Infraestructura	Monitorear Frecuencia de las Copias de Respaldo	La frecuencia establecida para la realización de copias de respaldo debe ser probada para establecer su practicidad y si es necesario replantear o mejorarla sobre la marcha, verificando que la copia de respaldo se realiza correctamente en los tiempos previstos.	Monitoreos Periódicas Opciones de Mejora.

FLUJOGRAMAS



CONTROL DE CAMBIOS			
VERSIÓN INICIAL	**DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO**	**FECHA**	**VERSIÓN FINAL**
00	Se crea procedimiento para asegurar la información contenida en la infraestructura donde se salvaguarda información, sistemas de información, Bases de Datos, archivos a través de la generación de copias de seguridad y respaldo, garantizando la integridad y disponibilidad en la continuidad de los procesos, además de su recuperación ante posibles eventos de desastre.	27/11/2024	**01**