0. CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Responsable	Descripción de Cambios realizados
1	2020-12-21	Néstor Ruiz Contratista Área de TIC	Emisión Inicial de acuerdo con la actualización del mapa de procesos de la entidad, en LMD anterior corresponde al código: 3AP-GTI-PD-04
2	2021-07-22	ANDRES ORLANDO BRICEÑO DIAZ	Se requiere la actualizacion del procedimiento en el marco de los lineamientos de actualización de instrumentos documentales para la gestion de tecnologias de la Informacion

1. LIDER DE PROCESO: CARLOS ALFONSO GAITAN SANCHEZ

1.1 OBJETIVO DEL PROCEDIMIENTO: Establecer los lineamientos para garantizar la disponibilidad, seguridad y confidencialidad de la información mediante el resguardo de la información digital considerada crítica por el IDARTES, así como la restauración de la misma.

1.2 ALCANCE DEL PROCEDIMIENTO: El procedimiento inicia con la identificación de la información y culmina con la copia o la restauración de la información, tanto de la sede Administrativa Principal como en los escenarios del Idartes y Centros CREA, realizando la administración y custodia de las cintas o medios de respaldo propio o externo que se generen de esta actividad.

1.3 RESPONSABLES DEL PROCEDIMIENTO: 120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN

2. GLOSARIO:

ANS: Acuerdos de niveles de servicio.

ANTIVIRUS: Programa diseñado para identificar, aislar o eliminar un virus del computador.

APLICACIÓN VAULT: Herramienta que hace parte de la Suite de Google Apps para almacenamiento y consulta de copias de seguridad de cuentas de correo de licenciamiento Basic.

BACKUP: Copia de respaldo de la información realizada en medio magnético.

CATEGORIA: Se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente o del grupo de trabajo responsable de su resolución. Se identifican los servicios afectados por el incidente.

CENTROS CREA: Centros de formación artística orientados a la comunidad, dependientes de la Subdirección de Formación.

CORREO ELECTRÓNICO: Es un servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos.

GLPI: Herramienta que gestiona las incidencias o solicitudes de soporte de los usuarios de la entidad. Su sigla, traducidas de francés a español, significan: Gestión Libre del Parque Informático

GOOGLE DRIVE: Servicio de herramientas colaborativas de la Suite de Google Apps para almacenamiento en nube y ofimática online.

HARDWARE: Componentes eléctricos, ópticos, electrónicos, electromecánicos y mecánicos que conforman un instrumento o sistema de computador.

INFORMACIÓN: Agrupación de datos con un significado específico.

LICENCIAMIENTO BASIC DE GMAIL: Tipo de cuenta de Gmail con opciones limitadas en cuanto a seguridad y respaldo.

LICENCIAMIENTO BUSINESS DE GMAIL: Tipo de cuenta de Gmail con opciones avanzadas en cuanto a seguridad y respaldo reservada para directivos y jefes de área.

SOFTWARE: Programas que se ejecutan en el computador para realizar una función determinada.

USUARIO: Servidor público que tiene a su cargo un computador y/o una cuenta de correo por medio de los cuales puede acceder a los recursos y servicios que ofrece una red.

USUARIOS ADMINISTRADORES: Usuarios con privilegios para instalación y configuración de software y hardware en el equipo asignado que por sus deberes funcionales requieren este perfil.

3. CONDICIONES GENERALES:

Identifica la información misional a respaldar

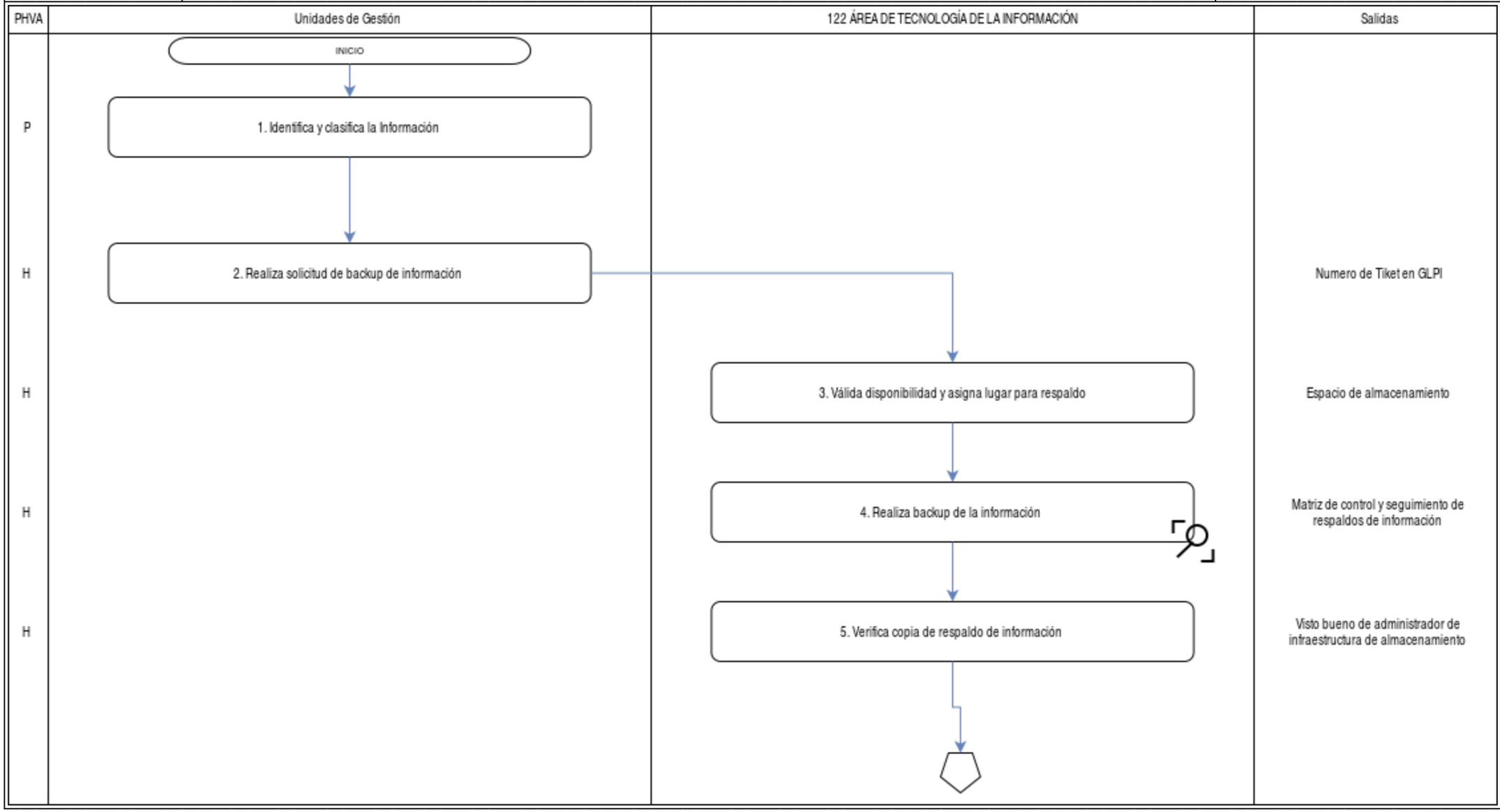
Solicita a través de la mesa de ayuda el respaldo de información

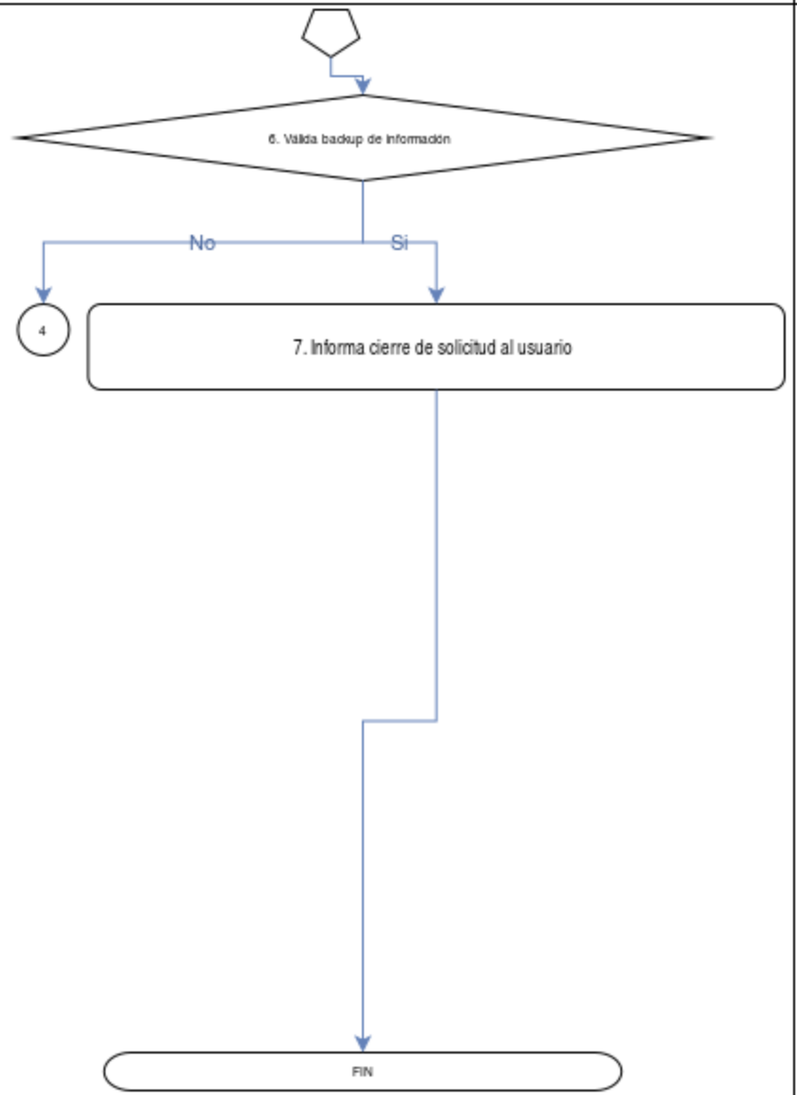
4. RELACIÓN CON OTROS PROCEDIMIENTOS Y PROCESOS: Esquema gráfico de la relación del procedimiento con otros procedimientos y/o procesos del IDARTES.

Procesos que se requieren como proveedor	Que insumos requiero del proveedor	Procedimiento	Que se obtiene del procedimiento	Para quien va dirigido el servicio o producto
• TODAS LAS ÁREAS	Información identificada, organizada Disponibilidad de tiempo	COPIA Y RESTAURACION DE LA INFORMACIÓN	Copias de seguridad de la información misional	• TODAS LAS ÁREAS

5. ICONOGRAFÍA DEL DIAGRAMA DE FLUJO: Iconografía asociada al diagrama del flujo del procedimiento.

5.1 DIAGRAMA DE FLUJO: Secuencia lógica de las actividades establecidas en el procedimiento.


PHVA
Unidades de Gestión
122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN
Salidas
INICIO
P
1. Identifica y clasifica la Información
H
2. Realiza solicitud de backup de información
Numero de Tiket en GLPI
H
3. Válida disponibilidad y asigna lugar para respaldo
Espacio de almacenamiento
H
4. Realiza backup de la información
Matriz de control y seguimiento de respaldos de información
H
5. Verifica copia de respaldo de información
Visto bueno de administrador de infraestructura de almacenamiento

PHVA	Unidades de Gestión	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Salidas
V H			Correo informativo al usuario

5.2. DESCRIPCIÓN DE LAS ACTIVIDADES: Características específicas de las actividades del procedimiento.

No.	Ciclo PHVA	Ciclo de Gestión	Descripción del Ciclo de Gestión	Actores	Responsable	Tiempo (Horas)	Documento o Registro
1	P	Identifica y clasifica la Información	Identifica y organiza la información de la cual se realizará la copia de seguridad. Analiza qué tipo de información se va a respaldar en el backup conforme a la política de operación 9.	Unidades de Gestión	Usuario propietario de la Información	1 día	
2	H	Realiza solicitud de backup de información	Realiza solicitud de respaldo de la información al grupo de Tecnología a través canales establecidos para el soporte técnico.	Unidades de Gestión	Usuario propietario de la información, jefes de área, control interno o líderes de procesos	1 día	Numero de Tiket en GLPI
3	H	Válida disponibilidad y asigna lugar para respaldo	Verifica la disponibilidad, calidad y espacio en las cintas o espacio en servidores de almacenamiento donde se realizará el backup de la información.	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Administrador de infraestructura de almacenamiento	1 día	Espacio de almacenamiento
4	H	Realiza backup de la información	Realiza la copia de la información Selecciona el espacio asignado de acuerdo con lo establecido en la política de operación 13, el personal de soporte que tiene el Tiket asignado genera la copia de respaldo de la información y documenta en la matriz de control la información de al copia realizada	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	El personal de soporte	1 día	Matriz de control y seguimiento de respaldos de información
5	H	Verifica copia de respaldo de información	Valida con el administrador de infraestructura de almacenamiento que se haya realizado la copia de la información conforme a lo solicitado por el usuario	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Personal de soporte	1 día	Visto bueno de administrador de infraestructura de almacenamiento
6	V	Válida backup de información	¿La información respaldada en el espacio asignado es idéntica a la solicitada por el usuario?	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	El personal de soporte	3 horas	
7	H	Informa cierre de solicitud al usuario	Documenta en el tiket de GLPI la trazabilidad realizada para culminar el backup solicitado por el usuario y se informa el cierre de su solicitud	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	personal de soporte	4 horas	Correo informativo al usuario

6. POLÍTICAS DE OPERACIÓN:

1. La Entidad no está sujeta a responsabilidad de pérdida de información ajena a la institucional, los documentos digitales personales deben estar en una carpeta independiente

2. Los backups deben ser almacenados en una unidad de almacenamiento de red asignada por el Ingeniero de conectividad

3. Para todos las copias de seguridad de Discos duros, documentos, archivos y/o bases de datos; se debe aplicar los criterios de respaldo con grados de backup completos, parcial e incremental y con frecuencias mensuales, semanales y diarias.

4. Para casos concernientes a incidentes de seguridad de la información se realizará la imagen de todo el disco duro como evidencia aportar a una posible investigación y aplicar el procedimiento de atención de incidentes de seguridad.

5. Para respaldos de la información del correo y drive de la plataforma workspace se deben tener en cuenta los caso de cobertura así: a) Terminación, suspensión o cesión de contrato, b) Situación de riesgo informático que amerite la suspensión de la cuenta del usuario, c) Firma de paz y salvo, d) Por solicitud de las directivas; las copias de seguridad para cuentas de licenciamiento Basic - Business - Enterprise se deben realizar con un respaldo completo de correo electrónico y se debe incluir el contenido de Google Drive; en casos de suspensión es necesario que el supervisor o jefe de área informe a la mesa de ayuda que se presenta la novedad contractual para proceder con el backup y será sujeto a concepto técnico, el respaldo al contenido alojado en el servicio de drive de Google con el fin de determinar si es necesario el backup o si procede la transferencia de la información a otra cuenta dentro del dominio con la responsabilidad de custodia que conlleva sobre el propietario de los documentos.

6. Toda solicitud de transferencia de propiedad de google drive de una cuenta a otra, se realizará con previa autorización del supervisor o jefe de área, así mismo, toda solicitud de transferencia de propiedad de google drive de una cuenta a otra, por cesión contractual o reasignación de funciones, será solicitada por medios de la herramienta de mesa de ayuda

7. Las transferencias de copias de respaldo del google drive de una cuenta a otra, transfiere la totalidad del contenido almacenado, no se realizarán traslados parciales de contenido.

8. Conforme a lo estipulado por la Oficina Asesora Jurídica, no se permite la entrega de información a personal que culmine su vínculo contractual por seguridad de la información; en caso de que se requiera realizar alguna consulta al backup realizado a su información, será sujeto a solicitud aprobada por la oficina asesora jurídica, líder de oficina o Subdirecciones, y se deben generar la solicitud de consulta la cual debe ser canalizada a través de un correo electrónico a la Oficina Asesora de Planeación y tecnologías de la información permitiendo dejar evidencia en la mesa de ayuda; el correo de solicitud debe contener como mínimo el nombre del funcionario, área a la que pertenece, motivo de la consulta y palabras claves.

9. Para respaldos de la información de la sede principal y de las sedes CREA se deben tener en cuenta los siguientes aspectos: a) El formateo, restauración y respaldo de la información debe solicitarse a través de la herramienta de mesa de ayuda y previamente autorizado por el Jefe oficina asesora de planeación y tecnologías de la información o el Supervisor contractual o coordinador del grupo de tecnología; b) El grupo de soporte de los centros CREA, es el encargado de realizar los Backup de información en los computadores institucionales, con periodicidad semanal, a través del software de automatización de backup incremental a una unidad de almacenamiento centralizado asignada por el Ingeniero Networking y debe ser coordinado con el oficial de seguridad de la información y el ingeniero Networking; c) De no estar habilitado el software se requiere que el backup se realice de forma manual en cada uno de los equipos institucionales de las carpetas de sesión de usuario: Mis Documentos, Escritorio y Descargas; d) Se debe programar con una periodicidad trimestral una prueba de restauración coordinada con el Ingeniero de Seguridad de la Información y el Ingeniero de conectividad y documentarse por medio de un caso en la herramienta de mesa de ayuda.

10. Para respaldos de la información de las bases de datos se deben tener en cuenta los siguientes aspectos: a) Las bases de datos que hacen parte integral del sistema de información serán respaldadas diariamente de forma automática por medio de un script que se ejecuta en el servidor de bases de datos hacia un espacio de almacenamiento asignado por el Ingeniero de conectividad y monitoreado por el Ingeniero Administrador de Bases de Datos; b) El respaldo de la información se realizará diariamente de forma incremental y de forma completa, teniendo en cuenta el tiempo definido para ello; c) Se debe realizar trimestralmente pruebas de restauración por parte del ingeniero Administrador de bases de datos para garantizar la seguridad de la información y se documentará en el sistema de seguimiento a requerimientos tecnológicos. d) La persona encargada como Ingeniero administrador de Bases de datos es responsable de la generación de backup de todas las bases de datos, de los sistemas de información incluyendo DB.

11. Se realizará monitoreo de los registros de logs y eventos de los sistemas de almacenamiento para los respaldos de información, y en caso de encontrar alguna alarma o error del sistema de backups, se debe hacer seguimiento para corregir las fallas detectadas con acciones de mejora continua, así mismo, las cintas de respaldo serán identificadas conforme lo permite la librería de backup y en otros mecanismos de respaldo se deberán identificar con el contenido y fecha de realización, al igual con el número de veces que ha sido usado el mecanismo.

12. Se realizará semestralmente ejercicios o pruebas de restauración de la información programados con el fin de realizar el seguimiento y control de las actividades de respaldo y verificando su correcta restauración para establecer acciones de mejora y contribuir a generar actividades de recuperación en caso de un siniestro o daño a la infraestructura tecnológica del Idartes; el oficial de seguridad de la información coordinará con el profesional del grupo tecnológico y el ingeniero de conectividad ejercicios de prueba para la restauración de la información; se realizará una selección aleatoria de un grupo de información a restaurar para validar la integridad, disponibilidad y accesibilidad de la información y los tiempos de ejecución de las actividades planteadas; se ejecutará una restauración de la información sobre una ubicación temporal, y se comprobará la restauración de la información, se documentará la actividad y se eliminará posteriormente; en la documentación de la prueba se Almacenará el log de la herramienta de generación de copias con el resultado de la operación de restauración en el registro de operaciones de comprobación de respaldo periódicas de la Entidad

13. Para realizar el control de los respaldo y restauraciones se usará el formato o documento denominado "matriz de control y seguimiento de copias y respaldos" para el seguimiento, donde el personal de soporte responsable de realizar un respaldo de información, debe realizar la actualización del documento "matriz de control y seguimiento de copias y respaldos" conforme a las actividades realizadas de copias y restauraciones de la información; el documento contendrá la siguiente información: a) Fecha en que se realiza el backup; b) Información referente a propietario de la información; c) Nivel de backup; d) Grado de Backup; e) Frecuencia; f) Tiempo de retención; g) tamaño del contenido h) Responsable que realiza el backup; i) Ubicación del backup

7. POSIBLES PRODUCTOS O SERVICIOS NO CONFORME:

Actividad	Producto y/o Servicio	Criterio de Aceptación	Corrección	Registro
4. Realiza backup de la información: Realiza la copia de la información Selecciona el espacio asignado de acuerdo con lo establecido en la política de operación 13, el personal de soporte que tiene el Tiket asignado genera la copia de respaldo de la información y documenta en la matriz de control la información de al copia realizada	Copia de seguridad de la información	La copia de respaldo de la información cumple con la política de operación 9	Repetir la copia de respaldo conforme a los parámetros establecidos en la política de operación 9	Matriz de control de copias y respaldos

8. DOCUMENTOS ASOCIADOS:

Los documentos asociados del presente procedimiento se pueden acceder a través del mapa de procesos

9. NORMATIVA ASOCIADA:

RESOLUCIÓN 305 de 2008 “Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre”

ACUERDO 57 DE 2002 “Por el cual se dictan disposiciones Generales para la implementación del Sistema Distrital de Información SDI, se organiza la Comisión Distrital de Sistemas”

DECRETO 3816 de 2003 “Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública”

DIRECTIVA 5 de 2005 “Políticas Generales y directrices que orienten el desarrollo tecnológico”

DECRETO 619 de 2007 “Por el cual se establece la Estrategia de Gobierno Electrónico en el Distrito”

Ley 1273 de 2009 Congreso de la República Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado ""de la protección de la información y de los datos""· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

Decreto 235 de 2010 Ministerio del Interior y Justicia Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

Conpes 3701 de 2011 Conpes Lineamientos de política para la Ciberseguridad y Ciberdefensa

Ley 1581 de 2012 Congreso de la República Por el cual se dictan disposiciones generales para la protección de datos personales

Decreto 2364 de 2012 Ministerio del Interior y Justicia Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones

Decreto 19 de 2012 Presidencia de Colombia Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública"

Resolución 396 de 2012 Idartes Por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - IDARTES.

Decreto 596 de 2013 Alcaldía Mayor de Bogotá Por el cual se dictan medidas para la aplicación del Teletrabajo en organismos y entidades del Distrito Capital

Ley 1712 de 2014 Congreso de la República Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones

Resolución 383 de 2014 Idartes Por la cual se modifica la Resolución No 396 de 2012, "por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - IDARTES"

Conpes 3854 de 2016 Conpes Política Nacional de Seguridad Digital. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo

RESOLUCIÓN 3436 DE 2017: Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015.

RESOLUCIÓN 4 DE 2017: Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas – CDS Por la cual se modifica la Resolución 305 de 2008 de la CDS

DECRETO 728 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de las zonas de acceso público a internet inalámbrico

DECRETO 1413 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales

RESOLUCIÓN 2710 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por la cual se establecen lineamientos para la adopción del protocolo IPv6

DECRETO 728 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo deGobierno

CIRCULAR 30 DE 2017: Alta Consejería de Tics. Implementación CSIRT de Gobierno

CIRCULAR 36 DE 2017: Alta Consejería de Tics. Lineamientos de avance del modelo de seguridad y privacidad de la información

RESOLUCIÓN 3436 DE 2018: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015.

DECRETO 612 DE 2018: Departamento Administrativo de la Función Pública. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

DECRETO 1008 DE 2018: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

CIRCULAR 2 DE 2018: Ministerio de Tecnologías de la Información y las Comunicaciones. Cumplimiento legal y normativo respecto a seguridad de la información.

CONPES 3920 DE 2018: Conpes Big Data, la política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.

LEY 1955 DEL 2019: Presidencia de Colombia. Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

DECRETO 2106 DE 2019: Departamento Administrativo De La Función Pública. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Pública Efectiva

CONPES 3975 DE 2019: Conpes - Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.

DECRETO 620 DE 2020: Departamento Administrativo De La Función Pública. Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales

RESOLUCIÓN 0500 DE 2021. Ministerio De Tecnologías De La Información y las Comunicaciones. 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

10. RECURSOS:

1. Equipos de computo.

2. Servidores NAS/SAN/Cloud de almacenamiento.

3. Software para copiar y almacenar información.

4. Recurso humano para soporte y administración de almacenamiento

ANDRES ORLANDO BRICEÑO DIAZ 2021-06-29 08:05:45	CARLOS ALFONSO GAITAN SANCHEZ 2021-07-22 11:54:00	AURORA CAMILA CRESPO MURILLO 2021-06-29 08:19:20	CARLOS ALFONSO GAITAN SANCHEZ 2021-07-22 11:58:37	