PROPÓSITO
El propósito de este documento es orientar a los servidores públicos y/o contratistas de la UNP con respecto a la definición de reglas para el uso y manejo de los medios removibles que contengan información institucional y brindar lineamientos para la protección de datos, prevención de riesgos de pérdida de información, evitando la generación de incidentes de seguridad afectando así suconfidencialidad, disponibilidad e integridad que se encuentren almacenadas en estos medios.
ALCANCE
Este documento inicia desde la solicitud de habilitación de uso de medios removibles por las áreas de la entidad que así lo requieran el cual presta mesa de servicios a través de sus canales de comunicación y solicitud y termina con la entrega de servicio en las condiciones establecidas en el presente documento. Este documento aplica para todos los procesos de la entidad.

RESPONSABILIDADES

RESPONSABLES	**RESPONSABILIDADES**
Coordinador GTE	- Realizar la aprobación de solicitud por parte de los servidores públicos y/o contratistas para el uso de medios removibles - Velar por el cumplimiento de los lineamientos y políticas definidas para el uso de medios removibles
Líder del sistema de MSPI	- Es el responsable del análisis de la justificación del acceso del medio removible tal como se deja en la descripción de las actividades
Líder de mesa de servicios / Equipo asignado	- Es el responsable en realizar la actividad de solicitud del servicio de resguardar información en algún medio removible - Aplicar las medidas de protección de la información - Es el responsable del análisis de la solicitud remitida al área para aprobación
Asesores, Sub directores, Servidor Público y/o Contratista	- Responsable de solicitar el servicio para fines de respuesta a diferentes entidades externas y dar cumplimiento a requisitos o el desarrollo normal de las funciones de la UNP. - Velar por el cumplimiento de los lineamientos y políticas definidas para la aplicación de este procedimiento de solicitud de servicio de los medios removibles.

DEFINICIONES	
TÉRMINO	**DEFINICIÓN**
Medio de almacenamiento removible	Todo dispositivo con capacidad de almacenar información, que puede encontrarse endisquetes, discos de videos digital (DVD) y compactos (CD), cintas, memorias USB, discos duros externos, unidades de almacenamiento removibles, entre otros. (Elaboración propia).
Información	Conjunto organizado de datos contenido en cualquier documento que los sujetos obligadosgeneren, obtengan, adquieran, transformen o controlen. (Ley 1712 de 2014)
Activo De información	Los activos de información son datos o información propietaria en medios electrónicos, impresos u otros medios, entre los cuales se encuentran los públicos, y los considerados sensitivos o críticos para los objetivos de la Entidad. (Norma ISO 27000)
Amenaza	Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, lasamenazas pueden materializarse dando lugar a un ataque en el equipo. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)
Backup	Se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos. (Elaboración propia).
Ciberseguridad	Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (Norma ISO 27000).
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidaspara mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. Enuna definición más simple, es una medida que modifica el riesgo. (Norma ISO 27000).

DEFINICIONES	
TÉRMINO	**DEFINICIÓN**
Custodio del activo de información:	es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de informaciónconfiados. (Elaboración propia).
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (Norma ISO 27000)
Incidente de seguridad de la información	Un incidente de seguridad de la Información está indicado por un único evento o una seriede eventos de Seguridad de la Información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la entidad y de amenazar laseguridad de la información". (Norma ISO 27000)
Información Pública Clasificada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
Información Pública Reservada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
Integridad	Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.(Norma ISO 27000)
Medio de almacenamiento físico	Es todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidadde ningún aparato que procese su contenido para examinar, modificar o almacenar datos. Por ejemplo: Archivadores, gavetas, carpetas, etc. (Elaboración propia).
Propietario de la información	es la unidad organizacional o proceso donde se crean los activos de información. (Elaboración propia).

DEFINICIONES	
TÉRMINO	**DEFINICIÓN**
Responsable por el activo de información	es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidirla forma de usar, identificar, clasificar y proteger dichos activos a su cargo. (Elaboración propia).
Riesgo de seguridad de la información	posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad paracausar una pérdida o daño en un activo de información. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)
Sistema de Gestión de Seguridad de la InformaciónSGSI	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque degestión y de mejora continua. (Norma ISO 27000).

MARCO LEGAL
Ley 1712 de 2014: Conocida como la Ley de Transparencia y del Derecho de Acceso a la Información Pública, es regular el derechode acceso a la información pública que tienen todas las personas, los procedimientos para el ejercicio y la garantía del derecho fundamental, así como las excepciones a la publicidad de la información pública. y su normatividad reglamentaria Ley estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. y su normatividad reglamentaria ISO/IEC 27001:2022: Sistemas de Gestión de la Seguridad de la Información Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL hoy Gobierno Digital. Resolución 1519 de 2020 de Min Tic “Reglamentación de aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública” Norma Técnica Colombiana NTC-ISO/IEC 27002 Tecnología de la Información. Técnica de Seguridad. Código de Práctica para Controlesde Seguridad de la Información. Norma Técnica Colombiana ISO/IEC 27001:2022
DOCUMENTOS RELACIONADOS
✓ GTE-MA-02 Manual de Políticas Específicas de seguridad y privacidad de la información. ✓ GTE-FT-40 Formato Solicitud de Servicios medios removibles ✓ GTE-FT-34 Formato acuerdo de confidencialidad para Servidores públicos, contratistas y/o terceros ✓ ABC - "Ley de Transparencia y del Derecho de acceso a la información pública"

CONSIDERACIONES GENERALES

La seguridad de la información permite asegurar la confidencialidad, integridad y disponibilidad de la información. Los medios removiblespermiten transportar datos, esto expone a la misma a riesgo de pérdida o alteración, incluso, divulgación no autorizada además de que se expone la red a amenazas de virus y accesos no autorizados.

El manejo de la información institucional en Medios Removibles está expuesta a riesgos, como pérdida, fuga o modificación, que compromete no solamente la información sino también la infraestructura tecnológica de la Entidad, por lo tanto, el Servidor público y/o contratista que los use será quien asuma las sanciones de ley aplicables en esta materia, siendo responsable de la seguridad.

La norma ISO/IEC 27001:2022 entrega una serie de lineamientos 5.1 La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos, 5.37 Procedimientos operativos documentados Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite..para tener en cuenta a la hora de establecer una Política sobre el usode medios Removibles en el Control 8.3 restricción de acceso a la información ", en sus ítems A.7.7 escritorio y pantallas limpias (aquí se debe tener un lineamiento en esta política y tener en cuenta el siguiente lineamiento: Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todas las partes interesadas deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: Documentos impresos, CDs, dispositivos de almacenamiento y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida de manera inmediata. control A.7.8, este control indica que se debe proteger los equipos que procesan información confidencial para minimizar el riesgo de fuga de información debido a la emanación electromagnética. a.7.10 Medios de almacenamiento 8.3.1 "Gestión de Medios removibles", 8.3.2 Disposición de los medios, 8.3.3. "Transferencia de medios físicos", y

Este documento describe el procedimiento de seguridad de la información definido para la puesta en marcha de un procedimiento que permita gestionar de manera efectiva el uso de los medios removibl.es. Es importante tener en cuenta lo siguiente:

Gestión de medios removibles:

- Los medios removibles no pueden ser empleados para la extracción de copias de respaldo y/o seguridad con miras a recuperaciónante desastres, solo pueden ser utilizados como herramientas de apoyo frente al transporte de los datos e información requeridapara el desarrollo normal de las funciones de la UNP.
  Será responsabilidad de cada uno de los servidores públicos y/o contratistas de la UNP, generar las medidas pertinentes, proporcionales y adecuadas para proteger la información transportada y almacenada en medios de almacenamiento removible, evitando accesos no autorizados, daños, pérdida o extravío del contenido, y en caso de surgir algún incidente frente a la seguridad de la información deberá informarse de manera inmediata por los medios que sean dispuestos a la mesa de servicio para ejecutarlas actividades que haya lugar para la atención de dicho incidente.

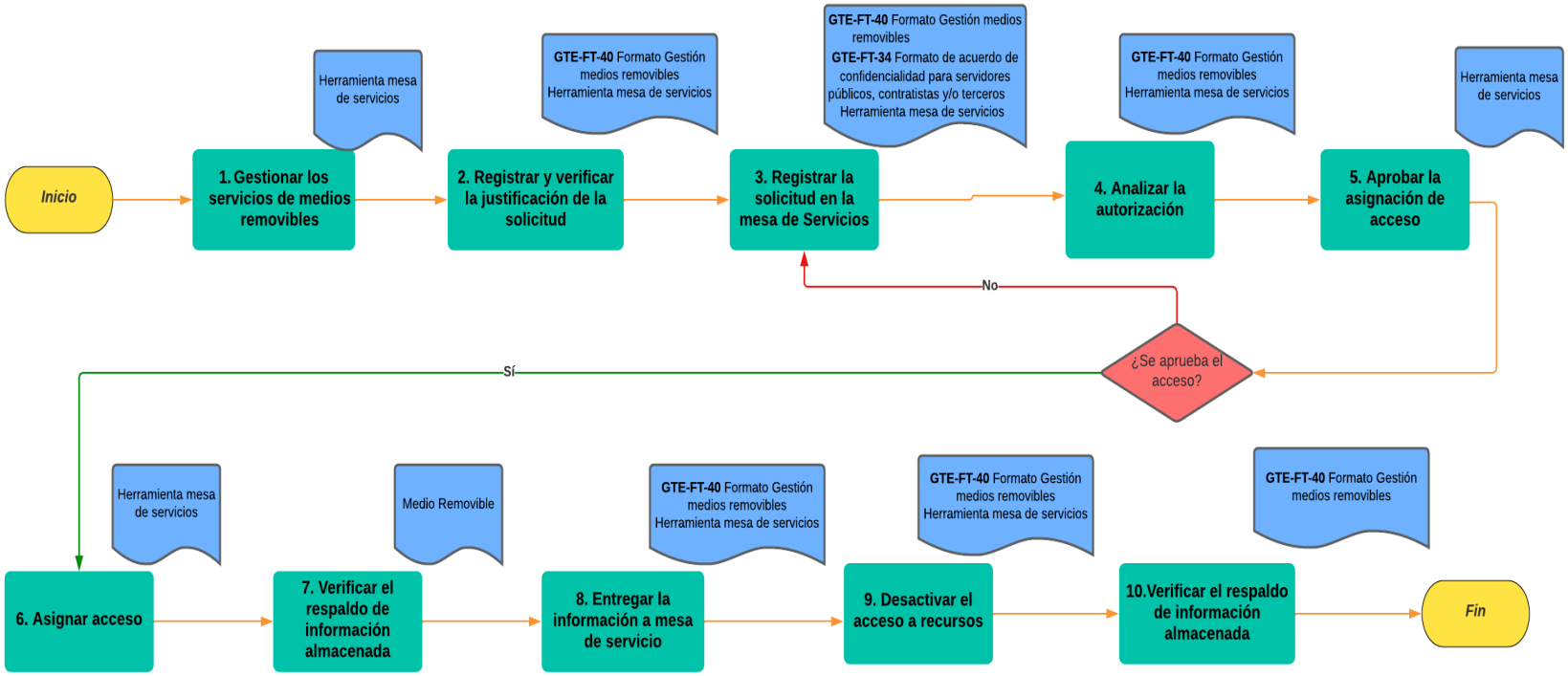
DESCRIPCIÓN DEL PROCEDIMIENTO				
N° ACTIVIDAD	**RESPONSABLE**	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**REGISTRO**
1	**Mesa de servicios**	**Gestionar los servicios de medios removibles**	La administración y/o Servicio de medios de dispositivos removibles estará a cargo de la mesa de servicio quien apoyará la gestión.	Herramienta mesa de servicios
2	**Jefes responsables de los procesos**	**Registrar y verificar la justificación de la solicitud**	El jefe de la oficina solicitante debe dejar muy claro y justificado porque solicita tener una información en dispositivos removibles ya que son los responsables de la información en los medios removibles en todo momento y lugar. Y adjuntar la solicitud de información la cual genera el servicio. El servidor público y/o contratista es responsable de la información en los medios removibles en todo momento y lugar.	**GTE-FT-40** Formato solicitud de servicios medios removibles Herramienta mesa de servicios
3	**Servidor público y/o contratista**	**Registrar la solicitud en la mesa de Servicios**	El servidor público y/o contratista realizará la solicitud a través de la herramienta mesa de servicio donde se le asignaráun ticket para su gestión y aprobación. Adjuntar **GTE-FT-40** Formato Solicitud de Servicios medios removibles **Nota:** El formato debe estar completamente diligenciado en todos sus campos y {firmado por los jefes responsables del proceso	Herramienta mesa de servicios **GTE-FT-34** Formato de acuerdo de confidencialidad para servidores públicos, contratistas y/o terceros **GTE-FT-40** Formato solicitud de servicios medios removibles

DESCRIPCIÓN DEL PROCEDIMIENTO				
N° ACTIVIDAD	**RESPONSABLE**	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**REGISTRO**
4	**Coordinador de GGT**	**Analizar la autorización**	Es responsabilidad el coordinador de GGT analizará, evalúa y autorizará la solicitud y comunicará a mesa de servicios definiendo los medios removibles	**GTE-FT-40** Formato solicitud de servicios medios removibles Herramienta mesa de servicios
5	**Coordinador Grupo de Tecnología / Líder de Mesade servicio,**	**Aprobar la asignación de acceso**	En caso de que la solicitud sea autorizada por el coordinador del Grupo de tecnología con apoyo con el líder de la mesa de servicio comunica al personal asignado del equipo coordinara el día y la hora cuando se prestara el servicio para que proceda a realizar la actividad. En caso de que No sea autorizada la solicitud se procederá a informar al área correspondiente las razones de la negación**.**	Herramienta mesa de servicios
6	**Coordinador Grupo de Tecnología / Líder de Mesade servicio**	**Asignar acceso**	El agente de la mesa de servicio encargado de la solicitud de los permisos informara a través de la herramienta de mesa de servicios mediante el ticket generado que el acceso ha sido asignado y el tiempo que está disponible el recurso y cerrar la solicitud en la herramienta.	**Herramienta mesa de servicios**
7	**Servidor público y/ocontratista**	**Verificar el respaldo de información almacenada**	El Servidor público y/o contratista deben revisar los medios removibles que le fueron entregados y comprobar que la información solicitada se encuentra completa.	**Medios removibles**

DESCRIPCIÓN DEL PROCEDIMIENTO				
N° ACTIVIDAD	**RESPONSABLE**	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**REGISTRO**
8	**Servidor público y/ocontratista**	**Entregar la información a mesa de servicio**	Cuando el Servidor público y/o contratista considere que ya no es requerida la información institucional guardada en el medio removible, o en caso de que su vinculación laboral o contractual haya finalizado, se debe generar el caso a mesa de servicio notificándole que puede proceder al transferir la información institucional a los medios que la Entidad ha establecido para este propósito (Pandora (SharePoint) - OneDrive) o en el equipo asignado por inventario de la UNP. Mesa de servicio deberá realizar borrado de la información contenida en éste y dejar evidencia del proceso en conjunto con el Servidor público y/o contratista quien solicito el servicio y deberá adjuntar las evidencias al ticket realizado. Se cerrará todo el caso en la Herramienta mesa de servicios. cuando se firme la última actividad en el formato **GTE-FT-40** Formato Solicitud de Servicios medios removibles	**GTE-FT-40** Formato solicitud de servicios medios removibles Herramienta mesa de servicios
9	**Líder de Mesa de servicio / Equipo designado**	**Desactivar el acceso a recursos**	Una vez, realizada la actividad por mesa de servicios y entregada los medios tecnológicos donde contiene la información solicitada. Se procede a cerrar el acceso y dejar los recursos con lo previamente asignado	**GTE-FT-40** Formato solicitud de servicios medios removibles Herramienta mesa de servicios

DESCRIPCIÓN DEL PROCEDIMIENTO				
N° ACTIVIDAD	**RESPONSABLE**	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**REGISTRO**
10	**Coordinador Grupo de Tecnología / Líder de Mesade servicio / Equipo designado**	**Verificar el respaldo de información almacenada**	El grupo de tecnología asignado por su coordinador deberá asegurar y preservar la información almacenada y manejada del solicitante, esta información deberá permanecer en custodia por la institución y conservar la integridad de esta. Una vez se haya finalizado el acceso de los recursos asignados, se deberá firmar la paz y salvo del solicitante y verificar el estado físico de los medios removibles de la entidad. **Nota:** Los medios de almacenamiento removibles como discos duros, y dispositivos USB, deben ser controlados por la persona a la cual se asigne el permiso (utilizar extracción segura, no forzar los conectores, escaneo con antivirus y desconectar el dispositivo cuando no se use).	**GTE-FT-40** Formato solicitud de servicios medios removibles

FLUJOGRAMA


Inicio
1. Gestionar los servicios de medios removibles
Herramienta mesa de servicios
2. Registrar y verificar la justificación de la solicitud
GTE-FT-40 Formato Gestión medios removibles
Herramienta mesa de servicios
3. Registrar la solicitud en la mesa de Servicios
GTE-FT-40 Formato Gestión medios removibles
GTE-FT-34 Formato de acuerdo de confidencialidad para servidores públicos, contratistas y/o terceros
Herramienta mesa de servicios
4. Analizar la autorización
GTE-FT-40 Formato Gestión medios removibles
Herramienta mesa de servicios
5. Aprobar la asignación de acceso
Herramienta mesa de servicios
¿Se aprueba el acceso?
No
Sí
6. Asignar acceso
Herramienta mesa de servicios
7. Verificar el respaldo de información almacenada
Medio Removible
8. Entregar la información a mesa de servicio
GTE-FT-40 Formato Gestión medios removibles
Herramienta mesa de servicios
9. Desactivar el acceso a recursos
GTE-FT-40 Formato Gestión medios removibles
Herramienta mesa de servicios
10.Verificar el respaldo de información almacenada
GTE-FT-40 Formato Gestión medios removibles
Fin

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Se crea procedimiento, con el fin de dar cumplimiento al requerimiento establecido en la ISO/IEC 27001:2013 en el Anexo A. a la hora de establecer una Política sobre el uso de medios Removiblesen el Control 8.3 “Manejo de Medios”, en sus ítems 8.3.1 “Gestión de Medios removibles”, 8.3.2 Disposición de los medios, 8.3.3. “Transferencia de medios físicos”, y 11.2.7 Disposición segura.	24/10/2023	**01**
01	Se fortalece el procedimiento para administrar mejor los dispositivos removibles con responsabilidades más fijas y actividades definidas por medio de mesa de servicios.	21/05/2024	**02**