
	PROCEDIMIENTO DE GESTIÓN DE MEDIOS REMOVIBLES	Código:
		Versión:
Proceso asociado	<NOMBRE DEL PROCESO ASOCIADO>	

Objetivo	Brindar los lineamientos para la adecuada gestión de los medios removibles en la <NOMBRE DE LA ENTIDAD>, a fin de propender por la disponibilidad, integridad y confidencialidad de la información que maneja la Entidad.
Responsable del documento	<NOMBRE DEL LÍDER DEL PROCESO ASOCIADO>

Definiciones

1. **Activo de información:** Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Entidad y, en consecuencia, debe ser protegido.
2. **Autenticación:** es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
3. **Centros de cableado:** son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.
4. **Centro de cómputo:** es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.
5. **Cifrado:** es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.
6. **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
7. **Control:** es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
8. **Criptografía:** es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
9. **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 información confiados.
10. **Disco duro removible:** es aquel disco duro de almacenamiento de información el cual se conecta al equipo de cómputo por medio de alguna interfaz de conexión externa.
11. **Disponibilidad:** es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

	PROCEDIMIENTO DE GESTIÓN DE MEDIOS REMOVIBLES	Código:
		Versión:
Proceso asociado	<NOMBRE DEL PROCESO ASOCIADO>	

12. **Equipo de cómputo:** dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
13. **Integridad:** es la protección de la exactitud y estado completo de los activos.
14. **Interfaz:** Es aquel componente físico o lógico por medio del cual pueden interactuar dos sistemas o elementos independientes.
15. **Medio removible:** es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
16. **Propietario de la información:** es la unidad organizacional o proceso donde se crean los activos de información.
17. **Puerto USB:** Es la interfaz de comunicación por medio del bus universal en serie. es un bus de comunicaciones que sigue un estándar que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre computadoras, periféricos y dispositivos electrónico.
18. **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 decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
19. **SSI:** Subsistema de Seguridad de la Información.
20. **Sistema de información:** es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Superintendencia Nacional de Salud o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.
21. **Unidad de CD/DVD Rom:** es un disco compacto con el que utilizan rayos láser para leer información en formato digital. El CD-ROM estándar fue establecido en 1985 por Sony y Philips.² Pertenece a un conjunto de libros de colores conocido como Rainbow Books, que contiene las especificaciones técnicas para todos los formatos de discos compactos.
22. **Puerto:** Es una noción con varios usos. En la informática, el término se emplea para nombrar a una clase de conexión que posibilita el envío y la recepción de información.



**BOGOTÁ
MEJOR
PARA TODOS**

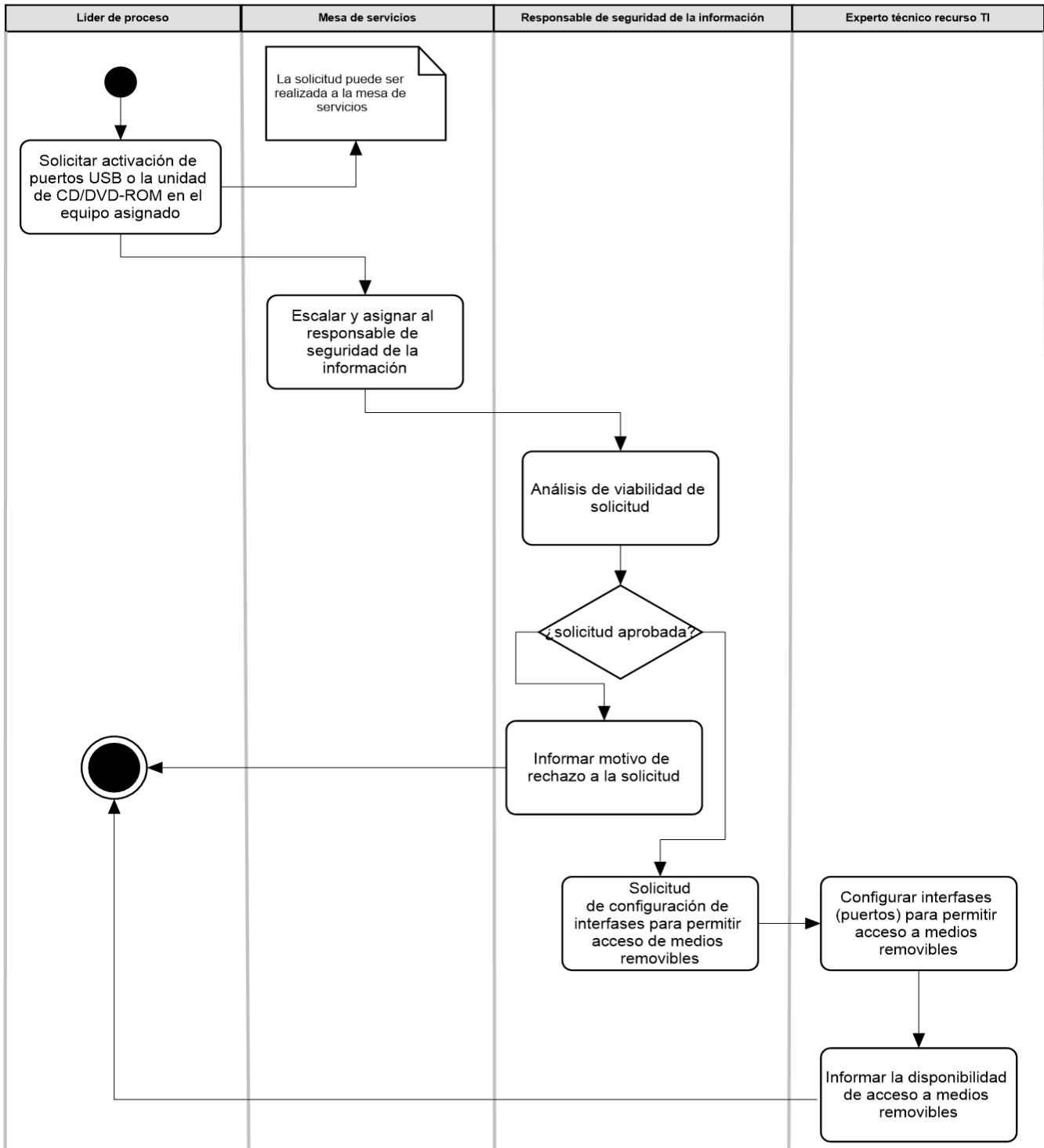
PROCEDIMIENTO DE GESTIÓN DE MEDIOS REMOVIBLES


Código:

Versión:

Proceso asociado

<NOMBRE DEL PROCESO ASOCIADO>



	PROCEDIMIENTO DE GESTIÓN DE MEDIOS REMOVIBLES	Código:
		Versión:
Proceso asociado	<NOMBRE DEL PROCESO ASOCIADO>	

Marco normativo

Modelo de seguridad y privacidad de la información – Ministerio de las TIC

ISO/IEC 27001:2013

Políticas

[Los siguientes aspectos se puede adoptar como lineamientos y políticas de operación, y es a potestad de la entidad decidir cuáles adoptar.]

- a. Solo pueden ser conectados a los equipos de cómputo, medios de almacenamiento externo autorizados por la <Oficina de TI o quien haga sus veces>.
- b. Los medios de almacenamiento removibles como cintas, discos duros removibles, y dispositivos USB que contengan información institucional, deben ser controlados y físicamente protegidos por el funcionario responsable de la información.
- c. La información que es almacenada en medios removibles y que debe estar disponible por largo tiempo, debe ser protegida y controlada adecuadamente para sus disponibilidad y adecuada salvaguarda.
- d. A todo medio removible devuelto se le debe practicar el debido proceso de borrado seguro de la información contenida.
- e. La responsabilidad de la información contenida en los medios removibles es del funcionario que está a cargo de este y la gestión deberá hacerse de acuerdo con las directrices y políticas establecidas en la Entidad Distrital.