



**MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS
COMUNICACIONES**

RESOLUCIÓN NÚMERO 002256 DE 06 DE NOVIEMBRE DE 2020

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

LA MINISTRA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

En ejercicio de sus facultades legales, regulatorias y en especial de las que le confieren los artículos 4 de la Ley 87 de 1993, 61 de la Ley 489 de 1998, 2.2.2.2.1 del Decreto 1083 de 2015 y 5 del Decreto 1064 de 2020 y

CONSIDERANDO QUE:

La Constitución Política de Colombia en su artículo 15 consagra que todas las personas tienen derecho a su intimidad personal, familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

El artículo 17 de la Ley Estatutaria 1581 de 2012, "Régimen General de Protección de Datos Personales", y el artículo 2.2.2.25.3.1. del Decreto 1074 de 2015, "Decreto Único Reglamentario del Sector Comercio Industria y Turismo", consagraron la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental de Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho.

La Ley 1712 de 2014, sobre transparencia y derecho de acceso a la información pública nacional, adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; junto con lo dispuesto en el Libro 2. Parte VIII, Título IV "Gestión de la Información Clasificada y Reservada" del Decreto 1080 de 2015, "por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura", el cual establece las directrices para la calificación de información pública, en el mismo sentido, el Título V de la misma Parte y Libro, establecen los instrumentos de la gestión de información pública (1) Registro de Activos de Información; (2) Índice de Información Clasificada y Reservada; (3) Esquema de Publicación de Información; (4) Programa de Gestión Documental.

El artículo 2.2.9.1.1.3. del Decreto 1078 de 2015, subrogado por el artículo 1 del Decreto 1008 de 2018, determinó que uno de los principios de la Política de Gobierno Digital es el de Seguridad de la Información, a través de este se busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano

El artículo 2.2.22.2.1 del Decreto 1083 de 2015, establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

El Documento CONPES 3854 establece la *Política Nacional de Seguridad Digital en la República de Colombia*, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital y se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

El Documento CONPES 3995 formula la *Política Nacional de Confianza y Seguridad Digital en la República de Colombia*, estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, fortaleciendo las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; actualizando el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

A su vez, el parágrafo del artículo 16 del Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, mediante la Resolución 1905 de 2019, modificada por la Resolución 1590 de 2020, actualizó el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo Único de TIC, derogó las Resoluciones 911 de 2018 y dictó funciones en el marco de la política de Gobierno Digital y Seguridad Digital.

De otra parte, la Ley 527 de 1999 en artículo 2º literal c), define la firma digital "como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".

El artículo 1 del Decreto 2364 de 2012 por medio del cual se reglamenta el artículo 7º de la Ley 527 de 1999, define la firma electrónica como: métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

Ahora bien, en el marco de la Ley 1341 de 2009 y el Decreto 1414 de 2020, el Ministerio de Tecnologías de la Información y las Comunicaciones expidió la Resolución 1124 de 2020, a través de la cual actualizó la *Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios en el Ministerio/Fondo Único de TIC*.

En el año 2019 el Congreso de la República expidió la Ley 1978, "Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones". En particular, el artículo 21 de esa misma Ley

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

modificó el artículo 34 de la Ley 1341 de 2009, señalando, entre otros aspectos, que el Fondo de Tecnologías de la Información y las Comunicaciones, se denominaría en adelante Fondo Único de Tecnologías de la Información y las Comunicaciones

En desarrollo del artículo 14 de la Ley 1978 de 2019, el Gobierno nacional expidió los decretos 1064 y 1065 de 2020. Con el primero, modificó la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y derogó el Decreto 1414 de 2017. Con el segundo, modificó la planta de personal del MinTIC, incorporando y trasladando funciones al interior de su estructura, con la consecuente modificación de la nominación de algunos de los cargos del nivel ejecutivo.

Teniendo en cuenta los cambios normativos, es necesario actualizar la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios, así como definir los lineamientos frente al uso y manejo de la información, e incluir disposiciones sobre firma electrónica, para el Ministerio/Fondo Único de TIC.

El Comité del Modelo Integrado de Gestión-MIG, mediante acta de comité #43 de 2020 con cierre a la 1:10 p.m del viernes 16 de octubre del 2020, aprobó este acto administrativo con 10/10 votos a favor, ninguno en contra.

En mérito de lo expuesto,

RESUELVE:

CAPÍTULO I DISPOSICIONES GENERALES

ARTÍCULO 1. Objeto. La presente resolución tiene como objeto actualizar la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios en el Ministerio de Tecnologías de la Información y las Comunicaciones y del Fondo Único de TIC (en adelante Ministerio/Fondo Único de TIC), así como definir lineamientos frente al uso y manejo de la información.

ARTÍCULO 2. Ámbito de aplicación. La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios del Ministerio/Fondo Único de TIC, aplica a todos los niveles funcionales y organizacionales del Ministerio/Fondo Único de TIC, a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas y del sector de las Tecnologías de la Información y las Comunicaciones, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio de TIC compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a la entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación.

De igual manera, esta política aplica a toda la información creada, procesada o utilizada por el Ministerio/Fondo Único de TIC, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

ARTÍCULO 3. Política general de seguridad y privacidad de la información, seguridad digital y continuidad de la Operación de los Servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones. El Ministerio/Fondo Único de TIC, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios y regulatorios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo así por el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones - TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país.

ARTÍCULO 4. Objetivos. La Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del Ministerio/Fondo Único de TIC tendrá los siguientes objetivos:

1. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
2. Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información y de seguridad digital y continuidad de la operación de los servicios.
3. Mitigar el impacto de los incidentes de seguridad y privacidad de la información y de seguridad digital, de forma efectiva, eficaz y eficiente.
4. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información del Ministerio/Fondo Único de TIC.
5. Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información.
6. Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital.
7. Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.
8. Definir, operar y mantener el Plan de Continuidad de la Operación de los servicios del Ministerio/Fondo Único de TIC

CAPÍTULO II

POLÍTICAS ESPECÍFICAS DE MANEJO DE INFORMACIÓN

ARTÍCULO 5. Política de seguridad de los recursos humanos. la Subdirección para la Gestión del Talento Humano del Ministerio de Tecnologías de la Información y las Comunicaciones, debe desplegar esfuerzos para generar conciencia y apropiación en los servidores públicos de la entidad, sobre sus responsabilidades en el marco de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios en el Ministerio/Fondo Único de TIC, con el fin de reducir los riesgos, el mal uso de las instalaciones y recursos tecnológicos y así asegurar la confidencialidad, integridad y disponibilidad de la información.

PARÁGRAFO 1. Con el mismo fin, la Subdirección de Gestión Contractual incluirá en las minutas de los contratos y convenios, cualquiera que sea su naturaleza o modalidad, cláusulas y obligaciones frente

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

el cumplimiento de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios en el Ministerio/Fondo Único de TIC, las cuales deberán ser divulgadas a través de los supervisores de los contratos, a proveedores, a operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones, obligaciones y las del Ministerio de Tecnologías de la Información y las Comunicaciones, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

PARÁGRAFO 2. La Subdirección para la Gestión del Talento Humano deberán fomentar la participación de los servidores de la entidad en las convocatorias para el fortalecimiento de capacidades en Seguridad digital realizadas por el Gobierno Nacional u organismos internacionales.

ARTÍCULO 6. Política de Gestión de Activos. La Subdirección Administrativa del Ministerio de TIC, con el acompañamiento permanente de la Oficina de Tecnologías de la Información, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y buen uso de los activos de información, con el objetivo de garantizar su protección. Dichos lineamientos se impartirán teniendo en cuenta los siguiente literales, que serán consolidados y publicados en el macroproceso de apoyo "Gestión Documental" por la Subdirección Administrativa.

- a. **Inventario de Activos:** Los activos del Ministerio de Tecnologías de la Información y las Comunicaciones deben ser identificados, clasificados, valorados y controlados para garantizar su uso, protección y recuperación ante desastres. Por tal motivo, la Oficina de Tecnologías de la Información – TI, diseñará una metodología con los lineamientos necesarios para llevar el inventario de los activos de información, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la entidad defina.
- b. **Protección:** Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la información, así como de mantener y actualizar el inventario de activos de información relacionados con sus servicios (información física o digital, software, hardware y recurso humano), bajo los parámetros que establezca la Oficina de Tecnologías de la Información.
- c. **Archivos de Gestión:** La Subdirección Administrativa deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental y Tablas de Control de Acceso, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información física del Ministerio de Tecnologías de la Información y las Comunicaciones.
- d. **Clasificación de la Información:** La Subdirección Administrativa deberá establecer una metodología para la clasificación y rotulado de la información del Ministerio de Tecnologías de la Información y las Comunicaciones, en el marco de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014, reglamentada por el Título 1 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 y el Decreto 1080 de 2015 y demás normatividad que reglamente la clasificación de información de las entidades públicas del país. Así mismo, la Oficina de Tecnologías de la Información implementará una herramienta informática que permita rotular la información digital y la Subdirección Administrativa mecanismos para rotular la información física, de acuerdo con la metodología establecida.

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

e. Firma de documentos: Las firmas de documentos que produzca el Ministerio/Fondo Único de TIC será válida en cualquiera de los siguientes métodos, garantizando la confiabilidad, integridad, autenticidad y disponibilidad de la información de los documentos expedidos por los servidores públicos y contratistas en el marco de sus funciones y competencias:

- I. En físico con firma autógrafa mecánica.
- II. Con firma digital de persona natural asignadas por la Oficina de Tecnologías de la Información según lo dispuesto por la Ley 527 de 1999.
- III. Con firma electrónica, de acuerdo con lo dispuesto en el Decreto 2364 de 2012 y el Decreto 1287 de 2020, para lo cual la Oficina de Tecnologías de la Información deberá adquirir o implementar un aplicativo integrado con el sistema de gestión documental que contenga como mínimo lo siguiente:
 1. Control seguro de acceso y uso al aplicativo, sincronizado con el directorio activo, garantizando que solo personal vinculado pueda hacer uso del mecanismo de firma electrónica,
 2. Múltiples controles para la autenticación y firma del documento electrónico, garantizando que el firmante es quien dice ser,
 3. El sistema debe solicitar la firma digitalizada o escaneada y quedar estampada en el documento junto con el nombre completo, cargo, correo electrónico institucional del servidor o contratista que firma,
 4. Identificador único provisto por el sistema que permita la verificación de la veracidad del documento,
 5. Fecha de creación y finalización de la firma provisto por el servidor y sincronizado con la hora legal colombiana de acuerdo con lo establecido en el numeral 14 del artículo 6 del Decreto 4175 de 2011,
 6. Estado del trámite de firma,
 7. Firma digital de persona jurídica del Ministerio/Fondo Único del TIC según sea el caso,
 8. En ningún caso se debe utilizar firmas facsímil, salvo en aquellos que se autorice por Resolución expedida por la Ministra de TIC, indicando para que fin y por qué medios podrá ser utilizada.

ARTÍCULO 7. Política de Control de Acceso. Los propietarios de los activos de información, teniendo en cuenta el tipo de activo, deberán adoptar las medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías e infraestructura física (instalaciones y oficinas) establecidas, todo esto con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física de personal no autorizado y así propender por salvaguardar la integridad, disponibilidad y confidencialidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones.

ARTÍCULO 8. Política de Criptografía. La Oficina de Tecnologías de la Información dispondrá de herramientas que permitan el cifrado de la información clasificada y reservada para proteger su confidencialidad, integridad y disponibilidad. El cifrado de la información se realizará por solicitud de los usuarios o de manera general cuando así lo requiera el Ministerio de Tecnologías de la Información y las Comunicaciones.

ARTÍCULO 9. Política de Privacidad. El Ministerio/Fondo Único de TIC deberá disponer, a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, de los controles necesarios para la protección de la información de los servidores públicos, contratistas y partes interesadas

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

externas, en los términos de la Ley 1581 de 2012 y sus decretos reglamentarios, así como la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC.

PARÁGRAFO 1. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, deberá diseñar un formato de autorización y uso de datos personales, así como su tratamiento, en lo que respecta al uso de datos semiprivados, privados y sensibles; dicho formato debe ser claro y detallado en lo referente a la recolección de la información de los servidores públicos y contratistas del Ministerio/Fondo Único de TIC; así mismo, deberá ser firmado por todos los servidores públicos y contratistas como parte de sus obligaciones.

PARÁGRAFO 2. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, diseñarán y actualizará los formatos de autorización, por parte de los ciudadanos, de la captación y uso de imágenes, videos o cualquier medio audiovisual, de conformidad con lo dispuesto en las normas vigentes sobre protección de datos personales, en especial la Ley 1581 de 2012 y el Decreto 1074 de 2015, así como su autorización libre, expresa e inequívoca al Ministerio/Fondo Único de TIC o a quien este autorice o encargue, para el uso del recurso audiovisual en el marco del cumplimiento de su misión.

Los formatos deberán prever la opción en que el ciudadano sea menor de edad y se deberá establecer un procedimiento para el caso en que el ciudadano no autorice dicho tratamiento.

PARÁGRAFO 3. La toma de material audiovisual a los ciudadanos mayores o menores de edad sólo se podrá realizar por los servidores públicos o contratistas avalados por la Oficina Asesora de Prensa y en cumplimiento de las funciones de acompañamiento a programas propios del Ministerio de Tecnologías de la Información y las Comunicaciones o donde éste fuere invitado de manera oficial. Los datos que se recolecten solo podrán ser tratados para el cumplimiento de la finalidad para la cual se ha dispuesto el tratamiento.

ARTÍCULO 10. Política de Seguridad Física y del Entorno. El Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, debe adoptar medidas para la protección del perímetro de seguridad de sus instalaciones físicas para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones), con el fin de mitigar los riesgos, amenazas externas, ambientales y evitar afectación a la confidencialidad, integridad y disponibilidad de la información de la entidad.

PARÁGRAFO 1. La Subdirección Administrativa, en coordinación con el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, deberá garantizar la protección de los datos, semiprivados, privados y sensible recolectados de los servidores públicos, contratistas y visitantes, en lo que refiere el artículo 9 de la presente resolución y establecer mecanismos alternativos para quienes no autorizan el tratamiento de sus datos.

PARÁGRAFO 2. Todos los servidores públicos, contratistas y visitantes que se encuentren en las instalaciones físicas del Ministerio de Tecnologías de la Información y las Comunicaciones deben estar debidamente identificados, con un carné, documento o distintivo que acredite su tipo de vinculación, dichos elementos deben portarse en un lugar visible.

PARÁGRAFO 3. Los visitantes en las instalaciones del Ministerio de Tecnologías de la Información y

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

las Comunicaciones siempre deben permanecer acompañados por un colaborador de la entidad, ambos debidamente identificados.

PARÁGRAFO 4. El personal de empresas, cooperativas o entidades que desempeñe funciones de forma permanente en las instalaciones del Ministerio de Tecnologías de la Información y las Comunicaciones, deben estar identificados con carné y chalecos o distintivos de la empresa o entidad y portar el carné de la Administradora de Riesgos Laborales - ARL.

ARTÍCULO 11. Política de Seguridad de las Operaciones. La Oficina de Tecnologías de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación. Así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información e implantará un comité de control de cambios, para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de producción sean controlados y debidamente autorizados, así mismo implementará mecanismos para controlar la información en los ambientes de desarrollo y prueba. De igual manera, proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la entidad, al igual que desarrollará mecanismos de contingencias y recuperación ante desastres con el fin de propender por la disponibilidad de los servicios de TI en el marco de la operación del Ministerio de Tecnologías de la Información y las Comunicaciones.

La Oficina de Tecnologías de la Información deberá realizar y mantener copias de seguridad de la información de la entidad en medio digital y el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, velará que ésta sea reportada por el responsable de esta, con el objetivo de recuperarla en caso de cualquier tipo de falla. La Oficina de Tecnologías de la Información efectuará las copias respectivas, de acuerdo con el esquema definido previamente, en un procedimiento que enmarque la gestión de las copias de seguridad de la información digital, sistemas de información, bases de datos y demás recursos tecnológicos de la entidad.

Dicho procedimiento se hará bajo la dirección de la Oficina de Tecnologías de la Información, con el apoyo de los líderes de proceso y deberá estar alineado con la gestión documental de la entidad, con el fin de determinar la información a respaldar, la periodicidad, los tiempos de retención, recuperación, restauración y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información.

PARÁGRAFO. En el evento que alguna dependencia haga uso de una plataforma tecnológica fuera de las instalaciones físicas y en el marco de las funciones misionales u operacionales del Ministerio de Tecnologías de la Información y las Comunicaciones, deberá cumplir con lo establecido en la presente política y los lineamientos dispuestos por el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, para tal fin.

ARTÍCULO 12. Política de Seguridad de las Comunicaciones. La Oficina de Tecnologías de la Información establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios tecnológicos que dependen de ellas; así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información del Ministerio/Fondo Único de TIC.

La Oficina Asesora de Planeación y Estudios Sectoriales establecerá mecanismos estratégicos para que el intercambio de información con las partes interesadas internas o externas, se realice asegurando

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

su integridad. En el evento que los acuerdos de intercambio de información requieran del desarrollo de servicio web (*web service*) o de cualquier otro medio tecnológico, el intercambio deberá realizarse con los controles criptográficos definidos en el artículo 8° de esta Resolución y será coordinado por la Oficina de Tecnologías de la Información con los mecanismos establecidos para tal fin.

PARÁGRAFO. Como parte de sus términos y condiciones iniciales de trabajo, funciones u obligaciones, todos los servidores públicos o contratistas del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, sin importar su nivel jerárquico, firmarán un acuerdo o compromiso de confidencialidad y no divulgación, que será elaborado por la Subdirección para la Gestión del Talento Humano y la Subdirección de Gestión Contractual de este Ministerio con el apoyo del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, según el tipo de vinculación, en lo que respecta a la información de del Ministerio/Fondo Único de TIC. Dicho documento original será conservado y archivado en forma segura en la historia laboral de los servidores públicos y en la carpeta de los procesos contractuales para el caso de los contratistas.

En el caso de persona jurídica proveedora de servicios para el del Ministerio/Fondo Único de TIC, en la respectiva carpeta del contrato deberá reposar el acuerdo o compromiso de confidencialidad y no divulgación debidamente suscrito por el representante legal.

ARTÍCULO 13. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas. La Oficina de Tecnologías de la Información garantizará porque el desarrollo interno y externo de los sistemas de información, cumplan con los requerimientos de seguridad adecuados para la protección de la información del del Ministerio/Fondo Único de TIC, para lo cual establecerá una metodología que detalle los requerimientos de seguridad para el desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas de información.

En el marco del Plan Estratégico de Tecnologías de la Información (PETI), la Oficina de Tecnologías de la Información es la única dependencia de la entidad con la capacidad de adquirir, desarrollar e implementar soluciones tecnológicas para el Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, así como de avalar la adquisición y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros, conforme a los requerimientos de las dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en el Ministerio.

En consecuencia, cualquier software que opere en el Ministerio de Tecnologías de la Información y las Comunicaciones deberá contar con la autorización de la Oficina de Tecnologías de la Información y deberá reportarse y entregarse cumpliendo con los lineamientos técnicos y presupuestales de dicha oficina, con el fin de salvaguardar la información, brindar el soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente o siniestro.

PARÁGRAFO. En caso de que alguna dependencia adquiera, desarrolle o realice mantenimientos a sistemas de información dentro del desarrollo misional u operacional del Ministerio de Tecnologías de la Información y las Comunicaciones, deberá cumplir con lo establecido en la presente política y deberá solicitar acompañamiento de la Oficina de Tecnologías de la Información.

ARTÍCULO 14. Política de Seguridad para Relación con Proveedores. El Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Subdirección de Gestión Contractual, establecerá, en el manual de contratación, las disposiciones necesarias para asegurar que la información que se genere, custodie, procese, comparta, utilice, recolecte, intercambie o a la que se tenga acceso con ocasión del contrato, se utilice dentro del marco de la seguridad y privacidad de la

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

información por parte de los proveedores. En el mismo sentido y a través del seguimiento a la ejecución, se garantizará que los supervisores en conjunto con la Oficina Para la Gestión de ingresos del Fondo sean los responsables de aplicar las políticas y procedimientos de seguridad de la información durante la ejecución de los contratos, estos lineamientos deberán ser comunicados a los proveedores con el apoyo de la Oficina Asesora de Prensa.

PARÁGRAFO. Tratándose de relaciones contractuales del Ministerio/Fondo Único de TIC, estas disposiciones deberán ser incorporadas en los términos, minutas o acuerdos con los que se relacione estos, a efectos de garantizar su implementación.

ARTÍCULO 15. Política de Gestión de Incidentes de Seguridad de la Información. El Ministerio de Tecnologías de la Información y las Comunicaciones, a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, promoverá entre los servidores públicos y contratistas de la entidad, el reporte y seguimiento de incidentes relacionados con la seguridad de la información y sus medios. Así mismo, asignará responsables para el tratamiento de los mismos, quienes investigarán y solucionarán los incidentes reportados, de acuerdo a su sana crítica.

Solo el Ministro de Tecnologías de la Información y las Comunicaciones o su delegado están autorizados para reportar incidentes de seguridad ante las autoridades de defensa nacional, policía, fiscalía y de control; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía. La delegación de esta potestad se podrá ser formal, por medio de acto administrativo.

ARTÍCULO 16. Política de la Continuidad de la Operación de los Servicios. El Ministerio de Tecnologías de la Información y las Comunicaciones dispondrá los planes necesarios para la continuidad de la operación de los servicios, los cuales serán operados por los líderes de los procesos. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, la Oficina Asesora de Planeación y Estudios Sectoriales, la Subdirección Administrativa y la Oficina de Tecnologías de la Información liderarán conjuntamente la elaboración del Análisis de Impacto del Negocio (BIA) y del Plan de Continuidad de la Operación de los Servicios.

PARÁGRAFO: El Plan de Continuidad de los Servicios del Ministerio de Tecnologías de la Información y las Comunicaciones contendrá el Plan de Continuidad de Tecnologías y los Planes de Emergencia y Contingencia, así como cualquier estrategia orientada a la continuidad de la prestación del servicio del Ministerio.

ARTÍCULO 17. Política de Cumplimiento. El del Ministerio/Fondo Único de TIC, a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad y privacidad de la información, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional, para lo cual dispondrá una Matriz de Requisitos Legales para su control y seguimiento.

ARTÍCULO 18. Política de Seguridad de la Información en la gestión de proyectos. La Oficina de Planeación y Estudios Sectoriales deberá incluir los requerimientos y consideraciones en materia de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la metodología de gestión de proyectos de la entidad, garantizando que se implementen en las fases iniciales de los proyectos, en el mismo sentido, la Oficina de Control Interno deberá incluir dentro de su plan de auditorías la revisión de su cumplimiento e implementación.

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

PARÁGRAFO. La Subdirección de Gestión Contractual debe velar que en todos los estudios previos de los proyectos o contratos a celebrar el Ministerio/Fondo Único de TIC, se incluyan los requerimientos y consideraciones referentes a Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios que se están contratando.

ARTÍCULO 19. Política de Seguridad de la Sede Electrónica. La Oficina de Tecnologías de la Información será la encargada de administración y gestión de la sede electrónica del Ministerio/Fondo Único de TIC, en donde se deberán integrar todos los portales, sitios web, plataformas, ventanillas únicas, aplicaciones y soluciones existentes, para la operación de la sede electrónica se deberá definir e implementar, en concordancia con las dependencias responsables de trámites, procesos y procedimientos dirigidos a los ciudadanos, las medidas jurídicas, organizativas y técnicas que garanticen la calidad, seguridad, privacidad, disponibilidad, integridad, confidencialidad, accesibilidad, neutralidad e interoperabilidad de la información y de los servicios,

PARÁGRAFO 1. En la sede electrónica del Ministerio/Fondo Único de TIC, se deberán identificar fácilmente y de manera clara, los canales digitales oficiales de recepción de solicitudes, peticiones y de información, estos canales deben contar con los mecanismos de cifrado de información de que trata el artículo 8 de esta resolución.

PARÁGRAFO 2. El Ministerio de Tecnologías de la Información y las Comunicaciones a través del proceso de Gestión Documental, deberá disponer de un sistema de gestión documental electrónica y de archivo digital, asegurando la conformación de expedientes electrónicos con características de integridad, disponibilidad y autenticidad de la información.

PARÁGRAFO 3. La emisión, recepción y gestión de comunicaciones oficiales, a través de los diversos canales electrónicos, deberá asegurar un adecuado tratamiento archivístico, estar debidamente alineado con la gestión documental electrónica y de archivo digital e igualmente deberá contar con todas las consideraciones en materia seguridad, privacidad de la información, seguridad digital, continuidad de la operación de los servicios y demás lineamientos de los que trata esta resolución.

PARÁGRAFO 4. La Subdirección Administrativa, junto con el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, deberán establecer las estrategias que permitan el tratamiento adecuado de los documentos electrónicos y garantizar la confidencialidad, integridad, disponibilidad y acceso a largo plazo conforme a los principios y procesos archivísticos definidos por el Archivo General de la Nación en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones.

CAPÍTULO III

RESPONSABILIDADES DE LOS COLABORADORES FRENTE AL USO DE LOS SERVICIOS TECNOLÓGICOS

ARTÍCULO 20. Política de Seguridad Digital. Todos los colaboradores que hagan uso de los recursos tecnológicos del Ministerio de Tecnologías de la Información y las Comunicaciones tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y por ende, el cumplimiento de la misión institucional. Para ello, deben acatar las siguientes disposiciones:

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

- a. **Del uso del correo electrónico.** El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los servidores públicos y contratistas del Ministerio de Tecnologías de la Información y las Comunicaciones, cuyo uso se facilitará en los siguientes términos:
- i. El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la entidad es el asignado por la Oficina de Tecnologías de la Información, que cuenta con el dominio @mintic.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.
 - ii. El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la entidad.
 - iii. En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la ley lo permita.
 - iv. Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones), la cual establece la validez de los mensajes de datos.
 - v. La Oficina de Tecnologías de la Información implementará herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservada o clasificada, de conformidad con la Ley 1712 de 2014.
 - vi. Se prohíbe el envío de correos masivos (más de 30 destinatarios) internos o externos, con excepción de los enviados por los despachos del Ministro(a) de TIC, Viceministros (as), de la Secretaría General, Oficina Asesora de Prensa, Oficina Asesora de Planeación y Estudios Sectoriales, Dirección de Gobierno Digital, Grupo Interno de Trabajo de Gestión del Talento Humano o quien haga sus veces, así como de la Oficina de Tecnologías de la Información solamente en caso de ventana de mantenimientos de los servicios de TI. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.
 - vii. Todo mensaje de correo electrónico enviado por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante plataformas externas deberá hacerse con la cuenta de la entidad y utilizando el dominio @mintic.gov.co, con el fin de que no sean catalogados como spam o suplantación de correo.
 - viii. Para apoyar la gestión de correo electrónico de directivos, el titular debe solicitar a la mesa de servicios la delegación del buzón correspondiente, relacionando los colaboradores que podrán escribir o responder *en nombre del* titular, con el fin de mitigar la suplantación.
 - ix. Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios como incidente de seguridad según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento, lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, o explícitas referencias no relacionadas con la misión de la entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos). Está expresamente prohibido el envío y reenvío de mensajes en cadena.
 - x. La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la entidad.

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

- xi. Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral de las personas o instituciones.
- xii. Está expresamente prohibido distribuir información oficial de carácter clasificada o reservada del Ministerio de Tecnologías de la Información y las Comunicaciones a otras entidades o ciudadanos sin la debida autorización del despacho del Ministro(a) de TIC, de los Viceministros (as), de la Secretaria General, de la Oficina Asesora de Prensa, de la Oficina Asesora de Planeación y Estudios Sectoriales, previa revisión de la Oficina Asesora de Prensa en caso de comunicados y Oficina Asesora de Planeación y Estudios Sectoriales en caso de cifras oficiales.
- xiii. El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la ley.
- xiv. El correo electrónico institucional en sus mensajes debe contener una sentencia de confidencialidad, que será diseñada por la Oficina de Tecnologías de la Información con el apoyo de la Oficina Asesora de Prensa, dicha sentencia debe reflejarse en todos los buzones con dominio @mintic.gov.co.
- xv. Está expresamente prohibido distribuir, copiar o reenviar información del Ministerio de Tecnologías de la Información y las Comunicaciones a través de correos personales o sitios web diferentes a los autorizados en el marco de las funciones u obligaciones contractuales.
- xvi. Cuando un servidor público o contratista cesa en sus funciones o culmina la ejecución de contrato con el Ministerio de Tecnologías de la Información y las Comunicaciones, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa del Ministro(a) de TIC, Secretaria General, por orden judicial, por solicitud de la Oficina de Control Interno o del GIT de Control Disciplinario como parte de un proceso de investigación.

El Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Oficina de Tecnologías de la Información se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus servidores públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la entidad o de terceros operados en la misma, previa solicitud expresa del supervisor del contrato, jefe inmediato, Ministro, viceministros, Secretario General, Coordinador del GIT de Control Interno Disciplinario o del Subdirector para la Gestión del Talento Humano a la Oficina de Tecnologías de la Información. Para ello, al inicio de la relación laboral o contractual se deberá comunicar a los funcionarios y contratistas que el Ministerio de Tecnologías de la Información y las Comunicaciones realiza el referido monitoreo.

b. **Del uso de Internet:** La Oficina de Tecnologías de la Información, en conjunto con el Oficial de la Seguridad de la Información o quien haga sus veces, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía, funciones u obligaciones. Será responsabilidad de los funcionarios y contratistas las siguientes, entre otras:

- i. Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol o funciones que desempeña en el Ministerio de Tecnologías de la Información y las Comunicaciones y para las cuales esté formal y expresamente autorizado por su jefe o supervisor y solo se utilizará para fines laborales.

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

- ii. Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
- iii. Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la política de navegación del Ministerio de Tecnologías de la Información y las Comunicaciones.
- iv. Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
- v. Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.

El Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Oficina de Tecnologías de la Información se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la Entidad.

- c. **Del uso de los recursos tecnológicos:** Los recursos tecnológicos del Ministerio de Tecnologías de la Información y las Comunicaciones son herramientas de apoyo a las labores y responsabilidades de los servidores públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

- i. Los bienes de cómputo que provea la entidad se emplearán de manera exclusiva y bajo la completa responsabilidad del servidor público o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la Oficina de Tecnologías de la Información, salvo que medie solicitud formal de los Directores, Subdirectores, Jefes de Oficina o Coordinadores de Grupos, a través de la Mesa de Servicios.
- ii. Sólo está permitido el uso de software licenciado por la entidad y aquel que, sin requerir licencia, sea expresamente autorizado por la Oficina de Tecnologías de la Información.
- iii. En caso de que el servidor público o contratista deba hacer uso de equipos ajenos al Ministerio de Tecnologías de la Información y las Comunicaciones, éstos deberán cumplir con la legalidad del Software instalado, sistema operativo y antivirus licenciado, actualizado y solo podrá conectarse a la red del Ministerio de TIC una vez esté avalado por la Oficina de Tecnologías de la Información.
- iv. Los servidores públicos y contratistas deberán realizar y mantener las copias de seguridad de su información y entregarla a la entidad al finalizar la vinculación.
- v. Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional o que atenten contra los derechos de autor o propiedad intelectual de los mismos.
- vi. Los servidores públicos y contratistas deberán utilizar las herramientas tecnológicas que proporcione la Oficina de Tecnologías de la Información para gestionar la información digital del Ministerio de Tecnologías de la Información y las Comunicaciones.
- vii. No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y por ende, a la pérdida de la integridad de ésta.

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

- viii. No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos autorizados expresamente por la Subdirección Administrativa.
- ix. Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes, son las designadas para tal labor por la Oficina de Tecnologías de la Información.
- x. La Oficina de Tecnologías de la Información realizará control y monitoreo sobre los dispositivos de almacenamiento externos como USB, CD-ROM, DVD, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información clasificada y reservada.
- xi. La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Oficina de Tecnologías de la Información, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la Entidad.
- xii. La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato a la Oficina de Tecnologías de la Información por el servidor público o contratista a quien se le hubiere asignado; en caso de que el equipo de cómputo sea propiedad del Ministerio de Tecnologías de la Información y las Comunicaciones, deberá reportarse a la Subdirección Administrativa siguiendo los procedimientos establecidos para este tipo de siniestros, sin perjuicio de las acciones penales y disciplinarias que requiera adelantar según sea el caso.
- xiii. La pérdida de información deberá ser informada con detalle a la Oficina de Tecnologías de la Información, a través de la Mesa de Servicios, como incidente de seguridad.
- xiv. Todo incidente de seguridad que comprometa la confidencialidad, integridad o disponibilidad de la información física o digital deberá ser reportado a la mayor brevedad a la Oficina de Tecnologías de la Información, a través de la Mesa de Servicios, siguiendo el procedimiento establecido.
- xv. La Oficina de Tecnologías de la Información es la única dependencia autorizada para la administración del software del Ministerio de TIC, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.
- xvi. Todo acceso a la red de la entidad, mediante elementos o recursos tecnológicos no institucionales, deberá ser informado, autorizado y controlado por la Oficina de Tecnologías de la Información.
- xvii. La conexión a la red wifi institucional para servidores públicos y contratistas deberá ser administrada desde la Oficina de Tecnologías de la Información mediante un SSID (Service Set Identifier) único; la autenticación deberá ser con usuario y contraseña de directorio activo.
- xviii. La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas administradas por la Oficina de Tecnologías de la Información, las contraseñas deberán cambiar los lunes de cada semana.
- xix. La red wifi para servidores públicos y contratistas estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.
- xx. Los equipos deben quedar apagados cada vez que el servidor público o contratista no se encuentre en la oficina o durante la noche, esto, con el fin de proteger la seguridad y distribuir bien los recursos de la entidad, siempre y cuando no vaya a realizar actividades vía remota.
- xxi. Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la entidad debe acogerse a las políticas de "Trae tu propio dispositivo".
- xxii. Las herramientas corporativas instaladas en los dispositivos móviles personales serán gestionadas por la Oficina de TI con el fin de proteger la confidencialidad, integridad y

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

disponibilidad de la información de la entidad, garantizando el cumplimiento del artículo 9 de la presente resolución

- d. **Del uso de los sistemas o herramientas de información:** Todos los servidores públicos y contratistas del Ministerio de Tecnologías de la Información y las Comunicaciones son responsables de la protección de la información a la que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:
- i. Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los servidores públicos y contratistas no deben revelarlas a terceros, ni utilizar claves ajenas.
 - ii. Todo servidor público y contratista es responsable del cambio periódico de su clave de acceso a los sistemas de información o recursos informáticos.
 - iii. Todo servidor público y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.
 - iv. En ausencia del servidor público o contratista, el acceso a la estación de trabajo le será bloqueada con una solicitud a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. La Subdirección para la Gestión del Talento Humano debe reportar de inmediato, cualquier tipo de novedad de servidores públicos, a su vez los supervisores de contrato deben reportar oportunamente todas las novedades del contratista.
 - v. Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución del contrato con el Ministerio de Tecnologías de la Información y las Comunicaciones, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información que estos ostenten será almacenada en los repositorios de la entidad.
 - vi. Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución de contrato con el Ministerio de Tecnologías de la Información y las Comunicaciones, el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normativa vigente.
 - vii. Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución del contrato con el Ministerio de Tecnologías de la Información y las Comunicaciones deberá tramitar el paz y salvo, de acuerdo con el procedimiento establecido por la entidad.
 - viii. Todos los servidores públicos y contratistas de la entidad deben dar estricto cumplimiento a lo estipulado en la Ley 23 de 1982 "Sobre derechos de autor", la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

ARTÍCULO 21. Lineamientos de las Políticas de Seguridad de la Información. Todas las políticas identificadas en este documento se deberán desarrollar de manera detallada y clara en la Declaración de Aplicabilidad y en el Manual de Políticas de Seguridad de la Información.

CAPITULO IV REVISIÓN, VIGENCIA Y DEROGATORIA

ARTÍCULO 22. Revisión. La Política de Seguridad y Privacidad de la Información, Seguridad Digital y

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020"

Continuidad de los servicios del Ministerio/Fondo Único de las Tecnologías de la Información y las Comunicaciones, será revisada anualmente o antes, si existiesen modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y eficaz. Este proceso será liderado por el Oficial de Seguridad de la Información del Ministerio de TIC o quien haga sus veces y revisado y aprobado por el Comité del Modelo Integrado de Gestión o quien haga sus veces.

ARTÍCULO 23. Vigencia y Derogatoria. La presente resolución rige a partir de la fecha de su publicación y derogan las Resoluciones 2999 de 2008 y 1124 de 2020.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los 06 DE NOVIEMBRE DE 2020

Karen A

KAREN ABUDINEN ABUCHAIBE

Ministra de Tecnologías de la Información y las Comunicaciones

Proyectó: Andrés Díaz Molina – Asesor del Despacho de la Ministra – Oficial de Seguridad de la Información *ADP*
Revisó/Aprobó: Comité MIG – Acta sesión #43 de 2020
Iván Antonio Mantilla Gaviria – Viceministro de Conectividad *IVAN*
Germán Camilo Rueda – Viceministro de Transformación Digital *GERMAN*
Adriana Vanessa Meza Consuegra- Secretaria General *ADRIANA*
Diego Luis Ojeda León – Jefe Oficina de Planeación y Estudios Sectoriales *DL*
Arleth Patricia Saurith Contreras - Jefe de la Oficina de Tecnologías de la Información *ARLETH*
Manuel Domingo Abello Álvarez – Director Jurídico *MANUEL*
Luz Adriana Barbosa Bautista - Jefe Oficina para la Gestión de Ingresos del Fondo *LUZ*
Óscar Javier Cuenca Medina – Jefe Oficina Asesora de Prensa *OSCAR*
Yulid Andrea Ruiz Ossio – Asesora del Despacho de la Ministra *YULID*
Andrés Díaz Molina – Asesor del Despacho de la Ministra – Oficial de Seguridad de la Información *ADP*