RESOLUCION 512 DE 2019

(marzo 14)

<Fuente: Archivo interno entidad emisora>

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

<NOTA DE VIGENCIA: Resolución derogada por el artículo 23 de la Resolución 1124 de 2020>

Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información

Resumen de Notas de Vigencia

NOTAS DE VIGENCIA:

- Resolución derogada por el artículo 23 de la Resolución 1124 de 30 de junio 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 infomación y se deroga la Resolución 512 de 2019'.

LA MINISTRA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

En ejercicio de sus facultades legales y reglamentarias, en especial de las que le confieren las Leyes Nos. 87 de 1993 y 489 de 1998, los Decretos Nos. 1083 de 2015 y 1414 de 2017, y

CONSIDERANDO

Que la Constitución Política de Colombia, en su artículo 15, consagra que todas las personas tienen derecho a su intimidad personal y 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.

Que, en su artículo 209, la Constitución Política establece que la administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley; así mismo, en el artículo 269 Impone a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control Interno.

Que el Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3., incluye la seguridad de la Información entre los principios de la Política de Gobierno Digital; de igual manera, en el artículo 2.2.9.1.2.1. se establece que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales, y respecto de estos últimos indica que son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que el CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital en la República de Colombia.

Que el Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector de Función Pública), adoptó el Modelo Integrado de Planeación y Gestión - MIPG, definiéndolo en su artículo 2.2.22.3.2 como "... un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio".

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015, tal como fue sustituido por el Decreto 1499 de 2017, regula 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".

Que la Resolución 3021 de 2016 expedida por esta Entidad, actualizó el MIG de que trata la Resolución 1083 de 2013, articulando las disposiciones del Modelo de Responsabilidad Social Institucional, el Sistema de Gestión de Calidad, el Modelo Estándar de Control Interno, los lineamientos de Seguridad y Privacidad de la Información del Ministerio de TIC, y el Modelo Integrado de Planeación y Gestión del que habla el Decreto 2482 de 2012.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones, mediante la Resolución No. 911 de 2018, actualizó el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y derogó las Resoluciones 3174 de 2014, 3021 de 2016 y 453 de 2016.

Que, mediante acta 011 del 24 de febrero 2017, el comité MIG aprobó la política de seguridad en la Información.

Que según consta en acta del Comité del Modelo Integrado de Gestión - MIG # 29, convocado de manera extraordinario y en modalidad virtual del 25 al 27 de febrero de 2019, y teniendo en cuenta la mejora continua y lo estipulado en el Modelo de Seguridad y Privacidad de la Información - MSPI, aprobó la actualización y adopción de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios, ajustada a los cambios estipulados en la política de Gobierno Digital.

Que, dado lo anterior, se hace necesario adoptar mediante acto administrativo, la nueva Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios, así como definir los lineamientos frente al uso y manejo de la información.

En mérito de lo expuesto,

RESUELVE

CAPITULO I.

DISPOSICIONES GENERALES.

ARTÍCULO 1. OBJETO. <Resolución derogada por el artículo de la Resolución 1124 de 2020> La presente Resolución tiene como objeto adoptar la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios en el Ministerio de Tecnologías de la Información y las Comunicaciones/ Fondo de Tecnologías de la Información y

las Comunicaciones, así como definir lineamientos frente al uso y manejo de la Información.

ARTÍCULO 2. ÁMBITO DE APLICACIÓN. <Resolución derogada por el artículo de la Resolución 1124 de 2020> La Política de Seguridad de la Información, Seguridad Digital y Continuidad de los Servicios del Ministerio/Fondo de las Tecnologías de la Información y las Comunicaciones aplica a todos los niveles del Ministerio/Fondo de las TIC, a todos sus funcionarlos, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio compartan, utilicen, recolecten, procesen, intercambien o consulten su Información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea Interna o externamente a cualquier archivo de Información, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por el Ministerio TIC, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

ARTÍCULO 3. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS DEL MINISTERIO/FONDO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. <Resolución derogada por el artículo de la Resolución 1124 de 2020> El Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la Información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos, mediante una gestión Integral de riesgos y la Implementación de controles físicos y digitales previniendo así Incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las 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. <Resolución derogada por el artículo de la Resolución 1124 de 2020> La Política General de Seguridad y Privacidad de la Información y Seguridad Digital tendrá los siguientes objetivos:

1. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.

2. Gestionar los riesgos de seguridad y privacidad de la Información, Seguridad Digital de manera Integral.

3. Mitigar los Incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.

4. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la Información del Ministerio.

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 conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información como eje transversal del Ministerio.

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.

CAPITULO II.

POLÍTICAS ESPECIFICAS DE MANEJO DE INFORMACIÓN.

ARTÍCULO 5. POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS. <Resolución derogada por el artículo de la Resolución 1124 de 2020> El Grupo Interno de Trabajo de Gestión del Talento Humano de la Subdirección Administrativa y de Gestión Humana del Ministerio de TIC debe desplegar esfuerzos para que los servidores públicos de la Entidad entiendan sus responsabilidades frente a la seguridad de la Información, con el fin de reducir el riesgo de hurto, fraude, mal uso de las instalaciones y recursos tecnológicos, y de asegurar la confidencialidad, disponibilidad e Integridad de la Información.

PARÁGRAFO. Con el mismo fin, el Grupo Interno de Trabajo de Contratación Incluirá en las minutas de los contratos, cualquiera que sea la modalidad, cláusulas y obligaciones tendientes a la Seguridad de la Información y serán divulgadas a los contratistas a través de los supervisores.

ARTÍCULO 6. POLÍTICA DE GESTIÓN DE ACTIVOS. <Resolución derogada por el artículo de la Resolución 1124 de 2020> La Subdirección Administrativa y de Gestión Humana del Ministerio de TIC, con el acompañamiento permanente de la Oficina de Tecnologías de la

a. Inventario de Activos: Los activos del Ministerio de TIC deben ser identificados, clasificados, valorados y controlados para garantizar su uso adecuado, protección y recuperación ante desastres. Por tal motivo, se diseñará una metodología con los lineamientos necesarios para llevar el Inventarlo de los activos de información de su propiedad, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la Entidad disponga.

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, mantener y actualizar el inventarlo de activos de información relacionados con sus servicios (Información física o digital, software, hardware y recurso humano).

c. Archivos de Gestión: La Subdirección Administrativa y de Gestión Humana deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo a las Tablas de Retención Documental, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información física del Ministerio.

d. Clasificación de la Información: La Subdirección Administrativa y de Gestión Humana deberá establecer una metodología para la clasificación de la Información del Ministerio, en el marco de las Leyes 1712 de 2014, reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015 y 594 de 2000 (Ley General de Archivos), el Decreto 1080 de 2015 y cualquier

normatividad que reglamente la clasificación de información de las Entidades Públicas en el país. Así mismo, la Oficina de Tecnologías de la Información implementará una herramienta Informática que permita etiquetar la información digital y física, de acuerdo a la metodología establecida.

ARTÍCULO 7. POLÍTICA DE CONTROL DE ACCESO. <Resolución derogada por el artículo de la Resolución 1124 de 2020> Los propietarios de los activos de Información y teniendo en cuenta el tipo de activo, deberán establecer medidas de control de acceso: a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías e infraestructura física (instalaciones y oficinas) 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.

ARTÍCULO 8. POLÍTICA DE CRIPTOGRAFÍA. <Resolución derogada por el artículo de la Resolución 1124 de 2020> La Oficina de Tecnologías de la Información brindará a solicitud herramientas que permitan el cifrado para proteger la confidencialidad, Integridad y disponibilidad de la información clasificada y reservada, en sistemas de información, correo electrónico, mecanismos de transferencia de información Internas o externas.

ARTÍCULO 9. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO. <Resolución derogada por el artículo de la Resolución 1124 de 2020> El Ministerio de TIC, 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), y

Información, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración y buen uso de los activos de Información, con el objetivo de garantizar su protección. Dichos lineamientos serán consolidados y publicados en el macroproceso de apoyo “Gestión Documental” por la Subdirección Administrativa y de Gestión Humana.

además para mitigar los riesgos y amenazas externas y ambientales, con el fin de evitar afectación a la confidencialidad, disponibilidad e Integridad de la información de la Entidad.

PARÁGRAFO 1. Todos los servidores públicos, contratistas y visitantes que se encuentren en las instalaciones físicas del Ministerio de TIC deben estar debidamente Identificados, con un documento que acredite su tipo de vinculación, el cual deberá portarse en un lugar visible.

PARÁGRAFO 2. Los visitantes en el Ministerio siempre deben permanecer acompañados por un servidor público o contratista debidamente Identificado.

PARÁGRAFO 3. El personal de empresas contratistas que desempeñe funciones de forma permanente en las Instalaciones del Ministerio, debe estar Identificado con carné y chalecos o distintivos del contratista y portar el carné de la ARL.

ARTÍCULO 10. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES. <Resolución derogada por el artículo de la Resolución 1124 de 2020> La Oficina de Tecnologías de la

Información del Ministerio de TIC 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, y para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de prueba y producción sean controlados y debidamente autorizados. 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 al crecimiento de la Entidad, e implementará 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.

La Oficina de Tecnologías de la Información deberá realizar y mantener coplas de seguridad de la Información de la Entidad en medio digital, siempre que ésta sea reportada por el responsable de la misma, con el objetivo de recuperarla en caso de cualquier tipo de falla. Efectuará la copla respectiva de acuerdo con el esquema definido previamente en un procedimiento que enmarque la gestión, coplas de seguridad de la Información digital, sistemas de Información, bases de datos y demás recursos tecnológicos de la Entidad; el diseño de este procedimiento se hará en conjunto con los líderes de proceso, con el fin de determinar la Información a respaldar y la periodicidad del respaldo, los tiempos de recuperación y restauración, y los mecanismos para generar el menor Impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la Información.

ARTÍCULO 11. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES. <Resolución derogada por el artículo de la Resolución 1124 de 2020> La Oficina de Tecnologías de la Información establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios 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.

La Oficina Asesora de Planeación y Estudios Sectoriales establecerá mecanismos para que el intercambio de Información con las partes Interesadas internas o externas se realice asegurando su Integridad. En el evento que los acuerdos de intercambio de Información requieran del desarrollo de webservice o cualquier otro medio tecnológico, el Intercambio deberá realizarse con los controles criptográficos definidos en el artículo 8o de esta Resolución.

PARÁGRAFO 1. Como parte de sus términos y condiciones iniciales de trabajo, todos los servidores públicos o contratistas, sin Importar su nivel jerárquico, firmarán un acuerdo de confidencialidad y no divulgación que será elaborado por la Oficina Asesora Jurídica según el tipo de vinculación, en lo que respecta al tratamiento de la Información de la Entidad, y la autorización de tratamiento de datos personales. Dichos documentos originales serán conservados y archivados 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 Ministerio, en la carpeta del contrato deberá reposar el acuerdo de confidencialidad debidamente suscrito por el Representante Legal de la empresa.

PARÁGRAFO 2. La Oficina Asesora de Prensa con el apoyo de la Oficina Asesora Jurídica diseñará o actualizará los formatos de autorización de captación y uso de Imágenes, videos o cualquier medio audiovisual, para solicitar al propietario la captación y uso, 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, y que autorice de manera libre, expresa e Inequívocamente, el uso del recurso audiovisual al Ministerio de Tecnologías de la Información y las Comunicaciones o a quien este autorice en el marco del cumplimiento de su misión. Los formatos deberán prever la opción del propietario menor de edad.

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 avalada por la Oficina Asesora de Prensa o a quien el jefe de la misma autorice de manera expresa 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 formal.

ARTÍCULO 12. POLÍTICA DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS. <Resolución derogada por el artículo de la Resolución 1124 de 2020> La Oficina de Tecnologías de la Información velará porque el desarrollo Interno o externo de los sistemas de información cumpla con los requerimientos de seguridad adecuados para la protección de la información del Ministerio, para lo cual desarrollará una metodología que detalle los requerimientos de seguridad para el desarrollo, pruebas y puesta en producción 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. Así mismo, 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 deberá reportarse y entregarse a la Oficina de Tecnologías de la Información cumpliendo con los lineamientos técnicos y presupuéstales de la Oficina de Tecnologías de la Información 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.

ARTÍCULO 13. POLÍTICA DE SEGURIDAD PARA RELACIÓN CON PROVEEDORES. <Resolución derogada por el artículo de la Resolución 1124 de 2020> El Ministerio de Tecnologías de la Información y las Comunicaciones a través del Grupo Interno de Trabajo de Contratación establecerá mecanismos de control en la relación con sus proveedores, teniendo en cuenta que se debe asegurar la información a la que genere, custodie, procese o se tengan acceso, supervisando el cumplimiento de lo establecido en el marco de la seguridad y privacidad de la Información. El supervisor de cada contrato o convenio, en conjunto con la Oficina Asesora de Prensa, será responsable de divulgar las políticas y procedimientos de seguridad de la Información.

ARTÍCULO 14. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. <Resolución derogada por el artículo de la Resolución 1124 de 2020> El Ministerio promoverá entre los servidores públicos y contratistas 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 incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, de acuerdo con su criticidad. La Ministra y sus delegados son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; 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 hará por medio de acto administrativo.

ARTÍCULO 15. POLÍTICA DE LA CONTINUIDAD DEL SERVICIO. <Resolución derogada por el artículo de la Resolución 1124 de 2020> El Ministerio dispondrá los planes necesarios para la continuidad de la operación de los servicios, los cuales serán operados por los líderes de los procesos. La Oficina Asesora de Planeación y Estudios Sectoriales liderará la elaboración del Análisis de Impacto del Negocio (BIA) y del Plan de Continuidad de los Servicios.

PARÁGRAFO: El Plan de Continuidad de los Servicios del Ministerio 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 16. POLÍTICA DE CUMPLIMIENTO. <Resolución derogada por el artículo de la Resolución 1124 de 2020> El Ministerio 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 17. LINEAMIENTOS DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. <Resolución derogada por el artículo de la Resolución 1124 de 2020> Todas las políticas identificadas en este Capítulo se deberán reglamentar de manera detallada y clara en la Declaración de Aplicabilidad y en el Manual de Políticas de Seguridad de la Información.

CAPÍTULO III.

RESPONSABILIDADES DE LOS COLABORADORES FRENTE AL USO DE LOS SERVICIOS TECNOLÓGICOS.

ARTÍCULO 18. DISPOSICIONES. <Resolución derogada por el artículo de la Resolución 1124 de 2020> Todos los servidores públicos o contratistas que hagan uso de los recursos tecnológicos del Ministerio 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 cumplimento de la misión institucional. Para ello, deben acatar las siguientes disposiciones:

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, 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 fin 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, y se establecen las entidades de certificación y se dictan otras disposiciones.), la cual establece la legalidad de los mensajes de datos y las Implicaciones legales que conlleva el mal uso de éstos.

v. La Oficina de Tecnologías de la Información implementará herramientas tecnológicas que prevengan la pérdida o fuga de Información de carácter reservado o clasificado, de conformidad con la ley 1712 de 2014.

vi. Se prohíbe el envío de correos masivos (más de 30 destinatarios) Internos y externos, con excepción de los enviados por el despacho de la Ministra de TIC, de los Viceministros, de la Secretaria General, Oficina Asesora de Prensa, Oficina Asesora de Planeación y Estudios Sectoriales, Grupo Interno de Trabajo de Gestión del Talento Humano, 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 TIC mediante plataformas externas deberá hacerse con la cuenta de la Entidad y utilizando el dominio @mlntic.gov.co, con el fin de que los correos enviados 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,.plf, 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.

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 del Ministerio a otras entidades o ciudadanos sin la debida autorización del despacho de la Ministra de TIC, de los Viceministros, 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 Colombiana vigente.

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 y debe reflejarse en todos los buzones con dominio @mintic.gov.co.

xv. Está expresamente prohibido distribuir, copiar, reenviar Información del Ministerio a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.

xvi. Cuando un servidor público o contratista cesa en sus funciones o culmina la ejecución de contrato con el Ministerio, no se le entregará copia de los buzones de correo Institucionales a su cargo, salvo autorización expresa de la Ministra de TIC, Secretaria General, por orden judicial, por solicitud de la Oficina de. Control Interno o del GIT de Control Disciplinarlo como parte de un proceso de Investigación.

El Ministerio de TIC 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 coplas 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 Entidad, previa solicitud expresa del nominador, ordenador del gasto, supervisor del contrato, jefe Inmediato, Ministra, Viceministros, Coordinador del GIT de Control Disciplinarlo o Coordinador del Grupo Interno de Trabajo de Gestión del Talento Humano a la Oficina de Tecnologías de la Información.

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 y funciones. Será responsabilidad de los colaboradores 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 y para las cuales esté formal y expresamente autorizado por su jefe o supervisor, y solo se utilizará para fines laborales.

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.

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 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 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 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, éstos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red del Ministerio una vez esté avalado por la Oficina de Tecnologías de la Información.

iv. Es responsabilidad de los servidores públicos y contratistas mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas al Ministerio en custodia, al finalizar la vinculación con la Entidad.

v. Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, de 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. 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.

vii 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 y de Gestión Humana.

viii. Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o

reparar sus componentes, son las designadas para tal labor por la Oficina de Tecnologías de la Información.

La Oficina de Tecnologías de la Información realizará monitoreó 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. -

x. 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.

xi. 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, deberá reportarse a la Subdirección Administrativa y de Gestión Humana siguiendo los procedimientos establecidos para este tipo de siniestros.

xii. 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.

xiii. Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad 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.

xiv. La Oficina de Tecnologías de la Información es la única dependencia autorizada para la administración del software del Ministerio, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.

xv. 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.

xvi. 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.

xvii. 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 días lunes de cada semana y solo estarán disponibles en el horario laboral definido.

xviii. 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.

xix. 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.

xx. Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la Entidad debe acogerse a las políticas de “Trae tu propio dispositivo".

d. Del uso de los sistemas o herramientas de información: Todos los servidores públicos y contratistas del Ministerio son responsables de la protección de la información 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 1á 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 de clave de acceso a los sistemas de información o recursos Informáticos periódicamente.

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. El Grupo Interno de Trabajo de Gestión del Talento Humano Humana debe reportar tempestivamente cualquier tipo de novedad de servidores públicos; el Supervisor del contrato reportará oportunamente todas las novedades del contratista.

v. Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución de contrato con el Ministerio, todos los privilegios sobre los recursos Informáticos otorgados le serán suspendidos Inmediatamente; la Información del servidor público o contratista 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, 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. 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.

CAPITULO IV.

REVISIÓN, VIGENCIA Y DEROGATORIA.

ARTÍCULO 19. REVISIÓN. <Resolución derogada por el artículo de la Resolución 1124 de 2020> La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo 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 o quien haga sus veces y revisado y aprobado por el Comité del Modelo Integrado de Gestión o quien haga sus veces.

ARTÍCULO 20. VIGENCIA Y DEROGATORIA. <Resolución derogada por el artículo de la Resolución 1124 de 2020> La presente Resolución rige a partir de la fecha de su publicación.

PUBLÍQUESE Y CUMPLASE

Dado en Bogotá D.C., a los 14 MAR 2019

SYLVIA CONSTAÍN

Ministra de Tecnologías de la Información y las Comunicaciones

Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.
Compilación Juridica MINTIC
n.d.
Última actualización: 31 de mayo de 2024 - (Diario Oficial No. 52.755 - 13 de mayo de 2024)