Agencia Nacional del Espectro

REPUBLICA DE COLOMBIA

RESOLUCIÓN NÚMERO 000795 DEL 26 DIC. 2019

"Por la cual se adopta la Política del Sistema de Gestión de Seguridad y Privacidad de la Información, Seguridad Digital y se definen lineamientos frente al uso la información"

El DIRECTOR GENERAL DE LA AGENCIA NACIONAL DEL ESPECTRO

En ejercicio de sus facultades legales establecidas en la ley 1341 de 2009 y los Decretos 093 de 2010, el 1008 de 2018 y el 1499 de 2017

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, dispone que las personas 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 el artículo 209 de 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 TI 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, en la cual se establecen los lineamientos generales para gestión de incidentes de ciberseguridad, el modelo de prevención y partes interesadas para asegurar la infraestructura del Gobierno, aplicando el modelo de mando unificado entre instituciones.

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

REPUBLICA DE COLOMBIA ANE AGENCIA NACIONAL DEL ESPECTRO DESPACHO DIRECTOR GENERAL

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, 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 interna 462 del 5 de agosto del 2019, estable que el Comité Directivo debe aprobar el Plan de Implementación del Sistema de Gestión de Seguridad de la Información y asegurar los recursos para dar cumplimiento a este, junto con la aprobación de la política del Sistema de Gestión de Seguridad y privacidad de la ANE.

Que en reunión del viernes 18 de octubre de 2019 el Comité Directivo aprobó la Política de Gestión de Seguridad y Privacidad de la Información y Seguridad Digital que a continuación se adopta para la entidad.

Que, dado lo anterior, se hace necesario adoptar mediante acto administrativo, la Política del Sistema de Gestión de Seguridad y Privacidad de la Información y Seguridad Digital, 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.* Adoptar la Política del Sistema de Gestión de Seguridad y Privacidad de la Información y Seguridad Digital, así como definir lineamientos frente al uso y manejo de la información.

ARTÍCULO 2. *Ámbito de aplicación.* La Política del Sistema de Gestión de Seguridad y Privacidad de la Información y Seguridad Digital aplica a todos los funcionarios, contratistas, proveedores y pasantes de la ANE, y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la ANE compartan, utilicen, recolecten, procesen, intercambien, transformen o consulten información, así como los entes de control, entidades relacionadas que accedan, ya sea interna o externamente, a cualquier tipo de información física o digital, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por la ANE, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

ARTÍCULO 3. *Política del Sistema de Gestión de Seguridad y Privacidad de la Información y Seguridad Digital.* La Agencia Nacional del Espectro, mediante la adopción e implementación del Modelo de Seguridad y Privacidad, 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 incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y el óptimo desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo por la administración eficiente del espectro radioeléctrico a través de políticas, programas y proyectos, para ser referente nacional e internacional, influyente en grupos de interés y orientada a la ciudadanía en materia de espectro para garantizar la confianza digital.

PARÁGRAFO. Esta política tendrá como base la norma internacional emitida por la Organización Internacional de Normalización, para Colombia Norma Técnica NTC-ISO/IEC COLOMBIANA

27001:2013 "*Sistemas de Gestión de la Seguridad de la Información*" y el contexto normativo aplicable a esta.

ARTÍCULO 4. *Objetivos.* La Política del Sistema de Gestión de Seguridad y Privacidad de la Información y Seguridad Digital tendrá los siguientes objetivos:

1. Definir, formular 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 y Seguridad Digital.
4. Establecer los mecanismos de aseguramiento físico y digital para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información de la ANE.
5. Definir los lineamientos necesarios para la gestión 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 y cultura de Seguridad y Privacidad de la Información como eje transversal de la ANE.
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.

CAPÍTULO II
POLÍTICAS ESPECIFÍCAS DE MANEJO DE INFORMACIÓN

ARTÍCULO 5. *Política de seguridad de los Recursos Humanos.* El Grupo de Gestión del Talento Humano 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 de Contratación incluirá en las minutas de los contratos, cualquiera que sea la modalidad, cláusulas y obligaciones tendientes a la Seguridad de la Información, las cuales serán divulgadas a los contratistas a través de los supervisores.

ARTÍCULO 6. *Política de Gestión de Activos.* El proceso de Gestión Documental con apoyo del Grupo de Transformación Digital, Gestion de Tecnología y Seguridad de la Información establecerá los lineamientos específicos para la identificación, clasificación, valoración y buen uso de los activos de información, con el objetivo de asegurar su protección. Dichos lineamientos serán consolidados y publicados en el proceso de Gestión Documental. Condiciones generales de la Gestión de Activos:

a. **Inventario de Activos**: Los activos de información de la ANE deben ser identificados, clasificados, valorados y controlados para garantizar su uso adecuado, protección y recuperación ante desastres. Por tal motivo, se establece una metodología integral con los lineamientos necesarios para llevar el inventario 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 acorde a los lineamientos del Gobierno Nacional.

b. **Protección:** Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información en el marco de su función se encargarán

de implementar controles para proteger la información, mantener y actualizar el inventario de activos de información relacionado con sus servicios (Información física o digital, software, hardware y recurso humano).

c. **Archivos de Gestión**: El Proceso de Gestión Documental deberá incluir la implementación de los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información física de la ANE.

d. **Clasificación de la Información**: El Proceso de Gestión Documental deberá establecer una metodología para la clasificación de la información de la ANE, 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, el Grupo de Transformación Digital, Gestion de Tecnología y Seguridad de la Información incluirá la implementación de una herramienta informática que permita etiquetar la información digital y física, de acuerdo con la metodología establecida.

ARTÍCULO 7. *Política de Control de Acceso.* Los propietarios de los activos de información, 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 de la ANE.

ARTÍCULO 8. *Política de Criptografía.* El Grupo de Transformación Digital, Gestion de Tecnología y Seguridad de la Información brindará de acuerdo con los requerimientos de la entidad herramientas que permitan el cifrado de la información para proteger la confidencialidad, integridad y disponibilidad de la información clasificada y reservada, en sistemas de información, correo electrónico y mecanismos de transferencia de información interna o externa.

ARTÍCULO 9. *Política de Seguridad Física y del Entorno.* La ANE implementará 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 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 ANE.

PARÁGRAFO 1. Todos los servidores públicos, contratistas, pasantes y visitantes que se encuentren en las instalaciones físicas de la ANE 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 la ANE 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 de la ANE debe estar identificado con carné y chaleco o distintivos del contratista y portar el carné de la ARL.

ARTÍCULO 10. *Política de Seguridad de las Operaciones.* El Grupo Transformación Digital y Gestión

de Tecnología y Seguridad de la Información de la ANE será el encargado de la operación y administración de los recursos y servicios 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, los cambios efectuados sobre los recursos y servicios tecnológicos y sistemas de información en ambientes de prueba y producción serán 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 con el crecimiento de la ANE, 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 de la ANE.

El Grupo de Transformación Digital, Gestion de Tecnología y Seguridad de la Información deberá realizar y mantener copias de seguridad de la información de la Entidad en medio digital, siempre que ésta sea reportada por el responsable, con el objetivo de recuperarla en caso de cualquier tipo de falla, la completitud de la información debe ser verificada por el área funcional responsable. Así mismo este Grupo efectuará la copia respectiva de acuerdo con el esquema definido previamente en un procedimiento que enmarque la gestión, copias 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 procesos, 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.*** El Grupo de Transformación Digital, Gestion de Tecnología y Seguridad 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 de la ANE.

En el proceso de Direccionamiento Estratégico se establecerán mecanismos para que el intercambio de información con las partes interesadas internas o externas se realice asegurando su integridad. En el evento en 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 8° de esta Resolución y bajo los criterios legales establecidos.

PARÁGRAFO 1. Como parte de sus términos y condiciones iniciales de trabajo, todos los servidores públicos y contratistas, sin importar su nivel jerárquico, firmarán un acuerdo de confidencialidad y no divulgación que será elaborado por los Asesores Jurídicos de la entidad, 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 contratos para el caso de los contratistas.

En el caso de persona jurídica proveedora de servicios para la ANE, en la carpeta del contrato deberá reposar el acuerdo de confidencialidad debidamente suscrito por el Representante Legal de la empresa.

PARÁGRAFO 2. El Profesional de Comunicaciones y Participación Ciudadana junto con los Asesores Jurídicos diseñarán o actualizarán 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 para que autorice de manera libre, expresa e inequívocamente el

uso del recurso audiovisual a la ANE o a quien esta 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 sólo se podrá realizar por los servidores públicos, contratistas o pasantes, la cual debe estar avalada dentro del Proceso de Comunicaciones y Participación Ciudadana, siempre y cuando sean para programas propios de la ANE.

ARTÍCULO 12. *Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas.* El Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información velará porque el desarrollo externo de los sistemas de información cumpla con los requerimientos de seguridad adecuados para la protección de la información de la ANE y el marco de Arquitectura TI definido para la entidad, para lo cual desarrollará documentación 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), el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información es el único de la entidad con la capacidad de adquirir e implementar soluciones tecnológicas para la ANE, 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 ofrecer la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la ANE y la correcta integración al marco de Arquitectura de TI definido por la entidad.

En consecuencia, cualquier software que opere en la ANE deberá reportarse y entregarse al El Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información cumpliendo con los lineamientos técnicos y presupuestales 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, asimismo se deben entregar los derechos de autor de los sistemas de información, cuando esto pueda aplicarse.

ARTÍCULO 13. *Política de Seguridad para Relación con Proveedores.* La ANE a través del Grupo de Contratación establecerá mecanismos de control en la relación con sus proveedores, teniendo en cuenta que se debe asegurar la información que genere, custodie, procese o a la cual 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 el Profesional de Comunicaciones y Participación Ciudadana, 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.* La ANE promoverá entre los servidores públicos, contratistas y pasantes, 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. El Director o a quien él designe serán 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.

ARTÍCULO 15. *Política de la Continuidad del Servicio.* La ANE dispondrá los planes necesarios para la continuidad de la operación de los servicios, los cuales serán operados por los líderes de los procesos. El líder del proceso de Direccionamiento Estratégico 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 de la ANE contendrá Análisis de Impacto del

Negocio (BIA), el Plan de Continuidad de Tecnologías, los Planes de Emergencia y Contingencia, así como cualquier estrategia orientada a la continuidad de la prestación del servicio de la ANE.

ARTÍCULO 16. ***Política de Cumplimiento.*** La ANE 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.*** 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.*** Todos los servidores públicos, contratistas o pasantes que hagan uso de los recursos y servicios tecnológicos de la ANE tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable, entendiendo que el uso inadecuado 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, contratistas y pasantes de la ANE, cuyo uso se facilitará en los siguientes términos:

   I. El único servicio de correo electrónico autorizado para el gestión o transmisión de la información institucional en la Entidad es el asignado de conformidad con el Grupo de Transformación Digital y Gestión de Tecnología y Seguridad, que cuenta con el dominio @ane.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad.
   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. Las comunicaciones internas deben ser enviadas por correo electrónico o digitalmente por el sistema de Gestión Documental en la medida en que sea posible.
   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. El líder del Grupo de Transformación Digital y Gestión de Tecnología y Seguridad 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 Director General y los líderes de los procesos. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.

VII. Todo mensaje de correo electrónico enviado por la ANE mediante plataformas externas deberá hacerse con la cuenta de la entidad y utilizando el dominio @ane.gov.co, con el fin de que los correos enviados no sean catalogados como spam o suplantación de correo.

VIII. El correo notificaciones@ane.gov.co es exclusivo para notificaciones judiciales, por ende, ningún funcionario, contratista, pasante o tercero, ajeno a este tema, debe hacer uso de este.

IX. 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.

X. Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado al correo soporte@ane.gov.co, liderado por el Grupo Transformación Digital y Gestión de Tecnología y Seguridad 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.

XI. La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, redes sociales, casinos, o cualquier otra ajena a los fines de la entidad.

XII. 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.

XIII. Está expresamente prohibido distribuir información de la ANE a otras entidades o ciudadanos sin la debida autorización del líder del Proceso Comunicaciones y Participación Ciudadana.

XIV. El correo electrónico institucional en sus mensajes debe contener un aviso de confidencialidad que será diseñada por el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información con el apoyo del líder del proceso Comunicaciones y participación ciudadana o quien este delegue, y debe reflejarse en todos los buzones con dominio @ane.gov.co.

XV. Está expresamente prohibido distribuir, copiar y reenviar información de la ANE 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 sus funciones o culmina la ejecución del contrato con la ANE, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa del Director, por orden judicial o por solicitud del líder del Grupo de Gestión del Talento Humano como parte de un proceso de investigación disciplinaria, asimismo cualquier información de carácter institucional no debe ser extraída de la entidad por ningún medio.

La ANE se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional, de todos sus servidores públicos, contratistas o pasantes. 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 entidad, previa solicitud expresa del nominador, ordenador del gasto, supervisor del contrato, jefe inmediato, Coordinador del Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información.

REPÚBLICA DE COLOMBIA
ANE
DESPACHO DIRECTOR GENERAL
AGENCIA NACIONAL DEL ESPECTRO

b. **Del uso de internet:** El líder del Grupo Transformación Digital y Gestión de Tecnología y Seguridad 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. Serán responsabilidad de los colaboradores las siguientes, entre otras:

I. Los servicios a los que un funcionario pueda acceder en Internet dependerán del rol o funciones que desempeña en la ANE 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 de la ANE.
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.

La ANE 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 y servicios tecnológicos de la ANE son herramientas de apoyo a las labores y responsabilidades de los servidores públicos, contratistas y pasantes. 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 el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información, salvo que medie solicitud formal del Director, Subdirectores 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 el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información.
III. En caso de que el servidor público, contratista o pasante deba hacer uso de equipos ajenos a los de la ANE, éstos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red de la ANE una vez esté avalado por el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información.
IV. Es responsabilidad de los servidores públicos, contratistas y pasantes mantener en el espacio asignado de almacenamiento por el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información copia de seguridad de la información contenida en sus estaciones de trabajo.
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 su integridad.
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

ANE DESPACHO DIRECTOR GENERAL AGENCIA NACIONAL DEL ESPECTRO REPÚBLICA DE COLOMBIA

aquellos casos autorizados expresamente por el Grupo de Gestión de Gestión Administrativa, este grupo debe realizar validaciones de los puntos de red periódicamente.

VIII. Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y reparar sus componentes son las designadas para tal labor por el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información.

IX. La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es el Grupo Transformación Digital y Gestión de Tecnología y Seguridad 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.

X. La pérdida o daño de elementos o recursos tecnológicos o de alguno de sus componentes deberá ser informada de inmediato al Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información y el Grupo de Gestión Administrativa por el servidor público, contratista o pasante a quien se le hubiere asignado; en caso de que el equipo de cómputo sea propiedad de la ANE, deberá reportarse al líder del Proceso de Gestión de Recursos Físicos siguiendo los procedimientos establecidos para este tipo de siniestros.

XI. La pérdida de información deberá ser informada con detalle al Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información, a través de la Mesa de Servicios, como incidente de seguridad.

XII. Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información física o digital deberá ser reportado a la mayor brevedad al Grupo de Transformación Digital, Gestion de Tecnología y Seguridad de la Información, a través de la Mesa de Servicios, siguiendo el procedimiento establecido.

XIII. El Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información es el único autorizado para la administración del software de la ANE, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.

XIV. Todo acceso a la red de la entidad, mediante elementos o recursos tecnológicos no institucionales, deberá ser informado, autorizado y controlado por el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información.

XV. La conexión a la red wifi institucional para servidores públicos, contratistas y pasantes deberá ser administrada de conformidad con el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información mediante un SSID (Service Set Identifier) único; la autenticación deberá ser con usuario y contraseña de directorio activo.

XVI. La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas administradas por el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información; las contraseñas deberán ser cambiadas periódicamente.

XVII. La red inalámbrica para servidores públicos, contratistas y pasantes estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos por la ANE, el Grupo Transformación Digital y Gestión de Tecnología y Seguridad de la Información establecerá los mecanismos para la asignación.

XVIII. Los equipos de cómputo deben quedar apagados cada vez que el servidor público, contratista y pasante no se encuentre en las instalaciones de la entidad o durante la noche; 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.

d. **Del uso de los sistemas o herramientas de información:** Todos los servidores públicos, contratistas y pasantes de la ANE son responsables de la protección de la información a la que acceden y la cual 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, contratista y pasante es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.

III. Todo servidor público, contratista y pasante 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, contratista o pasante, el acceso a la estación de trabajo le será bloqueada con una solicitud al Grupo Transformación Digital y Gestión de Tecnología y Seguridad 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 de Gestión del Talento Humano debe reportar cualquier tipo de novedad de servidores públicos; los supervisores de contratos reportarán oportunamente todas las novedades del contratista que supervisan.

V. Cuando un servidor público, contratista o pasante cesa sus funciones o culmina la ejecución de contrato con la ANE, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información del servidor público, contratista y pasante será almacenada en los repositorios de la entidad.

VI. Cuando un servidor público, contratista o pasante cesa sus funciones o culmina la ejecución de contrato con la ANE, 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, contratistas o pasantes 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.*** La Política del Sistema de Gestión de Seguridad y Privacidad de la Información y Seguridad Digital de la ANE 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 Operativo de TIC y Seguridad de la Información y sometido a aprobación del Comité Institucional de Gestión y Desempeño o al Comité Directivo, según corresponda.

ARTÍCULO 20. ***Vigencia y Derogatoria.*** La presente Resolución rige a partir de la fecha de su publicación.

PUBLÍQUESE Y CÚMPLASE

Dado en Bogotá D.C., a los 20 DIC. 2019

MIGUEL FELIPE ANZOLA ESPINOSA
Director General

Proyectó: Sergio Carreño Pérez – Profesional Especializado del Grupo de TI – Oficial de Seguridad de la Información
Revisó: Juan Carlos Ramirez Valderrama - Asesor– Coordinador Grupo de Transformación Digital, Gestion de Tecnología y Seguridad de la Información
Aprobó: Comité Directivo – Acta sesión N° 18 de octubre de 2019

REPÚBLICA DE COLOMBIA ANE AGENCIA NACIONAL DEL ESPECTRO DESPACHO DIRECTOR GENERAL