RESOLUCIÓN No. 063 DEL 03 DE MAYO DE 2023

"Por la cual se adopta la Política de seguridad y privacidad de la información y seguridad digital, como uno de los elementos habilitadores de la Política de Gobierno Digital"

EL DIRECTOR GENERAL DE LA UNIDAD ADMINISTRATIVA ESPECIAL DE ALIMENTACIÓN ESCOLAR – ALIMENTOS PARA APRENDER,

En uso de sus facultades legales, en especial las que le confiere el artículo 2.2.9.1.1.2. y 2.2.9.1.3.2 del Decreto 1078 de 2015 y en desarrollo de los artículos 2 y 3 de la Resolución 00500 de 2021 y,

C O N S I D E R A N D O:

Que Decreto 1078 de 2015 Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, dispone en el artículo 2.2.9.1.2.1 que la Política de Gobierno Digital será definida por el MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Que el Título 9, Políticas y Lineamientos de Tecnologías de la Información, Capítulo 1 del Decreto 1078 de 2015, Subrogado por el artículo 1 del Decreto 767 de 2022, Política de Gobierno Digital, artículo 2.2.9.1.1.2. establece que "*Los sujetos obligados a las disposiciones contenidas en el presente capítulo serán las entidades que conforman la administración pública en los términos del artículo 39 de la Ley 489 de 1998 (…)"*

Que el Decreto 218 de 2020 establece que la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender creada en el artículo 189 de la Ley 1955 de 2019, es una entidad adscrita al Ministerio de Educación Nacional, con autonomía administrativa, personería jurídica y patrimonio independiente, la cual en el marco de lo establecido en el artículo 39 de la Ley 489 de 1998 constituye una entidad pública adscrita a un Ministerio que forma parte del Sector Descentralizado de la Administración Pública Nacional.

Que el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, dispone que los habilitadores transversales de la Política de Gobierno Digital, corresponde a las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital y están compuestos por Arquitectura, Cultura y Apropiación, Seguridad y privacidad de la Información y Servicios Ciudadanos Digitales.

Que el Decreto 767 de 2022 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" dispone al tenor del numeral 3.2 del artículo 2.2.9.1.2.1. que el habilitador transversal de la Política de Gobierno Digital, Seguridad y Privacidad de la Información "(…) busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.".

Que para desarrollar el habilitador transversal de "Seguridad y Privacidad de la Información" el MINTIC expidió la Resolución 00500 de 2021 que establece los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital y, establece los lineamientos y estándares

para la estrategia de seguridad digital, a los sujetos obligados señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015.

Que el artículo 5 ibid., establece que los sujetos obligados deben adoptar tanto la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue; como el Modelo de Seguridad y Privacidad de la Información – MSPI señalado en el Anexo 1 de la misma resolución, como habilitador de la política de Gobierno Digital.

Que mediante la Resolución 279 de 2022, la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender adoptó la Política de Seguridad y Privacidad de la Información y se definieron los lineamientos frente a su uso y manejo previendo en el artículo 6 que la evaluación y actualización de las Políticas de seguridad y Privacidad de la Información, será responsabilidad de la Subdirección de Información de la entidad.

Que la Subdirección de Información de la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender, en el marco de la evaluación de la Política de seguridad y Privacidad de la Información, recomendó actualizarla incluyendo buenas prácticas de seguridad digital para el manejo de los sistemas y tecnologías de información en la entidad y medidas de seguridad y privacidad efectivas para garantizar la integridad, confidencialidad y disponibilidad de la información, lo que permite prevenir y gestionar riesgos asociados a la seguridad cibernética, y garantizar el adecuado uso de las herramientas tecnológicas en el cumplimiento de los objetivos de la entidad, y prevenir y gestionar los riesgos y amenazas que puedan afectarla.

Que de conformidad con lo establecido en el numeral 9 del artículo 3 y el numeral 8 del artículo 8 de la Ley 1437 de 2011 "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo" el proyecto de resolución fue publicado y socializado entre el 03 de marzo y el 16 de marzo de 2023, para observaciones de los grupos de interés, incluida la ciudadanía en general.

En mérito de lo expuesto,

RESUELVE:

Artículo 1. *Objeto*. La presente resolución tiene por objeto adoptar la Política de seguridad y privacidad de la información y seguridad digital, como uno de los elementos habilitadores de la Política de Gobierno Digital de la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender, con el fin de promover la protección de la información que maneja la entidad.

Artículo 2. *Ámbito de aplicación*. Serán sujetos obligados de la presente resolución, todos los niveles funcionales y organizacionales de la Unidad, así como todos los funcionarios, contratistas, proveedores y demás personas o terceros que compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea de manera 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 la Unidad sin importar el medio, formato, presentación o lugar en el cual se encuentre.

Artículo 3. *Política General de Seguridad y Privacidad de la Información y Seguridad Digital*. Los sujetos descritos en el ámbito de aplicación deberán preservar y administrar la integridad, confidencialidad, disponibilidad, privacidad, legalidad y confiablidad de la información digital y física, que se produce en el marco de la operación de sus 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, regulatorios y a los de las normas técnicas colombianas, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo el desarrollo, la implementación y seguimiento a la Política Pública de Alimentación Escolar.

Artículo 4. *Objetivos de la Política General*. La política de seguridad y privacidad de la información y seguridad digital, tendrá los siguientes objetivos:

4.1 Establecer mecanismos de aseguramiento físico y digital para fortalecer la confidencialidad, integridad, disponibilidad, privacidad, legalidad y confiabilidad de la información de la Unidad.
4.2 Mitigar el impacto de los incidentes de seguridad y privacidad de la información y seguridad digital en la Unidad.
4.3 Gestionar los riesgos de seguridad y privacidad de la información y de seguridad digital.
4.4 Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital, orientados a la mejora continua y al alto desempeño del Sistema de gestión de seguridad y privacidad de la información.
4.5 Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios, y a los de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.
4.6 Definir y operar la continuidad de la operación de los servicios de la Unidad.

Artículo 5. *Política de seguridad y privacidad en el recurso humano.* Esta política asegura que tanto los funcionarios como los contratistas comprendan las responsabilidades en los roles que ejercen en la entidad y tomen conciencia respecto a la implementación de los lineamientos de seguridad y privacidad con el fin de preservar la disponibilidad, integridad y confidencialidad de la información de la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender. Para el efecto, El Oficial de Seguridad y Privacidad de la Información en coordinación con la Subdirección de Gestión Corporativa deberá, deberá:

5.1 Desplegar esfuerzos para generar conciencia y apropiación en los empleados públicos de la entidad, sobre sus responsabilidades con el fin de reducir los riesgos, el mal uso de las instalaciones y recursos tecnológicos y así asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información.

5.2 Incluir en las minutas de los contratos y convenios, cualquiera que sea su naturaleza o modalidad, cláusulas y obligaciones, las cuales deberán ser divulgadas a través de los supervisores de los contratos, a proveedores y aquellas personas o terceros que, debido al cumplimiento de sus funciones, obligaciones y las de la Unidad, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

5.3. Fomentar la participación de los empleados públicos 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 de Información y la Subdirección de Gestión Corporativa, en su marco de competencias, articularán el diseño y la adopción de los lineamientos específicos para la identificación, clasificación, valoración, rotulado (etiquetado) y buen uso de los activos de información, con el objetivo de garantizar su protección. Dichos lineamientos se construirán e impartirán teniendo en cuenta los siguientes criterios:

6.1 Inventario de Activos: Los activos de la Unidad deben ser identificados, clasificados, valorados y controlados para garantizar su uso, protección y recuperación ante desastres. La Subdirección de Información, 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.

6.2 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 establecidos.

6.3 Sistema de gestión de documento electrónico de archivo- SGDEA: La Subdirección de Gestión Corporativa con el apoyo de la Subdirección de Información, deberán implementar 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. Adicionalmente, para la emisión, recepción y gestión de comunicaciones oficiales, a través de los diversos canales electrónicos y físico, deberá asegurar un adecuado tratamiento archivístico.

6.4 Clasificación de la Información: La Subdirección de Información en conjunto con la Subdirección de Gestión Corporativa deberán establecer una metodología para la clasificación y rotulado (etiquetado) de la información de la Unidad, en el marco de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014 (ley de transparencia y acceso a la información), esta última reglamentada por el Título 1 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 y en el Título 3 de la Parte 8 del Libro 2 del Decreto 1080 de 2015 y demás normativa que reglamente la clasificación de información de las entidades públicas del país. Así mismo, la Subdirección de Información implementará una herramienta informática que permita rotular (etiquetar) la información digital.

6.5 Firma de documentos: Las firmas de documentos que produzca la Unidad 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, así:

6.5.1 En físico con firma autógrafa mecánica.

6.5.2 Con firma digital de persona natural asignadas por la Subdirección de Información según lo dispuesto por la Ley 527 de 1999 o la norma que la modifique, adicione o sustituya.

6.5.3 Con firma electrónica, de acuerdo con lo dispuesto en los Decretos 2364 de 2012, o la norma que lo modifique, adicione o sustituya, para lo cual la Unidad deberá adquirir o implementar un aplicativo que contenga como mínimo lo siguiente:

6.5.3.1 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,

6.5.3.2 Múltiples controles para la autenticación y firma del documento electrónico, garantizando que el firmante es quien dice ser.

6.5.3.3 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.

6.5.3.4 Identificador único provisto por el sistema que permita la verificación de la veracidad del documento.

6.5.3.5 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, o la norma que la modifique adicione o sustituya.

6.5.3.6 Estado del trámite de firma.

6.5.3.7 Firma digital del funcionario quien ejerce la representación de la Unidad, según sea el caso.

6.5.3.8 En ningún caso se debe utilizar firmas facsímil, salvo en aquellos que se autorice por resolución expedida por el Director de la Unidad, indicando para que fin y porqué medios podrá ser utilizada.

Parágrafo 1. Durante el proceso de transición e implementación de lo establecido en el numeral 6.5.3 del presente artículo, el proceso de firma de los documentos expedidos para el desarrollo misional y de apoyo de la Unidad, se seguirá realizando de acuerdo con lo definido en artículo 7 de la Ley 527 de 1999, reglamentado por el Decreto 2364 de 2012.

Artículo 7. *Política de control de acceso*. Los propietarios de los activos de información (cargo, proceso, dependencia u oficina), 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), 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, confidencialidad y privacidad de la información de la Unidad.

Artículo 8. *Política de criptografía*. La Subdirección de Información dispondrá de herramientas que permitan el cifrado de la información clasificada y reservada para proteger su confidencialidad, integridad, disponibilidad y privacidad.

Artículo 9. *Política de privacidad*. La Unidad deberá disponer, a través del Oficial de seguridad y privacidad de la información de los controles necesarios para la protección de la información de los empleados públicos, contratistas y partes interesadas externas, en los términos de la Ley 1581 de 2012 y sus decretos reglamentarios, así como la política de tratamiento de datos personales de la Unidad.

Parágrafo 1. El Oficial de Seguridad y Privacidad de la Información delegado en la Unidad, en conjunto con la Subdirección de Gestión Corporativa, diseñarán un formato de autorización y uso de datos personales, así como de su tratamiento, que deberá adoptar la Unidad, en lo que respecta al uso de datos semiprivados, privados, sensibles, de niños, niñas y adolescentes; dicho formato debe ser claro y detallado en lo referente a la recolección de los datos personales; así mismo, deberá ser firmado por todos los empleados públicos y contratistas como parte de sus obligaciones.

Parágrafo 2. El Oficial de Seguridad y Privacidad de la Información en conjunto con el Asesor de Comunicaciones, diseñarán y actualizarán 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 sus normas reglamentarias y el Decreto 1074 de 2015 o la norma que lo modifique, adicione o sustituya, así como su autorización libre, expresa e inequívoca a la Unidad 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 caso de 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 empleados públicos o contratistas avalados por el Asesor de Comunicación y en cumplimiento de las funciones de acompañamiento de la Unidad 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*. La Unidad, a través de la Subdirección de Gestión Corporativa y el Oficial de Seguridad y Privacidad de la Información, 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 clasificada o reservada, 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, disponibilidad y privacidad de la información de la entidad.

Parágrafo 1. La Subdirección de Gestión Corporativa, en conjunto con el Oficial de Seguridad y Privacidad de la Información, deberán garantizar la protección de los datos semiprivados, privados o sensible recolectados en el área de acceso a las instalaciones de la unidad de los empleados 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 empleados públicos, contratistas y visitantes que se encuentren en las instalaciones físicas de la Unidad deben estar debidamente identificados, con un carné, documento o distintivo que acredite su tipo de vinculación, en caso del carné, este debe portarse en un lugar visible.

Parágrafo 3. Los visitantes que se encuentren en las instalaciones de la Unidad siempre deben permanecer acompañados por un empleado público o contratista de la entidad debidamente identificado.

Parágrafo 4. El personal de empresas, cooperativas o entidades que desempeñe funciones de forma permanente en las instalaciones de la Unidad, deben estar identificados con carné o 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*. Esta política busca asegurar la operación y administración de los recursos tecnológicos que soportan la operación de la entidad. Para el efecto la Subdirección de Información, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad, disponibilidad y privacidad de la información e implantará un comité de control de cambios, reglamentado mediante unos lineamientos, 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, en los casos que aplique. 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 de la Unidad.

La Subdirección de 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, velará que ésta sea reportada por el responsable de esta, con el objetivo de recuperarla en caso de cualquier tipo de falla. La Subdirección de 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.

El diseño de este procedimiento se hará bajo la dirección de la Subdirección de 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 opere una plataforma tecnológica fuera de las instalaciones físicas y en el marco de las funciones misionales u operacionales de la Unidad, deberá cumplir con lo establecido en la presente política y los lineamientos dispuestos por el Oficial de Seguridad y Privacidad de la Información, para tal fin.

Artículo 12. *Política de seguridad de las comunicaciones*. Esta política busca fortalecer la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte de la Unidad, así como los controles utilizados para proteger la

información en la transferencia de información. Para el efecto la Subdirección de 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 de la Unidad.

La Subdirección de Información establecerá mecanismos estratégicos 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 servicio web (web service) o de cualquier otro medio tecnológico, el intercambio deberá realizarse con los controles criptográficos definidos en la entidad.

Parágrafo 1. Como parte de sus términos y condiciones iniciales de trabajo de todos los empleados públicos, sin importar su nivel jerárquico, o los contratistas de la Unidad, según el caso, firmarán un acuerdo o compromiso de confidencialidad y no divulgación, que será elaborado por la Subdirección de Gestión Corporativa con el apoyo del Oficial de Seguridad y Privacidad de la Información, según el tipo de vinculación, en lo que respecta a la información de la Unidad. Dicho documento original será conservado y archivado en la historia laboral de los empleados públicos y en la carpeta de los procesos contractuales para el caso de los contratistas.

Parágrafo 2. En el caso de persona jurídica proveedora de servicios para la Unidad, en la carpeta del contrato deberá reposar el acuerdo o compromiso de confidencialidad y no divulgación debidamente suscrita por el representante legal.

Artículo 13. *Política de seguridad para la adquisición, desarrollo y mantenimiento de sistemas*. Esta política busca asegurar que la seguridad digital sea una parte integral de los sistemas de información de la Unidad durante todo el ciclo de vida y aplica a todos los sistemas de información, incluyendo los sistemas de información que prestan servicios sobre redes públicas. La Subdirección de Información velará porque los desarrollos internos y externos de los sistemas de información, cumplan con los requerimientos de seguridad adecuados para la protección de la información de la Unidad, 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 Subdirección de Información es la única dependencia con la capacidad de adquirir, conforme con su ficha de inversión, desarrollar e implementar soluciones tecnológicas para la Unidad, 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 y privacidad de la información de los sistemas que operan en la entidad.

En consecuencia, cualquier software que opere en la entidad deberá contar con la autorización de la Subdirección de 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 de la Unidad, deberá cumplir con lo establecido en la presente política.

Artículo 14. *Política de seguridad para relación con proveedores*. Esta política busca establecer las condiciones para la prestación de los servicios, responsabilidades y controles que ayuden a proteger la información involucrada en las relaciones entre la Unidad con sus terceros, frente a interceptaciones, copia, modificación, divulgación y destrucción no autorizada, que puedan afectar los principios de integridad, disponibilidad y confidencialidad de la información. Aplica para todos los proveedores que para la

ejecución de su trabajo requieran acceder a la información o infraestructura tecnológica de la Unidad. La Subdirección de Gestión Corporativa, establecerá, en el Manual de Contratación, Supervisión e Interventoría 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 de un contrato, se utilice dentro del marco de la seguridad y privacidad de la información por parte de los proveedores. En el mismo sentido y a través del seguimiento a la ejecución, se garantizará que los supervisores de los contratos, convenios o acuerdos sean los responsables de aplicar las políticas y procedimientos de seguridad y privacidad de la información durante la ejecución de los contratos, estos lineamientos deberán ser comunicados a los proveedores a través de los canales dispuestos por la Unidad.

Parágrafo. Tratándose de relaciones contractuales de la Unidad, estas disposiciones deberán ser incorporadas en los términos, cláusulas, minutas o acuerdos con los que se relacionen estos, a efectos de garantizar su implementación.

Artículo 15. *Política de gestión de incidentes de seguridad de la información*. Esta política busca gestionar adecuadamente todos los incidentes de seguridad de la información reportados en la Unidad, dando cumplimiento a los procedimientos establecidos para el efecto. Aplica para todos los colaboradores y terceros de la Unidad que detecten un evento o incidente de seguridad y privacidad de la información, el cual deben reportar, adecuadamente, de acuerdo con los procedimientos establecidos en la Unidad. El Oficial de Seguridad y Privacidad de la Información, promoverá entre los empleados públicos y contratistas, el reporte y seguimiento de incidentes relacionados con la seguridad y privacidad de la información y sus medios. Así mismo, asignará responsables para el tratamiento de estos, quienes investigarán y solucionarán los incidentes reportados, de acuerdo con su criticidad.

El Oficial de Seguridad y Privacidad de la Información informará a la Dirección General de la Unidad, los incidentes de seguridad, para que este en el marco de sus competencias reporte e instaure las denuncias ante las autoridades pertinentes, tales como, de defensa nacional, policía, fiscalía y de control. La Dirección General o quien esta delegue, será el único canal de comunicación autorizado para hacer pronunciamientos oficiales ante las entidades externas, medios de comunicación o la ciudadanía.

Artículo 16. *Política de la continuidad de la operación de los servicios*. Esta política busca asegurar que todos los aspectos relacionados con la seguridad de la información se incluyan en los planes de continuidad de la operación de la Unidad y así proteger la información. Esta política aplica para la definición del plan de continuidad de operación de servicios y la recuperación en caso de desastres, en las cuales se deben incluir los requisitos de seguridad de la información. La Unidad 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, la Subdirección de Información y la Subdirección de Gestión Corporativa 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 de la Unidad contendrá el Plan de continuidad Tecnológico (DRP), los Planes de emergencia y contingencia, así como cualquier estrategia orientada a la continuidad de la prestación del servicio de la entidad.

Artículo 17. *Política de cumplimiento*. Esta política busca evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad y privacidad en la Unidad y asegurar que se revisen y actualicen periódicamente, como mínimo una vez al

año o cuando se presente una actualización en la normatividad que afecte la seguridad de la información. Esta será aplicada por todas las dependencias de la Unidad.

El Oficial de Seguridad y Privacidad de la Información con apoyo de la Asesora Jurídica y su personal de apoyo, velarán por la identificación, documentación, cumplimiento y asesoría de los requisitos legales enmarcados en la seguridad y privacidad de la información y seguridad digital, 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 de procedimientos y una matriz de requisitos legales para su control y seguimiento.

Artículo 18. *Política de seguridad de la información en la gestión de proyectos*. Esta política busca que desde la gestión de los proyectos se traten los lineamientos frente a la seguridad y privacidad de la información independientemente del tipo de proyecto. El Asesor de Planeación y el personal de apoyo, 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, el Asesor de Control Interno y personal de apoyo, podrá implementar seguimientos, monitoreos, planes de auditoría interna u otros mecanismos de control, para la revisión del cumplimiento e implementación de la política, dependiendo de las necesidades de la entidad..

Artículo 19. *Política de seguridad digital.* Esta política busca establecer un marco de referencia de gestión para iniciar y controlar la implementación de la seguridad digital al interior de la Unidad por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y grupos de interés y la incorporación de la seguridad digital en la gestión de los proyectos, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información definido por la Unidad, buscando preservar la confidencialidad, integridad y disponibilidad de la información. Aplica a todos los empleados públicos o contratistas que hagan uso de los recursos tecnológicos de la Unidad, que 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:

19.1 Del uso del correo electrónico. El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los empleados públicos y contratistas de la Unidad, cuyo uso se facilitará en los siguientes términos:

a) El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la entidad es el asignado por la Subdirección de Información, que cuenta con el dominio @uapa-pae.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

b) 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.

c) 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.

d) 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), o la que la modifique, adicione o sustituya, la cual establece la validez de los mensajes de datos.

e) La Subdirección de 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 o la que la modifique, adicione o sustituya.

f) Se prohíbe el envío de correos masivos (más de 20 destinatarios) internos o externos, con excepción de los enviados por la Dirección y Subdirección General, Asesor de Comunicación, Asesor de Planeación, Subdirección de Gestión Corporativa, así como de la Subdirección de Información solamente en caso de ventana de mantenimientos de los servicios de tecnología de la información. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.

g) Todo mensaje de correo electrónico enviado por la Unidad mediante plataformas externas deberá hacerse con la cuenta de la entidad y utilizando el dominio @uapa-pae, con el fin de que no sean catalogados como spam o suplantación de correo.

h) Para apoyar la gestión de correo electrónico de directivos y asesores, 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.

i) Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Subdirección de Información a través de la Mesa de Servicios como incidente de seguridad y privacidad de la información o seguridad digital, 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.

j) 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.

k) 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.

l) Está expresamente prohibido distribuir información oficial de carácter clasificada o reservada de la Unidad a otras entidades o ciudadanos sin la debida autorización de la Dirección o Subdirección General, del Asesor de Comunicación y del Asesor de Planeación, previa revisión del Asesor de Comunicación en caso de comunicados y del Asesor de Planeación en caso de cifras oficiales.

m) 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.

n) El correo electrónico institucional en sus mensajes debe incorporar un aparte con contenido de confidencialidad, que será diseñado por la Subdirección de Información con el apoyo del Asesor de Comunicación, dicha sentencia debe reflejarse en todos los buzones con dominio @uapa-pae.

o) Está expresamente prohibido distribuir, copiar o reenviar información de la Unidad a través de correos personales o sitios web diferentes a los autorizados en el marco de las funciones u obligaciones contractuales.

p) Cuando un empleado público o contratista cesa en sus funciones o culmina la ejecución de contrato con la Unidad, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa de la Dirección General, por orden judicial o por solicitud del Asesor de Control Interno como parte de un proceso de investigación.

q) La Unidad se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus empleados 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 nominador, ordenador del gasto, supervisor del contrato, jefe inmediato, Director General, Subdirector General, Subdirectores; a la Subdirección de Información. Para ello, al inicio de la relación laboral o contractual se deberá comunicar a los funcionarios y contratistas que la Unidad realiza el referido monitoreo.

19.2 Del uso de Internet: La Subdirección de Información, en conjunto con el Oficial de Seguridad y Privacidad de la Información, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones. Será responsabilidad de los colaboradores las siguientes, entre otras:

a) Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol, funciones u obligaciones que desempeña en la Unidad y para las cuales esté formal y expresamente autorizado por su jefe o supervisor y solo se utilizará para fines laborales.
b) 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.
c) Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la política de navegación de la Unidad.
d) Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
e) Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.
f) La Unidad 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.

19.3 Del uso de los recursos tecnológicos: Los recursos tecnológicos de la Unidad son herramientas de apoyo a las labores, responsabilidades y obligaciones de los empleados públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

a) Los bienes de cómputo que provea la entidad se emplearán de manera exclusiva y bajo la completa responsabilidad del empleado 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 Subdirección de Información, salvo que medie solicitud formal del Director, Subdirectores, Asesores, a través de la Mesa de Servicios.
b) Sólo está permitido el uso de software licenciado por la entidad y aquel que, sin requerir licencia, sea expresamente autorizado por la Subdirección de Información.
c) En caso de que el empleado público o contratista deba hacer uso de equipos ajenos a la Unidad, éstos deberán cumplir con la legalidad del Software instalado, sistema operativo y antivirus licenciado, actualizado y solo podrá conectarse a la red de la entidad una vez esté avalado por la Subdirección de Información.
d) Los empleados públicos y contratistas deberán realizar y mantener las copias de seguridad de su información y entregarla a la entidad al finalizar la vinculación.
e) 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.

f) Los empleados públicos y contratistas deberán utilizar las herramientas tecnológicas que proporcione la Subdirección de Información para gestionar la información digital de la Unidad.

g) 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.

h) 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 de Gestión Corporativa.

i) 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 Subdirección de Información.

j) La Subdirección de 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.

k) La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Subdirección de 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 (Subdirección de Gestión Corporativa).

l) La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato a la Subdirección de Información por el empleado público o contratista a quien se le hubiere asignado; en caso de que el equipo de cómputo sea suministrado por la Unidad, deberá reportarse a la Subdirección de Gestión Corporativa siguiendo los procedimientos establecidos para este tipo de siniestros, sin perjuicio de las acciones penales y disciplinarias que requiera adelantar según sea el caso.

m) La pérdida de información deberá ser informada con detalle a la Subdirección de Información, a través de la Mesa de Servicios, como incidente de seguridad y privacidad de la información.

n) Todo incidente de seguridad y privacidad que comprometa la confidencialidad, integridad, disponibilidad y privacidad de la información física o digital deberá ser reportado a la mayor brevedad a la Subdirección de Información, a través de la mesa de servicios, siguiendo el procedimiento establecido.

o) La Subdirección de Información es la única dependencia autorizada para la administración del software de la Unidad, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.

p) Todo acceso a la red de la entidad, mediante elementos o recursos tecnológicos no institucionales, deberá ser informado, autorizado y controlado por la Subdirección de Información.

q) La conexión a la red wifi institucional para empleados públicos y contratistas deberá ser administrada desde la Subdirección de Información mediante un SSID (Service Set Identifier) único; la autenticación deberá ser con usuario y contraseña de directorio activo.

r) La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas administradas por la Subdirección de Información, las contraseñas deberán cambiar los lunes de cada semana.

s) La red wifi para empleados públicos y contratistas estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos por la Unidad.

t) Los equipos deben quedar apagados cada vez que el empleado 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.

u) Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la entidad debe acogerse a las políticas de "Trae tu propio dispositivo".

v) Las herramientas corporativas instaladas en los dispositivos móviles personales serán gestionadas por la Subdirección de Información con el fin de proteger la confidencialidad, integridad, disponibilidad y privacidad de la información de la entidad, garantizando el cumplimiento del artículo 9 de la presente resolución.

19.4 Del uso de los sistemas o herramientas de información: Todos los empleados públicos y contratistas de la Unidad 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:

a) Las credenciales de acceso a la red y a los recursos informáticos (usuario y clave) son de carácter estrictamente personal e intransferible; los empleados públicos y contratistas no deben revelarlas a terceros, ni utilizar claves ajenas.

b) Todo empleado público y contratista es responsable del cambio periódico de su clave de acceso a los sistemas de información o recursos informáticos.

c) Todo empleado público y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.

d) En ausencia del empleado público o contratista, el acceso a la estación de trabajo le será bloqueada con una solicitud a la Subdirección de 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 Gestión de Talento Humano o quien haga sus veces debe reportar de inmediato, cualquier tipo de novedad de los empleados públicos, a su vez los supervisores de contrato deben reportar oportunamente todas las novedades del contratista.

e) Cuando un empleado público o contratista cesa sus funciones o culmina la ejecución del contrato con la Unidad, 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.

f) Cuando un empleado público o contratista cesa sus funciones o culmina la ejecución de contrato con la Unidad, 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.

g) Cuando un empleado público o contratista cesa sus funciones o culmina la ejecución del contrato con la Unidad deberá tramitar el paz y salvo, de acuerdo con el procedimiento establecido por la entidad.

h) Todos los empleados 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 20. *Lineamientos de las políticas de seguridad de la información*. La Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender, dentro de los seis (6) meses siguientes a la expedición de la presente, adoptará el desarrollo de las políticas de que tratan los artículos 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 y 19 del presente acto administrativo, en la Declaración de Aplicabilidad y el Manual de Política de Seguridad y Privacidad de la Información y Seguridad Digital, que serán publicadas en la herramienta documental de la entidad.

Artículo 21. *Designación del Oficial de Seguridad y privacidad de la Información.* El Director General de la Unidad designará el funcionario y asignará las funciones que ejercerá el Oficial de Seguridad y Privacidad de la Información, en los términos definidos en la presente resolución.

Artículo 22. *Revisión*. La Política de Seguridad y Privacidad de la Información y Seguridad Digital, será revisada anualmente y se harán ajustes antes, de existir modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y eficaz.

Artículo 23. Seguimiento. El cumplimiento de las Políticas de Seguridad y Privacidad de la Información y seguridad Digital serán verificadas a través del Asesor de Control Interno por medio de seguimientos, monitoreos u otros mecanismos de control.

Artículo 24. Transición. Las disposiciones previstas en la presente resolución se implementarán de manera gradual de acuerdo con el plan de trabajo presentado por la Subdirección de Información al Comité Institucional de Gestión y Desempeño.

Artículo 25. *Vigencia y derogatoria*. La presente resolución rige a partir de la fecha de su publicación, deroga la Resolución 0279 de 2022.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los 03 días del mes de mayo de 2023

LUIS FERNANDO CORREA SERNA
Director General

Aprobó: Juan David Vélez Bolívar, Subdirector General
Jorge Andrés Rodríguez Parra, Asesor oficina de Planeación
Álvaro Fernando Guzmán Lucero, Subdirector de gestión Corporativa
Adriana Escobar Gómez, Asesora oficina de Control Interno
Alejandro Rey Fernández, Asesor oficina de Comunicaciones
Elisa María Cadena Gaona, Subdirectora de Fortalecimiento
Ana María Luisa Sierra Nova, Subdirectora de Análisis, Calidad e Innovación.

Revisó: Gustavo Adolfo Grisales, subdirector de información
Ana Janeth Jiménez Pinzón, Asesora Jurídica
Diana Carolina Bolaño – Apoyo Jurídico Dirección General
Henry Cruz – Apoyo Jurídico Dirección General

Proyectó: Sergio Andrés Ramos P, Contratista de la Subdirección de Información.