ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HÁBITAT
Unidad Administrativa Especial de
Servicios Públicos

UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS

RESOLUCIÓN NÚMERO 491 DE 2022

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información y se deroga la Resolución 613 de 2021".

LA DIRECTORA GENERAL DE LA UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS

En ejercicio de sus facultades legales y reglamentarias, en especial las establecidas en la Ley 489 de 1998, en el Acuerdo Distrital No.257 de 2006, en el Acuerdo No. 011 de 2014, en concordancia con los Acuerdos 01 y 02 de 2012 del Consejo Directivo de la Unidad Administrativa de Servicios Públicos del Consejo Directivo de la UAESP, y

CONSIDERANDO:

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

Que el numeral 6° del artículo 3º del Acuerdo 01 de 2012 *"Por el cual se modifica la estructura organizacional y se determinan las funciones de las dependencias de la Unidad Administrativa Especial de Servicios Públicos"*, faculta a la Dirección General para *"Liderar el Sistema Integrado de Gestión y los subsistemas de calidad, (…) y el Modelo Estándar de Control Interno (MECI) e impartir las directrices de acuerdo con las normas establecidas.".*

Que la Ley Estatutaria 1581 de 2012 *"Régimen General de Protección de Datos Personales"*, tiene como objeto *"(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."*

Que a su vez el artículo 2.2.2.25.3.1. del Decreto 1074 de 2015, *"Decreto Único Reglamentario del Sector Comercio Industria y Turismo",* consagró la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental de Habeas Data estableciendo dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho y velar porque los encargados del tratamiento den cabal cumplimiento a las mismas.

Que la Ley Estatutaria 1712 de 2014, *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones",* modificada por la ley 2195 de 2022*,* definió en su Artículo 1º, que: *"el objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información"*, disposición que fue reglamentada parcialmente por el Decreto 103 de 2015 y este último compilado en el Decreto 1081 de 2015.

Que el Decreto 1078 de 2015, *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"* determinó como principio de la Política de Gobierno Digital, el de Seguridad de la Información, a través del cual, se busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano.

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información y se deroga la Resolución 613 de 2021".

Que el Decreto 1083 de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública"*, establece las políticas de Gestión y desempeño Institucional, entre las que se encuentran "*Gobierno Digital*", antes "*Gobierno en Línea*" y "*Seguridad Digital".*

Que el Documento CONPES 3854 de 2016, establece la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades.

Que el Decreto 2106 de 2019 "*Por el cual se dictan normas para simplificar suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública"*, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital, siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Que en cumplimiento de todo lo anterior, la Unidad Administrativa Especial de Servicios Públicos – UAESP, expidió la Resolución No. 589 de 2019, mediante la cual se adoptó la "*Política de Seguridad de la Información".*

Que el documento CONPES 3995 de 2020, formula la Política Nacional de Confianza y Seguridad Digital en la República de Colombia, estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital, de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), expidió la Resolución 500 de 2021, "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital*".

Que la Unidad Administrativa Especial de Servicios Públicos, expidió la Resolución 613 de 2021*," Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información y se deroga la Resolución 589 de 2019".*

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, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*", establece como habilitador la Seguridad y Privacidad en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Que el Comité Institucional de Gestión y Desempeño, mediante Acta del 21 de junio de 2022, aprobó la actualización de la *"Política General de Seguridad y Privacidad de la información de la UAESP".*

Que teniendo en cuenta los lineamientos normativos en comento, es necesario derogar la Resolución No. 613 de 2021 y actualizar mediante el presente acto administrativo, la *"Política General de Seguridad y Privacidad de la Información*" en la Unidad Administrativa Especial de Servicios Públicos-UAESP.

Que, en mérito de lo expuesto,

RESUELVE:

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO PRIMERO. – Objeto: La presente Resolución tiene como objeto actualizar la Política General de Seguridad y Privacidad de la Información, así como definir y adoptar las

políticas específicas para el uso de la información en la Unidad Administrativa Especial de Servicios Públicos – UAESP.

ARTÍCULO SEGUNDO. - Alcance: La Política General de Seguridad y Privacidad de la Información aplica para todos los servidores (as) públicos (as), contratistas, proveedores, operadores, así como aquellas personas o terceros que utilicen, recolecten, procesen, intercambien, consulten y accedan a los activos de información de la Unidad Administrativa Especial de Servicios Públicos – UAESP.

De igual manera, la presente política está orientada a todos los procesos de la entidad, bajo el marco de gestión establecido en el Modelo Integrado de Planeación y Gestión - MIPG propuesto por el DAFP y el Modelo de Seguridad y Privacidad de la Información - MSPI.

ARTÍCULO TERCERO. – Objetivo general de la política: Establecer los lineamientos orientados a proteger y preservar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los activos de información gestionados por la Entidad, mediante una gestión integral de riesgos y la implementación de controles que prevengan la materialización de incidentes de seguridad y privacidad de la información, cumpliendo los requisitos legales, reglamentarios y regulatorios, orientados a la mejora continua, el uso efectivo y la apropiación de seguridad y privacidad de la Información.

ARTICULO CUARTO: - Objetivos específicos de la política:

1. Definir las políticas, procedimientos e instructivos en materia de seguridad y privacidad de la información.
2. Mitigar el impacto de los incidentes de seguridad y privacidad de la información.
3. Establecer mecanismos de control que permitan fortalecer la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la Información.
4. Fortalecer la cultura organizacional, a través de la concienciación, participación y apropiación de la seguridad y privacidad de la información, orientados a la mejora continua.
5. Cumplir los principios, requisitos legales, reglamentarios y regulatorios en materia de seguridad y privacidad de la información.
6. Garantizar la continuidad del negocio frente a posibles incidentes de seguridad y privacidad de la información.
7. Incrementar la confianza y la seguridad digital de los grupos de interés, mediante la implementación de un sistema de gestión de seguridad de la información -SGSI.

CAPITULO II
POLÍTICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO QUINTO: - Política de la Organización de la Seguridad de la Información: El responsable de la seguridad de la información, junto con la Oficina de Tecnología de la Información y Comunicaciones de la Unidad Administrativa Especial de Servicios Públicos, deberán mantener y documentar los contactos con las autoridades en materia de ciberseguridad y otros entes especializados para que puedan ser contactados en caso de presentarse un incidente de seguridad de la información que requieran de asesoría, acompañamiento o intercambiar conocimientos para mejorar el Sistema de Gestión de Seguridad de la Información y mejorar la respuesta ante incidentes.

PARÁGRAFO. Todos los proyectos deben contemplar un análisis de riesgos de seguridad de la información.

ARTÍCULO SEXTO: - Política de Dispositivos Móviles: La Oficina de Tecnologías de la Información y las Comunicaciones deberá establecer las condiciones necesarias para la

protección física, el uso seguro, como establecer contraseñas de acceso robustas, cifrar la información almacenada, mecanismos de respaldo y demás, necesarios para garantizar la seguridad y privacidad de la información de la Unidad Administrativa Especial de Servicios Públicos - UAESP, llevando el registro y control de los elementos entregados.

ARTÍCULO SEPTIMO: - Política de seguridad para el trabajo remoto: La Entidad brindará a los servidores (as) públicos (as) los equipos y herramientas necesarias para el cumplimiento de las funciones en las modalidades de trabajo remoto de acuerdo con los lineamientos o normatividad vigente que las regulen según el caso.

PARÁGRAFO. Los servidores (as) públicos (as) podrán disponer de sus propios equipos y demás herramientas, siempre que medie acuerdo con la Entidad. Si no se llega al mencionado acuerdo, la UAESP suministrará los equipos, sistemas de información, software o materiales necesarios para el desarrollo de las funciones.

ARTÍCULO OCTAVO: - Política de seguridad para el recurso humano: El proceso de Gestión de Talento Humano deberá incluir dentro del Plan Institucional de Capacitación, temáticas asociadas a la seguridad y privacidad de la información, que incluyan las políticas, roles, responsabilidades y obligaciones relacionada con el Modelo de Seguridad y Privacidad de la Información de la Unidad Administrativa Especial de Servicios Públicos - UAESP.

PARÁGRAFO. Con el mismo propósito, se deberá incluir una cláusula en las minutas de los contratos o por medio del mecanismo que considere oportuno la Subdirección de Asuntos Legales de la Unidad Administrativa Especial de Servicios Públicos - UAESP, que contenga las obligaciones en relación con el cumplimiento de la Política General de Seguridad y Privacidad de la Información.

ARTÍCULO NOVENO: - Política de gestión de activos de información: La Oficina de Tecnologías de la Información y Comunicaciones definirá y documentará el método de reporte, identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información y alineados al Programa de Gestión Documental.

ARTÍCULO DÉCIMO: - Política de control de acceso: Los custodios de los activos de la información deberán establecer las medidas de control de acceso adecuadas con el fin de mitigar riesgos asociados al acceso a la información y recursos de infraestructura de la Entidad.

PARÁGRAFO. La asignación de los privilegios de acceso de todos los usuarios en los sistemas información y servicios de red de la UAESP deberán regirse de acuerdo solo con las actividades que el usuario vaya a realizar.

ARTÍCULO DÉCIMO PRIMERO: - Política de Seguridad Física y del entorno: La Subdirección Administrativa y Financiera de la Unidad Administrativa Especial de Servicios Públicos, deberá establecer perímetros de seguridad para controlar el acceso físico a las instalaciones de la Entidad, Data Center, suministro de energía y otras áreas seguras, si las hubiere, teniendo en cuenta las normas de seguridad y salud en el trabajo.

ARTÍCULO DÉCIMO SEGUNDO: - Política de escritorio y pantalla limpia: Está prohibido guardar información en el escritorio del equipo de cómputo, para prevenir el acceso no autorizado. La ubicación para guardar la información dentro de los equipos de cómputo es la carpeta "Mis Documentos" o en la nube, de acuerdo con el proveedor de la herramienta autorizada por la Oficina de Tecnología de la Información y Comunicaciones, cuando estén por fuera del dominio o de la Entidad.

PARÁGRAFO 1. Se debe almacenar bajo llave los documentos en papel y los medios de almacenamiento externos o extraíbles en gabinetes y/u otro tipo de mobiliario seguro, cuando

contengan información sensible y no estén siendo utilizados, especialmente fuera del horario de trabajo.

PARÁGRAFO 2. Se prohíbe el uso de fotocopiadoras o escáneres no autorizados por la Entidad.

PARÁGRAFO 3. Se deben retirar inmediatamente los documentos que contengan información pública clasificada o pública reservada, una vez impresos.

ARTÍCULO DÉCIMO TERCERO: - Política de controles criptográficos: La Oficina de Tecnologías de la Información y Comunicaciones deberá establecer y documentar el proceso y controles criptográficos a implementar en los servicios que lo requieran.

ARTÍCULO DÉCIMO CUARTO: - Política de seguridad en las operaciones: La Oficina de Tecnologías de la Información y Comunicaciones es la encargada de la operación y administración de los recursos tecnológicos que soportan la operación de la Entidad, por ello, deberá documentar y mantener actualizados los procedimientos operacionales a nivel de Tecnologías de la Información (TI) para reducir riesgos asociados a la seguridad de la información y ponerlos a disposición de toda la Entidad.

ARTÍCULO DÉCIMO QUNTO: - Política de backups: La Oficina de Tecnologías de la Información y Comunicaciones deberá implementar herramientas y mecanismos para la gestión de respaldos de la información de la Entidad.

PARÁGRAFO. La Oficina de Tecnologías de la Información y Comunicaciones deberá documentar e implementar los procedimientos y controles necesarios para el respaldo y restauración de información de los equipos de cómputo, servidores, aplicaciones, bases de datos, sistemas de información o cualquier elemento de la infraestructura tecnológica que sea requerido por el responsable o custodio de la información.

ARTÍCULO DÉCIMO SEXTO: - Política de buen uso del internet y herramientas colaborativas: El uso del Internet estará limitado por la necesidad de acceso que se requiera en el desarrollo de las funciones u obligaciones contractuales.

PARÁGRAFO 1. Los dispositivos móviles propios de servidores (as) públicos (as), contratistas y terceros podrán tener acceso a internet mediante conexión limitada o restringida a los sistemas de información, atendiendo las medidas o controles de seguridad establecidos por la Oficina de Tecnologías de la Información y Comunicaciones.

PARÁGRAFO 2. El servicio de correo electrónico de la Entidad deberá usarse única y exclusivamente para actividades relacionadas directamente con las funciones propias del cargo o ejecución de las obligaciones contractuales. Por lo anterior, el único correo electrónico autorizado para la transmisión de información institucional es el que cuenta con el dominio "*@uaesp.gov.co".*

PARÁGRAFO 3. Es responsabilidad de todos, el adecuado manejo de las herramientas colaborativas asignadas, incluyendo los permisos y la información compartida con otras personas.

ARTÍCULO DÉCIMO SÉPTIMO: - Política de seguridad en las comunicaciones: La Oficina de Tecnologías de la Información y Comunicaciones deberá implementar y mantener una plataforma tecnológica que soporte los sistemas de información y servicios de red de la Entidad.

PARÁGRAFO. La Oficina de Tecnologías de la Información y Comunicaciones deberá brindar servicios o herramientas de intercambio de información seguras, como el correo electrónico, mensajería electrónica o herramientas colaborativas, las cuales deberán cumplir con

requerimientos técnicos, legales y de seguridad para evitar accesos no autorizados, ataques informáticos y de códigos maliciosos. Así mismo, deberá implementar controles, como el cifrado de información, que permita proteger la información contra divulgación o modificaciones no autorizadas.

ARTÍCULO DÉCIMO OCTAVO: - Política de adquisición, desarrollo y mantenimiento de sistemas de información: La Oficina de Tecnologías de la Información y Comunicaciones deberá definir y documentar el proceso para la solicitud de nuevos sistemas de información y modificaciones a los existentes, donde se contemple los requisitos, análisis e implementación de criterios de seguridad de la información.

ARTÍCULO DÉCIMO NOVENO: - Política de relación con los proveedores: La Subdirección de Asuntos Legales deberá verificar la inclusión en las obligaciones contractuales o en el mecanismo que consideren necesario, con terceros o proveedores, el cumplimiento de las obligaciones contractuales relacionadas con seguridad y privacidad de la información.

ARTÍCULO VIGÉSIMO: - Política de gestión de incidentes de seguridad y privacidad de la información: La Oficina de Tecnologías de la Información y Comunicaciones deberá documentar e implementar un procedimiento de gestión de incidentes de seguridad de la información, en el cual se contemple el reporte, la identificación, análisis, valoración, tratamiento y comunicación.

PARÁGRAFO 1. Es deber de todos los servidores (as) públicos (as), contratistas o terceros, reportar cualquier posible incidente, violaciones de acceso o acceso no autorizado y mal funcionamiento en el software o hardware del que se tenga conocimiento o experiencia directa, a través de la mesa de ayuda.

PARÁGRAFO 2. Está prohibido la realización de pruebas y el uso de herramientas, tales como sniffers, analizadores de protocolos y puertos, entre otros, para detectar, verificar, explorar, validar o confirmar cualquier posible vulnerabilidad o falla de seguridad sin la debida autorización por parte del responsable de seguridad de la Información o el jefe de la Oficina TIC.

ARTÍCULO VIGÉSIMO PRIMERO: - Política de Aspectos de seguridad de la información en la continuidad del negocio: La Oficina Asesora de Planeación, con el apoyo del responsable de seguridad de la información y los líderes de procesos, deberán diseñar y actualizar una metodología para la identificación de riesgos de seguridad y privacidad de la información para la continuidad de la operación de los servicios de la Unidad Administrativa Especial de Servicios Públicos. – UAESP.

PARÁGRAFO. La Oficina Asesora de Planeación, con el apoyo del oficial de seguridad de la información y los líderes de procesos, deberá elaborar el Plan de Continuidad del Negocio, incluyendo la definición de roles, responsabilidades y un plan de pruebas del mencionado plan.

ARTÍCULO VIGÉSIMO SEGUNDO: - Política de cumplimiento de requisitos legales: Todos los procesos de la Entidad deberán identificar la normativa referente a seguridad y privacidad de la información que les competa, 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, y remitirla a la Subdirección de Asuntos Legales con el objeto de consolidar y actualizar la información suministrada en la herramienta de verificación de requisitos legales.

ARTÍCULO VIGÉSIMO TERCERO: - Desarrollo de las políticas de seguridad y privacidad de la información: Todas las políticas identificadas en esta Resolución se desarrollarán de manera detallada y clara en el Manual de Políticas de Seguridad y Privacidad de la Información que deberá ser publicado y consultado en el Sistema Integrado de Gestión – SIG.

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información y se deroga la Resolución 613 de 2021".

CAPITULO III
REVISIÓN, VIGENCIA y DEROGATORIA

ARTÍCULO VIGÉSIMO CUARTO: - Revisión y Actualización: La Política General de Seguridad y Privacidad de la Información será revisada anualmente o antes si se requiere, con el fin de que sea oportuna, suficiente y eficaz.

El proceso de revisión será liderado por el Oficial de Seguridad y Privacidad de la Información, el Oficial de Protección de Datos Personales, la Oficina de Tecnologías de la Información y las Comunicaciones y deberá ser aprobada por el Comité Institucional de Gestión y Desempeño.

ARTÍCULO VIGÉSIMO QUINTO: - Publicación. Publíquese el contenido del presente acto administrativo de conformidad con los términos establecidos en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA).

ARTÍCULO VIGÉSIMO SEXTO – Recursos. Contra el contenido de la presente Resolución no procede recurso alguno, de conformidad con lo establecido en el artículo 75 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA).

ARTÍCULO VIGÉSIMO SÉPTIMO -Vigencia: La presente Resolución rige a partir de la fecha de su publicación y deroga la Resolución 613 de 2021 y las demás disposiciones que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE

Dado en Bogotá, D.C., a los quince (15) días del mes de septiembre de 2022.

LUZ AMANDA CAMACHO SÁNCHEZ
Directora General
Unidad Administrativa Especial de Servicios Públicos

Elaboró: Jerce Aurora Sandoval Macias – Oficina de Tecnologías de la Información y las Comunicaciones.
Juan Sebastián Perdomo Méndez – Oficina de Tecnologías de la Información y las Comunicaciones.

Revisó: Vanessa Rincón – Subdirección de Asuntos Legales
Swandy Arroyo Betancourt – Subdirección de Asuntos Legales

Aprobó: Etelvina Briceño Chiriví - Subdirectora de Asuntos Legales (E).
Yesly Alexandra Roa Mendoza - Jefe Oficina Asesora de Planeación.
Cesar Mauricio Beltrán López - Jefe Oficina de Tecnologías de la Información y las Comunicaciones.