UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS

RESOLUCIÓN NÚMERO 00648 DE 2023

"Por la cual se emiten directrices en la seguridad de la información en la gestión de proyectos en la Unidad Administrativa Especial de Servicios Públicos - UAESP"

EL DIRECTOR GENERAL DE LA UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS.

En ejercicio de sus facultades legales y reglamentarias, en especial las establecidas en el Acuerdo Distrital No. 257 de 2006, el Acuerdo 001 de 2012, Acuerdo 002 de 2012 y el Acuerdo No. 011 de 2014 expedido por el Consejo Directivo de la Unidad Administrativa de Servicios Públicos -UAESP, en el Decreto 059 de 2023 y,

CONSIDERANDO:

Que la Unidad Administrativa Especial de Servicios Públicos - UAESP, es una Unidad Administrativa Especial del Orden Distrital del Sector Descentralizado por Servicios, de carácter eminentemente técnico y especializado, con personería jurídica, autonomía administrativa y presupuestal y con patrimonio propio, adscrita a la Secretaría Distrital del Hábitat (Acuerdo Distrital No 257 de 2006), que tiene por objeto "*Garantizar la prestación, coordinación, supervisión y control de los servicios de recolección, transporte, disposición final, reciclaje y aprovechamiento de residuos sólidos, la limpieza de vías y áreas públicas; los servicios funerarios en la infraestructura del Distrito y del servicio de alumbrado público*".

Que el artículo 4 de la Ley 1341 de 2009 "*Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC y se crea la Agencia Nacional de Espectro y se dictan otras disposiciones*", señala que el Estado intervendrá en el sector de las tecnologías de la información y las comunicaciones, en desarrollo de los principios de intervención contenidos en la Constitución Política, de la siguiente manera:

> "*ARTÍCULO 4°.* Intervención del Estado en el sector de las Tecnologías de la Información y las Comunicaciones. *En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines:*
>
> *(...)*
>
> *11. Promover la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones.*"

Que la Ley Estatutaria 1581 de 2012 "*Por la cual se dictan disposiciones generales para la 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 de acuerdo con lo señalado en el artículo 18 de la mencionada Ley, es deber de los encargados del tratamiento de la información conservarla en condiciones de seguridad, como se menciona a continuación:

> "***Artículo 18. Deberes de los Encargados del Tratamiento.*** *Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *(...)*
>
> *b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*".

"Por la cual se emiten directrices para la seguridad de la información en la gestión de proyectos en la Unidad Administrativa Especial de Servicios Públicos - UAESP"

Que por otro lado, el Acuerdo 001 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"*, establece en el artículo séptimo las funciones de la Oficina de Tecnologías de la Información y las Comunicaciones, de la siguiente manera:

"(...)

1. *Asesorar a la Dirección General y dependencias de la Unidad en materia informática y de Telecomunicaciones.*
2. *Planear y controlar los recursos informáticos y de telecomunicaciones para satisfacer las necesidades y requerimientos de los usuarios y clientes UAESP, de conformidad con las políticas, metodologías, estándares informáticos, de calidad, seguridad y la normatividad vigente.*
3. *Realizar estudios, investigación y análisis de tendencias tecnológicas para su posible aplicación en la Unidad, actualización e implantación de estándares informáticos y de calidad de toda la plataforma tecnológica.*
4. *Formular el Plan Estratégico de la informática y las telecomunicaciones y el Plan de Acción de la Oficina de acuerdo con las políticas institucionales, el modelo de operación por procesos, tecnologías apropiadas y metodología adoptada.*
5. *Adaptar las políticas que en materia de tecnologías de la Información y las Comunicaciones dicten los gobiernos nacional y Distrital.*
6. *Administrar los sistemas de información, aplicativos ofimáticos y bases de datos, adquiridos o desarrollados internamente para atender los requerimientos de información de los procesos y dependencias de la Unidad de acuerdo con la tecnología disponible, metodología, herramientas adoptadas y procedimientos establecidos.*
7. *7. Dirigir el funcionamiento, mantenimiento y adecuación de los equipos redes y elementos que conforman la plataforma tecnológica de la Unidad."*

Que en el artículo 10 del Decreto 2573 de 2014 *"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones"*, establece los plazos, los sujetos obligados del orden nacional y los sujetos obligados del orden territorial, para implementar las actividades establecidas en el Manual de Gobierno en Línea, ahora Manual de Gobierno Digital, el cual está establecido en el Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capitulo 1, titulo 9, parte 2, libro 2), para la Implementación de la Política de Gobierno Digital, en los componentes de TIC para servicios, TIC para el Gobierno abierto, TIC para la Gestión, Seguridad y Privacidad de la Información.

Que el Decreto 1083 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública"*, en su artículo 2.2.22.2.1. establece las políticas de gestión y desempeño Institucional, entre las que se encuentran *"Gobierno Digital"*, antes *"Gobierno en Línea"* y *"Seguridad Digital"*; adoptadas y desarrolladas en el Modelo Integrado de Planeación y Gestión MIPG de la UAESP.

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"*, incorpora la compilación y racionalización de las normas de carácter reglamentario que rigen en el sector, con el objeto de establecer los lineamientos generales de la Política de Gobierno Digital, entendida como el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con la finalidad de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio.

Así mismo, el Decreto en mención establece en su artículo 2.2.17.1.6 el principio de Seguridad, privacidad y circulación restringida de la información indicando que, toda la información de los usuarios que se genere, almacene, transmita o trate en el marco de los servicios ciudadanos digitales, deberá ser protegida y custodiada bajo los más estrictos esquemas de seguridad digital y privacidad con miras a garantizar la autenticidad, integridad, disponibilidad, confidencialidad, el acceso y circulación restringida de la

"Por la cual se emiten directrices para la seguridad de la información en la gestión de proyectos en la Unidad Administrativa Especial de Servicios Públicos - UAESP"

información, de conformidad con lo estipulado en el habilitador transversal de seguridad de la información de la Política de Gobierno Digital.

Que en virtud de lo anterior, las entidades distritales deben contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio, en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital, que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, se deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Que la Resolución No. 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*", tiene por objeto definir y adoptar las políticas específicas para el uso de la información en la Unidad Administrativa Especial de Servicios Públicos – UAESP. Así mismo, el objetivo general de esta política es 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.

Que la norma ISO 27001 versión 2022, proporciona un marco de trabajo reconocido internacionalmente para la gestión de la seguridad de la información, toda vez que se efectuaron algunos cambios en la lista y clasificación de controles de seguridad de la información como la identificación de los procesos y sus interacciones, los objetivos deben estar documentados y estar disponibles como "información documentada" para todas las partes interesadas, también las organizaciones deben definir criterios para los procesos operativos y controlar esos procesos de acuerdo con los criterios, evaluar y monitorear sus controles, los cuales deben ser comparables y reproducibles para que la organización pueda analizar las tendencias y las evaluaciones internas, también deben cubrir todos los requisitos de la organización, no sólo la norma ISO 27001.

Que en concordancia, con lo expuesto, teniendo en cuenta que la seguridad de la información es un aspecto fundamental en la gestión de proyectos en la Unidad Administrativa de Servicios Públicos – UAESP, deben dictarse directrices de seguridad de la información en los proyectos que desarrolle esta entidad para garantizar la seguridad digital y la privacidad de la información de las partes interesadas que interactúan dentro de los mismos.

Que para lo anterior es fundamental que los objetivos de la política de seguridad y privacidad de la información se incluyan en los objetivos del proyecto o se establezcan elementos que permitan afianzar dicha política, se identifiquen y gestionen los riesgos de seguridad de la información y se clasifiquen los activos de información para establecer los controles necesarios.

Que la Subdirección de Asuntos Legales, realizó el respectivo control de legalidad, el cual recae única y exclusivamente sobre la revisión de las normas que sustentan el acto administrativo, la vigencia de las mismas, su conducencia, pertinencia y/o aplicabilidad dentro de los casos o situaciones objeto de decisión, así como que dicha decisión se profiera acorde a derecho, en tal sentido, no le compete ni avala la revisión de datos técnicos, financieros, contables o de competencia del área misional responsable de la elaboración del acto.

Que en mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO: Emitir las directrices para la seguridad de la información a los responsables de la gestión de los proyectos en la Unidad Administrativa Especial de Servicios Públicos -UAESP, las cuales se señalan a continuación:

"Por la cual se emiten directrices para la seguridad de la información en la gestión de proyectos en la Unidad Administrativa Especial de Servicios Públicos - UAESP"

a) Incluir los objetivos de la seguridad de la información, en los objetivos de todos los proyectos de la Unidad Administrativa Especial de Servicio Públicos - UAESP.

b) Identificar y clasificar en cada proyecto que sea responsabilidad de la Unidad Administrativa Especial de Servicios Públicos - UAESP, los activos de información de acuerdo con los criterios definidos por la entidad, o aquellos que mejor se ajusten a las necesidades del proyecto o a las buenas prácticas de seguridad de la información.

c) Identificar y gestionar en todos los proyectos, los riesgos de seguridad de la información utilizando la *metodología que defina para el efecto la entidad* o aquella que mejor se ajuste a las necesidades del proyecto o a las buenas prácticas de seguridad de la información.

d) Integrar la seguridad de la información en todas las fases del proyecto, desde su planificación hasta su evaluación, implementando medidas de seguridad adecuadas y oportunas en cada etapa del proyecto para garantizar la protección de la información y los datos personales. La seguridad de la información debe ser considerada como un factor clave en todas las decisiones relacionadas con el proyecto y ser parte integral de la gestión de proyectos en la Unidad Administrativa Especial de Servicios Públicos - UAESP.

e) Los responsables de la gestión de los proyectos deben establecer mecanismos de monitoreo de los lineamientos de seguridad de la información en la gestión de proyectos de la Unidad Administrativa Especial de Servicios Públicos - UAESP.

Los citados mecanismos deben medir el grado de cumplimiento de las directrices contenidas en este artículo, identificar desviaciones y tomar las medidas necesarias para corregirlas. Así mismo, se debe asegurar que se protejan adecuadamente los datos personales y se respeten los derechos de privacidad y protección de datos personales de las personas cuya información sea procesada o almacenada en el marco de los proyectos de la UAESP.

f) Los responsables de la gestión de proyectos en la Unidad Administrativa Especial de Servicios Públicos -UAESP deben establecer un conjunto de controles de seguridad en los activos de la información, estos deben ser apropiados, que aborden los riesgos y protejan los activos de información. Para garantizar una gestión efectiva y eficiente de la seguridad de la información en la UAESP, incluida la protección de datos personales, esos controles deben ser proporcionales a la naturaleza del riesgo y al nivel de criticidad de los activos de información, y pueden incluir, entre otros:

- **Control de acceso y autenticación**: La adopción de medidas que regulen el acceso físico y lógico a los sistemas y recursos de información, como la autenticación multifactor, contraseñas robustas, la gestión de identidades y el control de acceso basado en roles.

- **Control en el respaldo y recuperación de datos**: La implementación de procedimientos y sistemas de respaldo de información periódicos, así como la creación de planes de contingencia y recuperación ante incidentes, con el fin de asegurar la continuidad del negocio en caso de fallos o desastres.

- **Control en el monitoreo y detección de intrusiones**: La utilización de herramientas de monitoreo y detección de intrusiones en tiempo real, que permitan identificar y responder rápidamente a actividades sospechosas o no autorizadas, así como la implementación de sistemas de registro de auditoría y análisis de registros de eventos.

- **Control en las actualizaciones y parches de seguridad**: La aplicación regular de actualizaciones y parches de seguridad en los sistemas y software utilizados en el proyecto, con el fin de corregir vulnerabilidades conocidas y fortalecer la protección contra amenazas emergentes.

- **Control en las Pruebas de seguridad**: La realización periódica de pruebas de seguridad, como pruebas de penetración y análisis de vulnerabilidades, para identificar y corregir posibles brechas en la seguridad.

"Por la cual se emiten directrices para la seguridad de la información en la gestión de proyectos en la Unidad Administrativa Especial de Servicios Públicos - UAESP"

- **Concientización y capacitación en seguridad**: La implementación de programas de concientización y capacitación en seguridad de la información para todos los involucrados en el proyecto, con el objetivo de promover una cultura de seguridad y garantizar que los usuarios sean conscientes de las buenas prácticas de seguridad.

- **Control en la Protección de datos personales**: La implementación de medidas técnicas y organizativas adecuadas para proteger los datos personales, cumpliendo con las leyes y regulaciones de privacidad aplicables. Esto puede incluir el cifrado de datos, el acceso restringido a la información personal, la pseudonimización o anonimización de datos cuando sea posible, y la implementación de políticas y procesos para la gestión adecuada de los datos personales.

- **Control en el consentimiento y derechos de los interesados**: El establecimiento de mecanismos para obtener el consentimiento informado de los individuos cuyos datos personales son procesados en el proyecto, así como para garantizar el ejercicio de sus derechos de privacidad, como el acceso, rectificación, cancelación y oposición.

ARTÍCULO SEGUNDO: El cumplimiento de las directrices establecidas en la presente Resolución es obligatoria para todos los responsables de la gestión de proyectos en la Unidad Administrativa Especial de Servicios Públicos – UAESP, de tal manera que se asegure la protección de la información en todo momento en la Entidad. Por lo anterior, deben aplicarse independientemente de la metodología y tipo de proyecto, garantizando la implementación de medidas de seguridad de la información en todas las etapas de los proyectos.

ARTÍCULO TERCERO: La presente Resolución rige a partir de la fecha de su publicación.

ARTÍCULO CUARTO: En contra de la presente Resolución no proceden recursos de conformidad con la Ley 1437 de 2011.

PÚBLIQUESE Y CÚMPLASE

Dada en Bogotá, D.C., a los 16 AGO. 2023

JUAN CARLOS LÓPEZ LÓPEZ
DIRECTOR GENERAL

Proyectó: Juan Sebastián Perdomo Méndez – Profesional Universitario Oficina TIC.
Revisó: Carlos Roberto Tarazona Alvarez / Abogado Contratista UAESP – 214 - 2023 / Subdirección de Asuntos Legales
Swandy Arroyo Betancourt / Profesional Subdirección de Asuntos Legales
Nancy Daniela Rodríguez Ortiz – Abogada contratista Cto 345 de 2023 / Subdirección de Asuntos Legales
Wilson Capera Rodriguez – Contratista / Dirección General
Aprobó: Cesar Maurício Beltrán López – Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones
Arturo Galeano Ávila – Subdirector de Asuntos Legales.
Yesly Alexandra Roa Mendoza – Jefe de la oficina Asesora de Planeación
Miguel Antonio Jiménez Portela – Subdirector Administrativo y Financiero