RESOLUCIÓN No. 00734 DE JUNIO 18 DE 2024

"Por medio de la cual se establece la Política de Tecnologías de Información y Comunicaciones – Política TIC - de la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EICE E.S.P".

LA AGENTE ESPECIAL DE LA EMPRESA DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE YOPAL E.I.C.E. E.S.P., EN ADELANTE LA EMPRESA, EN USO DE SUS FACULTADES LEGALES Y ATRIBUCIONES ESTATUTARIAS, Y

CONSIDERANDO:

Que la Superintendencia de Servicios Públicos Domiciliarios ordenó la toma de posesión de la EMPRESA DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE YOPAL EICE ESP (EAAAY EICE ESP) mediante la Resolución No. SSPD – 20231000620935 del 04/10/2023.

Que la Empresa de Acueducto, Alcantarillado y Aseo de Yopal es una empresa Industrial y Comercial del estado del orden municipal, creada mediante Decreto 026 de 1997 y el Acuerdo No. 009 de 2010.

Que la Superintendencia de Servicios Públicos Domiciliarios determinó el objeto de la toma de posesión de la EMPRESA DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE YOPAL EICE ESP (EAAAY EICE ESP) mediante la Resolución No. SSPD – 202410000479785 del 02/02/2024, la cual determinó que la modalidad de la toma de posesión será la de Administración.

Que mediante Resolución No. 0520 del 18 de mayo de 2018, LA EMPRESA adopta el Modelo Integrado de Planeación y Gestión – MIPG – y en el artículo No. 2, numeral 5 se establece la Política de Gobierno Digital; TIC para servicios y TIC par gobierno abierto, acceso a la información pública y lucha contra la corrupción.

Que el Ministerio de la Información y las Comunicaciones (MinTIC), a través del Decreto 1008 del 14 de junio de 2018 publicó la política de Gobierno Digital, cuyo objetivo es incentivar el uso y aprovechamiento de las TICs para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en entorno de confianza digital. Y que dicho decreto forma parte del Modelo Integrado de Planeación y Gestión – MIPG y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para el Resultado con Valores, que busca promover una adecuada gestión interna de las entidades y un buen relacionamiento con el ciudadano a través de la participación y prestación de

servicios de calidad. Este Decreto da paso a la Política de Gobierno Digital y deja atrás la Estrategia de Gobierno en Línea.

Que el numeral 3.2.1.3. del manual operativo del sistema de gestión MIPG versión 2 que trata la Política de Gobierno Digital, busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones – TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

Que mediante Resolución No. 1484 del 28 de octubre de 2019, LA EMPRESA adoptó la política de Gobierno Digital, TIC para el estado y TIC para la sociedad de la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EIEC ESP, en maco del Modelo Integrado de Planeación y Gestión – MIPG.

Que mediante Resolución No. 1485 del 28 de octubre de 2019, LA EMPRESA adoptó la política de Gestión de Riesgos de Seguridad Digital parra la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EIEC ESP, complemento a la resolución No. 0525 del 18 de mayo de 2018 Política de Gestión del Riesgo.

Que mediante Resolución No. 00732 de junio 18 de 2024, LA EMPRESA actualizó el Plan Estratégico de Tecnologías de Información (PETI), ampliándolo al ámbito de las comunicaciones, con lo cual estableció el Plan Estratégico de Tecnologías de Información y Comunicaciones (PETIC) para el período comprendido entre el año 2024 y el 2026.

Que el PETIC establece, en el marco de Gobierno, la definición de una única política de TIC para LA EMPRESA que integre los componentes básicos de las tecnologías de la información y las comunicaciones con el cumplimiento de la normatividad vigente y la gestión de riesgos de seguridad informática y la inclusión de lineamientos básicos y claros en cada uno de los pilares que las conforman.

Que en virtud de lo anterior, la Política de TIC integrará la Política de Gobierno Digital, TIC para el Estado y TIC para la sociedad en la Empresa Acueducto, Alcantarillado y Aseo de Yopal EICE ESP con la Política de Gestión de Riesgos de Seguridad Digital en la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EICE ESP, las complementa y amplia, ajustándolas a las necesidades actuales de LA EMPRESA y en cumplimiento de la normatividad vigente.

En virtud de lo expuesto, la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EICE ESP,

RESUELVE

ARTÍCULO PRIMERO. GENERALIDADES. Adóptese las siguientes generalidades como marco de actuación de la Política de TIC. Las políticas, en LA EMPRESA, tienen como objeto ***orientar la acción*** y son fundamentales en la administración para lograr una adecuada "*delegación de autoridad*".

Se puede decir que una política es:

Una guía para las decisiones administrativas.

El punto de vista de la organización.

Un modo de orientación y dirección de los diversos sectores de la gestión (acción y efecto de administrar)

Criterios generales que tienen por objeto orientar la acción.

Se puede decir que una política tiene como función:

Precisar la filosofía de LA EMPRESA, para la operación de los procesos.

Establecer un marco de actuación que permita controlar las delegaciones administrativas de autoridad.

Fijar los límites para que las personas habilitadas pueden tomar decisiones y realizar actos administrativos.

Anticipar condiciones y situaciones e indicar cómo enfrentarse a ellas.

Se puede decir que una política debe:

Describir el concepto representativo del contenido de la misma.

Establecer en forma clara, precisa y concisa el criterio que orientará a los participantes.

Servir de guía en la toma de decisiones respeto a las acciones a seguir para el logro de los objetivos del proceso.

Evitar tanto la asignación de funciones y/o la descripción de actividades, como la limitación temporal de autoridad.

Se puede decir que una política debe contener:

Referencia a un proceso que se debe normar.

Un inicio con el sujeto de la actividad a normar, es decir, contestar ¿qué se debe?

Continuar con el verbo "debe" o "debe ser", conjugando en forma impersonal.

Finalizar con el objeto directo ¿para qué?

Si se requiere, se aclarará con un completo indirecto o circunstancial.

Preferentemente debe expresarse en un párrafo de máximo 5 a 7 renglones.

ARTÍCULO SEGUNDO*: DEFINICIONES*. Adóptese las siguientes definiciones en el marco de la Política TIC de LA EMPRESA para que sirvan de referente aclaratorio para dicha Política y su aplicación en LA EMPRESA.

- **Acuerdos de Niveles de Servicio (ANS).** Es un contrato entre dos partes, el proveedor del servicio (en este caso la Oficina de TIC) y el *cliente*, donde se definen: ***1)*** los servicios a entregar, ***2)*** las métricas asociadas con estos servicios, ***3)*** niveles de servicio aceptables e inaceptables, ***4)*** *las* responsabilidad por parte la Oficina de TIC y el *cliente*, ***5)*** los costos de la implantación, operación y soporte, y ***6)*** las acciones a tomar en circunstancias específicas.

- **Arquitectura Empresarial:** Es un mecanismo utilizado para traducir las necesidades de negocio en soluciones tecnológicas, está conformada por 3 pilares o puntos de vista independientes e interrelacionados:

  a) Punto de vista del negocio: Este punto de vista trata con aspectos funcionales, procesos y organización de LA EMPRESA. Está relacionado con el marco de procesos que se toma como referencia en LA EMPRESA para la definición y operación de sus procesos.

  b) Punto de vista de Información: Está relacionado con la información requerida para el desarrollo de los procesos de LA EMPRESA, las reglas de negocio aplicadas a las necesidades de información y los mecanismos de integración de la información a través de los diferentes procesos. La arquitectura de información conlleva modelos de negocio, modelos organizacionales, modelos de procesos, modelos de objetos y modelos de datos.

  c) Punto de vista tecnológico TIC: Está relacionado con los componentes de tecnología (Hardware, Software, Metodologías, Comunicaciones, Seguridad) que soportan los procesos misionales (de la cadena de valor) y los no misionales (de soporte administrativo) de LA EMPRESA.

- **Arquitectura de una Aplicación**: Define por cada aplicación, los diversos módulos y componentes y la interrelación, interfases y dominios de gestión de cada uno de ellos, de acuerdo con la arquitectura de sistemas.

- **Arquitectura Objetivo**: La arquitectura objetivo es la visión en el mediano y largo plazo de la evolución integrada de la arquitectura empresarial, de acuerdo con la estrategia y metas de LA EMPRESA, así como las tendencias organizacionales y tecnológicas en el sector en el que Ésta desarrolla su objeto social.

- **Arquitectura Tecnológica**: Es un conjunto de guías (conceptos, principios, reglas, patrones, estándares) utilizados para construir nuevas capacidades en TIC al interior de LA EMPRESA.

- **Cliente**. Puede ser un empleado, un contratista, un usuario/suscriptor o un cliente de LA EMPRESA que hace uso de los servicios de TIC. Es un Cliente Interno cuando tiene una relación laboral con LA EMPRESA y es un Cliente Externo cuando la relación está determinada por un contrato de prestación de servicio (hacia/desde LA EMPRESA).

- **Gobierno TIC**: Es una metodología de trabajo orientada a proveer las estructuras que unen los procesos de los recursos de información TIC con las estrategias y los objetivos de LA EMPRESA. El Marco de Gobierno para las TIC integra e institucionaliza las mejores prácticas de planificación y organización, adquisición e implementación, entrega de servicios y soporte, y monitoreo del rendimiento de TIC para asegurar que la información de la empresa y las tecnologías relacionadas soportan los objetivos del negocio.

- **Información pública.** Es toda información que LA EMPRESA genere, obtenga, adquiera, o controle en su calidad de obligado.

- **Información clasificada.** Es la información que estando en poder o custodia de LA EMPRESA en su calidad de obligado, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se esté inmerso en los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional), esto bajo circunstancias legítimas y necesarias.

- **Información reservada.** Es aquella información que estando en poder o custodia de LA EMPRESA en su calidad de obligado, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).

- **Infraestructura TIC:** Plataformas de Tecnologías de Información y Telecomunicaciones (hardware y software) compuesta por: ***1)*** las redes de voz, datos y video, ***2)*** los servidores de la red y de aplicaciones, ***3)*** los dispositivos de almacenamiento masivo, ***4)*** los dispositivos de seguridad, ***5)*** las impresoras y scanner de la red, ***6)*** el hardware y software de usuarios finales, ***7)*** las herramientas y/o software básico que se requiere para el desarrollo y uso de

los sistemas de información y ***8)*** el sistema de administración centralizada de la misma infraestructura.

- **Marco de Gobierno de TIC:** *"Es el conjunto de responsabilidades y prácticas ejercidas por el consejo y la dirección ejecutiva con el objetivo de proporcionar dirección estratégica, asegurar que los objetivos se alcanzan, que los riesgos se gestionan adecuadamente y verificar que los activos de la empresa se utilizan de una manera responsable"* (IT - Governance Institute).

- **Modelo de Seguridad y Contingencia TIC:** Es el conjunto de lineamientos, normas, procedimientos y estándares de seguridad y contingencia que contribuyen al desarrollo armónico de la infraestructura TIC y marca claramente las directrices que permitirán alcanzar la confidencialidad, integridad y disponibilidad de la información de LA EMPRESA, así como la continuidad de sus operaciones ante un evento que las interrumpa.

- **PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES (PETIC):** Es el programa de desarrollo y evolución de las TIC en LA EMPRESA, éste consolida la visión de TIC a la luz de la estrategia empresarial y la correspondiente estrategia de TIC, así como la identificación de los proyectos TIC, con su respectivo presupuesto de Inversión y gastos en todo su ciclo de vida.

- **PLAN DE CONTINGENCIA Y PLAN DE CONTINUIDAD:** Mientras que el Plan de Contingencia de TICs está relacionado con las acciones que debe ejecutar el área de TIC para la recuperación o el restablecimiento de los servicios que presta a LA EMPRESA, sus usuarios y clientes; el Plan de Continuidad se refiere a las actividades y/o procedimientos que llevan a cabo los procesos cuando las plataformas tecnológicas no están disponibles por un la ocurrencia y/o materialización de un riesgo que las dejan inoperantes

- **Seguridad Informática:** Es la protección exclusiva de las plataformas informáticas; se enfoca primordialmente en herramientas, tecnología y servicios de TI.

- **Seguridad de la Información:** Se refiere a la protección de la información independiente del medio o sitio en el cual se encuentre almacenada, de los sistemas tecnológicos para procesarla o de las personas que la administran.

- **Servicio TIC:** Es el resultado de la interrelación de los procesos, los colaboradores y la infraestructura tecnológica que se presta bajo condiciones estándar o especiales para satisfacer y exceder las expectativas del cliente interno o del negocio bajo el cumplimiento de los Acuerdos de Niveles de Servicio pactados.

- **Sistemas de Información:** Es el conjunto de componentes de Tecnología de información que en forma interrelacionada con los datos generan información que ayudan a la operación del negocio o a la toma de decisiones que apoyan a el cumplimiento de los objetivos de las áreas y las estrategias del negocio.

- **Solución TIC:** Es el conjunto o sistema de tecnología compuesto por uno o varias aplicaciones y la infraestructura requerida para que dichas aplicaciones puedan operar.

- **Soporte de la Infraestructura TIC:** Comprende labores de mantenimiento y evolución realizadas en el hardware de TIC que están orientadas a lograr el buen funcionamiento del mismo.

- **Software Básico:** Es el software en configuración estándar que debe estar instalada en todos los computadores conectados a la red de datos de LA EMPRESA. Está conformado por:

  Sistema Operativo: Versión de sistema operativo Windows estable y disponible en el mercado

  Antivirus actualizado

  Agentes de gestión

  Control automático de inventario.

  Instalación centralizada de software.

  Herramienta para control remoto.

  Herramientas de automatización de oficina: 1) Microsoft Office (Excel, Word, Outlook). 2) Internet Explorer. 3) Visores: Presentaciones, Diagramas, Archivos tipo PDF, Videos y Audio.

  Igualmente las herramientas de desarrollo y de administración instaladas en los servidores.

- **Software Específico:** Es cualquier aplicativo y/o software especializado que apoya exclusivamente alguna de las actividades de los diferentes procesos de LA EMPRESA; se instala en las plataformas Adquiridas específicamente para dicha

función o en los computadores de los usuarios que lo requieran en los diferentes procesos.

- **Software Corporativo:** Son los aplicativos y/o el software de uso general para toda LA EMPRESA; generalmente apoyan los procesos no misionales (de soporte del negocio).

- **Tecnologías de Información y Comunicaciones (TIC):** Las TIC son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes, es decir, son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos, tales como: computadoras, teléfonos móviles, televisores, reproductores portátiles de audio y video o consolas de juego entre otros.

- **Uso de las TIC:** Planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de las TIC para cumplir con las necesidades del negocio. Incluye tanto la demanda como la oferta de servicios TIC por dependencias internas, unidades especializadas de TIC, proveedores externos y empresas prestadoras de servicios públicos.

- **Usuarios de la Información:** Se consideran usuarios de la información aquellos que requieren acceso a ésta y que se encuentran realizando alguna actividad oficial relacionada con la misión de LA EMPRESA. Entre estos se encuentran: empleados, contratistas, practicantes, temporales, consultores, asesores, usuarios/suscriptores, clientes y sus empleados, proveedores, canales de distribución o cualquier entidad que utilice los sistemas de información o la infraestructura tecnológica en cumplimiento de las responsabilidades asignadas.

- **Usuarios TIC:** Son todas aquellas personas que hacen uso de los servicios de TIC para la ejecución de sus responsabilidades en LA EMPRESA.

ARTÍCULO TERCERO. FUNDAMENTOS DE LA POLÍTICA DE TIC. Adóptese los siguientes fundamentos de la Política de TIC*:* La política de TIC, como parte del Marco de Gobierno para las TIC de LA EMPRESA, busca mantener la continuidad del servicio, el crecimiento ordenado y equilibrado de la infraestructura TIC, la optimización de los recursos tecnológicos y el uso efectivo de los mismos por parte de los usuarios, todo esto enmarcado en la normatividad aplicable en el ámbito de las Tecnologías de la Información y las Comunicaciones, la seguridad informática, la minimización del riesgo informático y toda la normatividad aplicable a LA EMPRESA.

A continuación se describen los principales fundamentos de las políticas TIC en LA EMPRESA.

Alineación al pensamiento estratégico de LA EMPRESA. La actuación del proceso de TICs se basa en la alineación y apoyo al pensamiento estratégico de LA EMPRESA.

Los lineamientos proporcionan los elementos y conceptos que deben ser considerados y van en línea con el contenido de la política TIC, precisando la interpretación y comprensión de la misma. Es decir, los lineamientos son precisiones sobre la forma en que debe interpretarse y aplicarse la política TIC al interior de LA EMPRESA.

Los procedimientos, son el conjunto de acciones que operacionalizan la Política y sus lineamientos. Estos procedimientos están muy relacionados con las actividades operativas definidas en los procesos, su definición está a cargo del área de TIC con el apoyo de los procesos que ella así lo requiera y decida.

ARTÍCULO CUARTO. ALCANCE DE LAS POLÍTICAS TIC. Establézcase el alcance de las Políticas TIC *en los siguientes términos:* La política TIC será aplicada sin excepciones en todas las áreas y por todos los funcionarios y contratista que laboren en cualquier momento para LA EMPRESA. Adicionalmente, la política de TIC ...

- Hace parte del marco de gobierno y de actuación de la organización TIC.
- Define y armoniza las relaciones con los usuarios TIC.
- **Es de estricto cumplimiento** y la violación a la misma acarreará para quien la infrinja las sanciones disciplinarias establecidas en el reglamento interno de LA EMPRESA.
- Se aplicará igual a los usuarios externos de las TIC, para lo cual se incluirá explícitamente en el contrato que LA EMPRESA suscriba con ellos, la sanción a que dé lugar la violación de las políticas y procedimientos de seguridad de LA EMPRESA.
- Se aplicará en todas las actividades relacionadas con los procesos asociados a TICs o que hagan uso de éstas en LA EMPRESA.

ARTÍCULO QUINTO. POLÍTICA DE TIC: Establézcase la Política de TIC como: La Gestión de Tecnología de Información y Comunicaciones permite a LA EMPRESA disponer de la tecnología (hardware, software, telecomunicaciones e información) requerida por los diferentes actores que intervienen en su operación y adaptarse oportunamente a los cambios generados por el entorno, sus procesos y la visión de negocio, operando bajo un modelo de prestación de servicios con las mejores prácticas de mercado como una forma de apalancar la sostenibilidad y el crecimiento empresarial de manera segura en ambientes digitales.

ARTÍCULO SEXTO. LINEAMIENTOS. Adóptese los siguientes pilares para los Lineamientos de la Política de TICs:

- Gestión de Recursos.
- Plan de Continuidad.
- Reposición de equipos.
- Sistemas de Información.
- Gestión de soluciones y contratos.
- Propiedad Intelectual.
- Usuarios TIC.
- Seguridad Informática o Seguridad de la Información.

ARTÍCULO SÉPTIMO. LINEAMIENTOS PARA LA GESTIÓN DE RECURSOS: Establézcase los lineamientos para la Gestión de los Recursos TICs, entendida ésta gestión como la manera en que se debe llevar a cabo la operación de TICs en LA EMPRESA, su alineación con el Plan Estratégico y la Estrategia que esté definida por LA EMPRESA. En particular debe considerar:

- La elaboración de un Plan Estratégico de TIC en LA EMPRESA, que consolide la visión de TIC a la luz de la estrategia empresarial y la correspondiente estrategia de TIC, así como la identificación de los proyectos TIC requeridos, con su respectivo presupuesto de Inversión y gastos que se generan durante su ciclo de vida.
- El proceso TIC, como responsable de la infraestructura TIC de LA EMPRESA, debe definir los respectivos proyectos para modernización y expansión de la infraestructura para que ésta responda al crecimiento **vegetativo** de LA EMPRESA y a las nuevas necesidades de infraestructura de los nuevos servicios y sistemas. Esta expansión debe hacerse de una manera gradual y articulada con las propuestas de valor del negocio.
- El desarrollo de las TIC debe basarse en el apoyo en la obtención del logro de las estrategias de negocio de LA EMPRESA, buscando conseguir ventajas

competitivas, mayor productividad de los procesos y flexibilidad ante los cambios del negocio.

- La expansión de la infraestructura TIC debe hacerse con base en estudios de capacidad.
- Las decisiones sobre las plataformas de almacenamiento se tomarán con base en criterios financieros, tecnológicos, funcionales y la perspectiva de los usuarios alineados con un proceso de Administración del Ciclo de vida de la Información.
- Para la puesta en producción, todo proyecto de cambio a la infraestructura de TIC estará acompañado de su respectiva autorización, previo cumplimiento de las pruebas y su aseguramiento de calidad.
- Los equipos suministrados por LA EMPRESA, computadores de escritorio y dispositivos móviles (incluye computadores portátiles), no deben ser objeto de alteraciones en su hardware. Toda modificación a los equipos debe ser autorizada y realizada por personal de soporte técnico de los equipos de trabajo de la Oficina de TICs o quien haga sus veces.

ARTÍCULO OCTAVO. PLAN DE CONTINGENCIA Y PLAN DE CONTINUIDAD. Establézcase los siguientes lineamientos para el *Plan de Contingencia y Plan de Continuidad* de LA EMPRESA.

PLAN DE CONTINGENCIA:

- La Oficina de TIC, o quien haga sus veces, se encarga de elaborar el plan de contingencia de TIC, es decir, define las acciones que debe ejecutar para la recuperación o el restablecimiento de los servicios que presta a LA EMPRESA, sus clientes y asociados.
- El plan de contingencia deberá contemplar toda la tecnología que está en operación y que es necesaria para la prestación de los servicios TIC.
- El plan de contingencia deberá definir el tiempo mínimo de recuperación del servicio en condiciones de operación limitada y el tiempo máximo de recuperación en condiciones de operación plena para las diferentes áreas de LA EMPRESA.

PLAN DE CONTINUIDAD:

- Las diferentes áreas de LA EMPRESA se encargan de elaborar el plan de continuidad de cada proceso a su cargo en caso de presentarse alguna contingencia, es decir, cada una (y en conjunto) definen las acciones que deben ejecutar en sus procesos para garantizar que LA EMPRESA sigue prestando sus servicios mientras la Oficina de TIC, o quien haga sus veces, está ejecutando la recuperación o el restablecimiento de los servicios de TIC.
- El plan de continuidad deberá indicar la forma en que cada proceso opere en caso de activarse la contingencia por parte de la Oficina de TIC, o quien haga sus veces.

- Cada líder funcional de módulo será el encargado de coordinar la creación y actualización de los planes de contingencia para cada módulo que esté a su cargo, indicando en ellos temas como: a) En qué momento se activa el Plan de Continuidad; b) Quién puede activar el Plan; c) La coordinación con la Oficina de TIC, o quien haga sus veces, para alinear los sistemas de información con los procesos una vez se reestablezca el servicio afectado por la activación de una contingencia.
- Toda plataforma TIC, sistema de información, conjunto de datos, debe poseer y mantener estrategias de confiabilidad, disponibilidad y recuperabilidad que le permitan mantener la continuidad de la tecnología, de acuerdo con las necesidades y requerimientos de los procesos de negocio que soporta
- Los nuevos desarrollos o adquisiciones de soluciones TIC deben considerar los aspectos de continuidad dentro de las especificaciones técnicas mínimas exigidas a los proveedores, es decir, contar con un Plan de recuperación definido y que tenga presente la clasificación de criticidad del modelo de datos, y/o los módulos del software que lo componen.

ARTÍCULO NOVENO. REPOSICIÓN DE EQUIPOS. Establézcase los siguientes lineamientos para la ***REPOSICIÓN DE EQUIPOS*** al interior de LA EMPRESA, la que deberá considerar:

- Los criterios técnicos, funcionales y económicos son los que determinan la reposición de los equipos y otras tecnologías de la infraestructura TIC en LA EMPRESA.
- La reposición de las plataformas TIC debe hacerse teniendo en cuenta principalmente las limitaciones que éstas presenten en su desempeño y que comprometan el cumplimiento de los ANS pactados con los usuarios y/o clientes de LA EMPRESA.
- Para la reposición del software se debe tener en cuenta los cambios de versiones de los proveedores y los tiempos límites de soporte que estos presten a las versiones antiguas
- El porcentaje de ocupación de CPU en un servidor INTEL no debe superar el umbral de 60-70% y un servidor RISC no debe superar el 50-60% de uso de CPU. Esto implica que cuando se llegue a estos límites, la Oficina de TICs, o quien haga sus veces, deberá iniciar los procesos internos requeridos para realizar la contratación de capacidades adicionales de procesamiento.

ARTÍCULO DÉCIMO. SISTEMAS DE INFORMACIÓN. Establézcase los siguientes lineamientos para el manejo de los Sistemas de Información en LA EMPRESA, así:

- El software básico y los sistemas de información deben ser gestionados como un activo de LA EMPRESA.

- Las herramientas para el desarrollo de sistemas de información sólo deben ser usadas por personas que cumplan funciones de desarrollo de software en el proceso de TIC.
- El diseño de los Sistemas de Información debe contemplar criterios para diferenciar la información transaccional de la información histórica de tal forma que se puedan guardar en una infraestructura de almacenamiento jerárquica con diferentes niveles de disponibilidad y costo.
- Para el desarrollo de los Sistemas de Información se definirán los requerimientos de almacenamiento en los diferentes ambientes de desarrollo, prueba y producción.
- El usuario TIC es responsable por el cuidado de los elementos de la infraestructura TIC (hardware y software) puesta a su disposición e informará oportunamente cualquier novedad al respecto.
- En la medida de lo posible, el diseño de los sistemas de información se deben contemplar algoritmos de recorte de información.
- El proceso de TIC debe realizar una gestión de cambios a todos los proyectos informáticos en los ambientes de procesamiento definidos, en lo posible con la ayuda de herramientas automatizadas para tal fin.
- Los procedimientos de control de cambios que se adopten en un proyecto, deben definir los siguientes elementos: Quién puede solicitar un cambio, Cómo se solicita un cambio, Cómo se procesa un cambio, Quién aprueba un cambio, Criterios para aceptar, rechazar o posponer un cambio.

ARTÍCULO DÉCIMO PRIMERO. DE LOS USUARIOS TIC. Establézcase los siguientes lineamientos para la gestión de los usuarios TIC, quienes deberán tener especial cuidado de cumplir los siguientes puntos:

- La Política de TICs y sus lineamientos hacen parte del conjunto de normas y políticas institucionales de LA EMPRESA, por lo tanto, son aceptadas por cada una de las personas a ser contratadas como empleados o terceros/usuarios temporales que accedan a los recurso tecnológicos de LA EMPRESA.
- Se pactará un ANS, con el cliente interno responsable del proceso, cuando se requiera un nuevo servicio, se vayan a prestar los servicios actuales a nuevos usuarios o cuando los usuarios actuales requieran un servicio en condiciones especiales.
- La administración de requerimientos, atención de problemas e incidentes producto de los procesos de utilización, administración y operación de los sistemas de información y de la infraestructura tecnológica, se atenderán a través de la mesa de ayuda.
- Los usuarios TIC deben disponer de los recursos y servicios TIC (ajustados a las necesidades específicas de las responsabilidades a su cargo) y responderá de manera directa por la utilización adecuada de los mismos.

- El usuario TIC debe tener acceso a la información que requiere de acuerdo a sus responsabilidades en el proceso en que labora.
- Los líderes funcionales, usuarios TIC responsables del flujo de información en cada uno de los módulos de los sistemas de información, son los responsables de definir, administrar y gestionar los roles y permisos asociados al módulo que esté a su cargo y el acceso que otorgará a otras personas, al interior de LA EMPRESA, para que ellas puedan ejecutar sus responsabilidades. La materialización de la asignación de dichos permisos estará a cargo de la Oficina de TICs o quien haga sus veces.
- El uso racional de los recursos de almacenamiento es responsabilidad de todos los usuarios de las TIC al interior de LA EMPRESA; es decir, los usuarios de las TIC deberá, entre otras, depurar la información de sus correos, hacer limpieza de los archivos temporales y/o de los archivos que descargan desde internet, entre otras..
- Los usuarios de las TICs deben bloquear la sesión cuando se alejen del computador y/o dispositivo móvil.
- Informar a la Oficina de TIC o quien haga sus veces, de manera inmediata cualquier pérdida de equipos de cómputo o de alguno de sus componentes.
- Solo personal de Oficina de TIC o quien haga sus veces debe tener privilegios de administración sobre los equipos de cómputo.
- Los Usuarios TIC son los responsables de todas las transacciones o acciones efectuadas con su cuenta de usuario en cualquiera de los Sistemas de Información, la plataforma de correo, los equipos de cómputo y/o cualquier otro aplicativo y/o dispositivo tecnológico que LA EMPRESA ponga a su disposición para el desempeño de sus funciones.

ARTÍCULO DÉCIMO SEGUNDO. GESTIÓN DE SOLUCIONES Y CONTRATOS. Establézcase los siguientes lineamientos para la gestión de soluciones y contratos, los cuales deberán alinearse con los siguientes puntos:

- La contratación de cualquier componente que se requiera para la operación (parcial o total) de la Plataforma Tecnológica (hardware/software) de LA EMPRESA, deberá contar con su propio estudios de riesgos para las etapas de precontractual, contractual y post-contractual.
- Toda negociación de TIC debe abordarse como un proyecto con objetivos, alcances, recursos, cronogramas y responsabilidades claramente definidas, involucrando a todas aquellas dependencias y personas que tienen que ver con dicho proceso
- El informe de Estudios Previos del proyecto debe determinar la estrategia de adquisición de la solución. Además debe tener en cuenta las funcionalidades, los costos, el mercado y el soporte ofrecido, los beneficios tanto tangibles como intangibles, la capacidad operativa de la Empresa y los riesgos en su implantación

- Las alternativas de solución que deben analizarse en el informe de Estudios Previos son: La adquisición en el mercado de la solución TIC, la contratación del desarrollo a la medida o servicios tercerizados (de outsourcing).
- Todo contrato asociado con TIC debe tener cláusulas de actualización tecnológica, cambios durante la ejecución, manejo de actas de acuerdo, coordinación entre contratistas, calidad, protocolos de pruebas y proceso de aceptación de la solución contratada.
- Si un requerimiento relacionado con un paquete de software (adquirido a un tercero) no puede ser cubierto por la funcionalidad nativa del mismo, se buscarán otras alternativas diferentes a la de realizar modificaciones sustanciales al paquete (Core del sistema) que impidan la posibilidad de evolución a las nuevas versiones estándar del proveedor.
- En todo proyecto de TICs se deben llevar a cabo pruebas de usuarios finales, aseguramiento de la calidad y pruebas integrales

ARTÍCULO DÉCIMO TERCERO. PROPIEDAD INTELECTUAL. Establézcase los siguientes lineamientos para la garantizar la Propiedad Intelectual al interior de LA EMPRESA, garantizando el cumplimiento de los Derechos de Propiedad Intelectual de las plataformas TICs que operan en ella, en particular en los siguientes puntos:

- En los contratos de software se debe estipular la posibilidad de usar el software en un centro alterno de procesamiento, para el caso o el momento en que LA EMPRESA decida contar con uno.
- Sólo se podrá utilizar software que sea licenciado o expresamente autorizado su uso por parte del dueño de los derechos y se cuente con las respectivas licencias de uso por parte del proveedor contratista a nombre de LA EMPRESA.
- Se podrá utilizar software bajado de Internet de uso libre y sin costo, siempre y cuando se cuente con el análisis de que dicho software apoye efectivamente las funciones del área y esté libre de virus; además que el esquema de su licenciamiento permita la utilización y/o evaluación para fines comerciales
- En la negociación para la contratación del desarrollo de sistemas a la medida, se debe propender por la transferencia de conocimiento para que el área de TIC pueda continuar con el mantenimiento y evolución de los sistemas de información.
- Está prohibido el almacenamiento de archivos multimedia (videos, música, imágenes o libros electrónicos) y cualquier otro tipo de contenido que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en las carpetas de red y demás servicios de almacenamiento en internet suministrados por LA EMPRESA.
- Está prohibido el almacenamiento, uso, instalación y/o ejecución de software que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) y/o licenciamiento en la plataforma tecnológica de LA EMPRESA.

ARTÍCULO DÉCIMO CUARTO. SEGURIDAD INFORMÁTICA O SEGURIDAD DE LA INFORMACIÓN. Establézcase los siguientes lineamientos para la gestión de la seguridad informática o seguridad de la información al interior de LA EMPRESA. La seguridad informática es responsabilidad de todas y cada una de las personas (independiente del tipo de vínculo laboral y/o modalidad de contratación) que están al servicio de LA EMPRESA y/o hacen uso de las plataformas tecnológicas de TICs que ella les pone a su disposición para el cumplimiento de sus funciones y/u obligaciones. En particular deben considerar el cumplimiento de los siguientes lineamientos, sin limitarse a ellas y en consecuencia deben llevar a cabo todos las acciones que estén a su alcance para minimizar los riesgos informáticos y/o digitales y su posible materialización.

- La información y los recursos utilizados para su procesamiento, almacenamiento y/o transmisión deben ser utilizados únicamente para el cumplimiento de la misión y visión de LA EMPRESA, por lo cual es responsabilidad de cada empleado y/o tercero que tenga acceso a ella, evitar el abuso, derroche, uso ilegal o desaprovechamiento.
- Los líderes de cada uno de los procesos (independiente de la estructura organizacional que esté en operación) son los responsables de identificar y gestionar los activos de información que se requieren o hacen parte de su proceso; esto es, determinar la sensibilidad de cada uno de ellos, identificar/analizar y controlar los riesgos de acuerdo con los procedimientos establecidos para ello, establecer las reglas de uso cuando sea necesario, autorizar el uso por parte de otros usuarios, y/o solicitar la aplicación de controles cuando sea necesario
- Los empleados y terceros que tengan acceso a la información de LA EMPRESA deben tener atención especial en el manejo de información reservada y clasificada; para ello deberán cuidarse, entre otras cosas, de::
    - Dejarla a la vista de personas no autorizadas ni desatendida, ej: en los puestos de trabajo y zonas de impresión.
    - Mantenerla almacenada sólo en los sistemas de información suministrados por LA EMPRESA.
    - En lo posible, hacer uso de clave de seguridad cuando se esté imprimiendo o tener una persona atendiendo todo el proceso de impresión cuando la clave no sea posible llevarlo a cabo.
    - Solicitar al área de TIC el almacenamiento seguro de la información cuya pérdida pueda causar incumplimientos legales y/o la interrupción del proceso a su cargo.
    - Considerar como información ***Reservada*** toda aquella que está relacionada con Incidentes o vulnerabilidades de seguridad de la información, así como el detalle de las medidas para proteger las plataformas de TIC que establezca la EAAAY

- Reportar al área de TIC de manera inmediata cualquier situación que pueda afectar la integridad, disponibilidad y confidencialidad de la información.
- Abstenerse de crear, acceder, almacenar o transmitir material ilegal, pornográfico, que promueva la violación de los derechos humanos o que atente contra la integridad moral de las personas o de las instituciones
- Explotar las vulnerabilidades de las plataformas TIC de LA EMPRESA, esto está explícitamente prohibido.
- Grabar en audio y/o video las reuniones y/o sesiones de videoconferencias de LA EMPRESA a menos que todos los participantes estén al tanto de dicha grabación. En el acta de la reunión debe registrarse que la sesión fue grabada.

- La transferencia o la entrega de información clasificada o reservada sólo puede llevarse a cabo cuando exista un acuerdo de confidencialidad de información que lo regule.
- LA EMPRESA podrá realizar monitoreos y/o auditorías en las plataformas TICs que están al servicio de los empleados y/o terceros al servicio de aquélla para el cumplimiento de sus funciones y/o deberes laborales.
- Solamente el equipo de TIC, o un tercero autorizado por dicha Oficina, puede utilizar herramientas de diagnóstico de la seguridad de la información (herramientas de hacking) sobre los activos de información de LA EMPRESA.
- Solamente el equipo de TIC está autorizado para inhabilitar, desviar, apagar o desconectar los componentes y sistemas de la infraestructura de seguridad de la información de LA EMPRESA.
- El uso del correo electrónico deberá ser acorde con los siguientes aspectos:
  - Está prohibido el envío masivo de correos sin la autorización del personal directivo de la dependencia.
  - La Oficina de TIC establecerá el límite para el número de destinatarios y el tamaño de los mensajes de correo electrónico al interior de LA EMPRESA.
  - Está prohibido el envío de correos electrónicos con contenido que atente contra la integridad y la dignidad de las personas, así como con el buen nombre de LA EMPRESA.
  - Cuando un empleado y/o tercero al servicio de LA EMPRESA se retire o termine su relación contractual con Ésta, su cuenta de correo será desactivada.
  - Las cuentas de correo electrónico son propiedad de LA EMPRESA, son asignadas para la realización tareas propias de las funciones laborales y no deben utilizarse para ningún otro fin.
  - Todos los mensajes de correo electrónico pueden ser sujetos a análisis y conservación permanente por parte de LA EMPRESA.
  - Cuando se detecte un correo fraudulento, con fines maliciosos o con contenido sospechoso se debe informar inmediatamente esta situación a la Oficina de TIC.

- Está prohibido la instalación, ejecución y/o utilización de software diferente al preinstalado en los equipos de cómputo o al instalado por integrantes de los equipos de trabajo de informática.
- Los parámetros de configuración del sistema operativo solo deben ser modificados por integrantes de los equipos de trabajo de informática
- En el uso de la red, los usuarios deberán tener presente que está prohibido...
    - Almacenar archivos personales en carpetas de la red y demás servicios de almacenamiento en internet suministrados por LA EMPRESA.
    - El uso de servicios de descarga o intercambio de archivos que funcionan bajo el esquema P2P (person to person). Por ejemplo: Torrent, Ares, eMule, Limewire, Popcorn Time, entre otros.
    - Descargar archivos de audio y/o video a menos que lo requieran en virtud de sus responsabilidades laborales.
    - LA EMPRESA puede controlar y limitar la navegación a ciertos sitios, recursos o servicios de internet con el fin de proteger la seguridad y la disponibilidad del servicio de internet.
    - Deshabilitar o evadir los controles de navegación en internet.
    - El uso del servicio de internet de LA EMPRESA para acceder a páginas de transmisión de películas, programas de televisión, eventos deportivos, páginas de compra en línea o redes sociales.
    - El acceso remoto a los equipos y dispositivos de la plataforma de TIC salvo cuando la Oficina de TIC lo autorice para labores de soporte técnico, en cuyo caso deberá estar limitado al tiempo que dure la atención del evento.
    - Solo se almacenará información electrónica en los servicios tecnológicos suministrados por LA EMPRESA.
    - La red de visitantes está dispuesta únicamente para las personas que visitan temporalmente LA EMPRESA.
- Únicamente se conectarán a la red de datos de LA EMPRESA equipos de cómputo que:
    - Cumplan los requisitos técnicos establecidos por la oficina de TIC o quien haga sus veces.
    - Sean suministrados por LA EMPRESA o sean equipos externos que encuentren en esquema de convenio o contratos de alquiler.
    - La inclusión de dispositivos personales (tales como PCs, computadores portátiles, celulares, tabletas, impresoras, cámaras, y wearables) en la red corporativa está prohibida
    - Los dispositivos no autorizados que se encuentren en la red serán desconectados.
    - Está prohibido violar o evadir los controles de navegación en internet..
- Los contratos celebrados entre LA EMPRESA y contratistas con acceso a la información de Ésta, deben incluir cláusulas para mitigar riesgos de seguridad de la información.

- Siempre que LA EMPRESA requiera compartir información Clasificada o Reservada con un tercero, se debe formalizar previamente un acuerdo de confidencialidad.
- Deben aplicarse mecanismos de cifrado cuando exista un alto riesgo de comprometer la confidencialidad de la información *clasificada* o *reservada* de LA EMPRESA.
- Será sancionado con las acciones disciplinarias y legales correspondientes, el que utilizare registros informáticos, software u otro medio para de forma no autorizada, ocultar, alterar o distorsionar datos.
- Toda la información de ciudadanos o servidores públicos que incluya cédulas de identidad, datos de contacto o información financiera debe ser sólo accesible al personal de LA EMPRESA que necesite ese acceso en virtud de su trabajo.
- Las redes sociales institucionales deben ser protegidas de situaciones de acceso indebido y publicaciones no autorizadas:
    - Las credenciales de acceso (usuario y contraseña) de una cuenta institucional de redes sociales, sólo pueden ser conocidas por un único responsable designado.
    - Las contraseñas de acceso a las redes sociales institucionales deben cumplir los lineamientos para contraseñas establecidos en el presente documento.
    - Las contraseñas de redes sociales institucionales deben ser cambiadas cada tres meses como mínimo.
    - No debe establecerse la misma contraseña a más de una cuenta de redes sociales institucionales.
    - Se deben cambiar las contraseñas de acceso cada vez que se cambien los responsables del manejo de las redes sociales institucionales.
    - Copias de las credenciales de acceso a las redes sociales institucionales (usuarios y contraseñas) deben ser puestas en sobres firmados y sellados (un sobre por cada cuenta de redes sociales) estos sobres deben permanecer en un sitio seguro, como una caja de seguridad; de modo que puedan ser utilizados en caso de contingencias con el (los) responsable(s) de las redes sociales.
- El acceso a los datos y sistemas de información de LA EMPRESA a través de dispositivos móviles debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad de la información.
- El área de TICs o quien haga sus veces deberá realizar la identificación y valoración de los riesgos digitales de LA EMPRESA, para lo cual podrá solicitar la participación de representantes de las diferentes áreas de LA EMPRESA. Una vez identificados los riesgos, deberá procederse con la valoración y las opciones que puedan aplicarse para la mitigación de los mismos. Estos proceso de identificación/valoración deberá llevarse a cabo mínimo una vez al año, en todo caso, el mapa de riesgos deberá actualizarse cuando entre en operación nuevos elementos en la Plataforma Tecnológica y/o cuando sea emitida una nueva

normatividad y/o ante la ocurrencia de eventos en el medio y/o el sector que puedan implicar y/o conectarse con LA EMPRESA.

- El área de TIC deberá definir el procedimiento a utilizar para la realización de la identificación y valoración de los riesgos digitales de LA EMPRESA.

ARTÍCULO DÉCIMO QUINTO: La presente Resolución rige a partir de la fecha de su expedición y publicación, y deroga todas las disposiciones que le sean contrarias, así como las resoluciones 1484 del 28 de octubre de 2019 y 1485 del 28 de octubre de 2019, integrándolas en una sola.

COMUNIQUESE Y CUMPLASE

Dada en Yopal, a los dieciocho (18) días del mes de junio de 2024

JUDHY STELLA VELASQUEZ HERRERA
Agente especial EAAAY E.I.C.E. - ESP
Nombrada mediante Resolución No. SSPD 20231000620935

Proyectó: Juan Bernardo Saldarriaga Elorza / Líder 1 Oficina TIC (e)
Revisó: Iván Pavel Madero Pérez / Asesor Jurídico
Revisó: Adriana Rosas / Oficina de Planeación