PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN -PETI 2021 – 2022-

1. PRESENTACIÓN

Para la EAAAY EICE ESP, el Plan Estratégico de Tecnologías de la información- PETI - define la estrategia y operación que regirá a la entidad durante los próximos dos años (2021-2022), siendo ella vista, como un elemento que hace parte de los procesos Estratégicos y de apoyo; necesarios para desarrollar la prestación de servicios públicos, la gestión de resultados y valoración del medio ambiente, de los sujetos de control. Este es un documento de tipo escalable por la misma dinámica del sector, cuyas versiones irán siendo mejoradas de manera inmediata para así garantizar su implementación.

Este plan está dividido en lineamientos preliminares, para pasar al que se refiere al análisis de la situación actual, así como diagnósticos del Marco de Referencia que han sido articulados y direccionados en armonía con los lineamientos del MINTIC que ha distribuido los seis dominios de Tecnologías de la Información:

1. Estrategia TI
2. Gobierno TI
3. Información
4. Sistemas de Información
5. Servicios Tecnológicos
6. Uso y Apropiación

En una segunda parte se define el direccionamiento estratégico institucionalizado, para pasar a definir las alternativas de solución y una propuesta programática, también organizados acuerdo con los lineamientos del MINTIC.

Finalmente se presentan las acciones específicas de materialización.

2. JUSTIFICACIÓN

El presenté Plan presenta las acciones articuladas para brindar un mejor servicio TI dirigido a la ciudadanía, competir con las exigencias nacionales e internacionales de conectividad y las necesidades propias de la Empresa, reconociendo a las Tecnologías de la información y las Comunicaciones

cómo una herramienta necesaria para el control del sector al que pertenece la Empresa y que ya han venido siendo implementadas.

Lo anterior surge del entendimiento de nuestra Arquitectura Empresarial, el de la situación deseada y la definición del camino para tal fin a través de acciones concretas materializadas en un plan de acción de Gobierno Digital articulado a un portafolio de proyectos y/o plan de desarrollo tecnológico y al plan de seguridad Informática.

Dentro del Marco de Referencia diseñado por el MINTIC existen seis dominios, deben entenderse como que agrupan y organizan los objetivos, áreas y temáticas relativas a las TI. La normatividad nacional obliga a que cada dominio contenga su propio portafolio de instrumentos y herramientas de gestión que coincidan con los estándares y lineamientos (en su mayoría) adoptados por la Empresa, sin embargo, a través del PETI se hace necesario reorganizarlos y ajustarlos al diseñar el Marco de Referencia de la Arquitectura Empresarial.

Este documento, pretende ser una guía sencilla con información clara para la administración y gestión de la tecnología y del PETI en EAAAY EIC- ESP, así como también la formulación de políticas, lineamientos, estrategias y proyectos que garanticen su ejecución e implementación en el marco de tiempo y de recursos establecidos, los cuales deben ser replanteados periódicamente de acuerdo con la dinámica y las prioridades de la organización, así como también con evolución tecnológica. Adicionalmente, tiene como propósito documentar, definir y formalizar los proyectos para conformar el Plan Estratégico de Tecnologías de la Información PETI, para la EAAAY EIC- ESP

3. OBJETIVO GENERAL

Establecer las estrategias para la gestión de las Tecnologías de la Información y las Comunicaciones TI en Empresa Acueducto, Alcantarillado y Aseo de Yopal EIC E ESP, acordes con las necesidades de la Empresa y los lineamientos del programa de Gobierno Digital, como eje de desarrollo institucional para el periodo comprendido entre el 2021 y 2022, que contribuya al logro de los objetivos y metas institucionales.

3.1 OBJETIVOS ESPECIFICOS

El PETI de la Empresa Acueducto, Alcantarillado y Aseo de Yopal EIC E ESP, cuenta con los siguientes objetivos específicos acordes con las necesidades de la Empresa y la nueva política de Gobierno Digital:

- ✓ Fortalecer la plataforma tecnológica de la Entidad (Hardware y Software), manteniendo un esquema de alta disponibilidad y seguridad.
- ✓ Aumentar la automatización y eficiencia de los procesos soportados con tecnologías de la información.
- ✓ Fortalecer el uso de las Tecnologías de la información al interior de la Empresa Acueducto, Alcantarillado y Aseo de Yopal EICE ESP, desarrollando las actividades necesarias para garantizar su existencia, monitoreo, seguimiento, control y mejora continua.
- ✓ Establecer un portafolio de proyectos corto plazo (cuatro años vigencia máximo) que permitan dotar de manera oportuna a las diferentes dependencias y sedes con las Herramientas básicas para el desempeño de funciones.
- ✓ Generar espacios que permitan interactuar y atender a la ciudadanía haciendo uso de las TI.
- ✓ Garantizar la seguridad y la privacidad de la información

4. ALCANCE

El PETI tiene como finalidad el diagnóstico, análisis, definición y planeación de los proyectos de tecnología que se ejecutarán para EAAAY EICE ESP durante los años 2021-2022 o hasta que sea adoptado un nuevo instrumento, estos apoyarán el cumplimiento de los procesos y objetivos propuestos por la Empresa, además de las funciones asignadas al Área de Tecnologías y Sistemas de Información.

El PETI está articulado de manera global en relación con la adquisición e implementación de nuevas tecnologías y sistemas de información misional, funcional y gerencial, así como la modernización y actualización organizacional, la Gestión en seguridad de la información, esquemas de virtualización y la movilidad; así como la gestión del cambio.

5 .BENEFICIOS DEL PETI

La alineación del PETI con los objetivos estratégicos, el plan estratégico de la entidad y el plan nacional de desarrollo, así como un ejercicio básico e inicial de Arquitectura Empresarial y de TI, permite identificar y actualizar las necesidades tecnológicas, así como formular e implementar las políticas, metodologías y herramientas que permitan el aprovechamiento de los recursos tecnológicos y de inversión.

El PETI, constituye una guía de trabajo en el tiempo, que permite definir y administrar las diferentes políticas y proyectos que conduzcan al logro de los objetivos propuestos y a la ejecución de los diferentes proyectos de manera coordinada de acuerdo con las necesidades y prioridades de la EAAAY EICE ESP.

6. MARCO NORMATIVO

LEY 527 DE 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

LEY 594 DE 2000: Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

LEY 962 DE 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

DECRETO 1747 DE 2000: por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

LEY 1293 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

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-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones

DECRETO 19 DE 2012: Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

DECRETO 2609 DE 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

DECRETO 1377 DE 2013: Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales.

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.

LEY 1712 DE 2014: 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.

DECRETO 1078 DE 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

DECRETO 103 DE 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

DECRETO 415 DE 2016: Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

7. INFORMACIÓN INSTITUCIONAL

7.1 Misión: Aportar bienestar y calidad de vida a la sociedad yopaleña, con el suministro optimo y continuo de agua potable, la conducción sanitaria de residuos líquidos y la recolección y disposición final de basuras, aplicando en cada caso avances científicos y tecnología de punta; asimismo promoviendo el desarrollo y la calificación del talento humano, con criterio de compromiso social y calidez en el servicio.

7.2 visión: Ser una empresa líder en la prestación de los servicios públicos de acueducto, alcantarillado y aseo, con mayores indicadores de cobertura en la atención al cliente, niveles de excelencia en la aplicación tecnológica y efectividad en las operaciones económicas, que garanticen su crecimiento y la hagan auto sostenible.

7.3 Política De Gestión: La Empresa, brinda los servicios, mediante una gestión transparente, en cumplimiento de los objetivos estratégicos, aplicando la normatividad legal vigente.

Cuenta con la tecnología adecuada y funcionarios idóneos con actitud de servicio que direccionan a la empresa hacia la mejora· continua de la eficiencia, eficacia y efectividad de los procesos, preservando y manteniendo el equilibrio del recurso hídrico.

8. MAPA OPERACIONAL

Dentro de la reingeniería a procesos realizada en el año 2019 después de la planeación, el diligenciamiento de la matriz de alineación de los grandes pro pósitos contenidos en la plataforma estratégica, para la actividad empresarial de la EAAAY EICE ESP se determinó el mapa operacional, dónde el proceso de Gobierno Digital aparece los procesos estratégicos y gerenciales por la relevancia que toma con la normatividad vigente y la disposición de 1·a alta dirección para intervenir la TI de la empresa.

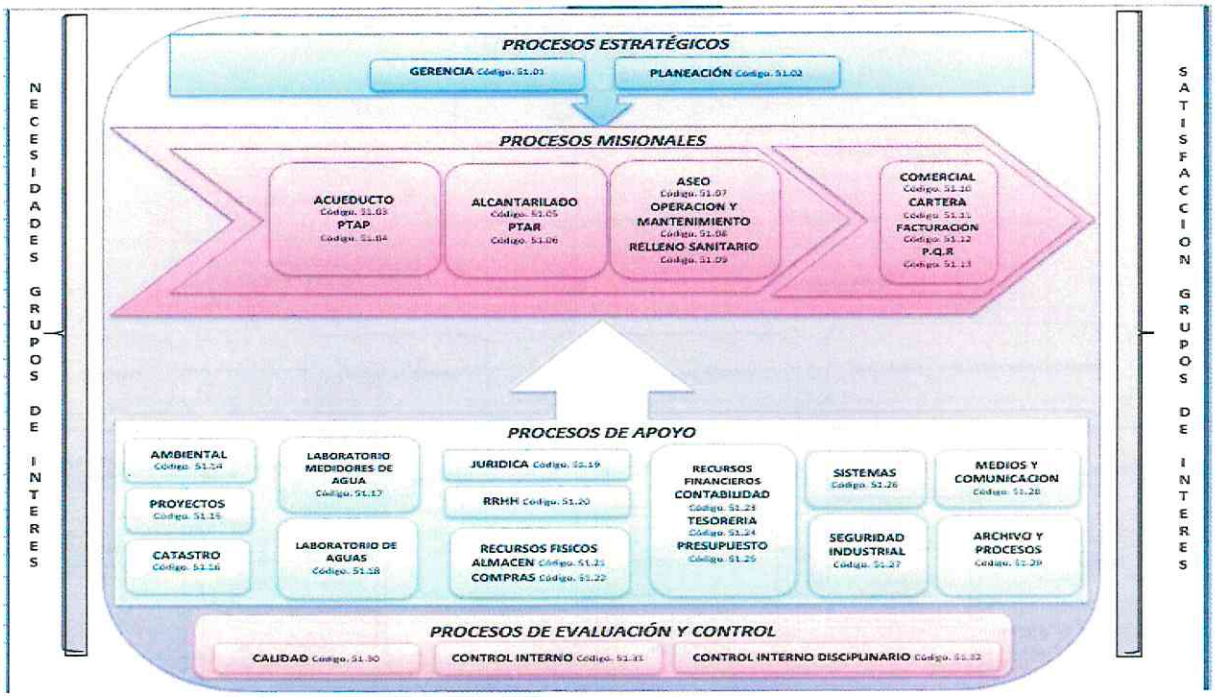


Figura 1. Mapa de Proceso

9. ESTRUCTURA ORGANIZACIONAL

Dando alcance al acuerdo 02 de la resolución 1856 de 2019 a través. del cual se adoptó el manual especifico de funciones, requisitos y competencias laborales de la Empresa Acueducto, Alcantarillado y Aseo de Yopal EICE ESP y se adoptó otras decisiones, se define la estructura y oficinas.

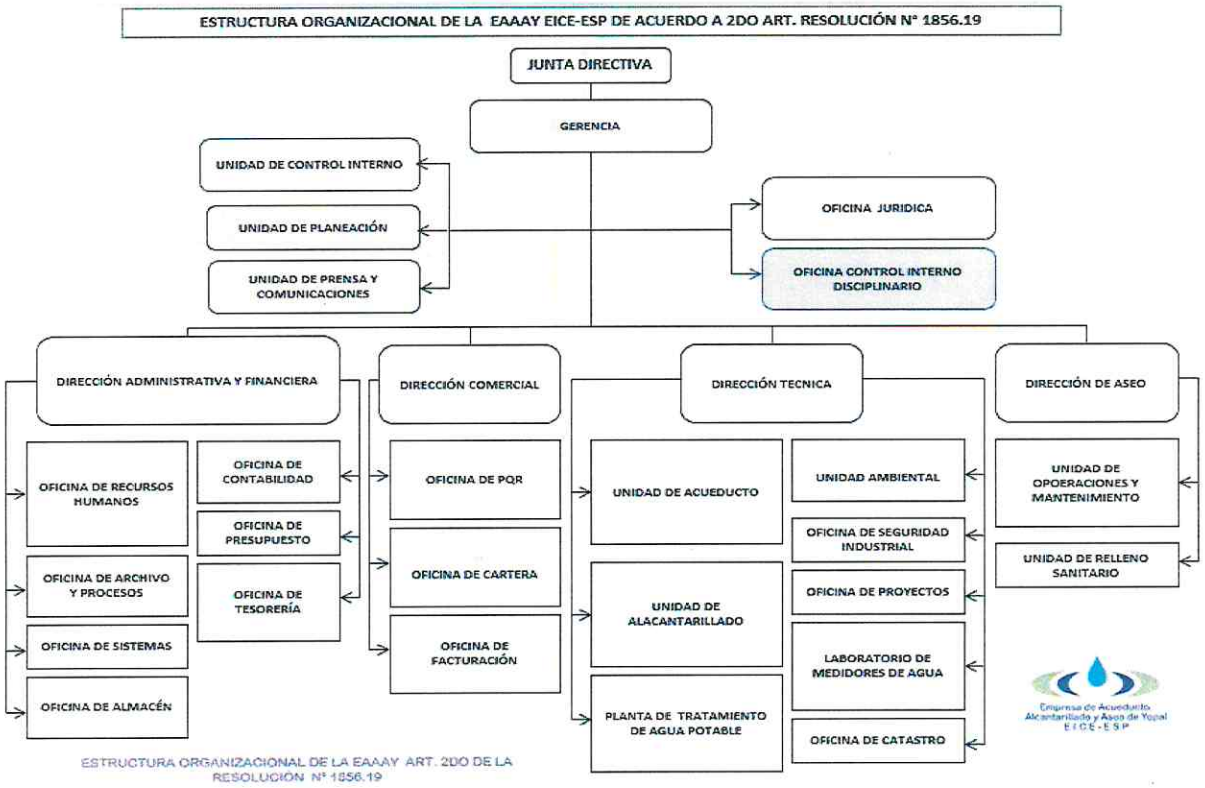


Figura 2. Mapa Organizacional

10. ANALISIS ESTADO ACTUAL

Para él análisis de la situación actual se tuvieron en cuenta los dominios del marco de Referencia de Arquitectura Empresarial para la Gestión de TI de MITC, el modelo operativo de TI y el análisis financiero, además de la recolección de la información, la observación de los procesos y las necesidades recolectadas, con el fin de hacer el levantamiento de activos por cada uno de los dominios y así identificaron las siguientes problemáticas:

Es necesario destacar el esfuerzo de la Empresa, en relación con la actualización y renovación de la plataforma tecnológica durante los últimos años, lo que ha permitido fortalecer y asegurar la infraestructura para atender los diferentes compromisos y retos de la Empresa.

Adicionalmente, se cuentan con políticas de TI que fortalecen la gestión y establecen lineamientos que garantizan la operación y seguridad, así como la utilización de Backups en la nube (Cloud).

De acuerdo con lo anterior, se agrupa la información y se presenta una breve descripción de los elementos identificados, en relación con los siguientes elementos:

- **Hardware:** Esta infraestructura está compuesta principalmente por la plataforma de: servidores, almacenamiento NAS, conectividad de diferentes elementos y estaciones de trabajo, seguridad, centro de datos. (Anexo: Inventario de Hardware).

  En este aspecto se tiene en cuenta el análisis de la demanda, frente a la capacidad de procesamiento y almacenamiento por volumen, consumo de energía e insuficiencias para atender algunos procesos. Adicionalmente, se evalúa la capacidad de almacenamiento tanto en servidores como en estaciones, los riesgos en su almacenamiento, manejo y custodia frente a posibles pérdidas o fugas de información.

  Este componente, cuenta con la gestión y el soporte de los Grupos de plataforma de TI, soporte TI y mesa de ayuda, los cuales se encargan de la administración y gestión de la infraestructura de hardware.

- **Software**: Este ítem comprende los sistemas de información y el software de utilidad de la entidad, que apoyan los diferentes procesos. En algunos casos, en estos sistemas de información, se debe buscar la actualización de acuerdo con la evolución tecnológica (WEB) y de la infraestructura, para reducir su obsolescencia.

  Se tiene establecido un equipo de trabajo, que tiene como objetivo la gestión, el soporte y mantenimiento de los sistemas de información desarrollados en la Entidad. (Anexo: Inventario de Software y Sistemas de Información).

- **Redes:** La Entidad cuenta con una arquitectura de red de cableado estructurado categoría 6, con el cumplimiento de estándares internacionales básicos y de seguridad, la cual es actualizada y administrada por el grupo de trabajo de la oficina de Sistemas. Se tienen esquemas de conectividad para las diferentes sedes a través de internet.

Actualmente, se gestiona esta arquitectura a través del grupo de redes, el cual realiza el análisis de la capacidad de la conectividad de las dependencias y la política para de segmentación de la red.

- **Telecomunicaciones:** Se encuentra con una plataforma que gestiona y soporta las comunicaciones de telefonía fija y móvil.

  Este componente es administrado por el grupo de telecomunicaciones, quien se encarga del soporte de la plataforma y de la entrega de servicios a las diferentes dependencias y sedes.

- **Seguridad**: Se encuentra un sistema de seguridad compuesto por diversos equipos (firewall, Antivirus y VPN entre otros), el cual es gestionado a partir del control de acceso mediante el Directorio Activo (DA) de Microsoft con sus respectivos servicios.

  El componente de hardware es administrado y gestionado por la oficina de Sistemas. Adicionalmente, se cuenta con el apoyo de soporte activo para las políticas de seguridad de la información y el sistema de gestión de la seguridad de la información.

- **Proyectos:** Se cuenta con un portafolio de proyectos que atiende los diferentes requerimientos de las diferentes oficinas, así como las necesidades básicas de la Empresa Estos proyectos dependen de la capacidad de la infraestructura de la entidad y del presupuesto asignado para su desarrollo e implementación.

- **Recurso Humano:** Se cuenta con un equipo de trabajo, que soporta la dinámica de los servicios y los requerimientos de las dependencias y sedes de la Empresa; se tienen roles y funciones definidos en el equipo de trabajo, de acuerdo con la formalización de los grupos de trabajo por especialidades en la estructura interna del Área, cubriendo las necesidades de la Empresa.

- **Usuarios Clientes:** Como factor importante para el análisis de la situación actual, se encuentra la identificación de los líderes de los procesos, quienes establecen la demanda de servicios para atender sus procesos y funciones, de acuerdo con sus necesidades

10.1 Análisis de Dominios TI

Tomando como referencia el marco de referencia de arquitectura empresarial de TI de MINTIC, además del análisis DOFA, para el análisis de la situación actual se complementa con el diagnóstico de cada uno de los dominios propuestos.

Dominio de Estrategia de TI

- ✓ El tamaño de los componentes a cumplir en el sector son amplios y numerosos, Por tal razón la implementación de proyectos TI debe tener un alto componente de planeación que asegure la eficiencia de los recursos y permita beneficiar con más y mejores servicios a los usuarios.
- ✓ La operación consume al personal de la Oficina de Sistemas por lo cual la proyección estratégica está a cargo solo del profesional de la Oficina de Sistemas.
- ✓ No existe un proceso para evaluar y mantener la arquitectura empresarial.
- ✓ No se cuenta con suficiente personal para capacitar y orientar en temas relativos a Gobierno Digital para todas las direcciones adscritas a la Empresa.
- ✓ El conocimiento de la estrategia de TI está concentrada en el área de Sistemas.
- ✓ La documentación de la estrategia TI, se encuentra en proceso de elaboración.
- ✓ Las competencias técnicas del equipo de trabajo para el desarrollo y consolidación de la estrategia TI. Deben desarrollarse.

Dominio de Gobierno de TI

- ✓ Sistemas y servicios de información no integrados, con baja calidad de datos.
- ✓ Sobrecarga de trabajo en roles, que dificulta la gestión de TI.
- ✓ Planta de personal del área de Sistemas insuficiente.
- ✓ El servicio de TI soportado en uno o más procesos totalmente alineado depende de algunas personas.

Dominio de Información TI

- ✓ La demanda de servicios y productos no planeados (urgencias), afecta la capacidad operativa y de gestión del área de TI.
- ✓ La documentación y el gobierno de todas las bases de datos es básico.

- ✓ No se tiene una arquitectura de información, gobierno de los datos institucional o de gestión del conocimiento, que guíe la implementación y desarrollo de los sistemas de información.
- ✓ Algunos procesos en la Empresa no están actualizados y estandarizados.

Dominio de Sistemas de Información

- ✓ Algunos de los sistemas de información se comportan como islas, ya que no cuentan con interfaces para agilizar los procesos de la Empresa.
- ✓ Se debe fortalecer y formalizar el proceso para el desarrollo de aplicaciones de acuerdo con la demanda y las prioridades de la Empresa.
- ✓ Persiste la obsolescencia tecnológica en algunas aplicaciones.

Dominio de Servicios Tecnológicos

- ✓ Documentación y estructuración básica de procesos enmarcados dentro de la gestión de TI de acuerdo con las mejores prácticas.
- ✓ Los usuarios, reportan los casos de soporte directamente a los administradores o directivos.
- ✓ Existen oportunidades de mejora en el aseguramiento de los servicios de tecnología.

Dominio de Uso y Apropiación de las TI

- ✓ Poco interés para el desarrollo de la gestión del cambio en los proyectos y el fortalecimiento de la cultura informática.
- ✓ La medición del impacto del uso y apropiación de las TI está en proceso de implementación.
- ✓ La satisfacción de usuarios con relación a las actividades, productos y servicios que brinda el Área de TI no se evidencia.

La Oficina de Sistemas, es una dependencia comprometida institucionalmente; como un elemento estratégico para la innovación, transformación y modernización de la Empresa, la cual ha venido trabajando en la actualización de la infraestructura, situación que refleja una situación actual favorable frente a los retos y el desarrollo tecnológico, con lo que se modela un escenario de evolución en el cual la Oficina de Sistemas actualiza y fundamenta el presente plan estratégico.

.

10.2 Catálogos De Servicios TI EAAAY EIC ESP

CATEGORIA	SERVICIO	DESCRIPCIÓN
INTERNET	Publicación de Pagina Web	Publicación de contenido digital para usuarios internos y externos (informes, imágenes; vídeos, noticias, normatividad y contratación) en el portal web de la Entidad, emitido por las diferentes subgerencias y oficinas.
	Internet	Habilitación de la conexión que permite un acceso controlando la red mundial de datos e internet desde el firewall y los equipos de cómputo u o dispositivos autorizados; para propósitos institucionales.
	Conexión WIFI	Autorización de la conexión de un dispositivo (PC, Celular, Tablet etc.) a la red inalámbrica de la Empresa
	Intranet y/o Usuarios	Red informática privada utilizada con tecnología de protocolo de Internet para compartir información o servicios de computación dentro de la empresa. Sólo los miembros internos autorizados de la organización acceden a ella mediante roles de usuarios.
	Correo Electrónico	Servicio de mensajería electrónica para intercambio de información institucional interna y externa por parte de los funcionarios de la Empresa
SOPORTE	Gestión y Control Cuentas de Usuarios	Autorización, administración y control del acceso de los usuarios bajo domino a la red de datos de EAAAY EICE ESP
		Apoyando, brindando en la

TECNICO	Asesoría Técnica	definición de especificaciones técnicas para adquisición o contratación de hardware, software y servicios tecnológicos de las oficinas y sedes de la Empresa.
	Telefonía	Servicio de comunicación telefónica mediante extensiones para funcionarios de la Empresa y de los usuarios que deseen comunicarse con la EAAAY EICE ESP.
	Impresión y Digitalización	Apoyo a los funcionarios de la empresa para solucionar los problemas de impresión y digitalización
Administración	Respaldo de Información	Servicio a través del cual se resguarda la información institucional almacenada en los equipos, servidores y NAS de la Empresa.
Sistemas De Información	Soporte a sistemas de Información y Plataformas WEB	Soporte y asesoría externa a funcionarios de las dependencias para dar solución a problemas y mejoras de algunas aplicaciones de operación local.

Dando con el resultado catálogo de servicios, se debe estructura un plan de choque con un tiempo de dos (02) años, con lo presupuestando en plan de acción de la Oficina de Sistemas y con el personal actual, esto implica la priorización de proyectos orientados a la estabilidad y actualización de la plataforma tecnológica, fortalecimiento de la calidad y disponibilidad de los servicios de TI.

Respecto a cumplimiento institucional relacionado con la estructura del PETI, el plan de Choque será implementado en esta vigencia ya que no se contaba con un plan estratégicos de años anteriores el cual se enmarca por las acciones establecidas en las guías técnicas del ministerio de las TIC, tendientes al fortalecimiento tecnológico de las entidades, y por tanto implementar plan estratégico para la vigencia de 2021.

Para implementar plan estratégico la oficina de sistemas cuenta con los siguientes componentes para la administración, gestión y control del catálogo de servicios TI:

- Infraestructura de servicio Cliente – Servidor de aplicativos que se utilizan en la Empresa.
- Plan de Mantenimiento preventivo de equipos de cómputo de la EAAAY descrito por resolución con sus respectivos formatos de seguimiento.
- Contamos con Planta Eléctrica para evitar daños eléctricos por parte del prestador del servicio.
- equipo de firewall para la gestión y control de acceso a internet y prevención de ataques informáticos.
- Cuarto de Sistemas con su respectivo piso falso para la protección de los servidores, NAS, switch, DVR, NVR y circuito de cámaras seguridad.
- UPS de 20 KVA para la protección de la energía regulada en las dependencias de: Gerencia, Administrativa y Comercial, igualmente se cuenta con UPS de 6 KVA para cada dirección Técnica y aseo, como para la sede de Archivo y Procesos.
- Servicio de Respaldo en la Nube de Base de Datos del Sistemas ERP
- Programación de copias de seguridad de los servidores y NAS.
- Sistema de cámaras de seguridad Noche – Día en la sede Administrativa y Archivo y Procesos.
- Red estructurada esta soportada con Switchs, UPS, FIREWALL, Red Regulada, NAS y Servidores.
- Configuración en cada computador con los correos institucionales con su plantilla en el Outlook.
- La empresa Cuenta con su página web propia con los lineamientos que exige Gobierno Digital www.eaaay.gov.co., prestando los servicios de tramites en linea como: PQR en linea, consulte su factura,

realizar pagos de facturas y conocer información de interés de la empresa.

- VPNs activadas con su respectivo Rol de usuario.

10.3 Proyectos Para Fortalecer Las TI 2020-2021

Se ha identificado técnicamente en cuanto al diseño, planificación e implementación de planes para el centro de datos, de elementos eléctricos, electrónicos, hardware y software, en funcionamiento de los equipos tecnológicos de la empresa.

Dentro de los racks informáticos - del Centro De Datos y sus componentes no se encuentran dispositivos homologados para la implementación de políticas públicas del Ministerio de Tecnologías de la Información y las Comunicaciones -MINTIC- como lo son el Marco de Referencia de Arquitectura Empresarial, ProtocoloIPv6 y el Modelo de Privacidad y Seguridad de la Información.

Las Entidades públicas de orden Nacional y Territorial, así como proveedores de servicios de Gobierno Digital y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información e IPv6, en función de lo dispuesto en el Marco de Referencia de Arquitectura Empresarial, la Estrategia de Gobierno Digital y la Seguridad y Privacidad de TI. Para entrar en el proceso de adopción de este nuevo protocolo, se debe realizar un inventario de los activos de información, revisar su actual infraestructura de computación y de comunicaciones, validar todos los componentes de hardware y software de que se disponga, revisar los servicios que se prestan, los sistemas de información, revisión de estándares y políticas para conocer el impacto de adopción de la nueva versión del protocolo IP, a fin de facilitar las labores de planeación e implementación de IPv4 a IPv6, garantizando que las operaciones continúen funcionando normalmente dentro de las entidades del estado.

11.MATRIZ DOFA

De acuerdo con el levantamiento de la información y el análisis realizado, se identifican los aspectos más relevantes agrupándolos en la matriz para su evaluación como parte de la metodología.

Debilidades

- ✓ Rotación de personal calificado
- ✓ Bajo interés por las políticas de TI, la seguridad, el uso y apropiación de la tecnología.
- ✓ Estructura del área insuficiente para atender la demanda.
- ✓ Subutilización de herramientas de TI.
- ✓ Arquitectura Empresarial, Arquitectura TI.
- ✓ Baja integración de los sistemas de información y las dependencias
- ✓ No se aplica el rehúso de información entre entidades

Oportunidades

- ✓ Evolución tecnológica.
- ✓ Políticas del estado relacionadas con TI y la automatización
- ✓ Buenas prácticas de TI.
- ✓ Políticas de MINTIC, Gobierno Digital, Colombia Compra Eficiente.
- ✓ Evolución de los Ciber-ciudadanos y Ciudades Inteligentes.
- ✓ Consolidar modelo de gestión de TI.
- ✓ Desarrollo de canales virtuales.

Amenazas

- ✓ Insatisfacción con servicios de TI
- ✓ Bajo compromiso e interés de algunas dependencias/funcionarios.
- ✓ Limitaciones presupuestales (recorte) y contractuales.
- ✓ Ciberdelincuencia que afecta la Seguridad de la información a nivel mundial
- ✓ Baja calidad del servicio de terceros.
- ✓ Bajos perfiles y salarios para selección de personal del área
- ✓ No adopción del Decreto 415 de 2016

Fortalezas

- ✓ Proceso de actualización de la infraestructura TI.
- ✓ Compromiso del equipo de trabajo.
- ✓ Estabilidad laboral.
- ✓ Plan de Mantenimiento preventivo anual sobre la infraestructura Tecnológica.

12. DEFINICIÓN DE LA ESTRATEGIA DE TECNOLOGÍAS DE INFORMACIÓN.

Para la definición de la estrategia de TI, se tienen en cuenta todas las capacidades y competencias del Área de Tecnologías y Sistemas de Información, que soportan los procesos directivos, misionales y de soporte de la Empresa. Además de realizar las siguientes actividades:

- ✓ **Análisis del entorno:** A partir de la revisión documental asociada a las tendencias del sector gobierno, teniendo en cuenta los factores políticos, económicos, sociales, tecnológicos, legales, ecológicos y/o ambientales que pudieran afectar positiva o negativamente a la Empresa.
- ✓ **Análisis Interno:** Con base en las entrevistas con el equipo directivo, en los planes de fortalecimiento y mejoramiento, en el proceso de autoevaluación, identificando fortalezas y debilidades.
- ✓ **Análisis DOFA.**
- ✓ **Los lineamientos estratégicos de la Empresa**
- ✓ **Definición de los objetivos estratégicos**.

Por lo anterior, se puede definir que la estrategia de TI, pretende potencializar las capacidades y competencias de tecnología informática para apoyar e implementar proyectos y servicios que soporten todos los procesos de la Empresa para una gestión eficiente y moderna.

13. ESTRATEGIAS PETI

Con el diagnóstico a realizar dentro del periodo 2021 y 2022, se definirán las estrategias de tecnología, que permitan apoyar la gestión y modernización de la Empresa; así como la gobernabilidad de la tecnología, las cuales se describen a continuación:

- ✓ Mantener la plataforma tecnológica acorde con los avances informáticos, de seguridad de la información y las necesidades de la Entidad.
- ✓ Actualizar e implementar Sistemas de Gestión de Información que apoyen la gestión y la toma de decisiones.
- ✓ Actualizar e implementar infraestructura que fortalezca la seguridad y la protección de información en la Empresa.
- ✓ Coordinar la implementación de la Política de Gobierno Digital.
- ✓ Identificar proyectos que permitan la innovación y la transformación de la Empresa.

14. RESPONSABLE DEL DOCUMENTO

Profesional de la Oficina De Sistemas de Empresa Acueducto, Alcantarillado y Aseo de Yopal EIC E ESP

JAIRO BOSSUET PÉREZ BARRERA
Gerente EAAAY EICE-ESP
Contratante

Elaboró: Cesar Barrera // Profesional Oficina Sistemas
Revisó: Adriana Cristina Rosas Valderrama // Profesional Planeación

1. INFORMACIÓN GENERAL

NOMBRE DEL PROCEDIMIENTO: Procedimiento de Seguridad y Privacidad de la Información

RESPONSABLE: Profesional Oficina de Sistemas

OBJETIVO: Describir las actividades del plan de seguridad y privacidad de la información, definido en la norma ISO 27001, identificando en cada fase las actividades a realizar dentro de la mejora continua del sistema de gestión de la seguridad de la información (SGSI) en el marco del modelo de referencia definido por el Ministerio de Tecnologías de Información – MINTIC-MSPI, con el fin de para soportar los procesos administrativos de la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EICE – ESP.

ALCANCE:

- ✓ La adopción del Modelo de Seguridad y Privacidad por parte de la Empresa **de Acueducto, Alcantarillado y Aseo de Yopal EICE – ESP** para contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.
- ✓ Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- ✓ Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- ✓ Monitorear y revisar el desempeño del SGSI
- ✓ Realizar mejoramiento continuo en base a la medición del objetivo

INSUMO: La gestión de activos de información, actividades de seguridad de la información, las pruebas de vulnerabilidades e intrusión lógica y física, los diagnósticos de capacidad de la infraestructura de TI y los diagnósticos de cumplimiento con normas y estándares de seguridad, son insumos para determinar amenazas, vulnerabilidades e impactos para la gestión de riesgos para desarrollar estas actividades se requiere recurso humano calificado.

PRODUCTO: Implementación del Modelo de Seguridad y Privacidad de la información

USUARIOS:

- ✓ Alta Dirección de la Empresa
- ✓ Ing. de Sistemas: Líder de proceso

- ✓ Jefe de la Oficina de Planeación
- ✓ Líder de Programa Gestión Documental
- ✓ Técnico/Tecnólogo de Sistemas: Mantenimiento y Soporte de Equipos de Computo

TÉRMINOS Y DEFINICIONES:

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
Análisis de Riesgo Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que

son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural.

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, 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 2014.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

2. ACTIVIDADES Y RESPONSABLES

ACTIVIDAD	FLUJOGRAMA	RESPONSABLE	DOCUMENTO O REGISTRO
Inventario de activos de información de la empresa	Ver Anexo	✓ Almacén ✓ Oficina de sistemas	Inventario de activos base de datos

Diagnóstico de activos de la empresa	Ver Anexo	Oficina de sistemas	Base de datos - hoja de vida de los equipos
La seguridad de los activos de información se logra con controles con políticas de seguridad de la información	Ver Anexo	Oficina de sistemas	-51.26.08.01.05 Control equipo Portátil externo -51.26.01.02 Entrega de accesorios. -51.26.08.01.02 Formato solicitud de registros y grabaciones de seguridad. -51.26.08.01.03 Control revisión de cámaras EAAAY. -51.26.08.01.04 Registro de Publicaciones
Capacitación de usuarios para manejo de sistemas de información aplicaciones equipos	Ver Anexo	✓ Personal interno capacitado ✓ Personal externo proveedores ✓ Profesional de sistemas	Listados de asistencia
Operatividad de los sistemas de información	Ver Anexo	Oficina de sistemas	-Requerimiento de sistema ERP -51.26.01.05 Tickets de soporte
Confiabilidad: acceso únicamente de personal autorizados.	Ver Anexo	Oficina de sistemas	

Integridad: exactitud y completitud de la información y procesos.	Ver Anexo	Oficina de sistemas	
Disponibilidad: acceso a la información y procesos por parte del personal autorizado, cuando lo requieran.	Ver Anexo	Oficina de sistemas	
Obselencia del sistema de información – reporte del administrador del activo a sistemas justificando el estado inactivo para realizar el proceso de baja en el almacén	Ver Anexo	Oficina de sistemas	Inventario de bajas
Control de accesos a sistemas de información	Ver Anexo	Oficina de sistemas	Bitácora usuarios registrados en el sistema
Solicitud de servicios de red – sistemas solo puede proporcionar acceso a redes y servicios de red y aplicaciones autorizados	Ver Anexo	Oficina de sistemas	Bitácora usuarios registrados en el sistema
Registro y cancelación de usuarios	Ver Anexo	Oficina de sistemas	Bitácora usuarios registrados en el sistema

Restringir y controlar la asignación y uso de acceso privilegiado	Ver Anexo	Oficina de sistemas	
Desarrollo de criptografía	Ver Anexo	Oficina de sistemas usuarios de aplicativos EAAAY	
Asegurar el acceso a los sistemas y a los equipos de servicio	Ver Anexo	Oficina de sistemas	Registro de usuario Servidor.
Áreas restringidas – actualizar los derechos de acceso	Ver Anexo	Oficina de sistemas	
Diseñar y aplicar una protección física contra desastres naturales y ataques provocados o accidentes – plan de riesgos	Ver Anexo	Oficina de sistemas	51.26.08.01.01 Plan de riesgos
Manipulación de equipos según instrucciones registro de custodios	Ver Anexo	Oficina de sistemas	

Mantenimiento correcto de equipos que aseguren su disponibilidad y su integridad continua	Ver Anexo	Oficina de sistemas	51.26.01.06 Plan de mantenimiento de equipos de computo
Controles de detección, prevención y recuperación protección de códigos malicioso – prohibido de software no autorizados	Ver Anexo	Proveedor – oficina de sistemas	51.26.08.01.01 Plan de riesgo
Establecer acuerdo con proveedores que puede acceder tratar almacenar comunicar de la infraestructura tecnológica	Ver Anexo	Proveedor – oficina de sistemas	Bitácora de mantenimiento de proveedores o contratista

3. DOCUMENTOS RELACIONADOS

- 51.26.08.01.01 Plan de Riesgos de seguridad y privacidad de la información.
- 51.26.08.01.02 Formato solicitud de registros y grabaciones de seguridad.
- 51.26.08.01.03 Control revisión de cámaras EAAAY.
- 51.26.08.01.04 Registro de publicaciones.
- 51.26.08.01.05 Control equipo portátil externo.

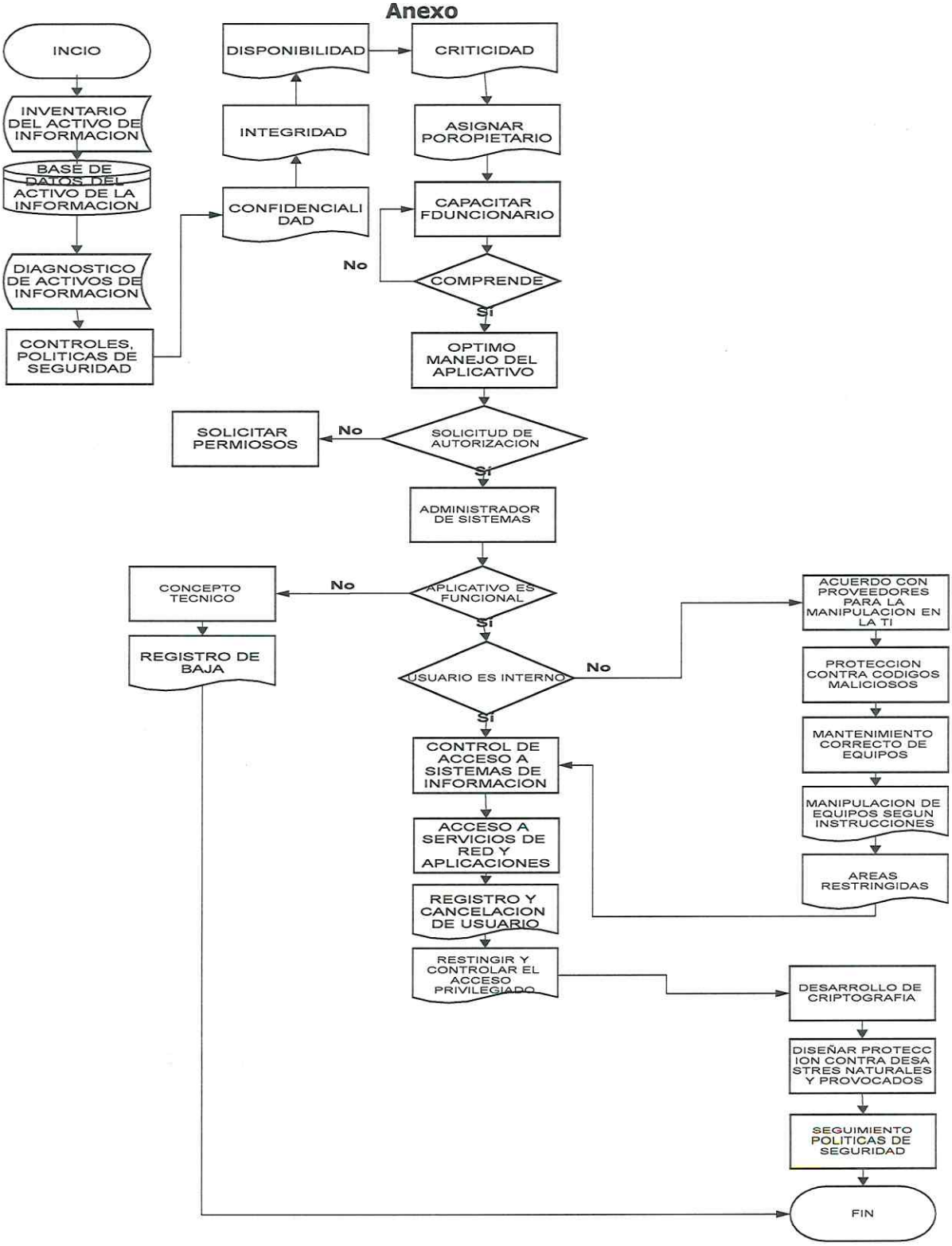
4. APROBACIONES

Elaboró	Revisó	Aprobó
Cesar Augusto Barrera Riveros **Líder del Proceso**	Adriana Cristina Rosas Valderrama **Representante por la Dirección SGC**	Jairo Bossuet Pérez Barrera **Representante Legal**

5. BITÁCORA DE ACTUALIZACIÓN

Versión	Fecha de Aprobación	Ítem Modificado	Motivo	Aprobado por:
01	2021-01-29	Todo	Aprobación Inicial	Comité de Gestión y Desempeño

Anexo


INCIO
INVENTARIO DEL ACTIVO DE INFORMACION
BASE DE DATOS DEL ACTIVO DE LA INFORMACION
DIAGNOSTICO DE ACTIVOS DE INFORMACION
CONTROLES, POLITICAS DE SEGURIDAD
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
CRITICIDAD
ASIGNAR POROPIETARIO
CAPACITAR FDUNCIONARIO
No
COMPRENDE
Si
OPTIMO MANEJO DEL APLICATIVO
SOLICITUD DE AUTORIZACION
No
SOLICITAR PERMIOSOS
Si
ADMINISTRADOR DE SISTEMAS
APLICATIVO ES FUNCIONAL
No
CONCEPTO TECNICO
REGISTRO DE BAJA
Si
USUARIO ES INTERNO
No
ACUERDO CON PROVEEDORES PARA LA MANIPULACION EN LA TI
PROTECCION CONTRA CODIGOS MALICIOSOS
MANTENIMIENTO CORRECTO DE EQUIPOS
MANIPULACION DE EQUIPOS SEGUN INSTRUCCIONES
AREAS RESTRINGIDAS
Si
CONTROL DE ACCESO A SISTEMAS DE INFORMACION
ACCESO A SERVICIOS DE RED Y APLICACIONES
REGISTRO Y CANCELACION DE USUARIO
RESTINGIR Y CONTROLAR EL ACCESO PRIVILEGIADO
DESARROLLO DE CRIPTOGRAFIA
DISEÑAR PROTECCION CONTRA DESASTRES NATURALES Y PROVOCADOS
SEGUIMIENTO POLITICAS DE SEGURIDAD
FIN

PLAN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

La protección de los activos informáticos es una de las tareas más importantes de la Oficina de Sistemas, especificada en la Caracterización del Proceso del SGC **2015 "Mantener y asegurar el funcionamiento óptimo de la infraestructura de hardware y software que conforman la plataforma tecnológica, así como la planificación, diseño, desarrollo, operación y actualización de los sistemas de información e infraestructura informática necesarios para soportar los procesos administrativos de la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EICE – ESP.".** Es por esto que es de vital importancia trazar políticas que permitan garantizar la operatividad de los Sistemas de Información, aún en circunstancia de afectación ante la materialización de los riesgos identificados.

RIESGOS PLANTEADOS

En la siguiente matriz se especifican los siguientes riesgos de seguridad y privacidad de la información según si nivel (Bajo, Medio o Alto):

#	AMENAZA	TIPO DE RIESGO *			ACCION PREVENTIVA (Para riesgos altos)	OBSERVACIONES
		B	M	A		
1	Desactualización de las tecnológicas: Computacional (Hardware) y de información (Software)		x			Los sistemas Ofrecen cada día herramientas más versátiles que le permiten a los usuarios obtener información más rápida y de fácil manejo.
						Software y Hardware se vuelven obsoletos al paso del tiempo.
						software mal utilizado por los Usuarios
2	Fallas eléctricas		x			Cableado Eléctrico sobrecargado de Equipos electrónicos.
						Daño en Equipos Electrónicos
						Perdida de información
						Posibilidad de Incendio
						Sobrecarga en cada línea y en la UPS.
3	Fallas en la conectividad a internet		x			Fallas en el acceso a internet por daños en la infraestructura del proveedor, en la última milla de conexión o por perdida en la interconexión nacional
4	Ataques informativos			x	-Actualización constante de las plataforma de firewall físico, firewall lógico de los servidores y equipos de cómputo,	-Ataques Internos a partir de descargas de software pirata, freeware o shareware sin la supervisión de Sistemas -Ataques externos provenientes de delincuentes Explotación de Vulnerabilidades de sistemas operativos

					antivirus. -Monitoreo del tráfico reportado por el firewall y diseño de nuevas reglas de filtrado -Socialización de las políticas de los recursos informáticos propiciando un uso correcto por parte de los funcionarios	
5	Resistencia al cambio de los sistemas de información		x		-Capacitación y sensibilización sobre las nuevas aplicaciones y la importancia de la mejora continua	-los usuarios al incorporarse un nuevo sistemas de información o realizar cambios en los existentes se niegan al uso de los mismos y argumentan que no debería cambiarse y que los nuevos o modificados no sirven
6	Adquisición, desarrollo o modificaciones de sistemas de información o infraestructura informática sin la coordinación		x		-Desarrollo y aplicación de la Políticas de Gestión de Proyectos de Ti	-Los proyectos que incorporen o modifiquen elementos a la infraestructura TI en hardware o software deben ser gestionados por Sistemas
7	Perdida de Datos por daño en servidores o dispositivos de almacenamiento			x	-Copias de seguridad diarias en la nube - Adquisición de un dispositivo profesional de almacenamiento externo en red y un Gabinete para backups	-La probabilidad de ocurrencia es baja, pero el riesgo tendría una afectación muy alta. -Actualmente la oficina de Sistemas tiene una política de Backups bien diseñada que ayuda a disminuir la probabilidad de ocurrencia, sin embargo factores extremos como incendio, terrorismo etc, podrían afectar de manera grave
8	Incorporación de nuevos funcionarios generando errores en el ingreso de la información	x				-Nuevos usuarios en los sistemas de información que por desconocimiento no realicen los procesos de manera correcta

9	Fallas irreparables en Servidores, Equipos de Red, Software de Sistemas Operativo o Software de Bases de Datos			x	-Mantener activo durante todo el año la garantía de los equipos servidores, de red o software de BD y SO	-Se debe mantener durante todo el año un contrato de mantenimiento correctivo y preventivo a todos costo que permita de manera rápida el cambio de partes dañadas o defectuosas
10	Fallas irreparables en Equipos de Computo o periféricos		x			-Se debe mantener durante todo el año un contrato de mantenimiento correctivo y preventivo a todos costo que permita de manera rápida el cambio de partes dañadas o defectuosas

10. APROBACIONES:

Elaboró	Revisó	Aprobó
CESAR AUGUSTO BARRERA RIVEROS **Líder del Proceso**	ADRIANA CRISTINA ROSAS V. **Representante por la Dirección SGC**	JAIRO BOSSUET PEREZ BARRERA **Representante Legal**

11. BITÁCORA DE ACTUALIZACIÓN

Versión	Fecha de Elaboración	Ítem Modificado	Motivo	Aprobado por
01	2021-01-29	Todo	Aprobación Inicial	Comité de Gestión y Desempeño

Empresa de Acueducto, Alcantarillado y Aseo de Yopal E.I.C.E - E.S.P	PROCESO GESTIÓN DE RECURSOS TECNOLÓGICOS		TIPO DE FORMATO FORMATO
	SOLICITUD DE REGISTROS Y GRABACIONES DE SEGURIDAD		CÓDIGO 51.26.08.01.02
	Empresa de Acueducto, Alcantarillado y Aseo de Yopal		
	FECHA DE ELABORACIÓN 2020-02-03	FECHA DE MODIFICACIÓN 2021-01-29	VERSIÓN 02

Fecha _____

Fecha(s) de la cual se solicita información	Tipo de Información solicitada	Rango de Hora (si aplica)	Comentarios adicionales
	Video_____ Registro de entrada/salida_____ Otro____cual?_____ _____		

Nota: *Para solicitud de videos o registro de entradas y salidas, es necesario suministrar el medio magnetico para el almacenamiento y entrega de la información.

Motivo solicitud de la información (Describa en detalle los hechos que motivan la solicitud de la información)

Datos Solicitante de la Información			
Nombre			
Cargo			
No. Cédula		Correo electronico	
Firma			

*Con mi firma y huella me comprometo ha hacer buen uso de la información que se me entregue y a no utilizarla en actividades al margen de la Ley o o que afecten el buen nombre del la empressa de Acueudto. Alcantarillado y aseo de Yopal

Autorizaciónes de la solicitud		
AUTORIZACIÓN ADMINISTRATIVA Y SISTEMAS Dependiendo de donde proviene la solicitud (Funcionarios o Externos) los jefes de Director administrativo y Oficina de sistemas de la EAAAY		FIRMAS
Director Administrativo y Financiero		
Oficina de Sistemas		

Empresa de Acueducto, Alcantarillado y Aseo de Yopal E.I.C.E - E.S.P NIT. 844.000.756-4	**CONTROL SOLICITUD DE REVISION DE CAMARAS EAAAY**		**Tipo de Documento:** Formato	
			Código: 51.26.08.01.03	
	Fecha de Elaboración: 2013-06-24	**Fecha Última Modificación:** 2021-01-29	**Versión:** 02	**Página:** 1 de 1

NOMBRE SOLICITANTE	NUMERO DE IDENTIFICACION	DEPENDENCIA	N° DE CAMARA O UBICACIÓN	FECHAS DE EVENTO	HORA INICIAL-FINAL DEL EVENTO	MOTIVO DE LA REVISION	FIRMA DE FUNCIONARIO

Nota Importante:
Las personas autorizadas para acceder a las grabaciones del CCTV, sólo tendrán acceso a las imágenes a manera de consulta; salvo en aquellos casos en que el material videográfico se requiera como prueba dentro de un proceso adelantado por autoridad civil, penal, fiscal o disciplinaria competente que conforme a las normas de procedimiento así lo solicite, la oficina de sistemas no entregará copia de grabaciones, ni certificará las imágenes grabadas, previa autorizacion de Gerencia o Direccion Administrativa.

Empresa de Acueducto, Alcantarillado y Aseo de Yopal E.I.C.E - E.S.P	REGISTRO DE PUBLICACIONES PORTAL		TIPO DE DOCUMENTO FORMATO
			CÓDIGO 51.26.08.01.04
	FECHA DE ELABORACIÓN 2021-01-29	FECHA DE MODIFICACIÓN 2021-01-29	VERSIÓN 01

FECHA SOLICITUD	FECHA PIBLICACIÓN Y/O ACTUALIZACIÓN	TEMAS	ACTIVIDADES	WEB	LINK O RUTA	AREA QUE SOLICITA Y OBSERVACIONES

Empresa de Acueducto, Alcantarillado y Aseo de Yopal E.I.C.E - E.S.P NIT. 844.000.755-4	**CONTROL EQUIPO PORTATIL EXTERNO**	**Tipo de Documento:** Formato
		Código: 51.26.08.01.05
	Fecha de Elaboración: 2012-02-14 / **Fecha Última Modificación:** 2021-01-29	**Versión** 02 / **Página:** 1 de 1

DATOS DEL SOLICITANTE

Nombre(s) y Apellidos: _____

Dependencia: 0 Gerencia 0 Administrativa 0 Comercial 0 Técnica 0 Aseo Otro: _____

Número de Identificación: _____

Celular:

Nro de Contrato: | Fecha inicio Contrato: | Fecha Terminacion Contrato

Objeto:

DATOS DE LA COMPUTADORA PORTÁTIL

Marca Del Equipo: _____

Modelo: _____

Número de serie: _____

Nombre del equipo en la Red: _____

Ip asignada por la EAAAY: _____

La computadora portatil ingresa con los siguientes programas instalados:

Programas instalados por la E.A.A.A.Y

0 QFDocument

0 Sysman

0 Otro (s)

Carpetas Compartidas:

0 Dtec 0 Dadf 0 DCom 0 Daseo 0 Archivo 0 Planeacion 0 Otro (s) (especifique)

Firma de Conformidad:

Fecha de Ingreso a la E.A.A.A.Y: (dd/mm/aaaa) _____

Fecha de Retiro de la E.A.A.A.Y (dd/mm/aaaa) _____

Nombre y Firma del Responsable o Propietario

Nombre y Firma del Responsable de la Devolución

Nota Importante

Al aceptar el ingreso de la computadora portátil y de sus accesorios. Automaticamente se hace responsable de los costos de posibles reparaciones, mantenimiento, robo o extravió, reposiciones totales o parciales de los componentes que resulten dañados por maltrato, mal uso, por sustitución no autorizada de componentes o desperfectos en el equipo. De igual forma el uso del internet y la disponibilidad del servicio esta sujeto a las politicas de seguridad de la empresa.