SOCIEDAD TEQUENDAMA

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN PETI 2023-2026 V.2

Bogotá, D.C.

ELABORO	REVISO	APROBÓ
Gloria Peña	Christian González	Christian González
Jefe de Tecnología de la Información y las Comunicaciones	Secretaria General	Secretaria General
Firma: 	Firma: 	Firma: 

Tabla de contenido

1. Introducción

El Gobierno Nacional, en cabeza del Ministerio TIC, viene trabajando para fortalecer 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, por tal motivo, MinTIC establece los lineamientos generales de la Política de Gobierno Digital, considerando los diferentes CONPES, leyes y decretos relacionados con la importancia de la ejecución y evolución del Gobierno Digital.

El propósito de este documento PETI de la Sociedad Tequendama está alineado con la Política de Gobierno Digital y apalanca los principios de la Transformación Digital (TD) Pública, buscando impactar positivamente la calidad de vida de los ciudadanos mediante el uso y aprovechamiento de las TIC, permitiendo habilitar, impulsar y mejorar la provisión de servicios digitales de confianza y calidad, los procesos internos seguros y eficientes, la toma de decisiones basadas en datos, el empoderamiento ciudadano a través de un Estado Abierto y el desarrollo de Territorios y Ciudades Inteligentes para la solución de retos y problemáticas sociales.

Para la construcción y actualización del PETI, es abordada la metodología propuesta por la guía técnica de estructuración del PETI (MinTIC) la cual busca validar el contexto institucional e identificar los elementos estratégicos que deben articularse y alinearse en la estrategia de TI. De igual forma, definir la equivalencia y compatibilidad respecto a las evidencias del Marco de Referencia de Arquitectura del MinTIC y del Formulario Único de Reporte de Avances a la Gestión (FURAG) del Modelo Integrado de Planeación y Gestión (MIPG), siempre enmarcados en el contexto de la Planeación Estratégica de la administración pública, con el ánimo de no duplicar información y contar con un direccionamiento que contemple todas las variables de TI.

2. Glosario

Aplicaciones: Son programas de computador que están diseñados con capacidades lógicas y matemáticas para procesar información. El término Aplicación se utiliza para agrupar un conjunto de programas que responden a requerimientos particulares del negocio o área de negocio.

Arquitectura Empresarial: Practica empresarial que analiza integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. Estas dimensiones deben hacer el enlace entre la Arquitectura de Negocio y la visión de TI. Se plantea la realización de la arquitectura misional o de negocio y la definición de la arquitectura de TI, cuya descomposición se hizo en seis dominios: Estrategia de TI, Gobierno de TI, Información, Sistemas de Información, Servicios Tecnológicos y Uso y Apropiación

Dato: Representación simbólica (numérica, alfabética, binaria, entre otras) de una medida cualitativa o cuantitativa o en general de cualquier valor. Un dato por sí mismo no constituye información ni conocimiento, como mínimo requiere una interpretación para poder generar conocimiento y/o información; pero también podría requerir procesamiento, otros datos y/o metadatos para ser generador de información.

Gobernabilidad: Define la capacidad de una organización para controlar y regular su propio funcionamiento con el fin de evitar los conflictos de intereses relacionados con la división entre los beneficiarios y los actores.

Gobierno de TI: Es un conjunto de procedimientos, estructuras y comportamientos utilizados para dirigir y controlar la organización hacía el logro de sus objetivos, utilizando las tecnologías de la información como herramienta de gestión.

Información: Unidad básica de conocimiento; en la definición básica de información "conjunto organizado de datos procesados, que constituyen un mensaje" es necesario entender la interpretación de datos como un proceso, por lo cual es este el factor desencadenador e infaltable para la generación de información.

Infraestructura: Conjunto de elementos lógicos y físicos que permiten que una determinada Solución funcione adecuadamente, tal y como fue diseñada.

Interoperabilidad: Es la acción, operación y colaboración de varias entidades para Intercambiar información que permita brindar servicios en línea a los ciudadanos, empresas Y otras entidades mediante una sola ventana de atención o un solo punto de contacto. Es decir, es la forma de ahorrarle a la gente los desplazamientos de un lugar a otro a la hora de realizar un trámite y de hacer el proceso menos engorroso.

PETI: El Plan Estratégico de Tecnologías de Información y Comunicación define las estrategias de la entidad en cuanto a TI, sistemas de información, servicios tecnológicos y del uso y apropiación de los anteriores. El modelo de gestión que apoya el PETI garantiza el valor estratégico de la capacidad y la inversión tecnológicas realizadas por la organización.

Plataforma: Es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible.

Servicio: Es un conjunto de actividades que buscan satisfacer las necesidades de un cliente.

Sistema de Información: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Definición de TIC: Las Tecnologías de la Información y las Comunicaciones (en adelante TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.

Catálogo de componentes de información – DEF.026 Es el inventario detallado y documentado del conjunto de componentes de información que tiene una institución o sector.

Catálogo de servicios de TI –DEF.027 Es un inventario detallado y documentado de los servicios de TI que la institución tiene implementados y que se encuentran activos, incluyendo los que están disponibles para ser desplegados. El catálogo de servicios de TI es el subconjunto del portafolio de servicios publicado para los usuarios.

Catálogo de servicios tecnológicos – DEF.028 Es un inventario detallado y documentado de los servicios tecnológicos que provee TI a la institución.

Catálogo de sistemas de información – DEF.029 Es un inventario detallado y documentado que contiene las fichas técnicas de los sistemas de información de una institución. Este es uno de los artefactos que se utiliza para describir la arquitectura de sistemas de información

Esquema de Gobierno TI – DEF.041 Es un modelo para la administración de las capacidades y servicios de TI de una institución. Incluye una estructura organizacional, un conjunto de procesos, un conjunto de indicadores y un modelo de toma de decisiones; todo lo anterior enmarcado en el modelo de gobierno de la entidad.

Estrategia TI – DEF.043 Es el conjunto de principios, objetivos y acciones concretas que reflejan la forma en la cual una entidad decide utilizar las Tecnologías de la Información para permitir el logro de su misión de una manera eficaz. La Estrategia TI es una parte integral de la estrategia de una entidad.

Indicador – DEF.050 En el contexto de la informática, un indicador es una medida de logro de algún objetivo planteado

Plan de comunicación de la Estrategia de TI – DEF.070 Toda estrategia debe ser comunicada de manera adecuada a los distintos interesados, dentro y fuera de una institución. El plan de comunicación define los tipos de usuarios a los que se informará, los tipos de contenido y medios de comunicación por usar, para divulgar la Estrategia de TI. Este plan es uno de los componentes de un PETI.

Plan de capacitación y entrenamiento – DEF.073 20 Define las actividades de capacitación y entrenamiento que se requieren para entrenar a los funcionarios de una entidad en aspectos específicos de una aplicación, una metodología, un producto, una tecnología o un proceso

Plataforma de interoperabilidad del Estado colombiano (PDI) – DEF.074 Conjunto de herramientas y políticas necesarias (Plataforma Base) para la interacción de soluciones y sistemas de información entre diversas Entidades del Estado. Define los esquemas que estandarizan y facilitan el intercambio de información entre entidades y sectores del sector público, el manejo de fuentes únicas de información, la publicación y habilitación de servicios.

Política de TI – DEF.075 Es una directriz u orientación que tiene el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI. Las políticas son usadas para dirigir las decisiones, para asegurar la consistencia y el apropiado desarrollo e implementación de los procesos, estándares, roles, actividades y servicios de TI.

Proyecto – DEF.077 Es un conjunto estructurado de actividades relacionadas para cumplir con un objetivo definido, con unos recursos asignados, con un plazo y un presupuesto acordados.

Servicio de TI – DEF.081 Es una facilidad elaborada o construida usando tecnologías de la información para permitir una eficiente implementación de las capacidades institucionales. A través de la prestación de estos servicios es que TI produce valor a la organización. Los servicios de información son casos particulares de servicios de TI. Los

servicios de TI deben tener asociados unos acuerdos de nivel de servicio.

Servicio Tecnológico – DEF.083 Es un caso particular de un servicio de TI que consiste en una facilidad directamente derivada de los recursos de la plataforma tecnológica (hardware y software) de la institución. En este tipo de servicios los Acuerdos de Nivel de Servicio son críticos para garantizar algunos atributos de calidad como disponibilidad, seguridad, confiabilidad,

Tablero de indicadores – DEF.084 Es un conjunto de indicadores cuya medición y seguimiento periódico brindará un mayor conocimiento sobre la situación real de una institución y el avance en el logro de sus objetivos. Un tablero de indicadores incluye una mezcla de indicadores estratégicos, tácticos y operativos

3. Siglas

AE Arquitectura Empresarial
SHT Sociedad Tequendama
PETI Plan Estratégico de Tecnologías de la Información
TI Tecnologías de la Información
TIC Tecnologías de la Información y Comunicación
MIPG Modelo Integrado de planeación y gestión

4. Análisis entorno y normatividad vigente

Marco Normativo

A continuación, se hace referencia a la normatividad a partir de la cual se realizaron los análisis, desarrollo e implementación de la tecnología y los sistemas de información del sector:

Marco Normativo	Descripción
Circular 018 de 2021	Implementación de la Resolución 1519 de 2020 por lo cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos y las comunicaciones (MinTIC) y la aplicación de la matriz ITA. (Aplicativo Índice de Transparencia y Acceso a la Información Pública.
Circular 02 de 2019	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
Circular Externa Conjunta No. 04 de 2019	Tratamiento de datos personales en sistemas de información interoperables.

Marco Normativo	Descripción
CONPES 3248 de 2003	La presente directiva fija las bases y los principios orientadores de la acción gerencial de los funcionarios para la modernización de la administración pública que se llevará a cabo durante el Gobierno que comienza. El CONPES, que hará las veces de Consejo Directivo para la Reforma de la Administración Pública, establecerá los lineamientos generales de este programa gubernamental, su alcance y sus mecanismos de evaluación.
CONPES 3292 de 2004	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
CONPES 3854 de 2016	Seguridad Digital para garantizar la seguridad de la información, o aquella norma que lo modifique o sustituya y las normas o lineamientos que al respecto emitan las autoridades nacionales.
Conpes 3920 de Big Data, del 17 de abril de 2018	La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.
Conpes 3975	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1078 de 2015	Artículo 2.2.5.1.2.2 Instrumentos- Marco de Referencia de Arquitectura Empresarial para la gestión de TI
Decreto 1151 de 2008	Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.

Marco Normativo	Descripción
Decreto 1413 de 2017	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
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".
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 2106 del 2109	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública
	Cap. II Transformación Digital Para Una Gestión Publica Efectiva
Decreto 2150 de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
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
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 2693 de 2012	Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.

Marco Normativo	Descripción
ecreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 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.
Decreto 4485 de 2009	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
Decreto 4890 de 2011	Por el cual se modifica parcialmente la estructura del Ministerio de Defensa Nacional y Se dictan otras disposiciones.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 620 de 2020	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Decreto 728 2016	Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Directiva 02 2019	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones
Directiva 03 de 2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Ley 1273 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.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Marco Normativo	Descripción
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAIS" "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1955 del 2019	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
Ley 2121 de 2021	Por medio de la cual se crea el régimen de trabajo remoto y se establecen normas para promoverlo, regularlo y se dictan otras disposiciones
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.
Norma Técnica Colombiana NTC 5854 de 2012	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.
Resolución 10584 de 2014	Por la cual se modifica parcialmente la resolución 1374 de 2012, - para ajustar las funciones del Grupo de Tecnología de Información y las Comunicaciones TIC.
Resolución 1374 de 2012	Por la cual se adiciona la resolución 127 de 2012 “Por la cual se crean y organizan Grupos Internos de Trabajo del Ministerio de Defensa Nacional”.
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
Resolución 3564 2015	Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
Resolución 500 de 2021	Lineamientos y estándares para la estrategia de seguridad digital
Resolución No. 3564 de 2015	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
Resolución 7870 de 2022	Política de seguridad y privacidad de la Información Sector Defensa

Marco Normativo	Descripción
Decreto 1263 de 2022	lineamientos y estándares para la Transformación Digital de la Administración Pública en el marco de la Política de Gobierno Digital, de conformidad con el artículo 147 de la Ley 1955 de 2019, o la norma que la modifique, adicione o sustituya.

5. Gobierno Corporativo

5.1 Misión

La Sociedad Tequendama se posiciona en el mercado como gestor y operador de diversas líneas de negocio que incluyen entre otras las relativas a activos inmuebles, hotelería, logística, catering, eventos y todo tipo de servicios que generen valor y provean soluciones a las entidades públicas y privadas, fortaleciendo la colaboración para fomentar sinergias empresariales y de negocio. Siempre ofreciendo a sus clientes la excelencia en el servicio desde un punto de vista organizativo, tecnológico, administrativo y operativo, y contribuyendo, desde su ámbito de actuación, a la mejora de la calidad de vida de los ciudadanos.

5.2 Visión

Progresar como empresa líder en diseño y desarrollo de soluciones de carácter multidisciplinar, desarrollando proyectos innovadores de alta calidad, rentables económica y socialmente, siendo reconocidos como una organización moderna, ágil y adaptable, que destaque en la gestión de la innovación para satisfacer las necesidades de sus clientes externos e internos, generando valor a sus accionistas y demás partes interesadas

5.3 Objetivos

Contar con una cultura organizacional que soporte la estrategia corporativa:

- Implementar el SIAO.
- Implementar un programa de competitividad laboral.
- Desarrollar una estrategia de comunicación que impacte a todos los niveles de la organización.
- Implementación del modelo SDO (Sistema de Desarrollo Organizacional).
- Desarrollo de liderazgo en red en los equipos de alto rendimiento.

Implementar modelos de negocio sostenibles:

- Modernización gobierno corporativo (Estructura, Estatutos, Manual).
- Estructuración y desarrollo de nuevos modelos de negocios.
- Optimizar el modelo empresarial existente (Propietarios y agentes).
- Generar modelos de evaluación financieros orientados al valor presente y futuro.
- Realizar campañas para reducir el impacto social y ambiental de nuestras actividades operativas.
- Generación de fuentes de financiación acorde a los modelos de negocios.

Incrementar la competitividad:

- Formular y desarrollar el plan de transformación tecnológica.
- Implementar el SIAO.
- Implementar un programa de competitividad laboral.

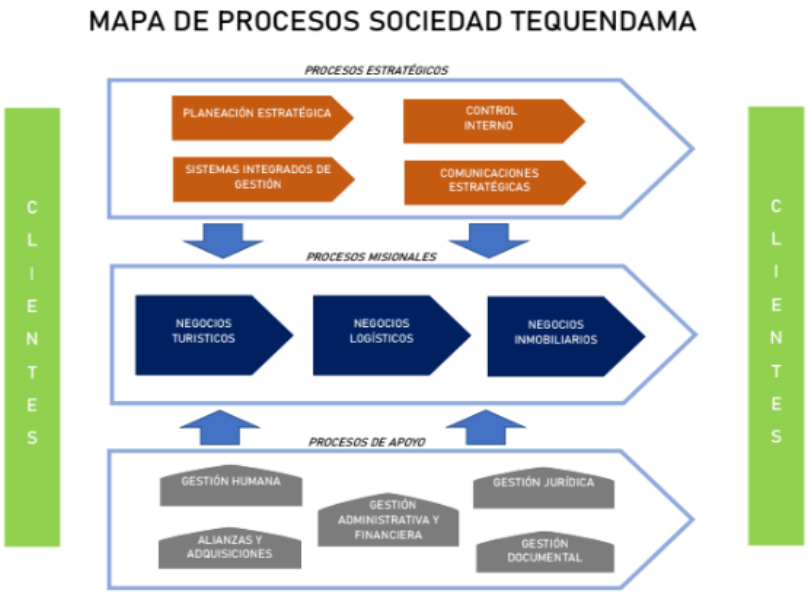
- Implementación Modelo de Innovación.
- Modernización gobierno corporativo (Estructura, Estatutos, Manual) .
- Optimizar el modelo empresarial existente (Propietarios y agentes).

Posicionar la marca de la empresa:

- Nuevos negocios enfocados al mejoramiento del posicionamiento de la marca Tequendama.
- Establecer estrategias para fortalecer la confianza en los grupos de valor.

6. Estructura Organización

7. Mapa de Procesos



8. Planeación Estratégica de TI

Desarrollar estrategias de TI para alinear sus objetivos, alcance y procesos de modo que la gestión y el aprovisionamiento agreguen valor a los servicios TI internos y externos dentro del marco de la política digital.

8.1 **Objetivo.**

Proporcionar a la Sociedad Tequendama el Plan Estratégico de Tecnología de Información y las Comunicaciones para el periodo 2023 – 2026, la hoja de ruta con iniciativas de TI, estableciendo los objetivos, inversiones de TI, metas y plan de comunicación.

Apoyar la toma de decisiones estratégicas para lograr mejores resultados y gestionar mas eficiente y eficazmente sus procesos, asegurando la infraestructura de red y los sistemas de vulnerabilidades en aspectos de seguridad.

Suministrar a los usuarios atención e información oportuna en la prestación de los servicios tecnológicos.

8.2 **Alcance**

El presente documento describe el Plan Estratégico de Tecnologías de Información y de Comunicaciones de la Sociedad Tequendama desplegando la estrategia de TI.

La Sociedad Tequendama es una sociedad anónima de economía mixta del orden nacional con régimen legal de las empresas industriales y comerciales del Estado, por tal motivo, el presente documento es flexible pudiendo ser ajustado o mejorado conforme las necesidades de la Sociedad Tequendama.

Los capítulos se encuentras enmarcados en la guía del MinTIC sobre la estructuración del Plan Estratégico de Tecnologías de Información – PETI.

Alinear la Política de Gobierno Digital al Marco de Referencia de Arquitectura definido por MinTIC, Gerencia de Proyectos de TI, Gestión y Gobierno de TI utilizando la metodologías, estructura, técnicas y herramientas que contiene el Plan Estratégico de TI, apoyando los procesos de Transformación Digital y de la cuarta revolución industrial en la administración pública.

8.3 Participantes interesados:

Grupo para la construcción del PETI		
Área	**Nombre de las personas**	**Función**
Planeación	Andrea Malagon	Garantizar que las acciones y mejoras propuestas estén alineadas con el Plan estratégico Institucional
Tecnologías de la Información	Gloria I. Peña - Jefe TIC	Orientar a las áreas en la definición de las acciones de mejora.
Áreas Misionales	Ana Jara - Gerencia de Negocios Turisticos Martin Orduz - Gerencia de Inversiones	Definir las oportunidades de mejora y posibles soluciones a cada una
Atención al Ciudadano	Juan Sebastian Gaviria - Desarrollo emprendimiento e innovación	Definir las necesidades de los usuarios de la entidad y posibles soluciones a cada una
Secretaría General (Financiera)	Christian Gonzales - Secretario General	Identificar el presupuesto que se debe asignar para cada acción.
Secretaría General (Representante legal)	Jorge I. Gomez - Gerencia General	Coordinar, hacer seguimiento y verificación de la implementación de las acciones definidas
Oficina de control interno	Henry Molano - Control Interno	Controlar y gestionar los riesgos asociados.
Áreas de apoyo	Christian Gonzales - Secretaria General	Velar por la adopción del modelo de Seguridad y Privacidad de la Información
Otros Participantes	**Área**	**Nombre**
	TIC	Gloria Ines Peña - Jefe TIC

8.4 Estrategia

Estrategia de TI 2023-2026	
Misión de TI	El Área de Tecnología de la Información y Comunicaciones - TIC lidera e incentiva el uso de las TIC en el la Sociedad, para la implementación de soluciones de TI que apoyen el logro de los objetivos estratégicos de la Sociedad Tequendama, a traves de la actualización de su infraestructura tecnologica para soportar la transformación digital apoyando los procesos de intercambio de información, interoperabilidad, seguridad y privacidad de la información, además de las funciones de Gestión de TI
Visión de TI	En el 2026, el Área de Tecnología de la Información y la Comunicaciones – TIC de la Sociedad Tequendama será reconocida por su capacidad para enfrentar los desafíos de la transformación digital y habrá logrado posicionar a la entidad en el uso y apropiación de nuevas tecnologías de TI que contribuyan al desarrollo del sector y apalanquen eficazmente el cumplimiento de las directrices del sector

Objetivos		
ID	ID	Nombre
S01		Aplicar estrategias de gestion del cambio para la apropiación de los proyectos tecnologicos
S02		Asegurar la seguridad de la informacion como resultado de la implementación de los proyecto que emprenderá la Sociedad
S03		Mejorar los procesos internos con seguridad y eficiencia a través de la optimizacipon de la gestión de tecnologías de información
S04		Contar con plataformas de informacion que contribuyan a la administración y optimización de la infraestructura de red y a la toma de decisiones
S05		Mejorar la percepcion de los usuarios frente al soporte y mantenimiento pasando de ser correctivos a predictivos
S06		Mejorar el proceso de atencion de requerimientos de soporte de los servicios de TI
S07		Facilitar la conectividad de todos los dispositivos tecnológicos usados para la conexión a internet con alcance IPv6
S08		Entregar a los usuarios herramientas que contribuyan a mejorar la productividad
S09		Establecer procedimientos específicos que respondan a interrupciones del servicio, identificando las aplicaciones y las plataformas consideradas críticas para la operación del negocio.
S10		Aplicar metodos, herramientas, procesos que contrinuyan a evitar amenazas a través de diferentes medios como emails, a detectar a tiempo códigos maliciosos, Reconocer conexiones sospechosas, Monitorear las bases de datos y Mantén los sistemas actualizados.
S11		Proteger a los usuarios y los activos de la organización de los ciberataques
S12		Eliminar el uso del papel en las operaciones rutinarias de la Sociedad para ser más amigables con el ambiente
S13		Impulsar el desarrollo sostenible o mejorar la calidad de vida de ciudadanos, usuarios o grupos de interés (Zona WiFi Gratis para los ciudadanos, usuarios)
S14		Implementar el intercambio de datos electrónicos con los sistemas que tiene el Estado para automatizar trámites dirigidos al ciudadano
S15		Aplicar un enfoque de Arquitectura Empresarial para el fortalecimiento de las capacidades institucionales y de gestión de TI
S16		Preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos mediante la aplicación del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado.
S17		Tomar decisiones basadas en datos a partir del aumento el uso y aprovechamiento de la información

9. Situación Actual TI

9.1 Servicios TI y Caracterizaciones

La Sociedad ofrece servicios a clientes internos y externos cuyo objetivo es mejorar la gestión mediante mecanismos de apoyo en la operación, administración, gestión y control con la aplicación de los lineamientos del Ministerio de la Telecomunicaciones, entre ellos la aplicación del Modelo de Arquitectura, MSPI y el SGSI con el objetivo de centralizar los lineamientos y documentación, evitando duplicidad, repetición y permitiendo que su actualización sea practica y sencilla

Dentro del marco de la AE buscamos aplicar los lineamientos abordando cada dominio no de forma completa sino disminuyendo el nivel de profundidad vertical y horizontal conforme al tamaño de la organización y de los recursos que se disponen.

9.1.1 Servicio de comunicaciones y acceso a red

Gestión de la conectividad de la red de comunicaciones y recursos de usuarios, grupos, aplicaciones y servidores, cuyo objetivo es garantizar la funcionalidad, estabilidad y continuidad de la infraestructura de red, brindando un medio de comunicación seguro y confiable para la trasmisión y recepción de información (voz, datos, videos e imágenes entre otros), estableciendo una comunicación ágil y segura.

Descripción del Servicio. El servicio de Comunicaciones facilita al usuario, a través de la red de la ST, el acceso a los sistemas de información y herramientas tecnológicas de la Entidad. Este servicio también contempla la Seguridad Perimetral y la Administración del Datacenter principal, incluyendo servicios de implementación, configuración y diagnóstico, soportados en los pilares de la seguridad informática (confidencialidad, integridad y disponibilidad de la información).

Está enfocado en brindar a los usuarios las siguientes actividades o productos para satisfacer sus necesidades:

- Red LAN (al interior de cada área de la ST).
- Red WAN (entre las sedes de la ST).
- Telefonía (análoga e IP).
- Acceso a redes Inalámbricas.
- Administración de Usuarios y Privilegios de acceso.
- Acceso a puertos USB y unidades de DVD/CD.
- Asignación de espacio de Almacenamiento a usuarios.
- Protección Antivirus.
- Filtrado Url navegación filtrado correo electrónico.
- Protección WAF a aplicativa web internos con IP pública.
- Firewall.
- VPN´s.

9.1.2 Servicios corporativos tecnológicos

Garantizar la funcionalidad y estabilidad de la infraestructura de servicios Corporativos tecnológicos de la SHT a los usuarios, de manera segura y confiable mediante el intercambio de mensajes a través de una cuenta de correo electrónico institucional, acceso a portales Web externos e internos y herramientas de comunicación institucional, que facilite el desarrollo de sus funciones y la trasmisión y recepción de información (voz, datos, videos e imágenes entre otros) con el exterior y a la vez establecer un sistema de gestión y comunicación interna/externa preservando la seguridad de la información de la ST.

Descripción del Servicio. Los servicios Corporativos facilitan al usuario, a través de la red de la ST, el acceso a correo corporativo y al World Wide Web a través de un navegador a portales y herramientas corporativas que permitan la integración de empleados, clientes y proveedores de la SHT y que soporten de manera apropiada la imagen corporativa de la Entidad. Está enfocado en brindar a los usuarios las siguientes actividades o productos para satisfacer sus necesidades:

- Portal Web.
- Correo Corporativo (desde el interior de la ST o sitios externos).
- Video Conferencia (entre las sedes de la ST y otros usuarios externos).
- Acceso a sistemas de información y administración de usuarios

9.2 Caracterización de los Servicios

Caracterización de Servicios

Servicios					Variables											
ID	Nombre del Servicio	Descripción del servicio	Áreas que participan	Tipo de usuario	Ingresos último año	Costos último año	# de solicitudes último año	Nivel de satisfacción del servicio	# de PQR recibidas	Nivel de complejidad actual	Nivel de criticidad	Nivel de valor al ciudadano	Tiempo promedio del ciclo del servicio	Nivel de riesgo de corrupción	Servicio en línea	Canal 1
SIA	Servicio de Internet administrativo	El servicio de internet para la recepción y transmisión de voz, datos, imágenes, videos, entre los integrants de la Sociedad, clientes y proveedores	TIC Financiero Compras Op.Logistica	Admiinstrativo				BUENO		Bajo	Medio	Medio		Bajo	Si	CWC Business
SIH	Servicio de Internet huespedes	El servicio de internet para la recepción y transmisión de voz, datos, imágenes, videos para huespedes de Suites Tequendama y Hotel Estacion de Buenaventura	TIC Suites Tequendama Hotel Estacion de Buenaventura	Cliente				BUENO		Bajo	Medio	Medio		Bajo	Si	CenturyLink
SSG	Seguridad gestionada	Servicio para conectarse y navegar con un alto nivel de seguridad, y gestionarmiento de incidencias y vulnerabilidades de la red . Minimizar los riesgos generales de seguridad, reducir el tiempo de inactividad de las aplicaciones y proteger los activos digitales. y estar preparados para DETECTAR, PROTEGER Y RESPONDER a cada posible amenaza, 24/7	TIC C&W Business SHT SEGURIDAD PERIMETRAL Y CONECTIVIDAD	Tecnico				BUENO		Medio	Medio	Medio		Bajo	Si	CWC Business
SCE	Servicio de correo electronico	Servicio de correo electronico. migracion a version google Business. backup y auditoria	Todos los empleados de SHT	Administrativo				BUENO		Bajo	Medio	Medio		Bajo	Si	
SCLOUDERP	Aplicativo ERP	es la plataforma integrada de sistemas de información que permite el manejo y control financiero, contable	Usuarios del area financiera , compras, operacion logistica	Administrativo				BUENO		Medio	Alto	Medio		Bajo	Si	
SCLOUDZEUS	Aplicativo PMS	Plataforma en la nube, integrada de sistemas de información que permite el manejo y control de los huespedes hospedados	Usuarios de Suites Tequendama, Catering y nuevos negocios hoteleros	Administrativo				BUENO		Medio	Alto	Medio		Bajo	Si	
SCLOUDNOM	Aplicativo Nomina	Plataforma enla nube, integrada de sistemas de información que permite el manejo y control de la nomina publica	Usuarios de Talento Humano	Administrativo				BUENO		Medio	Alto	Bajo		Bajo	Si	
SHIST	Servidor de historicos	Consulta de datos historicos de los aplicativos viejos: Contabilidad, Vertical hotelera y nomina	Financiero Talento HUmano Contrarlor Suites Tequendama	Administrativo				BUENO		Bajo	Medio	Bajo		Bajo	No	
SGD	Gestion documental	Plataforma enla nube, integrada de sistemas de información que permite el manejo y control del gestor documental, incluye flujos de informacion	Todos los empleados de SHT	Administrativo				BUENO		Medio	Medio	Bajo		Bajo	Si	
SCLOUDOPL	Aplicativo control de eventos	Plataforma enla nube que permite el manejo y control de los eventos y presupuesto	Operacion logistica	Administrativo				BUENO		Bajo	Bajo	Bajo		Bajo	Si	
SCLOUDVulnrabilidades	Escaneo Vulnerabilidades	Aplicacion por demanda	TIC	Tecnico				BUENO		Medio	Alto	Bajo		Bajo	Si	
SPW	Pagina web	Pagina informativa	Comunicaciones TIC	Administrativo				REGULAR		Medio	Alto	Bajo		Bajo	Si	
SCLOUDBackup	Solucion Backup	Copia de seguridad y recuperación en la nube equipos de computo	TIC Todos los empleados de SHT con equipo de computo	Tecnico				BUENO		Medio	Alto	Bajo		Bajo	Si	
SCLOUDAntivirus	Solucion Antivirus	Monitoreo, politicas, alertas	TIC Todos los empleados de SHT con equipo de computo	Tecnico				BUENO		Medio	Alto	Bajo		Bajo	Si	

9.3 Catálogo de brechas

Catálogo de brechas					
ID	ID Servicio	Descripción	Tiempo estimado total	Costo estimado inversión total	Proyecto en ejecución [SI, NO]
B001	Aplicar estrategias de gestion del cambio para la apropiación de los proyectos tecnologicos	Apoyar la transformacion digital de la Sociedad con estrategias de Gestin del cambio			NO
B002	Mejorar la percepcion de los usuarios frente al soporte y mantenimiento pasando de ser correctivos a predictivos	Generar estrategias para contar con información que contribuya a detectar predictivamente posibles incidencias y fallas para garantizar la operación de la Sociedad y la continuidad del nogocio			SI
B003	Facilitar la conectividad de todos los dispositivos tecnológicos usados para la conexión a internet con alcance IPv6	Mantener la capacitad de la Sociedad para soportar la Transformación digital			SI
B004	Proteger a los usuarios y los activos de la organización de los ciberataques	Aplicar metodos, herramientas, procesos para evitar / minimizar ataqes ciberneticos			SI
B005	Disminuir el uso del papel en las operaciones rutinarias de la Sociedad para ser más amigables con el ambiente	Definir, establecer y ejecutar estrategias para eliminar el uso del papel en las operaciones rutinarias de la Sociedad para ser más amigables con el ambiente			NO
B006	Optmizizacion de la infraestructura tecnologica	Tercerizar la gestion de la infraestructura de red para obtener información veraz, critica, actualizada, completa, exacta que ayuden a la toma de decisiones en el mejoramiento de la misma			SI
B007	Implementar zonas wifi para uso de los ciudadanos que visitan el centro internacional	Poner a disposicion de los ciudadanos zonas wifi gratis para su acceso a internet y la posibilidad de realizar tramites, capacitaciones, entretenimiento, consultas, etc			NO
B008	Interoperabilidad. Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad	Implementar procesos de interoperabiidad con instituciones publicas			NO
B009	Ciberseguridad	Plan de trabajo. Implementar politicas, alertas, controles, monitoreo para la proteccion de la infraestructura de red y los datos			SI
B010	Programa de Proteccion de datos	medidas de seguridad y de gestión de riesgos para sus bases de datos automatizadas y físicas, de acuerdo con la normatividad en Protección de Datos Personales.			SI
B011	Seguridad en el tráfico y almacenamiento de datos por cifrado avanzado	proceso de codificación de la información			NO

9.4 Catálogo de iniciativas de Planes de la Política de Gobierno Digital

Catálogo de iniciativas de Planes de la Política de Gobierno Digital											
ID	Nombre Iniciativa	Plan asociado	ID Servicios asociados	Descripción	Área Líder	ID Metas estratégicas	Áreas Involucradas	Tiempo total estimado	Fecha inicio estimada	Costo estimado inversión total	Brechas
IPGD002	Disminuir el uso del papel en las operaciones rutinarias de la Sociedad con el uso de firma digital		S11	Actualizar el sistema de informacion utilizado a la fecha conforme a lineamientos deel Archivo General de la NAcion y conforme para suplir el resultado del diagnostico de la situacion actual y sus mejoras	GESTION DOCUMENTAL		Todas		2024		
IPGD003	Zona WiFi Gratis para los ciudadanos		S12	Implementar zonas wifi en el Centro Internacional para proporcionar servicio al ciudadano facilittando su interaccion con las entidades del estado, brindando conectividad en pro de obtener servicios ágiles, sencillos y útiles para usuarios y grupos "Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad".	Desarrollo e innovacion		GERENCIA EMPRENDIMIENTO DESARROLLO E INNOVACION		2023-2026		
IPGD004	Interoperabilidad. Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad		S13	Implementar el intercambio de datos electrónicos con los sistemas que tiene el Estado para automatizar trámites dirigidos al ciudadano	TIC		SUITES		2023-2026		
IPGD005	Actualizar WIFI gestionado Suites (acces point)			Actuaizacion infraestructura de red	TIC		SUITES		2024-2025		
IPGD006	Avanzar en el Proyecto de Renovación tecnologica de equipos de computo.			Modernizacion de equipos	TIC		TODAS		2023		
IPGD007	Actualizar la página Web de la Sociedad			Rediseño de la pagina y validacion aplicacion ITA	COMUNICACIONES		COMUNICACIONES		2024		
IPGD008	Realizar la solución de backup			Copia de seguridad y recuperación en la nube equipos de computo	TIC		TODAS		2023		
IPGD009	Optimizar la infraestructura de red			renovación de dispositivos, servidores, sistemas operativos, hardware, software.	TIC		TIC		2023		
IPGD010	Estructurar mejoras en el Sistema de gestión de seguridad de la información			Politicas Proteccion de datos Politicas de segurida en proteccion de datos Politicas de seguridad proveedores y contratistas Solucion de antivirus Solucion de bACKUP	TIC		TIC		2023-2026		
IPGD011	Realizar la solución de Antivirus			Servicios de administración seguridad en Endpoint con EDR y XDR - SMS	TIC		TIC		2023		

9.5 Conforme a las Dimensiones de la AE tenemos:

9.5.1 Información

Basados en el dominio de arquitectura de información donde se define la estructura, almacenamiento, datos, servicios y flujos de información que soportan los procesos de la Sociedad trabajaremos en el levantamiento y actualización del componente de información.

9.5.1.1 Catálogo de los componentes de información.

La Sociedad tiene identificada la información que debe producir, las fuentes que la generan y el proceso de validación de esta, realizaremos el levantamiento de la información siguiendo las actividades propuestas en la metodología para su construcción y la aplicación de conceptos relacionados en AE, así mismo las actividades propuestas en el MSPI y SGSI uno será fuente y/o complementario del otro.

La Sociedad toma como base las diferentes guías que apliquen de forma general y practica sin llegar al detalle exhaustivo de las mismas. Como pasos básicos tendremos:

- Identificar la información que produce la entidad: Flujos de información, mapa de información, servicios de información, nuevos servicios de información para automatizar.
- Identificar los datos que conforman la información en términos del negocio, datos relevantes asociados con la misión y objetivo de la Sociedad, datos

georreferenciados.

Se utilizará una caracterización ampliada que consolida los diferentes conceptos (atributo y descripción)

9.5.1.2 Interoperabilidad.

En la actualidad tenemos integración en línea con MinCIT por medio de la vertical hotelera desde donde se envia la información del huésped principal y acompañantes en el momento de cada chek out del huésped principal, el envio se hace automático sin intermediación del usuario.

A medida que se realizan solicitudes de los organismos del estado procedemos con el análisis correspondiente para atender dicho requerimiento buscando siempre ser oportunos, enviar información de calidad y segura.

9.5.1.3 Apertura de datos

La Sociedad a la fecha no cuenta con portales de servicio de información al servicio de clientes, proveedores, empleados u otros, la entrega y/o presentación de información oficial se realiza por medio de reportes e informes publicados en su página web https://sociedadtequendama.com/ y gestor documental para las PQRs

9.5.2 Sistemas de Información

Conforme el dominio de la arquitectura de aplicaciones que define los componentes de los sistemas, las interacciones entre ellos y la relación con la información y la infraestructura de TI

La política de la Sociedad Tequendama sobre los sistemas de información es adquirir el servicio en la nube para la realización de sus operaciones financieras, administrativas, de nómina, de operación hotelera y e eventos, y así para las diferentes iniciativas que vayan surgiendo. Estos aplicativos ya vienen estructurados y trabajan por módulos; sin embargo, cuando se requiere algún desarrollo surten el proceso de solicitud, análisis, aprobación y entrega a satisfacción. Se pueden dar interacciones entre diferentes aplicativos para lo cual también deben realizar el proceso de solicitud mencionado.

Para la operación de los sistemas de información se requiere el concurso de las personas, los procesos, la tecnología, la información y el componente de seguridad. Los aplicativos optimizan y mejoran los procesos empresariales agilizando la operación, facilitando el análisis de información, y disponiendo de información en tipo real.

Se requiere implementar mecanismos de control y auditoria para poder tener mayor trazabilidad de las acciones realizadas sobre las bases de datos y sobre los accesos a los sistemas de información, dado que se presentan inconsistencias en los sistemas de información como errores en la funcionalidad e inconsistencia en ejecución de procesos.

Se requiere la generación de manuales de usuario el aplicativo financiero. Contable

A continuación, se relacionan los sistemas de información que operan en la Sociedad

Tequendama:

Microsoft Dynamics Business Central 365	ERP
PMS Zeus Hotel y POS	Vertical hotelero (HISTÓRICO)
MyHotel	Encuestas huéspedes
Nómina web Novasoft	Nómina pública
ZUM	Control presupuesto cliente
Orfeo	Gestor documental
PMS Zeus	Gestion hoteles y POS

9.5.3 Infraestructura Tecnológica

Con base en el dominio de infraestructura tecnológica definimos los elementos de la infraestructura de TI que soportan la operación como es el hardware, dispositivos, interfaces de comunicación y los servicios en la nube entre otros.

La Sociedad Tequendama busca orientar sus esfuerzos hacia la prevención sin descuidar el mantenimiento correctivo, para ello busca consolidar una base de datos de conocimiento para identificar incidencias repetitivas con resultados efectivos permanentes, definir alternativas de mejora en la red, investigar nuevas plataformas y fortalecer la seguridad informática, apoyados en los lineamientos de MinTIC y MND con Aliados estratégicos con experiencia y conocedores de última tecnología.

Se identifica la necesidad de implementar herramientas y mecanismos efectivos de seguridad e integridad de la información

Se requiere implementar Infraestructura adicional para soportar la continuidad de los procesos core del negocio

Se actualizará el plan de recuperación de desastres

9.5.4 Mantenimiento TICs

Realizar labores de mantenimiento preventivo de equipos de cómputo, servidores, impresoras, equipos activos, ups, planta telefónica y aire acondicionado y software, con el fin de prevenir incidentes mayores, problemas de funcionamiento y perdida de datos que puedan afectar la operación de los usuarios y de esta manera contar con un primer nivel de continuidad de la operación de la infraestructura tecnológica y lógica de la entidad, se planifican tareas de revisión y reparación de hardware y software para mantener los sistemas en niveles operativos.

El objetivo es conservar en condiciones adecuadas la operación de los dispositivos de hardware y software para mantener su vida útil obteniendo el mejor rendimiento y con

costos no elevados

Acciones a realizar para cumplir con el objetivo son:

- Contar con herramientas adecuadas, un equipo de trabajo cualificado, educando a los usuarios en el cuidado de los elementos tecnológicos de trabajo.
- Instalar, atender, mantener y actualizar todos los equipos de cómputo, celulares, impresoras de las diferentes áreas con el fin de garantizar el mejor desempeño posible
- Ejecutar una inspección periódica en las instalaciones, detectando cualquier desgaste, rotura, calentamiento de los dispositivos

9.5.5 Mesa de Ayuda

La mesa de ayuda es el servicio que ofrece información y soporte técnico a los usuarios de forma centralizada, su objetivo es gestionar, coordinar, atender y resolver incidentes relacionados con los activos tecnológicos lo más pronto posible. El personal de la mesa de ayuda debe proporcionar respuestas y soluciones a los usuarios finales

El registro de casos se realiza en el software mesa de ayuda, donde se clasifica los casos por criticidad, se realiza retroalimentación de los casos y se presentan recomendaciones y/o mejoras, cada ticket debe contemplar el incidente y la solución al mismo con el fin de crear una base de conocimiento.

La Sociedad cuenta con un aliado estratégico para atender la mesa de ayuda nivel 2, el personal de la Sociedad del área de TIC atiende el nivel 1 y las urgencias si es el caso. El nivel 3 y 4 se asigna al proveedor del hardware / software

Son servicios de administración de hardware, software y comunicaciones, que conforman la infraestructura de colaboración del negocio, que permiten ejecutar todas las actividades necesarias para la implantación y buen desempeño de la plataforma y que corresponden a actualizaciones, configuraciones, mantenimiento, gestión, soporte y solución de incidentes.

La mesa de servicios de la SHT tiene como principal objetivo brindar (de forma eficiente, eficaz, efectiva y oportuna) soluciones y asistencia funcional y técnica a los requerimientos de los usuarios finales sobre la operación y uso de todos los servicios. El Servicio de Soporte Tecnológico está enfocado en brindar a los usuarios soluciones en Instalación y Mantenimiento preventivo/correctivo de infraestructura tecnológica (hardware, software, comunicaciones y periféricos).

Condiciones de uso del servicio

- Solicitar el servicio mediante el envio de un correo electrónico a la mesa de ayuda
- Contar con un usuario de correo corporativo lo cual a su vez le permita acceso a la “mesa de ayuda”.
- Horario permitido de acceso: lunes a viernes de 8ªm – 5 pm y sábados de 8am - 1pm
- Niveles de Soporte:
  - 1er. Nivel de soporte: Solicitado en la “mesa de ayuda” y solución en sitio por parte del personal de ST

— 2°. Nivel de soporte: Ofrece un nivel de soporte y solución especializado en el servicio, es brindado por el aliado estratégico.
— 3°. Nivel de soporte: Este nivel de soporte está representado por el aliado estratégico y/o los proveedores externos.

9.5.6 Administración de la Plataforma Tecnológica

El objetivo de la Sociedad ha sido el optimizar y mejorar la plataforma tecnológica progresivamente incrementando su nivel de madurez tecnológica. A la fecha a hecho la transición de IPv4 a IPv6 configurando Dual Stark, es decir, la coexistencia IPv4-IPv6 es una solución de transición IPv6 para ISP con infraestructura IPv6 para conectar sus suscriptores IPv4 a Internet, seguido por la separación de servicios compartidos con el operador GHL, análisis y mejoramiento de la segmentación de la red, configuración del Directorio Activo y aplicar una seguridad gestiona.

Lo anterior con el fin de administrar la plataforma tecnológica y asegurar la continuidad operacional de los servicios TI y el funcionamiento continuo de cada parte de la misma.

9.5.7 Seguridad

Plataformas y aplicativos

El dominio de arquitectura de seguridad nos ayuda a identificar y diseñar los controles para asegurar la protección de la información en la arquitectura de información, de los sistemas de información y la infraestructura tecnológica

Los aplicativos optimizan y mejoran los procesos empresariales agilizando la operación, facilitando el análisis de información, y disponiendo de información en tipo real, por lo tanto, su administración es clave en relación con la seguridad de acceso de usuarios para ello consideramos la implementación de autenticación de doble factor adicional a la aplicación de los perfiles de acceso y la administración de la contraseña.

Otro elemento importante de gestionar son las plataformas digitales las cuales traen riesgos asociados a la privacidad y a la protección de datos, debido a que permiten acceder, visualizar y descargar aplicativos que facilitan la perdida de información parcial o total, fraude, amenazas técnicas, entre otras cosas.

Tratamiento de datos

Se realizará fortalecimiento en los siguientes temas relacionados con la Ley 1581 de 2012.

- Políticas de Protección de dato
- Organización interna para protección de datos
- Tratamiento de datos personales y finalidades
- Transmisión y Transferencia de dato
- Revisión documental
- Atención a consultas y reclamos
- Políticas de seguridad
- Consentimientos

- Auditorías
- Cultura organizacional y capacitaciones

Ítems sujetos a verificación:

- Sitio Web
- Organización Interna
- Instalaciones físicas
- Procesamiento de datos
- Gestión de consentimiento
- Procedimiento de atención a consultas y reclamos
- Aplicación de las medidas de seguridad en las bases de datos automatizadas y físicos
- Conocimiento de las políticas
- Ciclo de vida del dato
- Control de acceso a la red, Dispositivos y mecanismo de identificación
- Dispositivos móviles
- Gestión de activos
- Control de acceso
- Áreas Seguras
- Criptografía
- Seguridad de las Operaciones
- Seguridad de las Comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas
- Pruebas de estrés y Hacking Ético
- Gestión de proveedores - Encargados
- Gestión de incidentes de seguridad
- Guía de Responsabilidad Demostrad

La seguridad de la información se ha convertido en el factor más importante de mantener, sostener, mejorar, monitorear y gestionar permanentemente y para ello buscamos mejorar la topología de red con equipos gestionables, optimizar la segmentación de la red, aplicar seguridad gestionada, mantener aplicativos en la nube, contar con el directorio activo. De igual forma educar a los usuarios sobre cuidados, alertas y el manejo de sus equipos y accesos.

Dado el avance en temas de seguridad y disponibilidad de las plataformas y software en la nube se realizará una revisión de viabilidad de sistemas tanto de soporte a procesos misionales como de gestión de TI que puedan ser migrados a este modelo de servicio y operación tecnológica.

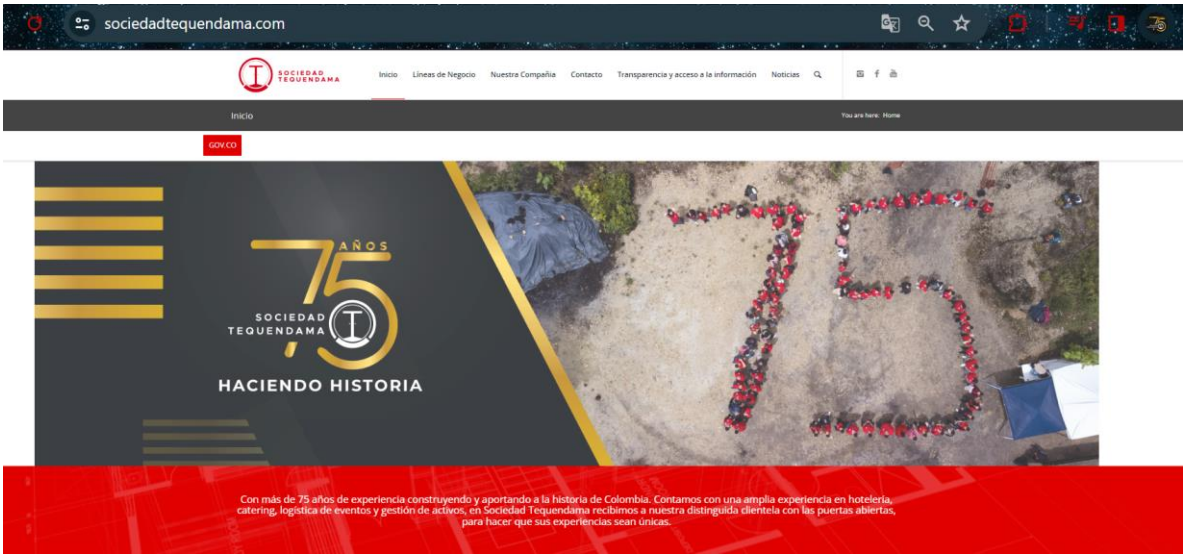
Finalmente, las copias de seguridad de la información son indispensables para garantizar disponibilidad de la información ante eventos desafortunados por perdida, daño, eliminación o alteración de la información, para ello existe mecanismos de Backp en la nube u on-premise que se deben tener para las bases de datos, los equipos de cómputo, y los correos electrónicos, contamos con backups de los sistemas de información en la nube de forma periódica

La ventaja de contar con copias de seguridad online es que son automáticas, no graban ubicaciones físicas, la información esta encriptada, se conservan diferentes versiones, se realiza de forma diaria, semanal, quincenal, semanal, anual, asegurando la información en un lugar diferente y se puede restaurar en cualquier momento.

Implementaremos una solución de backup que cubre todas las áreas, sistemas información, medios de comunicación, páginas web, etc

Página web

La Sociedad cuenta con una página web principal. https://sociedadtequendama.com/



La Sociedad Tequendama es una sociedad anónima de economía mixta de la orden nacional autorizada por la ley 83 de 1947, constituida por escritura pública 7.589 de 1948 (Notaría Segunda) vinculada al Ministerio de Defensa Nacional, sometida al régimen legal de las empresas industriales y comerciales del Estado, dotada de personería jurídica, autonomía administrativa y capital independiente.

Cuenta con diferentes líneas de negocio que cumplen con su objetivo:

LINEAS DE NEGOCIO

AGENCIA INMOBILIARIA TEQUENDAMA

La agencia inmobiliaria está orientada al sector público (entidades del estado), especialmente las pertenecientes al Ministerio de Defensa Nacional.

EVENTOS TEQUENDAMA

Las líneas de negocio de la agencia de eventos se encuentran orientadas a ambos mercados, destacando el sector privado, sobre el cual desarrollamos distintas estrategias para su convocatoria o relacionamiento.

OPERACIÓN LOGISTICA

Contamos con Alianzas estratégicas en cada una de las unidades de servicios requeridas por los clientes y amplia red de proveedores, para cumplir con la operación a nivel Nacional.

CATERING TEQUENDAMA

Lo invitamos a conocer nuestro portafolio de servicios y comprobar porque en Catering Tequendama estamos "Comprometidos con su satisfacción"

TEQUENDAMA SUITES AND HOTEL

Tequendama Suites and Hotel identifica su Razón de Ser, en la generación de experiencias bajo el esquema " Co-creating". Generar espacios para el relacionamiento de negocios para Huéspedes y Visitantes.

ECOHABS Y CABAÑAS PARQUE TAYRONA

El Parque Nacional Natural Tayrona reabre sus puertas con más y mejores servicios, con una infraestructura renovada y con el sello de calidad que ofrece la Sociedad Tequendama

PARQUEADERO TEQUENDAMA

Parqueadero Tequendama

OTRAS LÍNEAS DE NEGOCIO

La Sociedad Tequendama cuenta con otras líneas de negocio

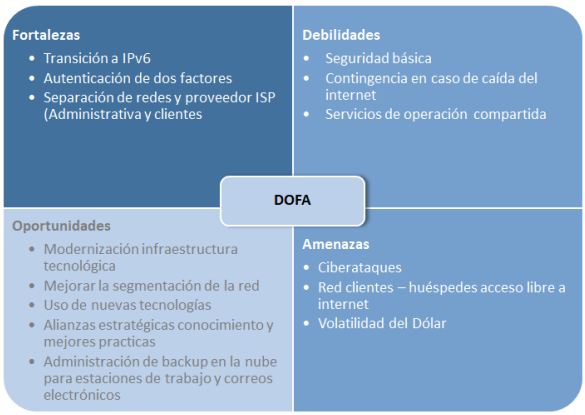
Se realizará fortalecimiento en los siguientes temas:

- Políticas de Protección de dato
- Organización interna para protección de datos
- Tratamiento de datos personales y finalidades
- Transmisión y Transferencia de dato
- Atención a consultas y reclamos
- Administración de las paginas

10. Análisis

10.1 Análisis de factores internos y externos – DOFA

Para la construcción del presente análisis DOFA se contó con la retroalimentación de las diferentes áreas de la Sociedad sobre los servicios de TI, escuchando las necesidades, incidencias, dudas, requerimientos, lo que estaba bien, lo que podría mejorar, con el objetivo de crear valor tecnológico:



10.2 Catálogo de hallazgos

10.2.1 Gobierno y Gestión TI

Continuar con la modernización del área en materia de estructura y gestión de los servicios TI con la aplicación de metodologías y mejores prácticas mediante la implementación de proyectos e iniciativas y el acompañamiento de aliados estratégicos.

10.2.2 Gestión de Riesgos TI

La Sociedad está enfocada en la identificación de los riesgos asociados a la Seguridad sin dejar de lado riesgos de otros ámbitos.

Descripción de la Materialización	Causas (Factores Internos o externos)	Consecuencias Potenciales
VULNERABILIDADES		
Se evidencias vulnerabilidades por parte de los usuarios, aliado estratégico y/o TIC	Falta de soluciones que detectan y evitan el malware, las cuales corrigen, investigan y proporciona una protección de los datos	Perdida de información, accesos no permitidos Afectación de datos personales Interrupción de las actividades
	Falta de monitoreo de amenazas internacionales y alertar inteligentes para mantener actualizado en malware, vulnerabilidad, desastres naturales y otros eventos globales	Capacidades débiles de detección de intrusos
PROTECCION DE DATOS		
PQRs	Falta de gestión de parches para software de Microsoft y de terceros en Windows para mantener la protección de datos de los clientes	Huecos de seguridad
Falta de Copias de seguridad	Falta de monitoreo de estado de unidad de disco para predecir problemas y alertas, adoptar medidas de precaución para proteger los datos y mejorar la disponibilidad	Perdida de información Reprocesos
Copias de respaldo Correo electrónico	Falta de aplicar métodos de seguridad incluido spam, phishing, BEC vulneración del correo electrónico de empresas, malware, amenazas persistentes avanzadas ATP	Perdida de información Incertidumbre en el alcance del ataque
ACTIVOS DE INFORMACION		
Errores humanos en cumplimiento de las labores	Inadecuada gestión de la información en los aplicativos. Falta de programación de sesiones de monitoreo de permisos de usuario	Error en el proceso operativo del aplicativo
		Errores en los datos
		Reprocesos operativos
		Falta de disponibilidad de la información procesada y manejada en los sistemas de información.
Mal funcionamiento del software	Software nuevo Especificaciones incompletas o no claras Ausencia de control de cambios	denegación del servicio
		Perdida parcial/total de la información
	Ausencia de inducción en el manejo de los aplicativos	Errores en los datos Retraso en las actividades diarias
	Asignación errada de perfiles y accesos a usuario	Perdida de información
		Reprocesos de validación y conciliación de la información
	Falta de actualización de manuales de usuarios	Retraso en las actividades diarias Errores en la operación de los aplicativos
Accesos abiertos	Falta de segmentación adecuada Conexiones sin protección Nivel de seguridad bajo	Vulnerabilidad del sistema, posibilidad de ataques
PÉRDIDA, DAÑO, MANIPULACIÓN O SUSTRACCIÓN DE INFORMACIÓN O DE EQUIPOS TECNOLÓGICOS		
Daño en equipos de cómputo.	Perdida de la información debido a bloqueos no controlados.	Necesidad de adquirir nuevos activos tecnológicos. Gastos no planificados.
	Equipos obsoletos Falta de mantenimiento preventivo Periodicidad de los backups	Perdida de información
INTERRUPCIÓN DEL SERVICIO DE LA PLATAFORMA TECNOLÓGICA		
Falta de disponibilidad del internet, servicios de criticidad alta afectados: ERP BC365, Vertical Hotelera, Nomina, correo electrónico, gestor documental y Videoconferencia/reuniones virtuales	Interrupción de servicios tercerizados y/o proveedores.	Afectación de procesos Pérdida de imagen institucional.
	Interrupciones y fallas del fluido eléctrico que afectan la plataforma tecnológica de la entidad. Desastres naturales, ataques terroristas y eventos catastróficos.	Necesidad de adquirir nuevos activos tecnológicos no planificados. Gastos no planificados.

Activo	Vulnerabilidad	Amenaza		Riesgo
Carpetas Usuarios Internos	Única copia, sólo una copia de la información	Modificación accidental de datos del sistema de información	R1	Usuario con permisos que accidentalmente modifica y/o elimina la información de Usuarios Internos.
Carpetas Usuarios Internos	Nivel de confidencialidad no definido con claridad	Acceso no autorizado al sistema de información	R2	Proprocionar acceso al sistema de información por no contar con niveles de confidencialidad claros en la carpetas de usuarios internos.
Backups Internos	Posibles riesgos electricos.	Interrupción del suministro eléctrico	R3	Fallas en el suministro eléctrico que impide la generación de backups o queden incompletas.
Contraseñas	Cuentas de usuario generadas por sistema en las que las contraseñas permanecen sin modificación	Mofication de información de los aplicativos	R4	Robo de contraseñas por falta de actualización y modificación de las mismas.
Contraseñas	Robo de información	Revelación de contraseñas	R5	Acceso a información por revelación de contraseñas.
Computadores	Acceso no autorizado a instalaciones	Robo	R6	Robo de equipos de cómputo o de soportes de información.
Computadores	Descargas de Internet sin control	Código malicioso	R7	Código malicioso por descargas sin control del servicio de internet
Servicio VPN.	Mal uso de las conexiones remotas	Identidad de usuario camuflada	R8	Funcionario camuflado haciendo mal uso de las conexiones remotas a través del servicio de VPN
Servicio de Correo Electrónico	Uso no controlado de sistemas de información	Perdida o filtrado de informacion sensible	R9	Perdida de información sensible por manejo inadecuado del correo electrónico
Ejecutables	Sistemas desprotegidos ante acceso no autorizado	Errores de aplicaciones	R10	Aplicación que no controla los intentos de acceso fallidos, permitiendo el ingreso no autorizado.
Servidores	Susceptibilidad del equipamiento a alteraciones en el voltaje	Colapso del servidor, información eliminada	R11	Colapso en los servidores e información elminada debido a la susceptibilidad del equipamiento a alteraciones en el voltaje.
Red Local	Inadecuada gestión de redes	Pérdida de conectividad	R12	Pérdida de conectividad por inadecuada gestion y capacidad de la red local.
Backups Internos	Perdida interna de informacion	Fallas en equipos	R13	Usuarios que no realizan copias de su información.
Cuartos de Telecomunicaciones	Posible daño a los servidores	Inundación	R14	Daño de servidores, switches, y equipos de cómputo y dispositivios de cmunicación por inundación en el cuarto de servidores.
Informacion	Ataques de phishing	Perdida de informacion	R15	El phishing se refiere al envio - recepcion de correos electronicos que pretender ser una fuente genuina.
Informacion	Ransomware	Perdida de informacion	R16	Sin acceso a determinadas partes o archivos del sistema
Informacion	DDoS	Perdida de informacion	R17	servicio o recursos no accesible a los usuarios principales.
Informacion	Perdida de datos (contraseñas)	Perdida de informacion	R18	Es importante cumplir con todos los requisitos para la creacion de contraseñas seguras.

11. Construyendo la Estrategia TI

11.1 Nuevas tecnologías

La Sociedad busca fortalecer las diferentes áreas de negocio con el apoyo de herramientas tecnológicas que apoyen su operación, administración y control, es por ello que su objetivo es continuar con la implementación de nuevas iniciativas y proyectos por lo cual se retomará el análisis de iniciativas y evaluación de la necesidad, definir una hoja de ruta, seleccionar y evaluar proveedores e implementar.

11.2 Sistemas de información

La Sociedad en el momento cuenta con aplicativos que soportan los procesos misionales y está en pro de su mejoramiento, por tal motivo esta alineado a investigar nuevas tecnologías que permitan contar con sistemas de información confiables, seguros, disponibles, con vigencia tecnológica, y alineados a los procesos misionales.

11.3 Infraestructura de Red

La Sociedad se encuentra en proceso de renovación tecnología de su infraestructura de red tanto física como lógica, ha implementado la transición de los protocolos Ipv4 a IPv6 aplicando el método Dual Stack, con ello dio vía libre a la actualización de dispositivos de red y al mejoramiento de la topología de red.

De otra parte, la seguridad a tomado un papel protagónico dado los constantes ciberataques y por ende perdida, robo y secuestro de la información por tal motivo urge la identificación e implementación mecanismos de seguridad, control y monitoreo, así como la actualización de las políticas y procedimientos que fortalezcan la seguridad en todos los niveles.

Proyectos

- Modernización de la infraestructura de red
- Modernización de equipos de computo
- Separación de servicios tecnológicos en el datacenter
- Análisis de mejora e implementación de Segmentación de la red
- Wifi gestionado
- Soluciones de Backups
- Solución de antivirus
- Seguridad gestiona en redes
- Finalización del montaje del servidor DA
- Robustecimiento de la protección de datos
- Data center ST: Diseño y construcción, ó Centro de datos alojado en la nube con administración

11.4 Seguridad de la información

Este tema de seguridad es prioridad de la Sociedad para todos los frentes y todos los niveles, por ello ha venido implementando esquemas de seguridad, pero aún falta mejoras y profundizar en su alcance.

El objetivo es fortalecer la seguridad de la información a través de la evaluación del estado actual y el análisis de riesgos a los que está expuesta la Sociedad, para definir controles relevantes que preserven la confidencialidad, integridad y disponibilidad de la información que captura, gestión y almacena la Sociedad en su proceso claves de negocio

Asimismo, evaluar la gestión sobre la protección de datos personales que mantiene la Sociedad en medios digitales, en cumplimiento a la regulación a vigente, con el fin de mitigar los posibles riesgos que pudieran impacta la seguridad de la información y cumplimiento normativo.

- Páginas web.
- Sistemas de información en la nube y uso de autenticador de doble factor
- Uso de antivirus en los equipos propios
- Solución de backup en la nube
- Restauración de backup en sitio
- Aplicación detallada de perfiles y accesos
- Sistemas de monitoreo
- Identificar vulnerabilidades den la red
- SGSI (implementación de políticas y procedimientos)
- DA (implementación de políticas y procedimientos)
- Políticas de la seguridad de la información
- Protección de datos personales
- Organización de la seguridad de la información
- Gestión de activos
- Control de acceso
- Seguridad física
- Seguridad de las operaciones
- Seguridad e las comunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas
- Relación con proveedores
- Gestión de incidentes de seguridad de la información
- Seguridad d la información de la continuidad del negocio

11.5 **Ciberseguridad**

La Sociedad Tequendama direcciona su enfoque de seguridad hacia la ciberseguridad, identificando la necesidad de avanzar en cinco capacidades fundamentales: identificar, detectar, proteger, responder y recuperar; teniendo presente la seguridad y privacidad de los datos, el ambiente geopolítico y el entorno regulatorio.

Estas capacidades o variables críticas permiten centrar la atención en las personas, los procesos y la tecnología de cada organización necesarios para tomar y ejecutar decisiones de ciberseguridad. NIST CSF (National Institute of Standards and Technology)

- El responsable debe identificar el alcance de los sistemas y activos de la Sociedad que se revisaran
- El Programa de ciberseguridad se puede adaptar para soportar diverso proceso de negocio, aplicaciones o sistemas con diferentes requisitos de seguridad

El programa de ciberseguridad contiene:

- Evaluaciones de riesgo y simulaciones de ciberseguridad
- Planes de continuidad de negocio, contingencia y recuperación en caso de incidentes de ciberseguridad
- Tablero de riesgos de ciberseguridad

Dado que la ciberseguridad es un proceso de monitoreo continuo, seguimiento y control es importante revisarlo frente a los objetivos del plan estratégico, las iniciativas de seguridad, y del desarrollo de capacidades de defensa frente a amenazas emergentes.

La seguridad en la nube es otro punto de revisión:

- El gobierno y la seguridad en entornos híbridos, donde cada proveedor de servicios cuenta con capacidades y requisitos de seguridad.
- Diseñar una arquitectura de seguridad que incluya todas las plataformas en la nube que utiliza la Sociedad. Validar todos los controles de seguridad para garantizar la protección de los datos y servicios
- Los lineamientos y mecanismos de seguridad en la nube deben ser definidos e implementados antes de su uso, donde se diseñan y administran controles con un enfoque preventivo. De allí la importancia de mantener actualizado el dominio de Seguridad del Modelo de arquitectura empresarial.
- Se deben asegurar las operaciones frente a la ciberseguridad, en especial a las posibles deficiencias de aliados y proveedores externos

Riesgos, frente a los riesgos estamos expuestos a:

- Incidentes de filtración y pérdida de datos:
    - Inactividad o interrupción de las operaciones

  - Afectación de la calidad del servicio y/o producto
  - Pérdida de contratos y oportunidades comerciales.

- Privacidad de los datos
  - Pérdida de clientes
  - Costos importantes para la recuperación de los datos
  - Datos de clientes perdidos
  - Sanciones por parte de entidades regulatorias

Debemos monitorear y priorizar los riesgos, y contar con apoyo adicional de una Auditoría interna/externa que contribuya a identificar, detectar y proteger

De igual forma, generar, simular y validar los planes de crisis, continuidad del negocio y recuperación de desastres. Es importante el contacto permanente con la alta dirección para establecer un enfoque coordinado que permita desarrollar capacidades de respuesta en el caso de que surjan problemas.

Comprender e informar sobre la vulnerabilidad a las amenazas asociadas a ransomware, con el fin de, definir planes de acción para reducir inmediatamente el riesgo y validar su implementación, además de desarrollar capacidades para ofrecer una reducción sostenible del riesgo cibernético.

Por lo anterior, debemos prepararnos para responder a un ataque de ransomware:

- Desarrollando planes de respuesta a incidentes y crisis
- Conociendo dónde están los datos críticos
- Asegurándonos de que se hayan generado y validado copias de seguridad fuera de línea y almacenamiento externo.
- Desarrollando o reteniendo la experiencia técnica para investigar y responder.

Por último, es importante la adopción, aplicación y manejo de nuevos conceptos como la ciberresiliencia (resiliencia cibernética) la cual describe la capacidad de un sistema u organización para resistir y/o recuperarse ante ataques o incidentes cibernéticos.

Construyendo la Ciberseguridad en Sociedad Tequendama

Un plan de ciberseguridad es esencial para proteger los sistemas y datos de una organización. A continuación, se definen las tareas a desarrollar dentro del Plan de ciberseguridad a saber

- Desarrollo e implementación del Acta de Compromiso con la Ciberseguridad en Sociedad Tequendama. Se elaborará un acta de compromiso con la Ciberseguridad a ser firmada por todos y cada uno de los funcionarios de la Sociedad Tequendama, sin importar el tipo de contratación.
- Desarrollo del Plan de Ciberseguridad para la Sociedad Tequendama

A. Evaluación y Análisis de Riesgos

- Identificar y evaluar los activos críticos: Determinar qué activos digitales (datos, sistemas, hardware, software) son los más importantes para la organización.

- Evaluar amenazas y vulnerabilidades: Analizar posibles amenazas, tanto internas como externas, y las vulnerabilidades que podrían afectar a esos activos.

B. Desarrollo de Políticas y Procedimientos de Ciberseguridad

- Elaborar políticas de seguridad: Definir las normativas y reglas que rigen el uso y acceso a los recursos digitales.
- Procedimientos operativos: Documentar los pasos específicos para implementar y mantener medidas de seguridad, incluyendo actualizaciones de software, copias de seguridad regulares, etc.

C. Detección y Respuesta

- Control de acceso: Establecer y hacer cumplir políticas de autenticación robusta, gestión de contraseñas y control de accesos.
- Seguridad de red: Implementar firewalls, sistemas de detección y prevención de intrusiones, y cifrado de datos para proteger la red.
- Monitoreo continuo: Establecer sistemas de monitoreo para detectar posibles intrusiones o anomalías en tiempo real.
- Plan de respuesta a incidentes: Desarrollar un plan detallado para responder a incidentes de seguridad, incluyendo notificación, mitigación y recuperación.

D. Educación y Entrenamiento

- Programas de concientización: Proporcionar capacitación regular a los empleados sobre buenas prácticas de seguridad cibernética y concientización sobre amenazas actuales.

E. Evaluación y Mejora Continua

- Auditorías de seguridad: Realizar evaluaciones regulares para asegurar la efectividad de las medidas de seguridad y realizar ajustes según sea necesario.
- Actualización del plan: Mantener el plan actualizado para adaptarse a las nuevas amenazas y tecnologías emergentes.

F. Gestión de Proveedores y Terceros

- Establecer políticas para garantizar que los proveedores externos cumplan con los estándares de seguridad al trabajar con la organización.

- Plan de respuesta a incidentes

A. Conformación equipo respuesta a incidentes: Designar un equipo responsable de manejar los incidentes de ciberseguridad. Identificar roles y responsabilidades dentro del equipo de respuesta a incidentes.

B. Fases respuesta a incidentes

- Preparación: Documentar el plan de respuesta a incidentes y asegurarse de que esté accesible y conocido por todos los involucrados. Realizar ejercicios

de simulación y capacitación para el equipo de respuesta a incidentes y otros empleados relevantes.

- Análisis: Establecer mecanismos de monitoreo continuo para detectar posibles incidentes. Crear procedimientos para investigar y evaluar la gravedad y el impacto del incidente.
- Contención y erradicación: Identificar y aislar la causa raíz del incidente para evitar su propagación. Tomar medidas para detener la actividad maliciosa y recuperar el control de los sistemas afectados.
- Recuperación: Restaurar los sistemas y datos afectados a un estado seguro y funcional. Verificar la integridad de los datos y sistemas restaurados.
- Lecciones aprendidas y mejoras: Realizar una revisión posterior al incidente para identificar áreas de mejora en el plan de respuesta a incidentes. Actualizar y mejorar el plan con base en las lecciones aprendidas.

- Notificación y Comunicación
  - Establecer un protocolo claro para notificar a las partes relevantes sobre el incidente.
  - Definir los canales de comunicación interna y externa para manejar la divulgación del incidente.
- Recopilación y preservación de la evidencia.
  - Detallar los procedimientos para recopilar y preservar evidencia relacionada con el incidente para fines legales o de investigación forense.

11.6 **Acciones de mejora**

Las acciones de mejora aplican en todos los aspectos antes descritos y también para los procesos de la gestión de TIC. Las políticas y proceso de la gestión TI se actualizarán conforme se va aplicando los requerimientos de MInTIC, y a medida que incorporan los proyectos de la Infraestructura de red, sistemas de información y seguridad con el apoyo de sus aliados. Así mismo, se actualizar sus procesos.

11.7 **Iniciativas de transformación**

Catálogo de iniciativas de transformación								
ID	Nombre Iniciativa	ID Servicios asociadas	Descripción	Área Líder	ID Metas estratégicas	Áreas Involucradas	Tiempo total estimado	ID Brechas
IT001	Gestion del cambio en proyectos de tecnologia	S03, S06, S07, S10, S11	Facilitar la transicion de pasar de un modelo de operación a otro con nueva tecnologia	GERENCIA GENERAL	3	Todas	1 año	B001
IT002	Disminuir el uso del papel en las operaciones rutinarias de la Sociedad con el uso de firma digital	S11	Actualizar el sistema de informacion utilizado a la fecha conforme a lineamientos deel Archivo General de la NAcion y conforme para suplir el resultado del diagnostico de la situacion actual y sus mejoras	GESTION DOCUMENTAL	3	Todas	1 año	B005
IT003	Zona WiFi Gratis para los ciudadanos	S12	Implementar zonas wifi en el Centro Internacional para proporcionar servicio al ciudadano facilittando su interaccion con las entidades del estado, brindando conectividad en pro de obtener servicios ágiles, sencillos y útiles para usuarios y grupos "Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad"	Desarrollo e innovacion	3	Todas	1 año	B007
IT004	Renovacion tecnologica equipos wifi SHT y Suites tequendama	S07	Actualizacion de equipos para soportar la transformacion digital	TIC	3	Suites	1 año	B006
IT005	Tercerizar la administracion, gestion y optimizacion de la infraestructura de Red	S03	Contar con plataformas tecnologicas centralizadas para la administración dela red, con el objetivo de mejorar la Gestion de los servicios TI y tomar decisiones agiles	TIC	3	Todas	3 años	B006
IT006	Interoperabilidad. Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad	S13	Implementar el intercambio de datos electrónicos con los sistemas que tiene el Estado para automatizar trámites dirigidos al ciudadano	TIC	3	Todas	1 año	B008
IT007	Implementacion protocolo Ipv6	S14	Implementar el intercambio de datos electrónicos con los sistemas que tiene el Estado para automatizar trámites dirigidos al ciudadano	TIC	3	Todas	1 año	B009
IT008	Renovaclon equipos de computo	S07	Facilitar la conectividad de todos los dispositivos tecnológicos usados para la conexión a internet con alcance IPv6	TIC	3	Todas	3 años	
IT009	- Modernización de la infraestructura de red	S04	actualización de dispositivos de red y al mejoramiento de la topología de red.	TIC	3	TIC	1 año	B009
IT010	- Separación de servicios tecnológicos en el datacenter	S04	Asegurar los servicios y administracion de la red de ST	TIC	3	TIC	1 año	
IT011	- Análisis de mejora e implementación de Segmentación de la red	S04	actualización de dispositivos de red y al mejoramiento de la topología de red.	TIC	3	TIC	3 meses	B009
IT012	- Soluciones de Backups	S02, S04	Contar con plataformas en la nube para garanizar el almacenamiento de informacion	TIC	3	Todas	1 año	B004 B009
IT013	- Seguridad gestiona en redes	S04, S16	Asegurar los servicios y administracion de la red de ST	TIC	3	TIC	1 año	B004 B009
IT014	- SGSI (implementación de políticas y procedimientos)	S16, S02	levantar, documentar y mejorar las politicas y procedimientos de seguridad y gestion de TI	TIC	3	TIC	1 año	B004 B009
IT015	- Robustecimiento de la protección de datos	S02, S03	Mejorar la seguridad y el acceso a las diferentes plataformas	TIC	3	Todas	1 año	B004 B009, B010
IT016	- Uso de antivirus en los equipos propios	S02, S04	Proteger la informacion de los usuarios	TIC	3	Todas	1 año	B004 B009
IT017	Ejercicios de simulación y respuesta a ataques cibernéticos y evaluación de vulnerabilidades	S02, S11	Proteger los activos de informaicon de la ST	TIC	3	TIC	1 año	B004 B009
IT018	Iniciativas tecnologicas	S02, S03, S05. S06, S07, S08, S09, S16	Realizar actividades de implementación y mantenimiento en los Software que se cuentan a nivel corporativo y a nivel de unidades de negocio.	TIC	2	Todas	3 AÑOS	B002 B003 B005 B006 B010
IT020	Análisis de datos para la toma de decisiones.	S05, S06, S15, S17	Realizar análisis de datos para la toma de decisiones.	TIC	2	Todas	1 AÑO	B005
IT021	Implementar un ommicanal para administrar, centralizar las redes sociales.	S05, S06, S15, S17	Desarrollar ommicanal para administrar, centralizar las redes sociales.	TIC	2	Todas	1 AÑO	B003 B005 B010
IT022	Data center ST	S04, S09, S15	Diseño y construcción, ó Centro de datos alojado en la nube con administración	TIC	3	TIC	1 AÑO	B006 B009
IT023	Fortalecimiento de la seguridad y comunicación de la infraestructura tecnologica.	S02, S03, S07, S09, S10, S11, S15, S16	Soporte tecnologico a los proyectos nuevos de la Sociedad para el fortalecimiento de la seguridad y comunicación de la infraestructura tecnologica.	TIC	3	TIC	1 AÑO	B002 B004 B006 B009

11.8 **Inversión en proyectos**

Ficha de Iniciativa Inversión	
Nombre	Iniciativas de transformacion Tecnologica
Descripción	Desarrollar estrategias de TI para alinear su proceso, objetivo y alcance de modo que la gestión y el aprovisionamiento adecuado agreguen valor a los servicios TI internos y externos dentro del marco de la política digital
Alineación a los Objetivos de la entidad	Realizar campañas para reducir el impacto social y ambiental de nuestras actividades operativas
Recursos	Propios
Costo estimado total	$ 8.322 M
Área líder	TIC
Fecha Inicio estimada	2023-2024
Fecha Fin estimada	12-2026

	Proyectos			2022											2026										
			Presupuesto	$ 1.019 M											$ 8.322 M										
	Área Líder	ID	Nombre de proyecto	E	F	M	A	M	J	J	A	S	O	N	D	E	F	M	A	M	J	J	A	S	O	N	D
Iniciativas de transformación	DESARROLLO E INNOVACION	IT003	Zona WiFi Gratis para los ciudadanos													Por definir											
	TIC	IT004	Renovacion tecnologica equipos wifi SHT y Suites tequendama													$ 1.600 M											
		IT005	Tercerizar la administracion, gestion y optimizacion de la infraestructura de Red													$ 236 M											
		IT006	Interoperabilidad. Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad													$ 191 M											
		IT007	Implementacion protocolo Ipv6													$ 93 M											
		IT008	Renovacion equipos de computo													$ 250 M											
		IT009	- Modernización de la infraestructura de red													$ 600 M											
		IT012	- Soluciones de Backups													$ 168 M											
		IT013	- Seguridad gestiona en redes													$ 144 M											
		IT014	- SGSI (implementación de políticas y procedimientos)													$ 45 M											
		IT015	- Robustecimiento de la protección de datos													$ 65 M											
		IT016	- Uso de antivirus en los equipos propios													$ 140 M											
		IT017	Ejercicios de simulación y respuesta a ataques cibernéticos y evaluación de vulnerabilidades													$ 1.200 M											
		IT018	Iniciativas tecnologicas																								
		IT020	Análisis de datos para la toma de decisiones.													$ 50 M											
		IT021	Implementar un ommicanal para administrar, centralizar las redes sociales.													$ 50 M											
		IT022	Data center ST																								
		IT023	Fortalecimiento de la seguridad y comunicación de la infraestructura tecnologica.													$ 750 M											

11.9 **Gastos**

	Proyectos			2022											2026										
			Presupuesto	$ 1.019 M											$ 8.322 M										
	Área Líder	ID	Nombre de proyecto	E	F	M	A	M	J	J	A	S	O	N	D	E	F	M	A	M	J	J	A	S	O	N	D
Iniciativas de	DESARROLLO E INNOVACION	IT003	Zona WiFi Gratis para los ciudadanos													Por definir											
Gastos de la operación	Dirección de tecnologias de la información y las comunicaciones	IO-001	Licenciamiento de SW												$332												$332
		IO-002	TV IP SUITES												$131												$131
		IO-003	Impresion y copiado												$77												$77
		IO-004	Correo electronico												$75												$600
		IO-005	Internet Huespedes												$54												$189
		IO-006	Equipos de computo alquiler												$69												$276
		IO-007	Internet Administrativo												$31												$189
		IO-008	Seguridad Gestionada												$26												
		IO-009	Lineas moviles corporativas												$32												$128
		IO-010	Soporte y Mtto planta telefonica												$17												$68
		IO-011	Soporte y Mtto ERP/Nomina												$31												$272
		IO-012	Desarrollos para interoperabiidad Gobierno digital																								$40
		IO-013	Gestion, Soporte y Mtto RED												$48												$192
		IO-014	Equipos de computo												$96												$246

En ejecución

11.10 Indicadores

Nombre	Objetivo	Frecuencia de medición	Variables y formulacion	Nota
Indicador de beneficio del servicio	Determinar el porcentaje de servicios (pertenecientes al catálogo de servicios de TI), considerados como beneficiosos para los usuarios de TI.	Semestral.	Variables y formulación #Serv =Número de servicios definidos en el catálogo de servicios de TI. #Aprob= Número de servicios definidos en el catálogo de servicios de TI, cuyo usuario final lo califica como "beneficioso y que aporta lo esperado". Indicador de beneficio del servicio = #Aprob / #Serv * 100	este indicador está relacionado con los objetivos estratégicos del Modelo de Gestión Estratégica de TI en el Estado[27] denominados Calidad de los Servicios, Eficiencia en la Gestión de la Entidad, Nivel de Satisfacción de Usuarios, Alinear la Gestión de TI con los Procesos de la Organización
Indicador de incidentes.	Controlar el porcentaje de incidentes significativos causados por riesgos no identificados por el proceso de evaluación de riesgos.	Semestral	Inc_Neg= # de Incidentes significativos que generaron pérdida para la entidad. Inc_Tot= # de Incidentes Totales. Indicador de Incidentes = #Inc_Neg / Inc_Tot * 100.	Un incidente significativo es aquel que ha causado impacto negativo en los integrantes de la Sociedad de manera masiva o que se ha provocado interrupción de uno o varios servicios de la entidad. El nivel de tolerancia a fin de calificar un incidente como significativo, deberá ser establecido por la entidad en conjunto con su área de riesgos.
Indicador de seguimiento a riesgos de TI.	Controlar el porcentaje de riesgos relacionados con TI, incluidos en las evaluaciones de riesgo de la entidad.	Semestral	#TotalR = Número total de riesgos incluidos en la evaluación de riesgos de la entidad. #RiesgosTI = Número total de riesgos de TI o relacionados con TI, incluidos en la evaluación de riesgos de la entidad. Indicador de seguimiento a riesgos de TI = #RiesgosTI / #TotalR * 100.	este indicador está relacionado con el objetivo estratégico del Modelo de Gestión Estratégica de TI en el Estado [27] denominado Alinear la Gestión de TI con los Procesos de la Entidad
Indicador ejecución PETI.	Controlar el porcentaje de iniciativas planeadas, relacionadas y ejecutadas en el PETI.	Anual	#IniciativasEjecutadas = Número deiniciativas ejecutadas de manera satisfactoria en el periodo y que corresponden al periodo de medición según lo planeado. #IniciativasPlaneadas = Número total de iniciativas planeadas a ejecutar en el periodo. Indicador ejecución PETI =#IniciativasEjecutadas / #IniciativasPlaneadas * 100.	este indicador está relacionado con los objetivos estratégicos del Modelo de Gestión Estratégica de TI en el Estado [27] denominados Alinear la Gestión de TI con los Procesos de la Entidad, Conseguir Recursos y Optimizar su Gestión para la Implementación del PETI.
Número de controles de seguridad digital implementados	Seguridad Informática (Seguridad de TI)	Mensual	Sumatoria de Controles Propuestos en Seguridad Informática	Por solicitud de resultados de análisis de vulnerabilidades

Adoptamos indicadores del Dominio de Gobierno de TI del Marco de Referencia de Arquitectura Empresarial de TI, los cuales representan una medida del logro de los objetivos, se adiciona un indicador de número de controles de seguridad