Plan Estratégico TI

INSTITUTO DE FINANCIAMIENTO, PROMOCIÓN Y DESARROLLO DE MANIZALES

Vigencia:	Enero 2026 – Enero 2028
Instancia de Aprobación:	Comité de gestión y desempeño institucional
Estado	Revisión para aprobación

Contenido

1. Introducción

El Plan Estratégico de Tecnologías de la Información – PETI 2026–2028 de INFIMANIZALES constituye el instrumento de planeación que orienta la gestión, uso y aprovechamiento estratégico de las Tecnologías de la Información y las Comunicaciones (TIC), como habilitador fundamental para el cumplimiento de la misión institucional, la generación de valor público y la sostenibilidad operativa de la Entidad.

El PETI se formula en concordancia con la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión – MIPG, el Plan Estratégico Institucional, el Plan de Acción y el Mapa de Procesos, permitiendo articular las iniciativas tecnológicas con los objetivos estratégicos y misionales de INFIMANIZALES.

Durante el periodo 2026–2028, la gestión de TI se enfocará en fortalecer la transformación digital, el gobierno de TI, la seguridad de la información, la continuidad del negocio y la ciberseguridad, reconociendo la creciente dependencia tecnológica de los procesos institucionales y la necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información.

El presente PETI define el estado actual de la gestión de TI, identifica brechas frente al estado deseado y establece un conjunto de iniciativas y proyectos estratégicos que permitirán evolucionar la capacidad tecnológica de la Entidad, apoyando la toma de decisiones, la eficiencia operativa y el cumplimiento normativo.

2. Alcance del documento

El Plan Estratégico de Tecnologías de la Información – PETI 2026–2028 aborda las fases definidas en la guía del Ministerio de Tecnologías de la Información y las Comunicaciones para la construcción del PETI, comprendiendo, analizando, construyendo y presentando el direccionamiento estratégico de TI de la Entidad.

El PETI se estructura bajo los dominios del modelo de gestión de TI del Estado Colombiano: Estrategia, Gobierno, Información, Sistemas de Información, Infraestructura de TI, Uso y Apropiación y Seguridad, incorporando de manera transversal la gestión del riesgo, la continuidad del negocio y la ciberseguridad.

El documento incluye el análisis del estado actual de las TIC en INFIMANIZALES, la identificación de oportunidades de mejora, la definición del estado objetivo de la gestión de TI y el portafolio de iniciativas y proyectos que permitirán apoyar la transformación digital de la Entidad durante la vigencia 2026–2028.

3. Objetivo General

Definir el direccionamiento estratégico y el plan de acción de la gestión de Tecnologías de la Información y las Comunicaciones de INFIMANIZALES para el periodo 2026–2028, alineando la estrategia de TI con el Plan Estratégico Institucional, el Plan de Acción y el Modelo Integrado de Planeación y Gestión – MIPG, con el fin de fortalecer la eficiencia operativa, la toma de decisiones, la seguridad de la información, la continuidad del negocio y la ciberseguridad,

garantizando el adecuado soporte tecnológico a los procesos misionales, estratégicos y de apoyo de la Entidad.

4. Contexto Normativo

A continuación, se listan las normas y documentos de referencia que aportaron al proceso de comprensión, análisis, y construcción del presente PETI:

Marco Normativo y de Referencia

- Ley 1341 de 2009 – Principios y conceptos sobre la sociedad de la información y las TIC
- Ley 1581 de 2012 – Protección de datos personales
- Ley 1712 de 2014 – Transparencia y acceso a la información pública
- Ley 1955 de 2019 – Plan Nacional de Desarrollo (Transformación Digital)
- Decreto 1078 de 2015 – Decreto Único Reglamentario del sector TIC
- Decreto 1499 de 2017 – Modelo Integrado de Planeación y Gestión – MIPG
- Decreto 612 de 2018 – Integración de planes institucionales al Plan de Acción
- Decreto 1008 de 2018 – Política de Gobierno Digital
- Decreto 2106 de 2019 – Simplificación y racionalización de trámites
- Decreto 620 de 2020 – Servicios Ciudadanos Digitales
- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital
- CONPES 3920 de 2018 – Política Nacional de Explotación de Datos (Big Data)
- CONPES 3975 de 2019 – Política Nacional de Transformación Digital e Inteligencia Artificial
- Norma Técnica Colombiana NTC 5854 de 2012 – Accesibilidad Web
- Lineamientos y guías del Ministerio TIC – Gobierno Digital y Arquitectura Empresarial

5. Motivadores Estratégicos

Motivador	Fuente
Estrategia Institucional	Plan de Acción
Lineamientos y Políticas	Transformación Digital Política de Gobierno Digital Modelo Integrado de Planeación y Gestión

5.1 Contexto Institucional

Infimanizales es el Instituto de financiamiento y promoción que contribuye al desarrollo administrativo, económico, social, urbanístico, rural, cultural, deportivo, financiero, institucional, turístico y físico-ambiental del Municipio de Manizales.

Infimanizales realiza la asesoría administrativa, financiera y técnica del ente territorial y sus entidades descentralizadas. Asimismo, se encarga de la financiación de inversiones públicas o sociales que se adelanten a través de entidades públicas de Manizales o en las que la participación del Municipio o de sus entidades descentralizadas sea superior al 50%.

El Instituto puede financiar inversiones en cualquier empresa de servicios públicos domiciliarios, cualquiera sea su naturaleza jurídica y en las cuales el Municipio o cualquiera de sus entidades descentralizadas tengan participación.

Se encarga de la prestación de servicios financieros y de garantía a las entidades públicas municipales de Manizales. Participa como socio o accionista en sociedades limitadas o por acciones, cuyo fin tenga relación directa con el objeto de Infi-Manizales.

5.2 ¿Quiénes Somos?

Somos un instituto público del orden municipal, con presencia local, regional y proyección nacional, que mediante un portafolio de inversiones, proyectos, servicios financieros y administración de bienes raíces, promovemos el desarrollo integral, salvaguardando los intereses de los ciudadanos, especialmente relacionados con el apropiado manejo de los recursos públicos, generando valor en los activos estratégicos de ciudad y mejorando la calidad de vida de las personas.

5.3 Código de integridad

Honestidad: Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia y rectitud, y siempre favoreciendo el interés general.
Respeto: Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.
Compromiso: Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.
Diligencia: Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos del Estado.
Justicia: Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

5.4 Sistema de Creencias

1. Creemos que el cambio es un proceso constante en búsqueda de la excelencia.
2. Creemos en la innovación y en la evolución para generar soluciones de alto impacto.
3. Creemos en lo que fuimos capaces, en el presente que nos compromete y en el futuro que nos inspira.
4. Creemos en las alianzas para el desarrollo de grandes proyectos e inversiones con rentabilidad económica y social.
5. Creemos en nuestra gente, en el desarrollo de su talento y en la inteligencia colectiva como fuerza impulsora del resultado.
6. Creemos en el aporte que le generamos a nuestros grupos de interés, por eso controlamos los recursos y somos responsables con nuestras decisiones
7. Creemos en un pensamiento que trasciende fronteras.

5.5 Objetivos estratégicos

Servicios Financieros:
Generar valor a través de un portafolio innovador que asegure la fidelización de clientes.

Inversiones en Empresas:
Generar valor a través de la gestión participativa y propositiva en las decisiones estratégicas de las empresas del portafolio.

Gestión de Proyectos:
Generar valor a partir de la identificación, planeación y ejecución efectiva de proyectos estratégicos que contribuyan al desarrollo.

Gestión de Bienes:
Generar valor maximizando el aprovechamiento de los bienes propios, involucrando al Instituto en inversiones y proyectos inmobiliarios con rentabilidad económica y social.

Gestión Institucional:
Agrupa objetivos transversales que impactan el desarrollo institucional de Infimanizales

6. Tendencias Tecnológicas

Durante el periodo 2026–2028, INFIMANIZALES enfocará la adopción y aprovechamiento de las tecnologías de la información en aquellas tendencias que aportan valor directo a la gestión institucional, fortalecen el control del riesgo y garantizan la continuidad de los servicios críticos. Las principales tendencias tecnológicas consideradas en el presente PETI son:

- **Fortalecimiento de la ciberseguridad**, mediante esquemas avanzados de monitoreo, detección y respuesta a incidentes, orientados a la protección de los activos de información y la mitigación del riesgo operativo y tecnológico.
- **Uso de servicios en la nube**, para el respaldo, la recuperación de información y la escalabilidad de los servicios tecnológicos, garantizando altos niveles de disponibilidad y resiliencia operativa.
- **Automatización y digitalización de procesos**, orientadas a reducir reprocesos, mejorar la eficiencia operativa y fortalecer la trazabilidad de las operaciones institucionales.
- **Aprovechamiento de la información para la toma de decisiones**, mediante el fortalecimiento de capacidades de análisis, reportes e indicadores que apoyen la gestión directiva y el control institucional.

La adopción de estas tendencias se realizará de manera gradual, controlada y alineada con la capacidad institucional, la normatividad vigente y la gestión integral del riesgo.

7. Nivel de Desarrollo y Uso de las Tecnologías de la Información

INFIMANIZALES cuenta con una plataforma tecnológica que soporta de manera adecuada los procesos estratégicos, misionales y de apoyo de la Entidad, evidenciando un nivel de madurez intermedio en la gestión de las tecnologías de la información.

Las soluciones tecnológicas existentes presentan un alto nivel de uso por parte de los funcionarios y contratistas, contribuyendo a la eficiencia operativa, la gestión de la información y el cumplimiento de las funciones institucionales. No obstante, se identifican oportunidades de mejora orientadas a la optimización, automatización y fortalecimiento de los controles tecnológicos, en coherencia con el enfoque de gestión del riesgo y mejora continua.

El PETI 2026–2028 contempla iniciativas orientadas a fortalecer progresivamente el nivel de madurez de la gestión de TI, priorizando la seguridad de la información, la continuidad del negocio y el uso eficiente de las herramientas tecnológicas.

8. Evaluación de la Gestión del Área de Tecnologías de la Información

La gestión del área de Tecnologías de la Información de INFIMANIZALES se orienta a garantizar la disponibilidad, seguridad y continuidad de los servicios tecnológicos que soportan los procesos institucionales, articulándose con los objetivos estratégicos y el modelo de operación de la Entidad.

El área de TI cuenta con capacidades técnicas y operativas para la administración de la infraestructura tecnológica, los sistemas de información y los servicios asociados, apoyándose en esquemas de soporte, mantenimiento y supervisión de proveedores especializados.

La evaluación de la gestión del área de TI se realiza a través del seguimiento al cumplimiento del PETI, el Plan de Acción institucional, los indicadores de gestión de TI y los mecanismos de control interno, promoviendo la mejora continua y la gestión efectiva del riesgo tecnológico.

9. Modelo Objetivo de Gestión de TI 2026–2028

Para el periodo 2026–2028, INFIMANIZALES proyecta una gestión de Tecnologías de la Información con un enfoque estratégico, orientado a la generación de valor público, la gestión del riesgo digital y la resiliencia operativa.

El modelo objetivo de TI contempla:

- Un Gobierno de TI fortalecido, alineado con el MIPG y soportado en instancias de decisión y seguimiento claras.
- Sistemas de información integrados, seguros y orientados a la automatización y trazabilidad de los procesos misionales, estratégicos y de apoyo.
- Infraestructura tecnológica robusta, con esquemas de alta disponibilidad, respaldo y recuperación ante desastres.
- Un enfoque alto en seguridad de la información y ciberseguridad, apoyado en servicios SOC, SIEM, SOAR, EDR y análisis de comportamiento.
- Capacidades institucionales para garantizar la continuidad del negocio, minimizando impactos ante incidentes tecnológicos o cibernéticos.
- Uso y apropiación de las TIC por parte de los funcionarios, promoviendo la eficiencia, la innovación y la mejora continua.

10. Iniciativas Estratégicas de TI

El portafolio de iniciativas y proyectos estratégicos de Tecnologías de la Información para el periodo 2026–2028 se define a partir del análisis del estado actual de la gestión de TI, la identificación de brechas frente al modelo objetivo y la alineación con el Plan Estratégico Institucional, el Plan de Acción y el Modelo Integrado de Planeación y Gestión – MIPG.

Las iniciativas priorizadas buscan fortalecer la seguridad de la información, la continuidad del negocio, la ciberseguridad, la eficiencia operativa y el gobierno de TI, garantizando el soporte tecnológico a los procesos misionales, estratégicos y de apoyo de INFIMANIZALES.

ID	Iniciativa / Proyecto TI	Objetivo	Dominio TI	Prioridad	Horizonte
TI-01	Fortalecimiento del Gobierno de TI	Consolidar el modelo de gobierno de TI alineado al MIPG y Gobierno Digital	Gobierno / Estrategia	Alta	Corto
TI-02	Actualización y seguimiento del PETI	Garantizar el cumplimiento y seguimiento periódico del PETI	Estrategia	Alta	Permanente
TI-03	Fortalecimiento del SGSI	Mantener y mejorar la gestión de seguridad de la información	Seguridad	Alta	Permanente
TI-04	Fortalecimiento de Ciberseguridad (SOC, SIEM, SOAR, EDR)	Reducir riesgos y mejorar la detección y respuesta a incidentes	Seguridad	Alta	Permanente
TI-05	Plan de Continuidad y Recuperación de Desastres (DRP)	Garantizar la continuidad de los servicios críticos	Infraestructura / Seguridad	Alta	Corto
TI-06	Optimización de Sistemas de Información	Mejorar usabilidad, integración y automatización	Sistemas de Información	Media	Mediano
TI-07	Automatización y digitalización de procesos	Reducir reprocesos y mejorar eficiencia operativa	Información / Sistemas	Media	Mediano
TI-08	Fortalecimiento de infraestructura tecnológica	Asegurar disponibilidad, capacidad y desempeño	Infraestructura	Media	Mediano
TI-09	Uso y apropiación de las TIC	Incrementar el aprovechamiento de las soluciones tecnológicas	Uso y Apropiación	Media	Permanente
TI-10	Gestión y calidad de datos	Fortalecer la confiabilidad y uso estratégico de la información	Información	Baja	Largo

11. Hoja de Ruta del PETI 2026–2028

La hoja de ruta del PETI 2026–2028 define la ejecución progresiva de las iniciativas estratégicas de TI, organizadas en el corto, mediano y largo plazo, de acuerdo con su nivel de prioridad, impacto institucional y capacidad operativa de INFIMANIZALES.

Horizonte	**Iniciativas principales**
Corto Plazo (2026)	Fortalecimiento del Gobierno de TI, actualización del PETI, fortalecimiento del MGSI, plan de continuidad y recuperación de desastres, fortalecimiento de ciberseguridad
Mediano Plazo (2027)	Optimización de sistemas de información, automatización de procesos, fortalecimiento de infraestructura, mejora en analítica e indicadores
Largo Plazo (2028)	Consolidación de la gestión de datos, madurez en uso y apropiación de las TIC, mejora continua del modelo de TI

12. Relación de las Iniciativas Estratégicas con los Procesos Institucionales

Las iniciativas definidas en el portafolio de proyectos de TI se encuentran alineadas con los procesos estratégicos, misionales y de apoyo de INFIMANIZALES, garantizando que las inversiones en tecnología respondan a necesidades reales del negocio, fortalezcan la gestión del riesgo y contribuyan al cumplimiento de los objetivos institucionales.

13. Sistemas de información

Dentro de los recursos informáticos de INFIMANIZALES, referentes al software y programas utilizados, la entidad cuenta con contratos para soporte, mantenimiento y actualizaciones, para los siguientes aplicativos.

APLICACIÓN	NOMBRE	DESCRIPCIÓN	PROVEEDOR
SISTEMA DE GESTIÓN INTEGRAL	SGI	PLANEACIÓN, GESTIÓN Y CONTROL DEL PORTAFOLIO DE INVERSIONES EN RENTA VARIABLE Y GESTIÓN DE PROYECTO	ALMERA
GESTIÓN DOCUMENTAL	DOCUNET	SOFTWARE ESPECIALIZADO EN LA ADMINISTRACIÓN, MANEJO DOCUMENTAL Y ARCHIVÍSTICO QUE PERMITE A TRAVÉS DE LA GESTIÓN ELECTRÓNICA DEL DOCUMENTO OPERAR DE FORMA ÁGIL EL CENTRO DOCUMENTAL DE LA ENTIDAD.	INNOVA SYSTEM

SOLUCIÓN INTEGRAL DE GESTIÓN DE RECURSOS FINANCIEROS, ADMINISTRATIVOS Y OPERACIONALES SERVICIO EN NUBE	IAS SOLUTION	SISTEMA DE INFORMACIÓN INTEGRADO Y ESPECIALIZADO EN ENTIDADES DE DESARROLLO TERRITORIAL, EL CUAL APOYA Y SOPORTA LOS PROCESOS FINANCIEROS, ADMINISTRATIVOS, LA EVALUACIÓN DE RIESGOS Y LA TOMA DE DECISIONES GERENCIALES, PROPIOS DE SU ACTIVIDAD O NÚCLEO DE NEGOCIO, ES PARAMETRIZABLE, ESCALABLE Y ROBUSTO, PERMITE GENERAR INFORMACIÓN Y REPORTES EN LÍNEA REQUERIDOS TANTO POR USUARIOS INTERNOS, EXTERNOS, ENTIDADES DE CONTROL Y ENTIDADES DE VIGILANCIA.	SOLUTION SYSTEMS LTDA

13.1 Sistema de gestión integral (SGI)

El Sistema de Gestión Integral de Almera es una herramienta tecnológica que, bajo el entorno web, apoya de forma integral las labores de planeación, gestión y control, logrando así alinear el modelo de operación de la empresa con las estrategias definidas por la alta dirección. Almera permite articular la gestión del día a día con la estrategia, articulándose además con el estándar de tecnología de la organización, asegurando la disponibilidad de información para los usuarios, permitiendo conectarse y consolidar la información bajo modelos de gestión como el Balanced Score Card.

INFIMANIZALES tiene implementado la solución base del SGI Sistema de Gestión Integral, con los módulos Almera BSC y Almera Mecanismos de Integración, que asocia:

- **Tablero de indicadores de gestión:** Permite la generación de indicadores para el monitoreo y control del desempeño financiero del Instituto y del grupo de empresas que hacen parte del portafolio de inversiones del Instituto.
- **Planes estratégicos y corporativos:** Facilita el control del plan estratégico institucional y de los cronogramas de trabajo asociados a la ejecución de proyectos de inversión o de desarrollo institucional.
- **Mecanismos de integración:** Este módulo permite documentar el desarrollo de reuniones asociadas al desarrollo de comités institucionales, seguimientos a proyectos o planes de acción.

13.2 Gestión documental – Docunet Web

Docunet es un ECM (Enterprise Content Manager), Solución tecnológica 100% web, especializada en la administración y control de sistemas de gestión documental y archivística, que permite a través de la gestión electrónica del documento, obtener los más altos niveles de oportunidad, efectividad y trazabilidad de la información[1].

[1] http://innova.com.co/productos/

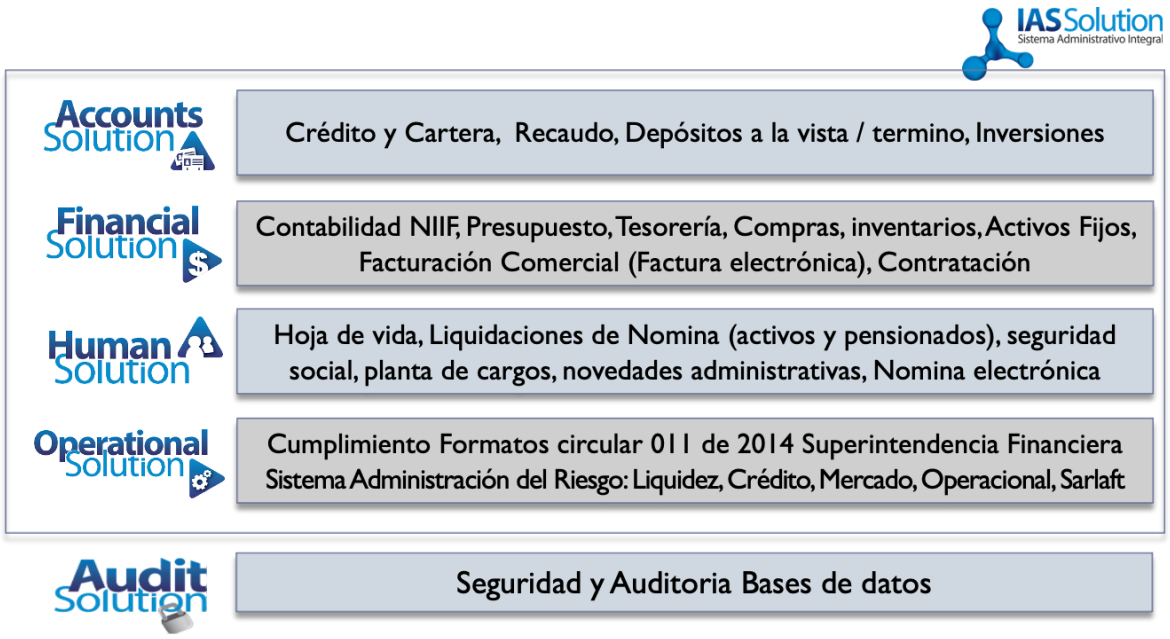
Está divido modularmente tal como se describe a continuación:

Modulo	Descripción
Parametrización	Este módulo permite definir los aspectos básicos de la operación del producto.
Seguridad	El módulo de seguridad permite definir los aspectos básicos de la malla de seguridad empleada por Docunet.
Explorador Documental	Dentro del explorador documental de Docunet se realiza la definición de la estructura para el manejo de carpetas, documentos y subdocumentos.
Explorador organizacional	En la estructura organizacional se realiza toda la definición y parametrización de la forma como está constituida estructura de la empresa.
Archivo	El módulo de archivo de Docunet permite la operación del día a día de los procesos de gestión documental que se realizan en la empresa, para ello cuenta con los siguientes elementos: • Explorador documental • Administración de contenidos • Consulta documental • Préstamo documental • Administración de lotes • Configuración del Repositorio de Archivos Docunet • Bandeja de reciclaje • Manejo de maestros • Reportes de producción • Creación de Información desde aplicaciones Externas • Realizar la exportación Documental
Tramite	Este módulo permite dar trámite a la documentación enviada y recibida.
Normas y procedimientos	El módulo de Normas y Procedimientos permite a la organización administrar los documentos y registros requeridos para un Sistema de calidad ISO 9001.

13.3 IAS SOLUTION

Software especializado en Institutos Financieros de desarrollo territorial que integra sus procesos misionales con sus procesos Administrativos y Financieros, soportando la gestión transaccional de las áreas Financiera, administrativa y de operaciones. Sobre un esquema de BD ORACLE Integrando la información en los módulos.

Sistema modular que integra sus procesos a través de un modelo relacional de base de datos Oracle en un esquema único, con un solo ingreso y autenticación, pero desplegando diferentes aplicaciones y menús personalizados de acuerdo con los privilegios, roles y perfiles asociados a los usuarios.



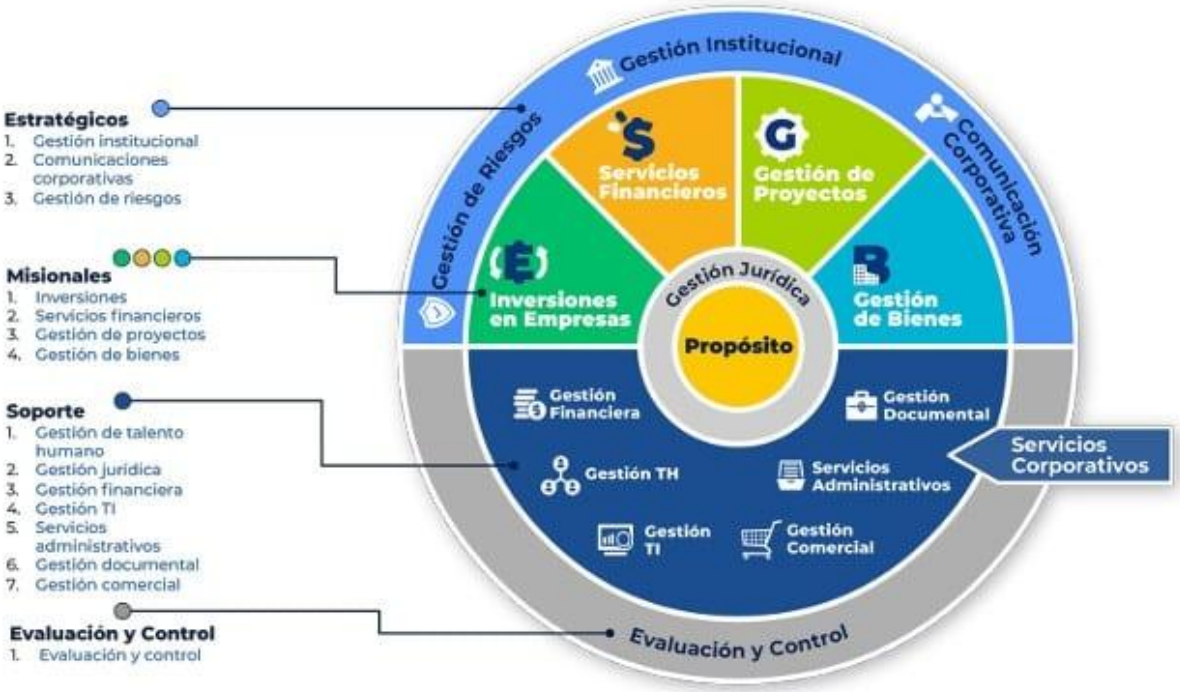
Con la implementación de este sistema integrado tenemos las siguientes ventajas:

- Automatización de los procesos misionales.
- Mayor seguridad en la gestión de la información.
- Adoptar buenas prácticas en concordancia con las circulares de la Superintendencia Financiera de Colombia.
- Dar cumplimiento de la normatividad vigente.
- Tener una plataforma tecnológica para realizar la operación y actividades objeto de Supervisión de la Superintendencia Financiera de Colombia.
- Contar con la integralidad de los procesos administrativos y financieros bajo una única plataforma que se comunique entre sí con todos sus módulos realizando transacciones de tipo operativo, comercial, depósitos, créditos, inversiones, transferencias, afectaciones presupuestales y contables por medio de los diferentes canales de cuenta del Infimanizales
- Mejorar características como usabilidad, escalabilidad, automatización, agilidad, cumplimiento de la ley y confianza en los procesos de la entidad.
- Eliminar reprocesos y doble digitación de la información entre los diferentes módulos.
- Obtener informes de manera casi inmediata y actualizada.
- Disponer de una herramienta para la gestión de riesgos financieros de mercado y riesgos financieros de liquidez.

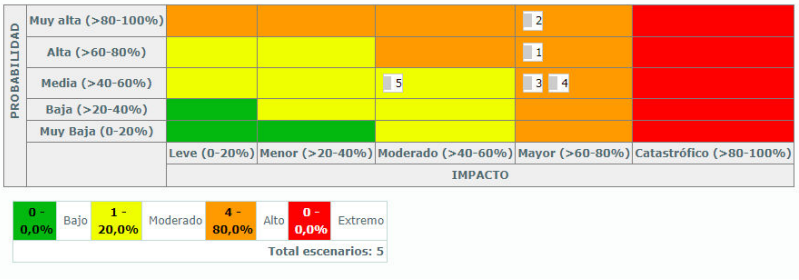
14. Estructura y Modelo Operativo de la Entidad

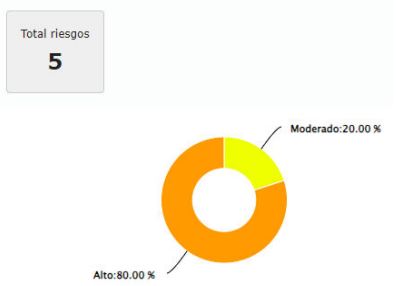
14.1 Estructura Organizacional

14.2 MODELO OPERATIVO - Mapa de Procesos



14.3 Definición y gestión de la Matriz riesgos de TI a nivel general





Unidad de riesgo	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Controles
Gestión de TI	Posibilidad de afectación reputacional por filtración o fuga de información debido a desconocimiento de las políticas de seguridad de la información y ciberseguridad del Instituto.	Media (>40-60%)	Moderado (>40-60%)	Moderado	1
Gestión de TI	Posibilidad de afectación económica por pérdida de la información debido a un suceso imprevisto que altera el normal funcionamiento de los equipos de computo y/o servidores de la entidad	Alta (>60-80%)	Mayor (>60-80%)	Alto	3
Gestión de TI	Posibilidad de afectación económica por falla en las aplicaciones que soportan las operaciones de la entidad debido a un suceso imprevisto que altera el normal funcionamiento de los sistemas de información de la entidad	Muy alta (>80-100%)	Mayor (>60-80%)	Alto	3
Gestión de TI	Posibilidad de afectación reputacional por queja, demanda o sanción de los grupos de valor y/o entes de control debido a pérdida de confidencialidad en activos de información del Instituto	Media (>40-60%)	Mayor (>60-80%)	Alto	1
Gestión de TI	Posibilidad de afectación reputacional por quejas de grupos de valor y/o sanciones de entes de control debido a pérdida de Integridad (modificación no autorizada) de la información posible ataque informático, falla eléctrica, errores de configuración, error humano en la aplicación de procedimientos, falla tecnológica, vulnerabilidades conocidos o desconocidos en el software y hardware	Media (>40-60%)	Mayor (>60-80%)	Alto	6

15. Gestión de Riesgos de TI

La gestión de riesgos de Tecnologías de la Información se desarrolla de manera articulada con el Sistema de Administración de Riesgos de la Entidad, considerando los riesgos tecnológicos, de seguridad de la información, ciberseguridad y continuidad del negocio.

El PETI incorpora la identificación, análisis, evaluación y tratamiento de los riesgos de TI, los cuales son gestionados a través de la matriz de riesgos institucional, los controles técnicos, administrativos y contractuales, y el fortalecimiento permanente de los esquemas de seguridad y monitoreo.

16. Alineación de TI con los Procesos

ESTRATEGICOS				
ID	**PROCESO**	**SISTEMA DE INFORMACIÓN**	**OPORTUNIDAD DE MEJORA EN TECNOLOGÍA**	**DETALLE**
001	Gestión Organizacional	Almera	Incentivar el uso y apropiación del software	Contrato de soporte y mantenimiento anual por parte del proveedor.
002	Comunicaciones Corporativas	Página WEB Redes Sociales	Envío de información oportuna para su actualización. Plan de comunicaciones Política de Seguridad y Privacidad de la Información	Contrato de soporte y mantenimiento anual por parte del proveedor. Contenidos mínimos publicados de acuerdo Ley de Transparencia y acceso a la información pública.

003	Gestión de Riesgos	Almera IAS Módulo Operational Solution	Gestión del Sistema de Administración de Riesgos (SAR) Gestión del Sistema de Administración de Riesgo Operativo (SARO) Plan de contingencia y continuidad del negocio, incluye sede alterna, seguridad de la información	Contrato de soporte y mantenimiento anual por parte del proveedor.

MISIONALES				
ID	**PROCESO**	**SISTEMA DE INFORMACIÓN**	**OPORTUNIDAD DE MEJORA EN TECNOLOGÍA**	**DETALLE**
001	Inversiones y servicios financieros	IAS Solution	Trazabilidad y seguimiento del ciclo completo del crédito. Digitalización de procesos	Base de datos ORACLE Contrato de soporte y mantenimiento anual por parte del proveedor.
002	Gestión de Proyectos	Almera **Licenciamiento:** Project 2019-2016 AutoCAD	Inversión en herramientas tecnológicas como: Software de business intelligence para gestión de información y presentaciones, Software de modelación 3D para arquitectura.	
003	Gestión de Bienes	Activos Fijos	Actualizar información módulo existente.	Base de datos ORACLE Contrato de soporte y mantenimiento anual por parte del proveedor.

SOPORTE				
ID	**PROCESO**	**SISTEMA DE INFORMACIÓN**	**OPORTUNIDAD DE MEJORA EN TECNOLOGÍA**	**DETALLE**
001	Gestión Humana	IAS SOLUTION	Capacitar funcionarios e implementar automatización de procesos.	Base de datos ORACLE Contrato de soporte y mantenimiento anual por parte del proveedor.
002	Gestión Jurídica	INFICONTRATOS Módulo de resoluciones Módulo Contratos en IAS	Automatizar el proceso. (Workflow) Uso y apropiación módulo contratación en IAS.	Base de datos Access MS SQL Server Oracle
003	Gestión Financiera	IAS SOLUTION	Capacitar funcionarios e implementar automatización de procesos. Implementación de indicadores de Inteligencia de Negocio	Base de datos ORACLE Contrato de soporte y mantenimiento anual por parte del proveedor. Comprende los módulos de: Contabilidad, presupuesto, tesorería, activos fijos y facturación de servicios).
004	Gestión Documental	Docunet Web	Implementación de las nuevas TRD para organizar estructura organizacional y estructura para la producción de documentos Implementar el (Workflow)	Base de datos: ORACLE Contrato de soporte y mantenimiento anual por parte del proveedor.

16.1 Otros servicios TI asociados en general a todos los procesos

Nombre	**Acceso a internet**
Descripción	Acceso a la red de colaboradores de la Entidad a través de dispositivos móviles y computadores portátiles. La velocidad de 300 GB concurrentemente
Categoría	Conectividad
Usuario objetivo	Todos los Funcionarios y contratistas de la entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	99%
Hallazgos u oportunidades de mejora	Nuevos equipos de acceso a la red inalámbrica.

Nombre	**Acceso a la red interna por VPN**
Descripción	Todos los funcionarios de la entidad
Categoría	Conectividad
Usuario objetivo	Funcionarios
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	99%
Hallazgos u oportunidades de mejora	--

Nombre	**Correo electrónico y herramientas colaborativas**
Descripción	• Gmail- Google Workspace con un almacenamiento general de 138 TB, almacenamiento en drive y acceso a aplicaciones de ofimática de Google
Categoría	Comunicación
Usuario objetivo	Funcionarios y contratistas de la entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	People Contact, Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	99%
Hallazgos u oportunidades de mejora	--

Nombre	**Servicio de entrenamiento y capacitación uso de las soluciones de TI**
Descripción	Servicio que suministra capacitación y entrenamiento sobre las funciones de los sistemas de información que maneja la entidad.
Categoría	Gestión de recursos
Usuario objetivo	Funcionarios de la entidad
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	De acuerdo con estimación
Hallazgos u oportunidades de mejora	--

Nombre	Telefonía IP – Convenio con People Contact
Descripción	Servicio de comunicaciones telefónicas entre usuarios internos y externos de la institución.
Categoría	Comunicación
Usuario objetivo	Funcionarios y contratistas de la entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	99%
Hallazgos u oportunidades de mejora	--

Nombre	Gestión de red interna colaboradores
Descripción	Gestión de la administración y configuración centralizada de la seguridad de la red institucional (internet).
Categoría	Comunicación
Usuario objetivo	Entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	99%
Hallazgos u oportunidades de mejora	

Nombre	Gestión de red de infraestructura tecnológica
Descripción	Gestión de la administración y configuración centralizada de la seguridad de la red que usan los Sistemas de información
Categoría	Comunicación
Usuario objetivo	Entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	99,97%
Hallazgos u oportunidades de mejora	--

Nombre	Antivirus
Descripción	Software que detecta y elimina virus y otras amenazas informáticas en la red, sistemas de información, PC, dispositivos móviles y demás.
Categoría	Seguridad
Usuario objetivo	Entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	99%
Hallazgos u oportunidades de mejora	

Nombre	Gestión de equipos de cómputo
Descripción	Adquisición, instalación, configuración y mantenimientos preventivos y correctivos de hardware y software de los equipos asignados a los funcionarios y contratistas de la Entidad
Categoría	Gestión de recursos
Usuario objetivo	Funcionarios y contratistas de la entidad
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	De acuerdo con estimación
Hallazgos u oportunidades de mejora	--
Nombre	Instalación de software en Equipos de computo
Descripción	Instalación de software por demanda en los equipos de computo de los funcionarios o contratistas
Categoría	Gestión de recursos
Usuario objetivo	Funcionarios y contratistas de la entidad
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	16 horas hábiles
Hallazgos u oportunidades de mejora	

Nombre	Videollamadas
Descripción	Acceso de servicio de video llamada a través de herramientas colaborativas Meet
Categoría	Comunicación
Usuario objetivo	Funcionarios y contratistas de la entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	99%
Hallazgos u oportunidades de mejora	-

Nombre	Página web institucional
Descripción	Sitio web institucional disponible a los ciudadanos que integra información sobre servicios institucionales, trámites, noticias, eventos de interés, políticas y normatividad.
Categoría	Comunicación
Usuario objetivo	Ciudadanos
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	99%
Hallazgos u oportunidades de mejora	--

Nombre	Soporte aplicaciones
Descripción	Gestión de incidentes y/o problemas presentados en las aplicaciones
Categoría	Gestión recursos
Usuario objetivo	Funcionarios y contratistas de la entidad

Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	99%
Hallazgos u oportunidades de mejora	--

Nombre	**Despliegue de software en producción**
Descripción	Preparación, configuración y despliegue de las soluciones generadas por el área de TI.
Categoría	Gestión recursos
Usuario objetivo	Usuarios de los sistemas de información
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico, mesa de servicio
Acuerdo de nivel de servicio	De acuerdo con estimación
Hallazgos u oportunidades de mejora	

Nombre	**Gestión de infraestructura de TI**
Descripción	Administración y monitoreo de servidores, servidores de aplicaciones, servidores web, sistemas de información, herramientas de software, soluciones en la nube y demás elementos de infraestructura de TI
Categoría	Gestión recursos
Usuario objetivo	Área de TI
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	De acuerdo con estimación
Hallazgos u oportunidades de mejora	--

Nombre	**Adquisición de licencias de software**
Descripción	Servicio de adquisición de licencias de software requeridas para usar en los diferentes procesos de la organización
Categoría	Gestión recursos
Usuario objetivo	Área de TI
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico, Software de mesa de servicio
Acuerdo de nivel de servicio	De acuerdo con estimación – cuantía proceso de contratación
Hallazgos u oportunidades de mejora	--

Nombre	Mantenimiento de aplicaciones – Proveedor de Software
Descripción	• Servicio que se encarga de realizar cambios en los sistemas de información para: • Corregir errores recurrentes • Actualizar software base • Aumentar la capacidad funcional de la aplicación
Categoría	Gestión recursos
Usuario objetivo	Usuarios de los sistemas de información
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico, Software de mesa de servicio
Acuerdo de nivel de servicio	99% y programación por parte del proveedor
Hallazgos u oportunidades de mejora	--

Nombre	Administración de bases de datos
Descripción	Servicio que se encarga de la administración de las bases de datos que maneja la entidad
Categoría	Gestión recursos
Usuario objetivo	Área de TI
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico, Software de mesa de servicio
Acuerdo de nivel de servicio	De acuerdo a estimación
Hallazgos u oportunidades de mejora	--

Nombre	Gestión de backup en la Nube
Descripción	Servicio que se encarga de generar respaldo de datos de los sistemas de información
Categoría	Gestión recursos
Usuario objetivo	Área de TI
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	No aplica
Hallazgos u oportunidades de mejora	--

Nombre	Gestión de perfiles de usuarios
Descripción	Servicio que permite asignar recursos organizacionales a los funcionarios y contratistas de la entidad, así mismo, provee los mecanismos de autenticación y autorización para el acceso a estos recursos
Categoría	Gestión recursos
Usuario objetivo	Todas las áreas de la entidad
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico
Acuerdo de nivel de servicio	De acuerdo a estimación

Hallazgos u oportunidades de mejora	--

Nombre	**Servicio de Virtualización de servidores**
Descripción	Servicio que permite virtualizar servidores físicos en varias máquinas virtuales, las cuales pueden proveer a su vez servicios de hosting a las diferentes soluciones de software.
Categoría	Gestión recursos
Usuario objetivo	Todas las áreas de la entidad
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico, Software de mesa de servicio
Acuerdo de nivel de servicio	99% y programación por parte del proveedor
Hallazgos u oportunidades de mejora	--

Nombre	**Servicio de supervisión de proveedores de TI**
Descripción	Servicio que permite asegurar que los proveedores cumplan con las obligaciones contractuales.
Categoría	Gestión recursos
Usuario objetivo	Área de TI
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, correo electrónico, informes de supervisión
Acuerdo de nivel de servicio	De acuerdo con estimación
Hallazgos u oportunidades de mejora	--

Nombre	**SOC SERVICIO DE MONITOREO A LA PLATAFORMA TECNOLÓGICA EN TEMAS DE CIBERSEGURIDAD**
Descripción	SOC CYREBRO: Monitoreo a plataforma de la entidad, verificación permanente de amenazas cibernéticas, Controlar, analizar y operar el entorno de Ciberseguridad de la organización
Categoría	Ciberseguridad e Infraestructura
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Permanentemente se establecen nuevas alertas, mejoras y configuraciones adicionales que tengan lugar, con el objetivo de optimizar el funcionamiento de las plataformas y la efectividad de estas. Minimizando permanentemente riesgos en temas de Ciberseguridad.

Nombre	**SERVICIO DE SIEM CORRELACIONADOR DE EVENTOS DE SEGURIDAD**
Descripción	CYREBRO SIEM: Construir un centro de operaciones de seguridad en donde centralice la información de múltiples fuentes de datos y además brinde la posibilidad de identificar ataques complejos que afectan múltiples puntos a la vez. Atención a alertas y eventos con corrección automática, Visualización de información, alertas y estadísticas de eventos de seguridad en toda la organización.
Categoría	Ciberseguridad e Infraestructura local o nube, Plataformas Misión Crítica y entornos de Endpoints, Herramientas de monitoreo de infraestructura
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	La herramienta entrega de manera permanente elementos de Ciberseguridad para realizar análisis heurístico, definir firmas de ataques, análisis de comportamiento, análisis con inteligencia artificial, etc

Nombre	**SERVICIO DE SOAR – ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA DE SEGURIDAD**
Descripción	CYREBRO SOAR: Herramienta que mediante una consola central integra características de seguridad de las aplicaciones y las consolida en flujos de trabajo de respuesta de amenazas optimizados y automatiza las tareas repetitivas de bajo nivel en esos flujos de trabajo. Además, esta consola permite a los SOC gestionar todas las alertas de seguridad generadas por estas herramientas en un único lugar.
Categoría	Ciberseguridad
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Mediante la implementación de este componente SOAR, se busca permanentemente reducir el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR), lo que mejora la posición general de seguridad de la organización. **La constante detección y respuesta a las**

	amenazas de seguridad más rápida puede suavizar el impacto de los ciberataques.

Nombre	**CARACTERÍSTICAS UEBA – ANÁLISIS DE COMPORTAMIENTO DE USUARIOS O ENTIDADES**
Descripción	CYREBRO UEBA: Poderoso conjunto de herramientas de seguridad para realizar un constante análisis de comportamiento de los activos de la entidad, incluidas las computadoras, servidores y elementos de red. UEBA identifica incidentes de seguridad tanto mediante análisis estadísticos y reglas definidas, o detectar comportamientos sospechosos sin patrones o reglas predefinidos
Categoría	Ciberseguridad
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Revisiones constantes para detectar amenazas internas, cuentas comprometidas de usuarios que hayan instalado malware, o detección de ataques de fuerza bruta digital e incluso detectar cuando existen usuarios con permisos de red innecesarios o mal perfilados.

Nombre	**SERVICIOS THEAT INTELLIGENCE – THEAT HUNTING CACERÍA DE AMENAZAS E INTELIGENCIA DE AMENAZAS**
Descripción	CYREBRO TH-TI + SERVICIOS GESTIONADOS: Gestión completa y permanente mediante herramientas TH-TI y Personal específico de analistas de SOC, que se encargan permanentemente de encontrar y combatir ataques basados en la red; identificar y analizar ciberamenazas
Categoría	Ciberseguridad
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Estrategia defensiva activa que busca iterativamente a través de redes para detectar indicadores de compromiso (IoC) y amenazas como Advanced Persistent Threats (APT) que eluden su sistema de seguridad existente. Permanentemente se generan hallazgos por esta actividad.

Nombre	**MDR-EDR: PROTECCIÓN Y RESPUESTA DE SEGURIDAD EN ENDPOINTS**
Descripción	EDR: SENTINEL ONE: Control de seguridad a dispositivos Endpoints, protección completa ante amenazas en equipos con diversos sistemas operativos determinando comportamientos, causa-raíz de las amenazas y con enfoque integral de prevención, detección y respuesta. .
Categoría	Ciberseguridad, Endpoints
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%

Hallazgos u oportunidades de mejora	Permanentemente se establecen nuevas alertas, mejoras y configuraciones adicionales que tengan lugar, con el objetivo de optimizar el funcionamiento de las plataformas y la efectividad de estas. Minimizando permanentemente riesgos en temas de Ciberseguridad.

17. Herramientas para medidas de protección de datos y prevención de accesos no autorizados.

ACRONIS CYBER PROTECT CLOUD:

Infimanizales cuenta con la solución **ACRONIS CYBER PROTECT CLOUD**, servicio de Cloud Backup con capacidad de un (1) TB para copias de seguridad de la plataforma de servidores y equipos de la entidad como respaldo a sus servicios informáticos.

- Esta solución nos permite hacer restauraciones en el sitio original y/o alterno.
- Las copias de seguridad se realizan de manera incremental en línea copiando solo los datos que han cambiado, manejando políticas de retención.
- Los datos son deduplicados, comprimidos y encriptados al ser transmitidos.
- El software cuenta con certificado FIPS 140-2 (Norma federal para el procesamiento de información), así como el respaldo a múltiples plataformas (Windows, Linux, Unix, Mac OS X).
- Las copias de seguridad se realizan de manera automática.
- En caso de indisponibilidad del canal de datos, la restauración se hace en sitio, en un tiempo no superior a dos horas.
- Se realizan acompañamiento constante al personal tanto de la configuración como respaldo de información y restauración de datos.

Se cuenta con un servicio y tecnología de DLP (Data Loss Prevention- Prevención de pérdida de datos) desplegado sobre los 20 activos más críticos de la organización.

Nombre	SOC SERVICIO DE MONITOREO A LA PLATAFORMA TECNOLÓGICA EN TEMAS DE CIBERSEGURIDAD
Descripción	SOC CYNET: Monitoreo a plataforma de la entidad, verificación permanente de amenazas cibernéticas, Controlar, analizar y operar el entorno de Ciberseguridad de la organización
Categoría	Ciberseguridad e Infraestructura
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio Google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Permanentemente se establecen nuevas alertas, mejoras y configuraciones adicionales que tengan lugar, con el objetivo de optimizar el funcionamiento de las plataformas y la efectividad de estas. Minimizando permanentemente riesgos en temas de Ciberseguridad.

Nombre	SERVICIO DE SIEM CORRELACIONADOR DE EVENTOS DE SEGURIDAD
Descripción	CYNET SIEM: Construir un centro de operaciones de seguridad en donde centralice la información de múltiples fuentes de datos y además brinde la posibilidad de identificar ataques complejos que afectan múltiples puntos a la vez. Atención a alertas y eventos con corrección automática, Visualización de información, alertas y estadísticas de eventos de seguridad en toda la organización.

Categoría	Ciberseguridad e Infraestructura local o nube, Plataformas Misión Crítica y entornos de Endpoints, Herramientas de monitoreo de infraestructura
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio Google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	La herramienta entrega de manera permanente elementos de Ciberseguridad para realizar análisis heurístico, definir firmas de ataques, análisis de comportamiento, análisis con inteligencia artificial, etc.

Nombre	**SERVICIO DE SOAR – ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA DE SEGURIDAD**
Descripción	CYNET SOAR: Herramienta que mediante una consola central integra características de seguridad de las aplicaciones y las consolida en flujos de trabajo de respuesta de amenazas optimizados y automatiza las tareas repetitivas de bajo nivel en esos flujos de trabajo. Además, esta consola permite a los SOC gestionar todas las alertas de seguridad generadas por estas herramientas en un único lugar.
Categoría	Ciberseguridad
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio Google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Mediante la implementación de este componente SOAR, se busca permanentemente reducir el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR), lo que mejora la posición general de seguridad de la organización. **La constante detección y respuesta a las amenazas de seguridad más rápida puede suavizar el impacto de los ciberataques.**

Nombre	**CARACTERÍSTICAS UEBA – ANÁLISIS DE COMPORTAMIENTO DE USUARIOS O ENTIDADES**
Descripción	CYNET UEBA: Poderoso conjunto de herramientas de seguridad para realizar un constante análisis de comportamiento de los activos de la entidad, incluidas las computadoras, servidores y elementos de red. UEBA identifica incidentes de seguridad tanto mediante análisis estadísticos y reglas definidas, o detectar comportamientos sospechosos sin patrones o reglas predefinidos
Categoría	Ciberseguridad
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio Google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Revisiones constantes para detectar amenazas internas, cuentas comprometidas de usuarios que hayan instalado malware, o detección de ataques de fuerza bruta digital e incluso detectar cuando existen usuarios con permisos de red innecesarios o mal perfilados.

Nombre	**ARQUITECTURA DE XDR – DETECCIÓN Y RESPUESTA AMPLIADAS**
Descripción	CYNET XDR: Permite integrar las herramientas de seguridad y unifica las operaciones de seguridad en todas las capas (usuarios, puntos finales, correo electrónico, aplicaciones, redes, cargas de trabajo en Cloud y datos) de Infimanizales, apoyando para detectar, y contener las amenazas de una forma más rápida y eficaz
Categoría	Ciberseguridad, Apoyo a las capas tecnológicas de Seguridad
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio Google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Con XDR, las soluciones de seguridad que no están necesariamente diseñadas para funcionar juntas pueden interoperar sin problemas en la prevención, detección, respuesta e investigación de amenazas. Dado que se cuenta en la entidad con diferentes proveedores y marcas tecnológicas, se hace necesario integrar todo.

Nombre	**SERVICIOS THEAT INTELLIGENCE – THEAT HUNTING CACERÍA DE AMENAZAS E INTELIGENCIA DE AMENAZAS**
Descripción	CYNET TH-TI + SERVICIOS GESTIONADOS: Gestión completa y permanente mediante herramientas TH-TI y Personal específico de analistas de SOC, que se encargan permanentemente de encontrar y combatir ataques basados en la red; identificar y analizar ciberamenazas
Categoría	Ciberseguridad
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio Google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Estrategia defensiva activa que busca iterativamente a través de redes para detectar indicadores de compromiso (IoC) y amenazas como Advanced Persistent Threats (APT) que eluden su sistema de seguridad existente. Permanentemente se generan hallazgos por esta actividad.

Nombre	**MDR-EDR: PROTECCIÓN Y RESPUESTA DE SEGURIDAD EN ENDPOINTS**
Descripción	CYNET Y EDR: SENTINEL ONE: Control de seguridad a dispositivos Endpoints, protección completa ante amenazas en equipos con diversos sistemas operativos determinando comportamientos, causa-raíz de las amenazas y con enfoque integral de prevención, detección y respuesta. .
Categoría	Ciberseguridad, Endpoints
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio Google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Permanentemente se establecen nuevas alertas, mejoras y configuraciones adicionales que tengan lugar, con el objetivo de optimizar el funcionamiento de las plataformas y la efectividad de estas. Minimizando permanentemente riesgos en temas de Ciberseguridad.

Nombre	**DLP SAFETICA ONE PROTECTION – Data Lost Prevention y Cumplimiento Normativo y Regulatorio.**
Descripción	DLP: Prevención de pérdida de información. Permite permanentemente descubrir, auditar y asegurar la información: identificación personal, datos financieros, datos de salud, etc. Visualización de datos confidenciales y control sobre cómo se

	accede y cómo se trabaja con ellos. Tenga un registro de auditoría claro de eventos de seguridad pasados Posibilidad de obtener informes de seguridad automatizados. Protección y cumplimiento de normas de seguridad, privacidad y protección de datos. Cumplimiento normativo entre otras de: ISO/IEC 27001, GDPR, PCI-DSS, HIPAA, CMMC, CCPA, TISAX, NIST, Regulaciones FedRamp, entre otras.
Categoría	Protección de Datos y Cumplimiento Normativo
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: Monitoreo 24 horas al día 7 días a la semana
Canal de soporte	Comunicación permanente vía WhatsApp, Telefónica, Espacio Google workspace SOC_INFI
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Cumplimiento normativo a regulaciones y estándares de seguridad y circulares específicas de SFC que miden cumplimiento por parte de Infimanizales. Normatividad cambiante que debe estar en constante verificación de cumplimiento de sus parámetros.

Nombre	**FIREWALL FORTINET – FORTIGATE 100E**
Descripción	Fortigate está implementado a nivel perimetral y filtra todo el tráfico de la organización. Tanto el tráfico entrante como saliente. Con reglas y parámetros de seguridad definidos por fabrica como las mejores prácticas.
Categoría	Protección de tráfico de red
Usuario objetivo	Todos los funcionarios de planta y contratistas de la entidad
Horario de prestación del servicio	24*7*365: 24 horas al día 7 días a la semana
Canal de soporte	Convenio Interadministrativo con People Contact - Comunicación permanente vía WhatsApp, Telefónica,
Acuerdo de nivel de servicio	SLA 99%
Hallazgos u oportunidades de mejora	Validación periódica de las políticas implementadas.

Nombre	Función que cumple	Proveedor	¿Tiene licencia?	Lenguaje en que está desarrollado	Versión del software	¿Tiene soporte?
PLATAFORMA SOC SIEM: Correlacionador de eventos de seguridad SOAR: Orquestación, Automatización y Respuesta de Seguridad – Reducción de tiempos de respuesta ante eventos de seguridad. **UEBA:** Características de análisis de comportamiento de usuarios o entidades	**PLATAFORMA SOC SERVICIO DE MONITOREO A LA PLATAFORMA TECNOLÓGICA EN TEMAS DE CIBERSEGURIDAD** Permite mantener una visibilidad completa sobre la infraestructura de la organización que es centralizado para tener una mejor visión de la superficie de ataque interna de la organización Otorgando la capacidad de las siguientes tecnologías en conjunto: • SIEM • SOAR • UEBA • XDR • Machine Learning • Aprendizaje Profundo	Cynet	SaaS Licencias, Servicios, Plataforma SOC, Analistas de SOC	Código propietario de Cynet	V 4.21.1.14	SI

XDR: Arquitectura de Detección y Respuesta ampliadas para integrar las diferentes marcas y tecnologías con las que cuenta Infimanizales. Servicios THEAT INTELLIGENCE – THEAT HUNTING: Cacería de Amenazas e Inteligencia de Amenazas	• Threat Hunting • Threat Intelligence • Honeypot o Tecnologías De Engaño • Tecnología Cynet Ramsomware Prevention Servicios de Analistas especializados de SOC, Análisis-Monitoreo 7*24 y Cacería permanente de amenazas.					

Nombre	Función que cumple	Proveedor	¿Tiene licencia?	Lenguaje en que está desarrollado	Versión del software	¿Tiene soporte?
Endpoint Protection Cloud	Antivirus para detectar y eliminar virus informáticos en los Endpoints	Kaspersky	SaaS	Código propietario de Kaspersky	14.2.0.27	SI
Endpoint Detection and Response MDR-EDR	Sistema de Detección y respuesta gestionada para la protección de los puntos finales, con capacidades de respuesta remota que reducen los MTTR en un 500% de tiempos de reacción.	Cynet	SaaS	Código propietario de Cynet	V 4.21.1.14	SI
DLP Data Lost Prevention Safetica DLP One Protection	Sistema de prevención de perdida de datos implementado en equipos críticos de la organización * Licenciamiento e incluidos servicios implementación por parte de Fabricante	Safetica ONE Protection DLP	SI	Código Propietario de Safetica	V 11.4.22	SI

18. Políticas de Seguridad y Copias

Los esquemas de seguridad de los aplicativos descritos obedecen a protocolos adoptados por sus desarrolladores, que, en todo caso, cumplen los estándares fijados por el mercado y la reglamentación.

18.1 Conservación custodia y seguridad de información documental y electrónica:

Para respaldo de la información Infimanizales cuenta de con una solución de Cloud Backup en Línea denominada Acronics donde se alberga la información crítica de forma externa a la organización y en línea, misma que permite la transmisión de datos de forma comprimida, deduplicada y encriptada con llave de 256 bits, y certificado de seguridad FIPS 140-2. Tal

herramienta admite en caso de caída inminente del canal de datos, que el proveedor del servicio proporcione copia del mismo para su restauración en sitio en un tiempo inferior a una hora.

Adicionalmente, a través del aplicativo Docunet se lleva el registro electrónico de la correspondencia recibida y despachada con número de radicación, fecha de recepción y/o envió, y una copia electrónica del documento.

Cada día se ejecutan tareas programadas para realizar las copias de seguridad de la información crítica del Instituto, y entre esta, las siguientes:

- ✓ Export Bases de Datos Oracle.
- ✓ Apoteosys.
- ✓ Docunet.
- ✓ Repositorio de Docunet.
- ✓ Base de datos Heinsohn Nomina
- ✓ Carpeta Público.
- ✓ Correspondencia.
- ✓ Ulises
- ✓ Pasivocol.
- ✓ Archivelogs BD Oracle.

18.2 Política General de Seguridad de la Información y Ciberseguridad

Establece los lineamientos generales para la seguridad de la información, teniendo en cuenta las demás políticas, normas y procedimientos que hacen parte de los procesos de la entidad, alineados con el contexto del direccionamiento estratégico y de gestión del riesgo garantizando la confidencialidad, integridad y disponibilidad de la información.

18.3 Plan de contingencia y continuidad del negocio.

El Plan de Contingencia y Continuidad del Negocio de INFIMANIZALES, contempla una serie de lineamientos, procedimientos y medidas preventivas, reactivas y correctivas para asegurar la continuidad de la operación en el evento de ocurrencia de un desastre o eventualidad que afecte la continuidad de los servicios del instituto. Igualmente, se definen los recursos mínimos requeridos, las personas implicadas en el plan, los roles para los funcionarios dentro de la entidad, los responsables de activar y desactivar los procedimientos de este plan y los protocolos a seguir durante una eventualidad.

19. Detalle de información de equipos de Infimanizales

Los equipos y demás elementos tecnológicos físicos, son parte esencial de la infraestructura tanto física, como digital de una organización. En ellos recae el almacenamiento y transferencia de los datos, referentes a los procesos que se realizan en el entorno empresarial. Es importante que éstos dispositivos físicos como terminales (computadores personales, de escritorio), periféricos (impresoras), conexiones de red y demás elementos, tengan la capacidad y la configuración adecuada, para mantener la confidencialidad, integridad y disponibilidad de la información manejada al interior y hacia los clientes de la entidad.

A continuación, se detalla la información referente a la infraestructura física de la entidad, los equipos de cómputo y de comunicaciones.

19.1 Inventario de Hardware y Software

INFIMANIZALES cuenta con equipos, servidores y demás elementos esenciales para ofrecer los servicios a los clientes y realizar los procesos adecuadamente. El detalle del inventario de hardware del instituto se encuentra en el documento **Equipos de cómputo Reporte Control Interno**

Total Equipos Portátiles	**24**
Total Equipos de Escritorio	**24**
Total Equipos Servidores	**2**
Equipos de computo y servidores en uso	**50**

Igualmente, se presenta la información sobre el licenciamiento de los aplicativos de la entidad:

	LICENCIAMIENTO
LICENCIAMIENTO	VMWARE VSPHERE
	LICENCIA SCHEDULE PRO SINGLE
	Office StandardMac 2019
	AutoCAD LT 2021
	AutoCAD LT 2023
	Project Standard 2019
	Office 365
	Office Professional Plus 2007 / Standard Edition 2007
	Offfice Standard 2016
	Abbyy FineReader 8,0 Professional Edition
	Mcafee MVISION Plus
	Corel Draw Graphics Suite X4
	LaberlView V .2 Pro
	Project Standard 2016
	Windows Server 2003 Small Business Server
	Windows Server 2003 Standard Edition
	Windows Server Standard Core 2019
	Windows Server 2019 - User CAL
	Windows Server Standard 2008 R2
	Windows Server 2008– Device CAL
	Exchange Server Standard 2010
	Exchange Server Standard 2010 User CAL
	Oracle Standard Edition One User Plus
	Discoverer Desktop Edition

19.2 Redes de Comunicaciones

La red de comunicaciones de INFIMANIZALES se encuentra dividida en varios aspectos importantes: plataforma tecnológica operativa, *networking* y plataforma virtual de la entidad.

Para la prestación del servicio de PBX, INFIMANIZALES y PEOPLE CONTACT como proveedor, se interconectarán mediante un canal de datos autónomo. Los números telefónicos asociados a INFIMANIZALES estarán en un Gabinete G430 de Avaya, donde se ubicarán las tarjetas PRI necesarias para recibir las llamadas de estos números telefónicos como también para las llamadas de salida generadas de las extensiones que estarán conectadas al gabinete G430. El gabinete G430 estará ubicado en las instalaciones de INFIMANIZALES. Este gabinete opera sobre la planta telefónica AVAYA de PEOPLE CONTACT S.A.S y en contingencia podrá operar autónomamente.

Mediante esta solución INFIMANIZALES se comunica entre extensiones sin consumir telefonía local. Se realizan 4 llamadas simultáneas hacia otras instituciones que tengan este mismo

servicio con PEOPLE CONTACT S.A.S (Invama, Concejo de Manizales, Aguas de Manizales y People Contact).

Las extensiones ubicadas en la Sede de INFIMANZIALES serán Avaya Hardphone con un teléfono físico que puede ser de Alta Gama o de Gama Estándar que varían por las funcionalidades que pueden tener. El servicio de internet en INFIMANIZALES es a través de Fibra Óptica, con una velocidad de 10 MB, provista por UNE Telecomunicaciones.

19.3 Solución Networking

People Contact ofrece una solución de *networking* para INFIMANIZALES, con el fin de cubrir las necesidades de conectividad, *networking* y seguridad perimetral, basadas en plataformas de fabricantes líderes en el mercado. Para brindar esta solución, se tienen los siguientes elementos:

Switches hp *networking* de la familia 5120

- Switches *full layer 2* y con soporte de rutas estáticas a nivel de capa 3.
- Puertos 10/100/1000 con capacidad de *stacking* y puertos tipo SFP a giga.
- 24 RJ-45 *autosensing* 10/100/1000 *ports* (IEEE 802.3Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE802.3ab Type 1000BASE-T); Duplex:10BASE-T/100BASE-TX: half or full; 1000BASE-T.
- *fullonly4 dual-personality ports; autosensing10/100/1000BASE-T or SFP.*
- Dos *port expansion module slots.*

La solución contempla los siguientes switches:

- Dos switches HP 5120-24G.
- Un switch HP 5120-48G.

Wireless

La solución de conectividad inalámbrica está soportada en equipos Fortinet considerando 2 *Access* Point para el cubrimiento del área:

- Una AP Fortinet FAP-221C.
- Un FortiWiFi F60C

Estos equipos son completamente compatibles con los estándares IEEE 802.11a/b/g/n/ac, trabajando en las bandas de 2.4 y 5 GHz. Indoor wireless AP — 1x GE RJ45 port, dual radio (802.11 a/n/ac and 802.11 b/g/n, 2x2 MIMO).

19.4 Seguridad perimetral (UTM)

Se ofrece una solución integrada para cubrir la seguridad perimetral de la red basada en un equipo tipo UTM de Fortinet: Fortigate 100E, que además de cumplir con las funcionalidades de UTM (Unified Treatment Management) es a su vez Access Point, permitiendo mejorar la cobertura inalámbrica de la red, como se detalla en la figura siguiente.

Las funcionalidades del UTM abarcan:

- Firewall
- VPN (IPsec y SSL)
- Antivirus perimetral
- Antispyware
- Antimalware
- Control de contenido
- Control de aplicaciones

20. Ciberseguridad

Infimanizales entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

21. Indicadores

Indicador: Cumplimiento del plan de acción del proceso (Meta 85%)

Variables (2)	Actividades terminadas Unidades Actividades planificadas Unidades
Fórmula	(Actividades terminadas / Actividades planificadas)*100

Indicador: Cumplimiento del PETI (Meta 85%)

Variables (2)	Actividades realizadas Unidades Actividades planeadas en el PETI Unidades
Fórmula	(Actividades realizadas / Actividades planeadas en el PETI)*100

22. Indicadores de Gestión de TI

Dimensión	Indicador	Descripción	Meta
Gestión TI	Cumplimiento del PETI	Porcentaje de iniciativas ejecutadas frente a las programadas	≥ 85%
Gestión TI	Cumplimiento Plan de Acción TI riesgos	Avance de actividades TI incluidas en el Plan de Acción	≥ 85%
Disponibilidad	Disponibilidad de servicios críticos	Tiempo de disponibilidad de sistemas y servicios críticos	≥ 99%
Seguridad de la Información	Incidentes de seguridad gestionados	Incidentes atendidos y gestionados oportunamente	100%
Ciberseguridad	Tiempo medio de detección (MTTD)	Tiempo promedio de detección de incidentes de ciberseguridad	≤ SLA
Ciberseguridad	Tiempo medio de respuesta (MTTR)	Tiempo promedio de respuesta ante incidentes	≤ SLA
Continuidad	Cumplimiento de	Ejecución de copias de	100%

Dimensión	Indicador	Descripción	Meta
	respaldos	seguridad de información crítica	
Continuidad	Pruebas de continuidad realizadas	Ejecución de pruebas del plan de continuidad y DRP	≥ 1 anual
Uso y apropiación	Funcionarios capacitados en TI	Porcentaje de funcionarios capacitados en el uso de TIC	≥ 80%

23. Conclusiones

El Plan Estratégico de Tecnologías de la Información – PETI 2026–2028 de INFIMANIZALES consolida el direccionamiento estratégico de la gestión de TI, permitiendo alinear las capacidades tecnológicas con los objetivos institucionales y los requerimientos normativos del Estado Colombiano.

El PETI constituye una hoja de ruta clara y realista para fortalecer la seguridad de la información, la ciberseguridad, la continuidad del negocio y la eficiencia operativa, garantizando que las inversiones en tecnología generen valor público, apoyen la toma de decisiones y contribuyan al desarrollo sostenible de la Entidad.

Su implementación y seguimiento permitirán a INFIMANIZALES avanzar hacia una gestión tecnológica madura, resiliente y orientada a la mejora continua.

Durante 2026 – 2028 Infimanizales gestionará la implementación de ecosistemas digitales para la prestación de servicios financieros. Teniendo como objetivos:

- Implementar el portal de clientes de los servicios financieros
- Implementar el módulo de indicadores financieros y de riesgos
- Automatizar el proceso de créditos de consumo
- Automatizar el proceso de consultas de listas vinculantes