PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN - PETI

2021-2024

GERENCIA DE TECNOLOGÍA

Versión 10.0

BOGOTÁ | Unidad Administrativa Especial de Catastro Distrital

CONTROL DE VERSIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS
5.0	16/12/2020	Versión aprobada por el Comité Institucional de Gestión y Desempeño de Catastro el 24 de diciembre de 2020.
7.0	28/12/2021	Versión aprobada por el Comité Institucional de Gestión y Desempeño de Catastro el 28 de diciembre de 2021
9.0	22/12/2022	Versión aprobada por el Comité Institucional de Gestión y Desempeño de Catastro el 22 de diciembre de 2022
10.0	12/12/2023	Versión para presentación y aprobación del Comité Institucional de Gestión y Desempeño de Catastro del 2023

AUTORES: Ricardo Munévar Molano, Diego Antonio Huertas Buitrago, Rocío Cedano García, Mauricio Herrera García, Carmen Beatriz Quiñones, Javier Andres Arias Sanabria, Juan Manuel Angel Cuartas, Javier Francisco Fúneme y equipo Gerencia de Tecnología

REVISIÓN Y APROBACIÓN: Héctor Henry Pedraza Piñeros – Gerente de

TABLA DE CONTENIDO

1 INTRODUCCIÓN 7
2 OBJETIVOS DEL PETI 9
2.1 Objetivo general 9
2.2 Objetivos específicos 9
3 ALCANCE 10
4 MARCO METODOLÓGICO 11
5 MARCO NORMATIVO 13
6 ENTENDIMIENTO ESTRATÉGICO 17
6.1 Contexto institucional 17
6.2 Alineación Estratégica 18
6.3 Objetivos estratégicos 19
6.4 Necesidades y oportunidades de TI - 20
6.5 Portafolio de Servicios de TI 22
7 SITUACIÓN ACTUAL 22
7.1 ESTRATEGIA DE TI 24
7.2 GOBIERNO DE TI 25
7.2.1 Procesos de Gestión de TI 26
7.2.2 Estructura Organizacional de TI 27
7.2.3 Esquema de Gobierno de TI 29
7.2.4 Indicadores de gestión de TI 30
7.2.5 Matriz riesgos de TI 32
7.2.6 Gestión de Proyectos TI 34
7.3 INFORMACIÓN 36
7.3.1 Arquitectura de Información 36
7.3.2 Gobierno componentes de información 43
7.3.3 Catálogos de componentes de información 43
7.3.4 Servicios intercambio de información 44
7.3.5 Calidad de componentes de información 46

7.4 SISTEMAS DE INFORMACIÓN 46
7.4.1 Arquitectura de Sistemas de Información 46
7.4.2 Catálogo de Sistemas de Información 49
7.4.3 Documentación técnica y funcional de los Sistemas de Información 49
7.4.4 Ciclo de vida de los Sistemas de Información 50
7.4.5 Mantenimiento y soporte de los sistemas de información 51
7.5 INFRAESTRUCTURA DE TI 54
7.5.1 Gestión de la operación de la infraestructura tecnológica 54
7.5.2 Capacidades de la infraestructura tecnológica 54
7.5.3 Inventario de la infraestructura tecnológica 99
7.5.4 Recuperación y disponibilidad en la Operación 101
7.5.5 Disposición de residuos tecnológicos 102
7.5.6 Implementación del Protocolo de Internet versión 6 (IPv6) 104
7.6 USO Y APROPIACIÓN 104
7.7 SEGURIDAD DE LA INFORMACIÓN 106
8 SITUACIÓN OBJETIVO (TO BE) 109
8.1 ESTRATEGIA DE TI 109
8.1.1 Planeación Estratégica de TI 109
8.1.2 Servicios de TI 110
8.1.3 Directrices y estándares para la gestión de la gobernabilidad de TI 110
8.1.4 Tablero de control de TI 110
8.2 GOBIERNO DE TI 110
8.2.1 Procesos de Gestión de TI 110
8.2.2 Planeación, ejecución y gestión de proyectos de TI 111
8.3 INFORMACIÓN 112
8.3.1 Arquitectura 112
8.3.2 Gobierno 113
8.3.3 Catálogo de componentes de información 114
8.4 SISTEMAS DE INFORMACIÓN 114

8.4.1 Catálogo de Sistemas de Información 114
8.4.2 Ciclo de vida de los sistemas de información 115
8.4.3 Arquitectura de Sistemas de Información 116
8.4.4 Soporte y mantenimiento de Sistema de Información 116
8.5 INFRAESTRUCTURA DE TI 117
8.5.1 Capacidades de infraestructura tecnológica 117
8.5.2 Arquitectura de infraestructura tecnológica 132
8.5.3 Sistema de Copias de respaldo 132
8.5.4 Administración de la operación 135
8.6 USO Y APROPIACIÓN 135
8.7 SEGURIDAD DE LA INFORMACIÓN 136
9 HALLAZGOS Y BRECHAS 137
10 PORTAFOLIO DE PROYECTOS DE TI 138
10.1 Identificación de proyectos de TI 138
10.1.1 Gestión y Gobierno de TI 139
10.1.2 Sistema de Gestión de Seguridad de la Información (SGSI) 140
10.1.3 Sistemas de Información 141
10.1.4 Infraestructura de TI 141
10.2 Hoja de Ruta y Presupuesto 143
11 PLAN DE COMUNICACIONES DEL PETI 146

1 INTRODUCCIÓN

Las tecnologías de la información y las comunicaciones; se han constituido en uno de los pilares importantes para el desarrollo del país y el impulso de la competitividad a nivel nacional y territorial. Las TIC habilitan la agregación de valor transversal en la economía y han transformado la manera en que las personas acceden a la información, se educan, trabajan, generan ingresos y se interrelacionan.

La magnitud del cambio es tan grande, sobre todo en el ámbito productivo, que incluso hoy en día se dice que el mundo está transitando por una Cuarta Revolución Industrial (o Industria 4.0), lo cual ha impulsado la transformación digital de los sectores productivos, de la administración pública, el desarrollo de iniciativas de ciudades inteligentes y, por ende, ha generado nuevas exigencias en la fuerza laboral y en la gestión integral del talento humano para el mercado de la economía digital.

Para apalancar la transformación digital del Estado Colombiano y con el objetivo de contribuir en la construcción de un Estado más eficiente en la gestión, transparente y participativo, y que preste mejores servicios a los ciudadanos y a las empresas a través del aprovechamiento de las TIC, el Gobierno nacional con el apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC ha realizado esfuerzos orientados a la adopción de tecnologías digitales para la provisión de sus servicios. La digitalización de las cadenas de trámites, la interoperabilidad entre entidades y el uso de la analítica de datos son una de las acciones principales realizadas en el sector.

En 2015 se actualizó el Decreto 1078 Estrategia de Gobierno en línea, el cual plantea una visión más unificada de la digitalización, a través de los ejes sectoriales de intervención que facilitan la masificación de la oferta y la demanda del Gobierno en Línea. De ahí, se destacan las TIC como herramientas transversales a varios sectores para mejorar la calidad de vida de los ciudadanos, a través de la implementación de TIC para servicios, TIC para el gobierno abierto, TIC para la gestión, seguridad y privacidad de la Información. Además, expone como instrumentos para la implementación de la estrategia de Gobierno en línea el Manual de Gobierno en Línea y el Marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información.

Para el 14 de junio del 2018, se subroga la estrategia de gobierno en línea con el Decreto 1008 del Ministerio de Tecnologías de la Información y las Comunicaciones, estableciendo la Política de Gobierno Digital, bajo los principios de innovación, competitividad, proactividad y seguridad de la información. Esta política muestra una visión más unificada de la transformación digital, pues abarca dentro de sus lineamientos las TIC de manera transversal a diferentes sectores, entre los que se destacan los componentes TIC para el Estado y TIC para la Sociedad y los habilitadores transversales de la Política de Gobierno Digital (arquitectura, seguridad y privacidad y Servicios Ciudadanos Digitales), en aras de habilitar y mejorar la provisión de servicios digitales de confianza y calidad,

lograr procesos internos, seguros y eficientes a través, del fortalecimiento de las capacidades de gestión de tecnologías de información y empoderar a los ciudadanos a través de la consolidación de un Estado abierto.

La Unidad Administrativa Especial de Catastro Distrital-UAECD ha tenido avances significativos en materia de eficiencia administrativa, participación y servicios al ciudadano por medios electrónicos. No obstante, la evolución constante de la sociedad y el avance del país hacia una economía digital caracterizada por factores como el conocimiento, la digitalización de la información, la interconexión y la innovación; hacen necesario el desarrollo de procesos de transformación digital que permitan contar con entidades públicas más proactivas e innovadoras para garantizar mejores condiciones de vida a los ciudadanos, así como, satisfacer necesidades y problemáticas a través del aprovechamiento de las tecnologías de la información y las Comunicaciones.

Teniendo en cuenta, los nuevos retos estratégicos de la UAECD relacionados con la implementación de Catastro Multipropósito y la transformación digital, se actualizó el plan estratégico de Tecnologías de la Información (2021 -2024), mediante el cual , la Gerencia de Tecnología tendrá la oportunidad de transformar digitalmente los servicios que brinda a sus grupos de interés, adoptar los lineamientos de la Gestión de TI del Estado Colombiano, desarrollar su rol estratégico al interior de la Unidad Administrativa Especial de Catastro Distrital-UAECD, apoyar las áreas misionales mientras se piensa en tecnología, liderar las iniciativas de TI que deriven en soluciones reales y tener la capacidad de transformar su gestión, como parte de los beneficios que un plan estratégico de TI debe producir una vez se inicie su ejecución.

La estructuración y la puesta en ejecución del PETI cuenta con importantes beneficios estratégicos y tácticos para la entidad:

- Apoyar la transformación digital de la entidad por intermedio de un portafolio de proyectos que estén alineados con los objetivos y metas de la alta gerencia, de tal manera que apalanquen y ayuden a la entidad alcanzar las metas de su estrategia en el corto, mediano y largo plazo.
- Fortalecer las capacidades de la Gerencia de Tecnología para apoyar la estrategia y modelo operativo de la entidad, teniendo en cuenta el nuevo reto de Catastro Multipropósito
- Identificar herramientas que ayuden a contar con información oportuna para la toma de decisiones y permitan el desarrollo y mejoramiento de la entidad.
- Adquirir e implementar buenas prácticas de gestión de TI.
- Adoptar Tecnología disruptiva para apoyar la gestión institucional.

Es así como el presente documento, denominado “Plan Estratégico de Tecnologías de la Información-PETI” se encuentra alineado con lo definido en dicho marco, sus guías y plantillas y funge como uno de los artefactos o productos definidos para mejorar la prestación de los servicios

de tecnologías de la información que presta Unidad Administrativa Especial de Catastro Distrital-UAECD, en el marco del cumplimiento de la política de Gobierno Digital.

Desde su formulación, se ha venido actualizando año tras año, respondiendo a las directrices de la dirección de la UAECD y se han cerrado o modificado brechas, según las prioridades y presupuesto asignado a la Gerencia de Tecnología.

2 OBJETIVOS DEL PETI

2.1 Objetivo general

Definir el norte a seguir por la Unidad Administrativa Especial de Catastro Distrital durante el periodo (2021 – 2024) a partir de las necesidades y oportunidades de mejoramiento de los interesados en lo relacionado con la gestión de TI para apoyar la estrategia y el modelo operativo de la entidad, apoyados en las definiciones de la Política de Gobierno Digital para la construcción de una administración eficiente, transparente y participativa que genere valor, convirtiéndose en el punto de partida de procesos de transformación digital que permitan contar con una Unidad Administrativa Especial de Catastro Distrital más proactiva e innovadora que garantice mejores y más servicios a los ciudadanos y la interacción con ellos, a través del aprovechamiento de las tecnologías de la información y las comunicaciones y las tecnologías disruptivas de la cuarta revolución industrial.

2.2 Objetivos específicos

Para dar cumplimiento al Objetivo general del PETI se definen los siguientes objetivos específicos:

1. Definir el portafolio de proyectos de TI idóneos y medibles en una línea de tiempo para cuatro años, con el fin de contribuir al logro de los objetivos estratégicos de la Unidad Administrativa Especial de Catastro Distrital y del Distrito Capital.
2. Fortalecer la gestión de TI e Incrementar el nivel de madurez de los procesos de Gestión de TI en la Unidad Administrativa Especial de Catastro Distrital para dar cumplimiento al propósito de la Política de Gobierno Digital “Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información” y garantizar la optimización y el uso de los servicios tecnológicos, sistemas de información e información que faciliten su asignación, uso y apropiación.

3. Definir e implementar un modelo de gestión de Gobierno de TI, que garantice la continuidad de negocio incorporando políticas, estándares y lineamientos de TI, contemplando medidas preventivas y de recuperación que no afecte el buen funcionamiento de la entidad.
4. Definir y gestionar un modelo que garantice la seguridad y privacidad de la información, definiendo políticas, lineamientos, controles y mecanismos para alcanzar los niveles requeridos de seguridad, privacidad y trazabilidad de los componentes de Información.
5. Incrementar la calidad y cantidad de los servicios en línea ofrecidos a los ciudadanos para dar cumplimiento al propósito de la Política de Gobierno Digital "Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad".
6. Fortalecer la gestión de la información para dar cumplimiento al propósito de la Política de Gobierno Digital "Tomar decisiones basadas en datos a partir del aumento en el uso y aprovechamiento de la información"
7. Aprovechar las tecnologías de la Cuarta Revolución Industrial (4RI) y otras tecnologías emergentes que permitan cumplir con la iniciativa de "Ciudad Inteligente" y transformación digital e innovación de la Unidad Administrativa Especial de Catastro Distrital.
8. Formalizar y divulgar el PETI y las políticas de TI como instrumento de direccionamiento estratégico y planificación de TI en la Unidad Administrativa Especial de Catastro Distrital.
9. Definir los recursos humanos, físicos, financieros y tecnológicos, para garantizar el cumplimiento del Plan Estratégico de las Tecnologías de la Información de la Unidad Administrativa Especial de Catastro Distrital y enfocar y optimizar la inversión tecnológica.
10. Avanzar en la transformación digital de la Unidad Administrativa Especial de Catastro Distrital como un proceso de cambio estratégico con visión a largo plazo para impactar positivamente la calidad de vida de los ciudadanos.
11. Dar cumplimiento a la Política de Gobierno Digital y a las directrices de Transformación Digital del estado colombiano.

3 ALCANCE

El Plan Estratégico de Tecnologías de la Información y Comunicaciones PETI de la Unidad Administrativa Especial de Catastro Distrital que se describe en el presente documento para el periodo 2021 – 2024, permitirá planear, definir y ejecutar los proyectos tecnológicos, a corto y mediano plazo, enmarcados principalmente en los nuevos lineamientos y normativa de la Política

de Gobierno Digital y Transformación Digital[1], el Plan de Desarrollo Distrital de Bogotá, el nuevo Plan Estratégico de la Unidad Administrativa Especial de Catastro Distrital y los planes del sector Hacienda de Bogotá D. C.

Adicionalmente, para su construcción se tendrán en cuenta el nuevo Marco de Referencia de Arquitectura propuesto por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC[2], los resultados del Formulario Único de Reporte de Avances a la Gestión (FURAG) del Departamento Administrativo de la Función Pública, el Modelo Integrado de Planeación y Gestión (MIPG) de la Unidad Administrativa Especial de Catastro Distrital, los requisitos de calidad de los sellos de excelencia y los lineamientos de los Servicios de los Ciudadanos Digitales del Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC.

Para lograr los objetivos propuestos y bajo el liderazgo de la Gerencia de Tecnología, el PETI se actualizará de forma conjunta y se involucrarán en la medida que se requieran, a las áreas misionales, estratégicas y de apoyo de la Unidad Administrativa Especial de Catastro Distrital, teniendo en cuenta que el resultado esperado es el de impactar positivamente la calidad de vida de los ciudadanos, generando valor público en cada una de las interacciones digitales entre ciudadano y Estado, mejorando la provisión de servicios digitales de confianza y calidad, lo que supondrá cambios organizacionales, de procesos y recursos de la entidad.

Teniendo en cuenta que el Plan Estratégico de Tecnologías de la Información - PETI es un proceso de planeación dinámico y que el Gobierno Nacional se encuentra en actualización permanente de los lineamientos relacionados con la Política de Gobierno Digital y la Transformación Digital, es importante llevar a cabo, por lo menos, una revisión anual al documento para actualizar las estrategias y el plan de implementación a largo plazo, así como para adicionar los planes de acción en el corto plazo.

El PETI incluye los motivadores estratégicos que hacen parte del entendimiento estratégico, la situación actual y objetivo de la gestión de TI, la identificación de brechas y definición del portafolio de iniciativas, proyectos y el mapa de ruta con el cual la entidad apoyará la transformación digital de la entidad

4 MARCO METODOLÓGICO

Para lograr la transformación digital del Estado y por ende en la Unidad Administrativa Especial de Catastro Distrital, la política de Gobierno Digital se constituye en el eje fundamental, en tanto

[1] https://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html
[2] https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8118.html

proporciona los estándares tecnológicos para optimizar la gestión de las entidades públicas, y brinda lineamientos para impactar positivamente la calidad de vida de los ciudadanos a través de las TIC.

La política de Gobierno Digital[3] que fue actualizada mediante decreto 767 del 16 de mayo 2022 busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC.

Ilustración 1. Elementos de la Política de Gobierno Digital

Adicionalmente, la Política de Gobierno Digital es una de las diecisiete políticas de gestión y desempeño institucional, que se desarrolla en el marco del Modelo Integrado de Planeación y Gestión y se encuentra en el Eje de Gestión para el Resultado con Valores.

Dada la transversalidad de los medios digitales en los procesos internos de la entidad y en el relacionamiento con los usuarios, la Política de Gobierno Digital está estrechamente relacionada con las políticas de: Planeación Institucional, Talento humano, Transparencia, Acceso a la Información Pública y Lucha Contra la Corrupción, Fortalecimiento Organizacional y Simplificación

[3] https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

de Procesos, Servicio al Ciudadano, Participación Ciudadana en la Gestión Pública, Racionalización de trámites, Gestión Documental, Seguridad Digital y Gestión del Conocimiento y la Innovación.

Para la estructuración del PETI se tuvo en cuenta los nuevos lineamientos de MinTIC para la estructuración del PETI y la nueva plantilla tipo del PETI socializada por MinTIC en octubre de 2020, como también el nuevo Marco de Referencia de Arquitectura Empresarial - MRAE v3.0 de mayo de 2023.

5 MARCO NORMATIVO

Las leyes, decretos y demás desarrollos normativos que guían las acciones para implementar la Política de Gobierno Digital, el Modelo de Arquitectura Empresarial (MAE) y la estructuración de Planes Estratégicos de Tecnología, son las siguientes:

Nombre	Descripción
Decreto 767 de 2022	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
CONPES 3995 del Consejo Distrital de Política Económica y Social	Política nacional de confianza y seguridad digital del 1º de julio de 2020
Plan Distrital de Desarrollo 2020-2024	Un nuevo contrato social y ambiental para la Bogotá del siglo XXI de mayo 27 de 2020
Decreto 620 de 2020	Lineamientos generales en el uso y operación de los servicios ciudadanos digitales, expedido el 2 de mayo de 2020
CONPES 04 del Consejo Distrital de Política Económica y Social del Distrito Capital	POLÍTICA PÚBLICA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN 2019-2038 del 12 de noviembre del 2019
CONPES 3975 del Consejo Nacional de Política Económica y Social	POLÍTICA NACIONAL PARA LA TRANSFORMACIÓN DIGITAL E INTELIGENCIA ARTIFICIAL” del 8 de noviembre de 2019

Nombre	Descripción
CONPES 01 del Consejo Distrital de Política Económica y Social del Distrito Capital	POLÍTICA PÚBLICA DISTRITAL DE TRANSPARENCIA, INTEGRIDAD Y NO TOLERANCIA CON LA CORRUPCIÓN del 6 de febrero del 2019
CONPES 3920 del Consejo Nacional de Política Económica y Social	POLÍTICA NACIONAL DE EXPLOTACIÓN DE DATOS (BIG DATA) del 17 de abril del 2018
Ley 1955 de 2019	Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".
Plan Nacional de Desarrollo 2018-2022	Pacto por Colombia Pacto por la Equidad
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 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.
Conpes 3920 de 2018	Política Nacional de Explotación de datos.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.
Resolución 2405 de 2016	Por el cual se adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su comité
CONPES 3854 del Consejo Distrital de Política Económica y Social	Política Nacional de Seguridad Digital del 12 de abril de 2016
Ley 1753 de 2015	Por el cual se expide el Plan Nacional de Desarrollo 2014-2018.
Resolución 3564 de 2015	Reglamentaciones asociadas a la Ley de Transparencia y Acceso a la Información Pública
Decreto 333 de 2014	Define el régimen de acreditación de las entidades de certificación, aplicable a personas jurídicas, públicas y privadas.

Nombre	Descripción
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.
Decreto 1510 de 2013	Por el cual se reglamenta el sistema de compras y contratación pública.
Decreto 2482 de 2012	Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión (Ley 489 de 1998, Ley 552 de 1994).
Ley 19 de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2578 de 2012	Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los Archivos del Estado.
Decreto 2609 de 2012	Por la 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 4170 de 2011	Mediante el cual se establece un sistema para la compra en entidades públicas, se determina que debe existir un Sistema de Información en el cual se almacene y se de trazabilidad a las etapas de contratación del país, garantizando la transparencia de los procesos.
Ley 1437 de 2011	Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
Conpes 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas (Ley 2550 de 1995).
Conpes 3670 de 2010	Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones.

Nombre	Descripción
Ley 1286 de 2009	Por la cual se modifica la Ley 29 de 1990, se transforma a Colciencias en Departamento Administrativo, se fortalece el Sistema Nacional de Ciencia, Tecnología e Innovación en Colombia y se dictan otras disposiciones.
Ley 1341 de 2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Decreto 4485 de 2009	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
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 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.
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 presten servicios públicos.
Decreto 4110 de 2004	Adopción de la norma técnica de calidad de la gestión pública.
Decreto 1524 de 2002	Establecer las medidas técnicas y administrativas destinadas a prevenir el acceso a menores de edad a cualquier modalidad de información pornográfica contenida en Internet o en las distintas clases de redes informáticas a las cuales se tenga acceso mediante redes globales de información.
Acuerdo 50 de 2000	Por el cual se desarrolla el artículo 64 del título VII "conservación de documento", del Reglamento general de archivos sobre "Prevención de deterioro de los documentos de archivo y situaciones de riesgo.

Nombre	Descripción
Acuerdo 47 de 2000	Por el cual se desarrolla el artículo 43 del capítulo V "Acceso a los documentos de archivo", del Reglamento general de archivos sobre "Restricciones por razones de conservación.
Ley 594 de 2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Ley 599 de 2000	Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático.
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 489 de 1998	Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.
Acuerdo 11 de 1996	Por el cual se establecen criterios de conservación y organización de documentos.
Ley 152 de 1994	Por la cual se establece la Ley Orgánica del Plan de Desarrollo.
Decreto 2620 de 1993	Por el cual se reglamenta el procedimiento para la utilización de medios técnicos adecuados para conservar los archivos de los comerciantes.
Ley 39 de 1981	Por la cual se elimina la exigencia del papel sellado y se suprime el impuesto correspondiente.

6 ENTENDIMIENTO ESTRATÉGICO

6.1 Contexto institucional

La misión institucional de la Unidad Administrativa Especial de Catastro Distrital está definida por las normas catastrales vigentes, expedidas por el Gobierno Nacional y el Instituto Geográfico Agustín

Codazzi - IGAC, así como por el Acuerdo 257 de 2006, a través del cual se definió la estructura, organización y funcionamiento de los organismos y de las entidades de Bogotá Distrito Capital.

En el Acuerdo 257 de 2006, se estableció que la Unidad tiene por objeto responder por la recopilación e integración de la información georreferenciada de la propiedad inmueble del Distrito Capital en sus aspectos físico, jurídico y económico, que contribuya a la planeación económica, social y territorial del Distrito Capital y a través del Acuerdo 130 de 2004 se creó la Infraestructura Integrada de Datos Espaciales para el Distrito Capital, producto del intercambio, análisis y producción de información georreferenciada, relativa al área urbana y rural del Distrito Capital y se le asigna a la UAECD la coordinación de dicha Infraestructura

La estrategia de la entidad 2020-2024, es el resultado de la planeación estratégica de la Unidad Administrativa Especial de Catastro Distrital a partir del Plan de Desarrollo Distrital (vigente) 2020-2024 que se aprobó mediante el proyecto de acuerdo Nº 123 DE 2020 SEGUNDO DEBATE y "POR MEDIO DEL CUAL SE ADOPTA EL PLAN DE DESARROLLO ECONÓMICO, SOCIAL, AMBIENTAL Y DE OBRAS PÚBLICAS DEL DISTRITO CAPITAL 2020-2024 "UN NUEVO CONTRATO SOCIAL Y AMBIENTAL PARA LA BOGOTÁ DEL SIGLO XXI.

6.2 Alineación Estratégica

A continuación, se relacionan la visión de TI, misión de TI y objetivos estratégicos de TI de la Gerencia de Tecnología alineada con la nueva planeación estratégica de la Unidad Administrativa Especial de Catastro Distrital orientada a generar valor y a contribuir al logro de los objetivos estratégicos incluyendo el reto de Catastro Multipropósito y la transformación digital de la entidad.

MISIÓN UAECD	MISIÓN TI – GERENCIA DE TECNOLOGÍA
La UAECD aporta al mejoramiento de la calidad de vida de los ciudadanos, la toma de decisiones de política pública, la reducción de la inequidad y la focalización de la inversión, gestionando información georreferenciada, integral e interoperable, haciendo uso de tecnologías de punta, aplicando un modelo innovador con participación ciudadana en los procesos de formación, actualización, conservación y difusión de la información con enfoque multipropósito en calidad de gestor y operador catastral en el territorio nacional	Gestionar eficientemente los servicios y recursos de Tecnologías de la Información y las Comunicaciones con capacidades innovadoras para acelerar la transformación digital como estrategia de cumplimiento de las metas y objetivos misionales de la UAECD para la operación y gestión de catastro multipropósito en el territorio nacional, preservando la historia predial de Bogotá y construyendo la propia para los territorios

VISIÓN UAECD	VISIÓN TI – GERENCIA DE TECNOLOGÍA
La UAECD en 2030 será referente latinoamericano y socio estratégico de las entidades nacionales y territoriales en la gestión y operación catastral multipropósito, con capacidad innovadora, experto talento humano, apropiación de tecnología y altos estándares de calidad, que consolide la Bogotá-Región inteligente y contribuya a la modernización del País en materia catastral	La Gerencia de Tecnología en el 2030 será un referente nacional e internacional en la implementación estratégica de la transformación digital de los procesos asociados a la gestión y operación de catastro multipropósito orientados a facilitar el acceso a la información al ciudadano, mediante el uso y apropiación de nuevas tecnologías

6.3 Objetivos estratégicos

UAECD	GERENCIA DE TECNOLOGÍA
Empoderar nuestro talento humano con competencias desde el ser, el saber y el hacer y fortalecer la participación activa de la ciudadanía en la gestión catastral con enfoque multipropósito.	Promover el uso y apropiación de las nuevas tecnologías de la Información y la cultura digital para la operación y gestión de catastro multipropósito a los funcionarios de la UAECD, clientes y ciudadanos en el territorio nacional
Garantizar la integralidad, interoperabilidad y difusión de la información catastral y geográfica con enfoque multipropósito en el marco de una ciudad-región inteligente como gestor y operador catastral en el territorio nacional.	Fortalecer la gobernabilidad y gestión de TI adoptando el marco de arquitectura empresarial para mantener la interoperabilidad, seguridad de la información, continuidad del negocio y gestión de datos que soporten y aseguren la prestación de trámites y servicios catastrales en línea en Bogotá y los territorios

Liderar la Infraestructura de Datos Espaciales y robustecer los modelos, metodologías y tecnologías con innovación y calidad en la gestión y operación catastral	Innovar mediante el uso y apropiación de tecnologías emergentes para optimizar y automatizar procesos en la operación y gestión catastral de la UAECD, con trámites y servicios digitales en línea a disposición de los ciudadanos
	Materializar las iniciativas y la visión estratégica de la UAECD a través de procesos de transformación digital, aplicando el modelo LADM-COL y fortaleciendo la participación ciudadana
Garantizar la sostenibilidad financiera y administrativa de la entidad para prestar el servicio público catastral, incorporando el fortalecimiento de la gestión comercial territorial.	Dotar a la UAECD de una arquitectura tecnológica flexible, que permita adaptarse oportunamente a las necesidades y cambios de la UAECD en la prestación eficaz del servicio de catastro multipropósito

6.4 Necesidades y oportunidades de TI -

En el actual repositorio de Arquitectura Empresarial se han modelado las primeras versiones del Modelo de Motivación del Negocio y del mapa de capacidades.

Modelo de motivación del negocio:

Este modelo describe la forma en que la misión y la visión se interrelacionan con los objetivos estratégicos, y su articulación con los procesos y la tecnología

.

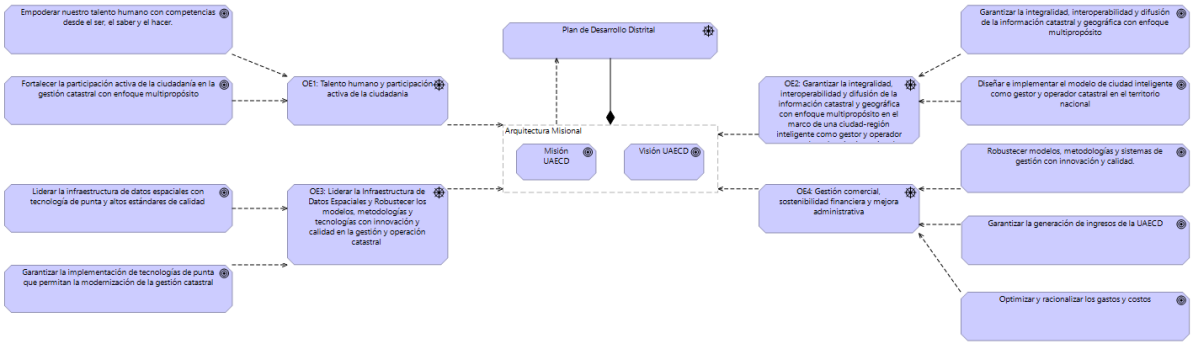


Ilustración 2. Modelo de Motivación del Negocio

Mapa de capacidades:

Representa una visión de alto nivel de la entidad y la forma en que se alinea la estrategia de negocio con la estrategia de TI, enfocado a Go Catastral

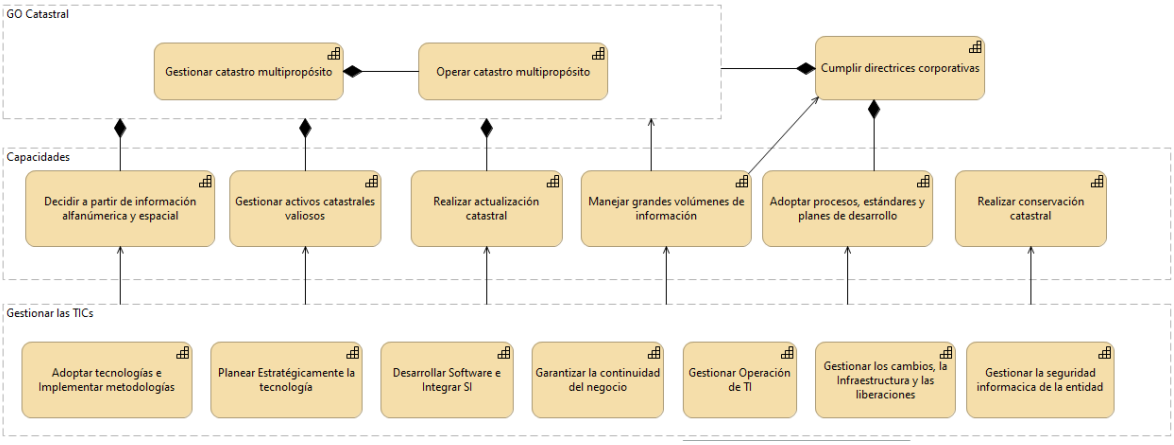


Ilustración 3. Modelo de Capacidades de Negocio

Los dos artefactos se construyeron en Archimate tomando como insumo el plan estratégico 2030 de la UAECD.

En el 2022, se formuló el plan de transformación digital enfocado a los procesos de Catastro Multipropósito Territorial, teniendo en cuenta los lineamientos de MinTIC del marco de referencia de transformación digital del estado colombiano y alineado con la misión TI, visión TI y objetivos estratégicos de TI de la estrategia de TI.

6.5 Portafolio de Servicios de TI

La Gerencia de Tecnología en el 2022 actualizó el portafolio de servicios de TI teniendo en cuenta cada uno de los dominios de gestión gobierno de TI según los lineamientos de MinTIC, que se encuentra en el siguiente enlace:

Portafolio de Servicios de TI (sharepoint.com)

A partir del nuevo portafolio de servicios de TI actualizado, se actualizó el Catálogo de Servicios de TI que se está integrando y actualizando en la mesa de servicios de TI administrada por la Gerencia de Tecnología, que se encuentra en el siguiente enlace:

Portafolio de Servicios de TI (sharepoint.com)

El documento técnico del Catálogo de Servicios de TI formalizado y que hace parte del Sistema de Gestión de Calidad de Catastro se encuentra publicado en:

Portafolio de Servicios de TI (sharepoint.com)

7 SITUACIÓN ACTUAL

Para el análisis y descripción de la situación actual de la Gestión de TI de la Unidad Administrativa Especial de Catastro Distrital se tomó como base el Modelo de Gestión y Gobierno de TI del Marco de Referencia de Arquitectura de la Política de Gobierno Digital, que permite generar las capacidades institucionales de TI que se requieren para prestar servicios de TI a los usuarios de cada entidad mediante el uso adecuado de las tecnologías de la información y las comunicaciones.

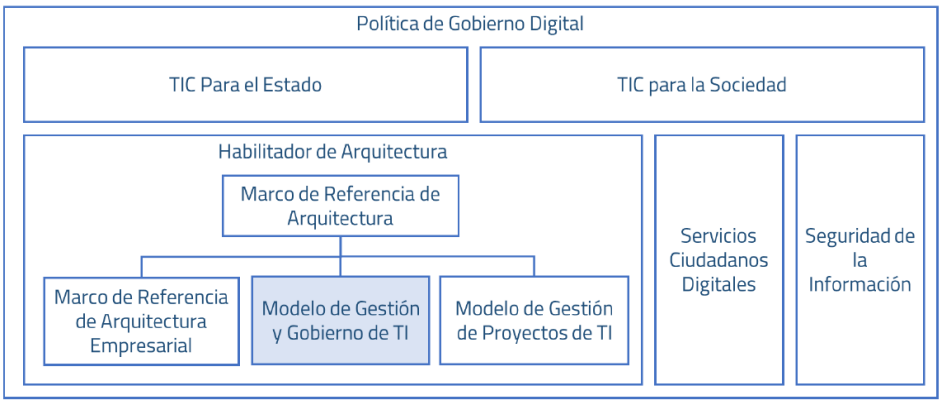


Ilustración 4. Modelo de Gestión y Gobierno de TI del Marco de Referencia de Arquitectura

El Modelo de Gestión y Gobierno de TI define principios que deben ser tenidos en cuenta para gestionar y gobernar las tecnologías de la información y las comunicaciones a nivel institucional, territorial y, sectorial y está compuesto por los siguientes seis (6) dominios que permiten alinear las necesidades del negocio mediante el uso adecuado de las TIC, los cuales son las dimensiones que agrupan y organizan los lineamientos del Modelo.

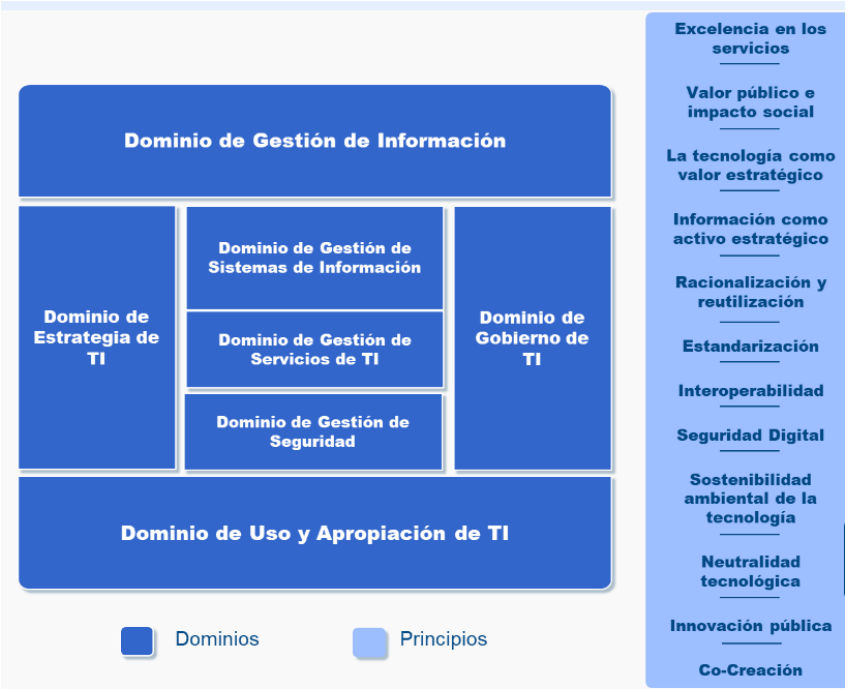


Ilustración 5. Dominios del Modelo de Gestión y Gobierno de TI

El análisis y levantamiento de información de la situación actual de la gestión de TI se efectúo a partir de cada uno de los dominios.

Los resultados del FURAG (Formulario Único de Reporte y Avance de la Gestión) vigencia de 2022 de la Política de Gobierno Digital, publicados por el Departamento Administrativo de la Función Pública, es de 80**,1%**, discriminado de la siguiente manera:

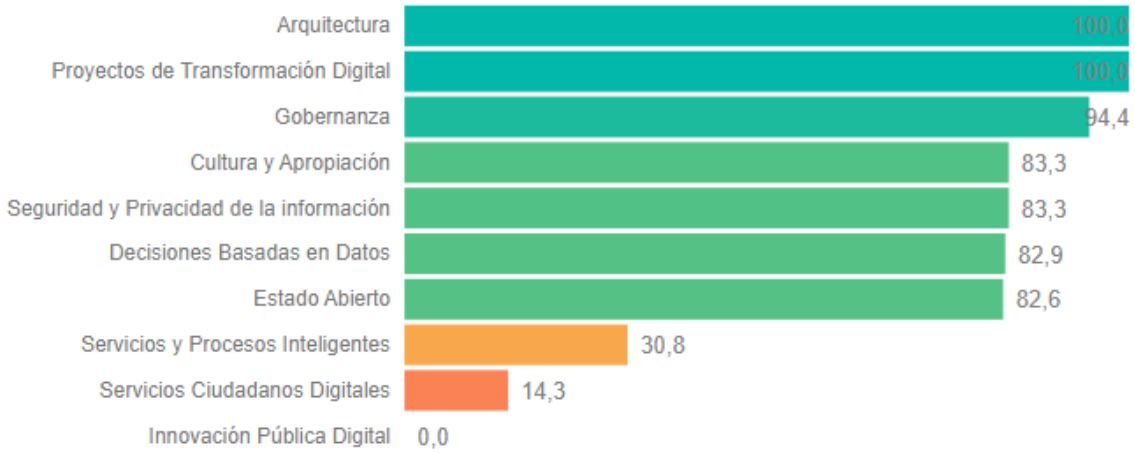


Ilustración 6. Resultados FURAG 2022 Política de Gobierno Digital

A continuación, se describen para cada uno de los dominios del Modelo de Gestión y Gobierno de TI el Marco de Referencia de Arquitectura Empresarial, la situación actual de la gestión de TI de la Unidad Administrativa Especial de Catastro Distrital.

7.1 ESTRATEGIA DE TI

A continuación, se describe la situación actual del dominio de estrategia de TI en cuanto a la planeación estratégica de TI en la Unidad Administrativa Especial de Catastro Distrital teniendo en cuenta los avances del 2023:

- Al inicio de la vigencia se realizó la planeación detallada de los siete (7) proyectos del portafolio del Plan Estratégico de Tecnologías de la Información – PETI de la UAECD para el 2023 y se realizó seguimiento y actualización, dando cumplimiento a lo planeado según los recursos que se dispusieron.

- Se elaboró y ejecutó plan unificado de comunicaciones de la gerencia de tecnología, el cual se socializó a través del Sitio de la Gerencia de Tecnología, correo electrónico y la red Yammer de la GT.
- Se realizó diseño e implementación de una nueva versión del Sitio de Gerencia que incluye tres pilares estratégicos (Organización, Proyectos y Datos e Indicadores) y en este último capítulo se muestra la "Gerencia en Cifras" con mejoras en la representación gráfica y cuantitativa de la gestión institucional.
- Se ajustaron los tableros de control de indicadores publicados en sitio de la Gerencia de Tecnología para el PETI, Plan de Acción Institucional (PAI) y Mesa de Servicios TI y se realizó diseño, implementación y puesta en producción del tablero de control de Contratación
- Se realizó la validación del inventario de Políticas de TI existentes y se inició la construcción de un documento consolidado de Políticas de TI de la Unidad.
- Se ejecutó el Plan de transformación digital y se actualizó para la vigencia 2024 enfocado a los procesos/procedimientos de Catastro Multipropósito que se intervendrán.
- Se modelaron los procesos/procedimientos de actualización y conservación catastral de GO CATASTRAL, usando la herramienta ARCHIMATE.

La información completa de lo anteriormente relacionado se encuentra en el sitio de la gerencia de tecnología Gerencia de Tecnología - Inicio (sharepoint.com) y en la herramienta ARCHIMATE.

7.2 GOBIERNO DE TI

En esta vigencia los avances principales de este dominio son:

- Se avanzó en la optimización de la gestión de accesos, en este sentido se automatizó la validación y creación de usuarios en el aplicativo SI-CAPITAL, se realizó la elaboración y entrega de documento para la creación de usuarios en DA y la respectiva Capacitación a funcionarios de mesa Nivel 1, elaboración de Manual de usuario para la gestión de acceso al aplicativo SIIC. Las estadísticas del mes de mayo arrojaron reducción de tiempo promedio en creación de usuario (83 a 19 horas). Estas tareas de optimización se realizaron con el fin de reducir los tiempos de respuesta en la gestión de usuarios, los retrasos que se puedan presentar en las épocas de mayor demanda y la acumulación de usuarios con permisos excesivos.
- Se realizaron campañas de divulgación del sitio de la Gerencia de Tecnología, el cual a la fecha ha tenido más de 83.000 visitas. De 69 personas encuestadas el 58% de conocen el sitio y de las personas que ingresaron casi la totalidad encontró lo que buscaba y lo recomendaría a compañeros de trabajo.

- Se elaboró una matriz de presupuesto estimado de las implementaciones de Catastro Multipropósito como fuente para el análisis de costo-beneficio de la infraestructura tecnológica de la UAECD.

A continuación, se describe la situación actual del dominio de Gobierno de TI que permite direccionar la toma de decisiones para gestionar las tecnologías de la información en la Unidad Administrativa Especial de Catastro Distrital.

7.2.1 Procesos de Gestión de TI

La Gerencia de Tecnología bajo su gobierno tiene el proceso misional "Gestión y desarrollo de las TICS"

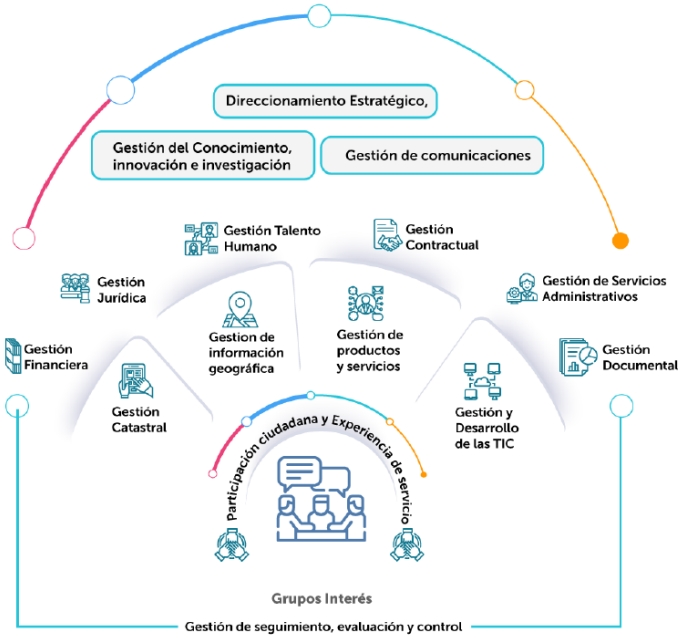


Ilustración 7. Cadena de Valor UAECD 2022

El objetivo del proceso es generar, desarrollar e implementar proyectos estratégicos de Tecnologías de la Información y las Comunicaciones, así como gestionar eficientemente el catálogo de servicios de TI y los recursos tecnológicos, fomentando su uso y apropiación, dinamizando la transformación digital de la UAECD, bajo los estándares de seguridad y privacidad de la información y continuidad del negocio.

El proceso inicia con la formulación de la planeación estratégica de TI, continua con la recepción y atención de requerimientos de usuarios para desarrollar las actividades estratégicas definidas, y finaliza con el seguimiento y mejora a los planes establecidos.

Los procedimientos del proceso son:

1. Procedimiento de Planeación Estratégica de TI:
2. Procedimiento de Gestión Mesa de Servicios
3. Procedimiento de Gestión de Desarrollo de Sistemas de Información
4. Procedimiento de Gestión de Infraestructura
5. Procedimiento de Cambios y Liberaciones
6. Procedimiento de Gestión de Seguridad y Privacidad de La Información
7. Procedimiento Implementación Continuidad del Negocio

7.2.2 Estructura Organizacional de TI

La Gerencia de Tecnología, de acuerdo con el organigrama institucional, es una de las gerencias que depende directamente de la dirección de la UAECD, como se muestra a continuación en el organigrama de la UAECD.

Ilustración 8. Ubicación Gerencia de Tecnología en estructura organizacional UAECD

La estructura organizacional de la Gerencia de Tecnología de la UAECD, está constituida por dos subgerencias: Subgerencia de ingeniería de Software y Subgerencia de Infraestructura Tecnológica, de acuerdo con la resolución Nº 1075 del 10 de noviembre del 2021 – "*Por el cual se modifica el Manual Especifico de Funciones y de Competencias Laborales de los empleos de la planta de personal de la Unidad Administrativa Especial de Catastro Distrital*", el cual se encuentra publicado en el portal web de la entidad.

En este sentido dicha resolución define el siguiente propósito principal de la Gerencia de Tecnología: "*Establecer y gestionar las metodologías, políticas, planes y estrategias para la implementación de los procesos, servicios, gobernabilidad y la gestión de tecnologías de la información con calidad y oportunidad alineados a los objetivos estratégicos de la Unidad y liderar la implementación de la Política de Gobierno Digital vigente, según los estándares definidos*".

Funcionalmente, la gerencia de Tecnología está conformada de la siguiente manera:

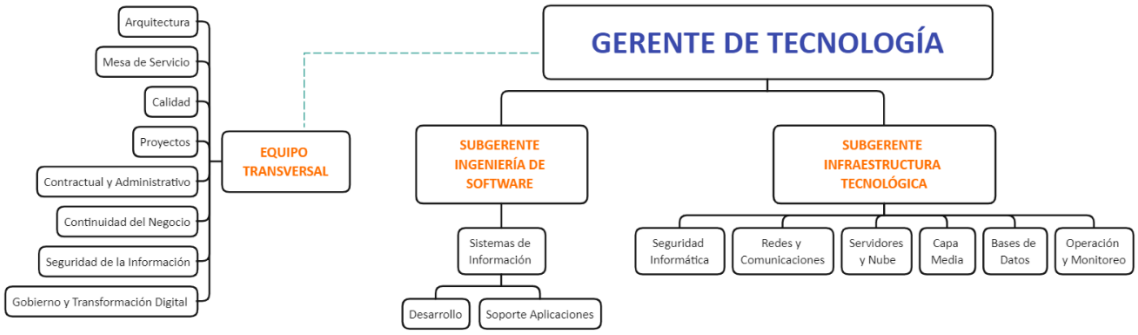


Ilustración 98. Organización Funcional Gerencia de Tecnología

El detalle de los equipos de la Gerencia de Tecnología se encuentra en el sitio de la Gerencia de Tecnología en el siguiente enlace:

Nuestro equipo (sharepoint.com)

7.2.3 Esquema de Gobierno de TI

El esquema de gobierno de TI de la Gerencia de Tecnología, alineado con la estrategia misional y el Modelo Integrado de Planeación y Gestión – MIPG, se realiza a través de la gestión por procesos de TI (ver numeral 6.2.1) y de acuerdo con la estructura organizacional (ver numeral 6.2.2).

Adicionalmente. en el 2022 se definieron las siguientes nuevas políticas con el fin de establecer los lineamientos y los límites necesarios para contar con un marco de gobernabilidad de las tecnologías de información, en el que los usuarios, desarrolladores y gerentes públicos tengan certeza de que cuentan con la tecnología de información, dispuesta según ciertos niveles de disponibilidad y desempeño, y la manera como pueden acceder e interactuar con ella, es definitivo para que la tecnología de información se convierta en un aliado del fortalecimiento institucional:

- Política de continuidad del negocio
- Políticas de gestión de recursos y servicios tecnológicos
- Políticas de gestión de software
- Política de gestión de proyectos con TI

7.2.4 Indicadores de gestión de TI

Dentro del marco normativo existente en materia de indicadores se destacan: Decreto 1499 de 2017 Por medio de la 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.

Los Indicadores son mecanismos que permiten controlar el comportamiento de factores críticos en la ejecución de los planes, programas, proyectos y de los procesos de la entidad.

Con el fin de realizar control y seguimiento a la gestión de TI, la Gerencia de Tecnología tiene incorporados en su proceso, los siguientes indicadores estratégicos y de gestión:

INDICADOR	TIPO	OBJETIVO	PERIODICIDAD
NIVEL DE DISPONIBILIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIDAD	Estratégico	Busca medir el nivel de disponibilidad de la infraestructura tecnológica de la Unidad, frente a la disponibilidad ofrecida en horas	Mensual
ÓRDENES DE CAMBIO GESTIONADAS OPORTUNAMENTE	Estratégico	Busca medir los requerimientos de sistemas de información viabilizados y gestionados oportunamente (en los tiempos ofrecidos)	Mensual
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CUMPLIDO	Estratégico	Realizar seguimiento al avance en la ejecución del plan de seguridad y privacidad de la información de la vigencia, de acuerdo a la programación establecida.	Mensual
PLAN DE CONTINUIDAD DEL NEGOCIO IMPLEMENTADO	Estratégico	Realizar el seguimiento al cumplimiento de las actividades propuestas para el plan del Plan de Continuidad de la UAECD	Mensual

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN - PETI IMPLEMENTADO	Estratégico	Realizar el seguimiento al cumplimiento de las actividades propuestas para el cumplimiento del plan estratégico de tecnologías de la información PETI	Mensual
NIVEL DE SATISFACCIÓN DE LOS USUARIOS EN RELACIÓN CON LA PRESTACIÓN DE SERVICIOS DE TI	Gestión del Proceso	Busca medir el nivel de satisfacción de los usuarios internos, por medio de la aplicación de encuestas de satisfacción del aplicativo de Mesa de Servicios	Trimestral
NIVEL DE EFECTIVIDAD DE LA PRESTACIÓN DEL SERVICIO DE TI	Gestión del Proceso	Medir el nivel de efectividad en la prestación del servicio percibida por el usuario interno de la Unidad, teniendo en cuenta el número de las solicitudes cerradas contra las solicitudes con transición de servicio a no conforme justificadas.	Trimestral
NIVEL DE OPORTUNIDAD EN LA SOLUCIÓN DE SOLICITUDES DE LOS SERVICIOS DE TI	Gestión del Proceso	Busca medir el porcentaje de solicitudes resueltas con oportunidad, respecto del total de las solicitudes solucionadas	Trimestral
INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE IMPIDEN LA PRESTACIÓN DE SERVICIOS DE TI	Gestión del Proceso	Busca determinar el número de eventos e incidentes de seguridad de la información que impiden la prestación de alguno de los servicios de TI , con el fin de disminuir los incidentes que generan afectación.	Trimestral
NIVEL DE CONOCIMIENTO EN SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD	Gestión del Proceso	Busca medir el nivel de conocimiento de seguridad de la información, mediante la aplicación de una encuesta realizada luego de la socialización de la información.	Semestral

Los indicadores de gestión pueden ser consultados en el aplicativo Pandora: https://pandora.idartes.gov.co/catastro/modadministrador/public/login

7.2.5 Matriz riesgos de TI

La Gerencia de Tecnología dispone de una matriz de riesgos de gestión y corrupción para identificar y gestionar las principales categorías y eventos de riesgos institucionales relacionados con las TIC en la Unidad Administrativa Especial de Catastro Distrital. Se encuentra publicada como anexo en la caracterización del proceso.

MATRIZ DE RIESGOS DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN	
Vigencia	2023
Versión	1
Descripción del cambio	Actualización por cambio en la cadena de valor y ajustes en la metodología de riesgos.

PROCESO	OBJETIVO ESTRATÉGICO	OBJETIVO DEL PROCESO	IDENTIFICACIÓN DEL RIESGO										Indicador clave asoci
			CÓDIGO RG -Gestión o RS - Seguridad + Nomenclatura del proceso + consecutivo Ej. RG-DIE-1 RS-DIE-2			Producto asociado / Activo de información	Tipo de riesgo (Solo para activos de información)	DESCRIPCIÓN DEL RIESGO -IR A LA HOJA ÁRBOL - Riesgos de Gestión: Posibilidad de afectación (qué)...por...(cómo)...debido a (por qué)" Riesgos de Seguridad de la información: Pérdida de disponibilidad/confidencialidad/integridad por (Amenaza) debido a la (Vulnerabilidad)	Asociado directamente al Objetivo Estratégico	Causas (Solo para riesgos de gestión)	Vulnerabilidades (Solo para activos de información)	Amenazas (Solo para activos de información)	Indicador clave -Solo RG-
										recuperación. * Falta de presupuesto o insuficiente presupuesto, fluctuación del dólar, no disponibilidad de equipos de infraestructura por parte de los proveedores			
			RG	GDT	5	Sistema Gestión de Seguridad de la Información implementado		**Posibilidad de afectación Reputacional por *Afectación en la prestación de los servicios tecnológicos *., debido a Pérdida, fuga o alteración de información de la UAECD**	NO	*Obsolescencia tecnológica y vulnerabilidades no solucionadas, accesos no autorizados *Falta de adopción de las políticas de Seguridad y Privacidad de la Información en sensibilización en temas de seguridad y privacidad de la información a los usuarios * Inadecuada gestión de copias de seguridad y deficiencias en almacenamiento de información			**Incidentes de Seguridad de la Información que Impiden la Prestación de Servicios de TI:** (Número total de eventos e incidentes de seguridad de la información que impidieron la prestación de servicios TI (de acuerdo con Instructivo de Gestión de Incidentes de Seguridad de la Información) cerrados en la vigencia / Número total de eventos e incidentes de seguridad de la información en el período
			RG	GDT	6	Atención a requerimientos		**Posibilidad de afectación Reputacional por *Insatisfacción de los usuarios *Afectación en la prestación de los servicios tecnológicos, debido a Incumplimiento de los Acuerdos de Servicio y la calidad de la atención**	NO	*Insuficiente personal para atender las solicitudes e incidentes *Desconocimiento por parte de los funcionarios acerca del funcionamiento de la mesa de servicio de TI *Fallas en la capacitación para el personal que brinda el servicio (primer y segundo nivel)			**Nivel de Oportunidad en la Solución de Solicitudes de los Servicios de TI:** (Número de solicitudes resueltas en los tiempos parametrizados en la mesa de servicios de TI / Número de solicitudes resueltas) * 100

Ilustración 109. Matriz de Riesgos

UAECD Catastro Bogotá

CONTEXTO INSUMO PARA LA MATRIZ DE RIESGOS

IDENTIFICACIÓN DEL CONTEXTO	
Identifique factores **(negativos)** o **(positivos)** que afectan al proceso	
CONTEXTO EXTERNO	
Factores del contexto	
A - AMENAZAS (factores negativos externos)	**O - OPORTUNIDADES (factores positivos externos)**
Identifique factores que representen una amenaza o una oportunidad en ejes como el: Económico, social y cultural, tecnológico, político, legales y reglamentarios, medio ambientales y de comunicación externa.	
1. ECONÓMICOS	
Incrementos significativos en el valor del dólar, que afecten la adquisición de tecnología y servicios.	
Afectación de las finanzas distritales asociado a la coyuntura del COVID-19 que afecte los recursos destinados a las entidades (presupuesto).	
2. SOCIALES Y CULTURALES	
El nivel salarial en relación al mercado privado que genere Rotación del personal por mejores ofertas en el mercado.	Posibilidad de implementar buenas prácticas, metodologías de otros catastros u otros referentes o ideas y tendencias innovadoras.
Rotación de personal asociada a la ejecución de directices de ingreso a carrera administrativa.	Aprovechamiento de capacitaciones en temas que fortalezcan la gestión catastral y nuevas tendencias como Big data, analítica de datos, gestión de riesgos, gestión de continuidad del negocio, entre otros.
Paro de trabajadores que afecte la operación.	
Motines, saboteo o bloqueo del Supercade del CAD.	
La coyuntura del COVID 19, que afecta la forma como se ejecutan actividades en sitio; así como podría generar afectación a la salud de los funcionarios.	
3. TECNOLÓGICOS	
Ataques cibernéticos.	Oferta de herramientas tecnológicas para la gestión disponibles en el mercado.
Daños y falta de mantenimiento en las subestaciones del CAD.	La mejora tecnológica o desarrollos de otras entidades que puedan ser aplicables a la entidad.
Incidentes en el DATACENTER de la SDH.	Posibilidad de generar o extender convenios de interoperabilidad.
Incumplimiento en la ejecución de contratos por parte de los proveedores de servicios tecnológicos.	Asistencia, acompañamiento o capacitación por parte de MINTIC, Universidades e instituciones especializadas (temas como uso y apropiación de las TICs).
Uso indebido de los privilegios otorgados a los administradores de las plataformas tecnológicas.	Posibilidad de realizar benchmarking con entidades destacadas en temas TICs.
Cambios tecnológicos transversales determinados por la administración distrital que afecten la gestión de las entidades distritales.	Posibilidad de aplicación de analítica con estrategias de BIG DATA, Machine Learning, Inteligencia artificial.
Caída de servicios que afecten la gestión de sistemas internos o de relacionamiento con el ciudadano.	

Contexto | MR_Gestion_Seguridad | Árbol_G | MR_Corrup1 | MR_Corrup2 | MR_Corrup3 | Act_Crit | Amenazas_SI | Vulnerabilidades_SI | Controles_ISO2

Ilustración 11. Contexto Insumo Matriz de Riesgo

La matriz incluye:

- Información de contexto interno y externo (análisis DOFA)
- Identificación de los riesgos (se tiene en cuenta el contexto estratégico en que opera la entidad, los objetivos y alcance de los procesos y los factores internos y externos del proceso).
- Valoración de los riesgos (establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial o inherente).
- Controles (medida que permite reducir o mitigar el riesgo).
- Plan de tratamiento de riesgos (decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser reducir, aceptar o evitar. Se analiza frente al riesgo residual).
- Seguimiento al plan de tratamiento de riesgos (El monitoreo y revisión de la gestión de riesgos, está alineada con la dimensión 7 de MIPG de Control Interno, que se desarrolla con

el MECI a través de un esquema de asignación de responsabilidades y roles, el cual parte del Esquema de líneas de defensa).

- Probabilidad de ocurrencia del riesgo (Para los riesgos de gestión y seguridad de información, la probabilidad es la posibilidad de ocurrencia del riesgo y está asociada a la exposición al riesgo, del proceso o actividad que se está analizando. La probabilidad está dada al evaluar con qué frecuencia se realiza la actividad que conlleva el riesgo por año, es decir, con base en el producto/activo seleccionado identificar con qué frecuencia se genera).
- Análisis de impacto (Para los riesgos de gestión y seguridad de la información, las variables principales de análisis son los impactos económicos y reputacionales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles, se toma el nivel más alto).

Adicionalmente, se dispone de la Matriz de Riesgo de Seguridad Digital del Proceso de Gestión y Desarrollo de las TIC, la cual fue alineada en la metodología de acuerdo con lo definido en la guía emitida por el DAFP Versión 5, se encuentra en la siguiente ruta:

https://catastrobogotacol.sharepoint.com/:x:/r/sites/GerenciaTecnologa-GOBIERNODIGITAL/_layouts/15/Doc.aspx?sourcedoc=%7BFE479E57-AD80-426D-9CA4-C1BA2A579367%7D&file=Matriz_riesgos_2022_GDT_IIITRI.xlsb&action=default&mobileredirect=true

7.2.6 Gestión de Proyectos TI

Con el fin de mejorar la planeación, ejecución y seguimiento a la gestión de proyectos de TI (Tecnologías de la Información) en el 2021 se inició la implementación de la herramienta metodológica de gestión de proyectos de TI, desarrollada de acuerdo con lo establecido en la Política de Gobierno Digital, específicamente lo descrito en Modelo de Gestión de Proyectos TI, de la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el cual hace parte de los lineamientos y documentos puestos a disposición de las entidades públicas del orden nacional, departamental y distrital. Esta metodología se ha estructurado de acuerdo con los dominios y lineamientos establecidos en el modelo gestión de proyectos de TI.

La metodología de gestión de proyectos de TI pone a disposición de la Gerencia de Tecnología las guías y plantillas que permitan estructurar, planear y gestionar los proyectos de TI, de acuerdo con los dominios que constituyen el modelo gestión de proyectos de MinTIC; los dominios son los siguientes:

Ilustración 12. Dominios del modelo de gestión de proyectos de MinTIC[4]

La siguiente tabla contiene el proyecto y la URL de cada uno de los proyectos de TI que se han ejecutado con el fin de cerrar las brechas priorizadas para la presente vigencia en el marco de la ejecución del PETI 2021-2024.

PROYECTO	URL DEL MICROSITIO DE CADA PROYECTO
PR01-Estrategia de Gestión de TI	https://catastrobogotacol.sharepoint.com/sites/PETI-EstrategiaGestionTI-2023
PR02-Modelo de Gobierno de TI	https://catastrobogotacol.sharepoint.com/sites/PETI-ModelodeGobiernodeTI-2023
PR03-Gestión Integral de Riesgo	https://catastrobogotacol.sharepoint.com/sites/PETI-GestionIntegraldeRiesgo-2023
PR04-Gestión de Proyectos de TI	https://catastrobogotacol.sharepoint.com/sites/PETI-GestiondeProyectosdeTI-2023
PR05-Gestión y Gobierno de Datos	https://catastrobogotacol.sharepoint.com/sites/PETI-GestionyGobiernodeDatos-2023
PR06-Arquitectura de Sistemas de Información	https://catastrobogotacol.sharepoint.com/sites/PETI-ArquitecturadeSistemasdeInformacion-2023
PR07-Arquitectura de Infraestructura de TI	https://catastrobogotacol.sharepoint.com/sites/PETI-ArquitecturadeInfraestructuradeTI-2023

En el siguiente enlace del sitio de la Gerencia de Tecnología en SharePoint, se encuentra información adicional de la Gestión de proyectos de TI:

[4] *EL modelo de gestión de proyectos fue actualizado en mayo de 2023 y se puede consultar en la siguiente URL: https://www.mintic.gov.co/arquitecturaempresarial/630/w3-propertyvalue-385301.html?__noredirect=1#data=%7B%22filter%22:%22%22,%22page%22:1%7D*

https://catastrobogotacol.sharepoint.com/sites/TI/SitePages/PETI.aspx

7.3 INFORMACIÓN

A continuación, se describe la situación actual del dominio de Información de TI en cuanto a la gestión del ciclo de vida de los componentes de información de la Unidad Administrativa Especial de Catastro Distrital.

7.3.1 Arquitectura de Información

En el 2023 la Gerencia de Tecnología avanzó en la práctica de la arquitectura empresarial como uno de los habilitadores de la Política de Gobierno Digital y se modelaron en ARCHIMATE los procesos de arquitectura empresarial para los dominios de Arquitectura Institucional, Sistemas de Información, Datos y Tecnología alineados al nuevo marco de arquitectura empresarial de MinTIC:

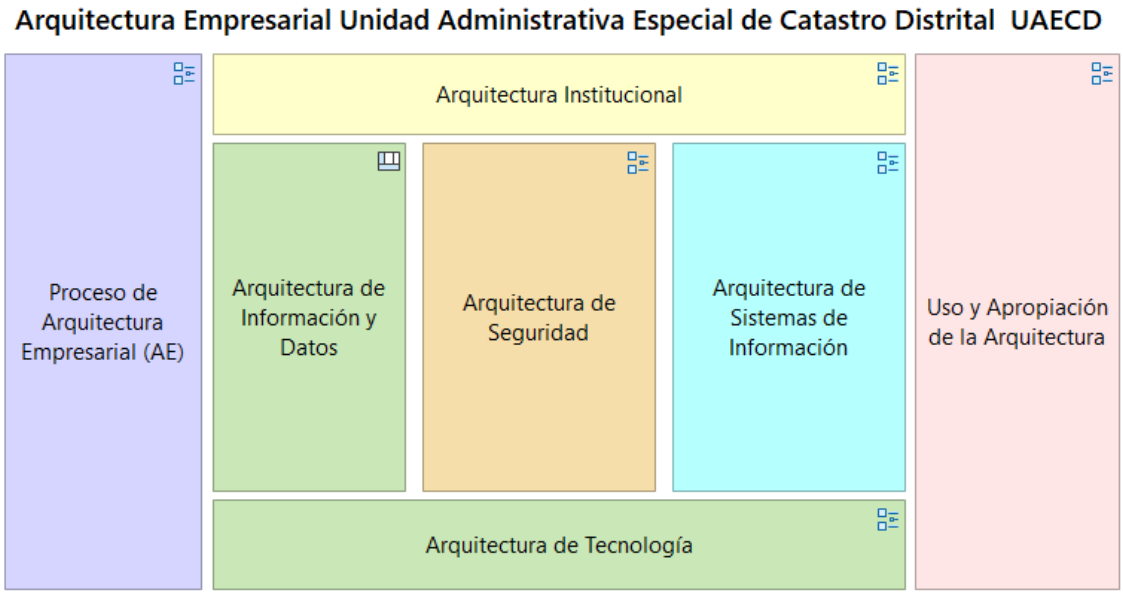


Ilustración 13. Marco de Referencia de Arquitectura Empresarial 3.0

Arquitectura Institucional:

El dominio de arquitectura institucional brinda las herramientas para que la entidad pueda desarrollar una descripción de su Arquitectura Institucional en su situación actual (línea base), que

corresponde a la forma como opera en el presente la entidad y, posteriormente, la descripción de su Arquitectura Institucional objetivo (o situación objetivo), que determina cómo la entidad debe operar para lograr sus objetivos, dando respuesta a las necesidades que la llevaron a desarrollar un ejercicio de Arquitectura Empresarial.

De los procesos de la Cadena de valor se hizo un ejercicio de arquitectura del proceso de "Gestión Catastral alineado al proceso de "Gestión y Desarrollo de las TIC".

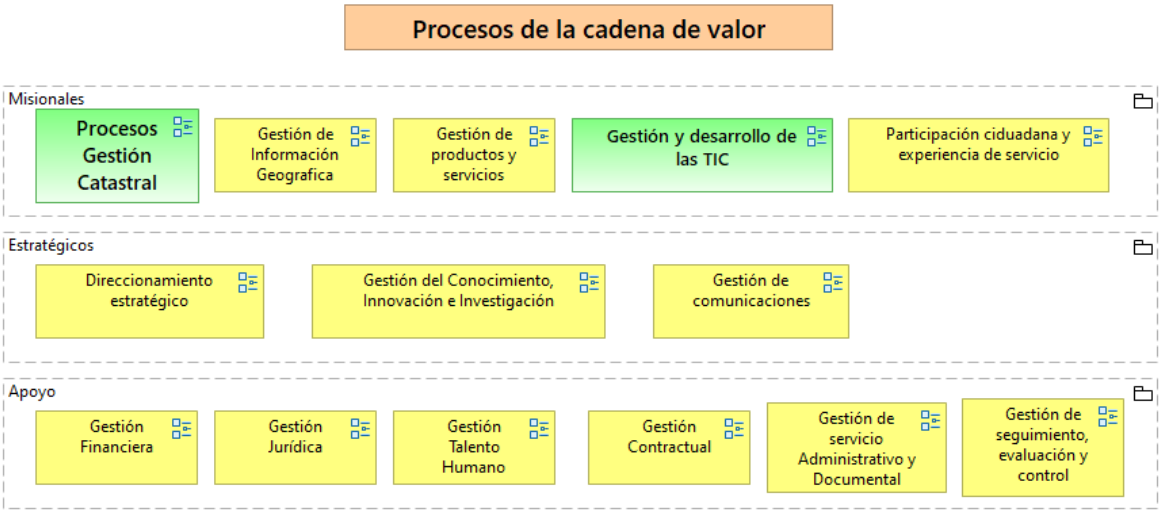


Ilustración 14. Procesos Cadena de Valor UAECD

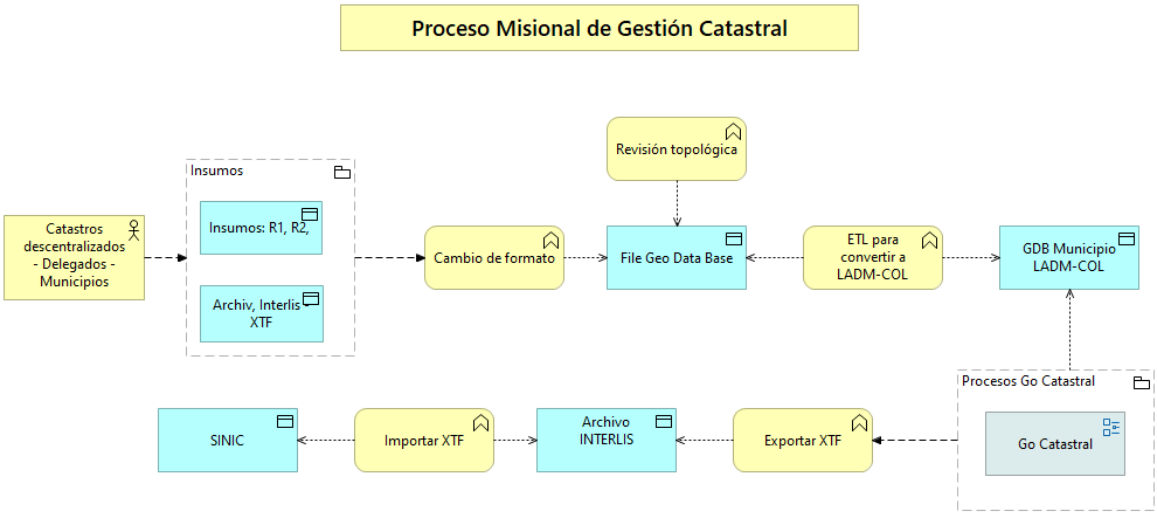


Ilustración 15. Modelado proceso de actualización y conservación catastral

Arquitectura de Sistemas de Información:

El dominio de arquitectura de sistemas de información identifica requerimientos, define patrones y técnicas para diseñar, desarrollar e integrar los componentes de software y las aplicaciones que forman parte de los sistemas de información que habilitan los procesos y servicios de la entidad.

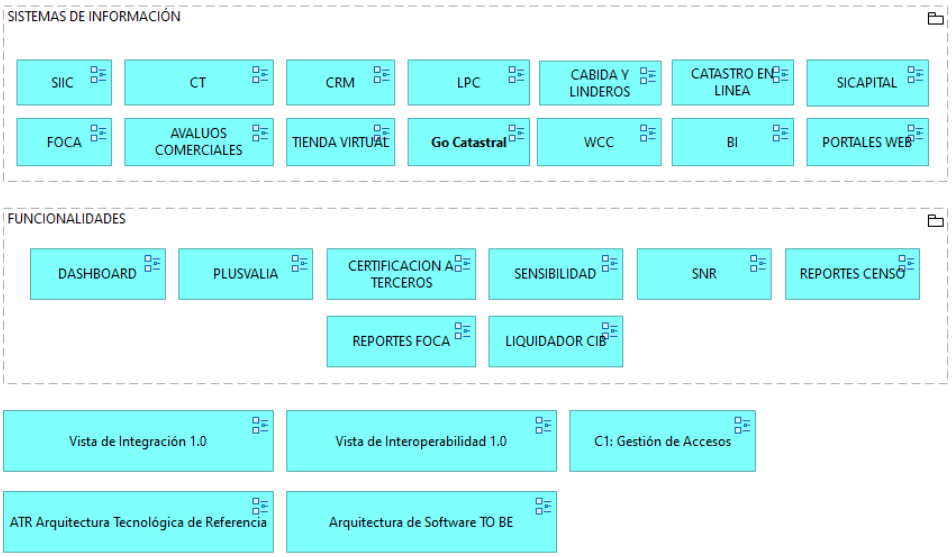


Ilustración 16. Sistemas de Información y Aplicaciones UAECD

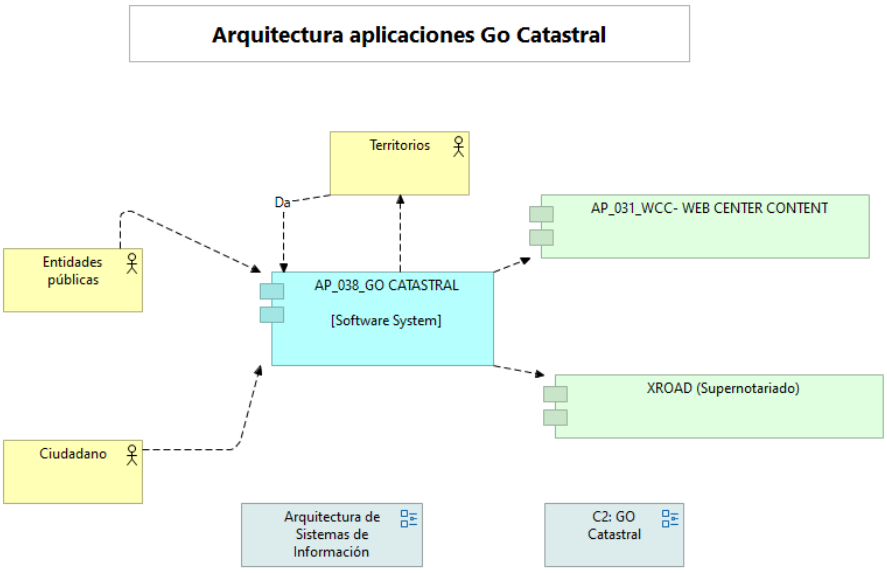


Ilustración 17. Modelado de arquitectura de aplicación Go Catastral

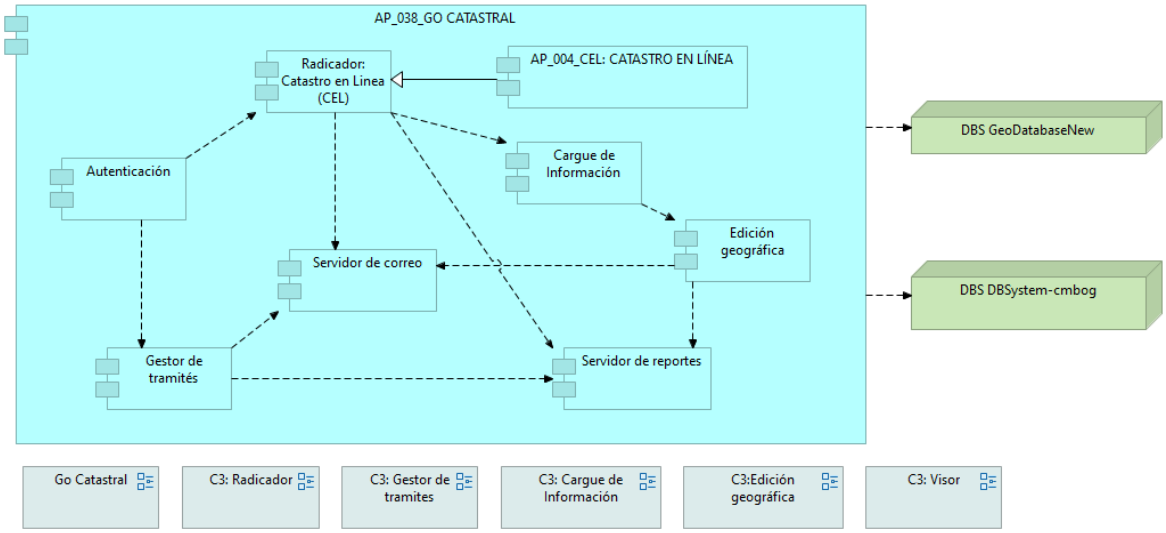


Ilustración 18. Modelado artefactos y relaciones aplicación Go Catastral

Arquitectura de Información y datos:

El dominio de arquitectura de información contiene los elementos para orientar a las entidades en la definición de la arquitectura de información que define la estructura con la cual está representada y almacenada la información y los datos de una organización, lo mismo que los servicios y los flujos de información que soportan los procesos de la entidad de la arquitectura institucional.

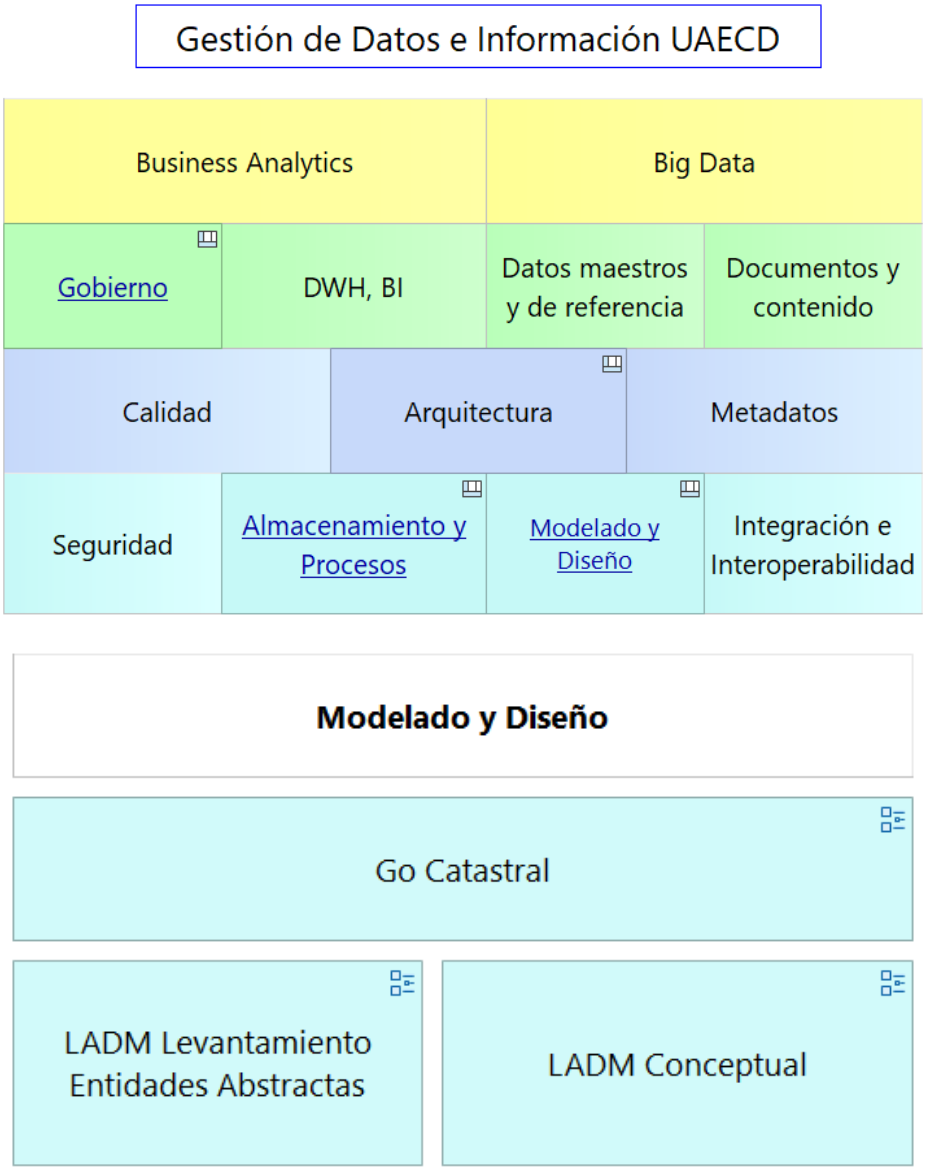


Ilustración 19. Modelado Arquitectura de datos Go Catastral

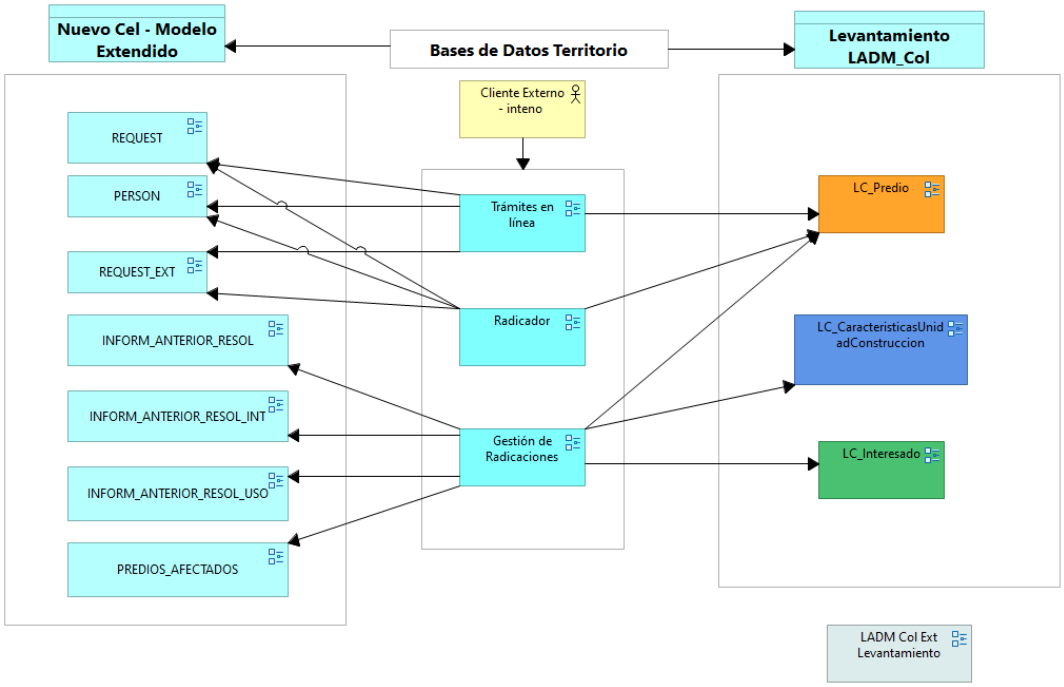


Ilustración 20. Modelado flujo de datos Go Catastral

Todos estos dominios orientados a los procesos de conservación y actualización catastral se articulan desde el dominio de uso y apropiación:

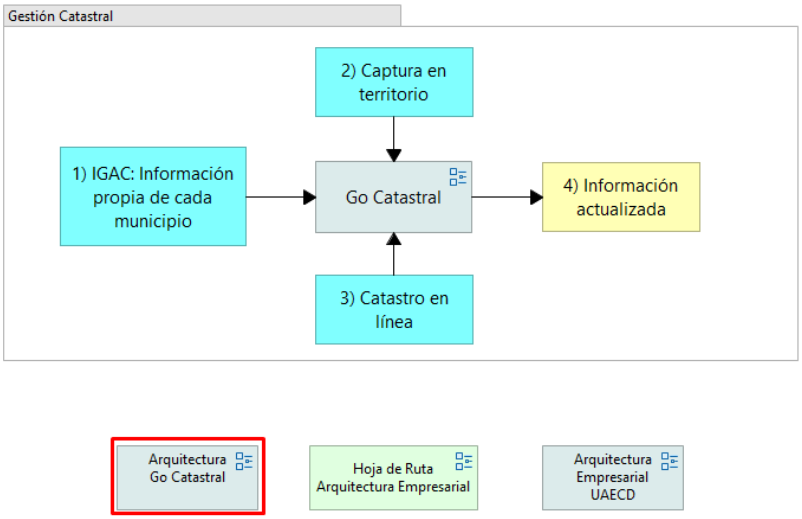


Ilustración 21. Modelado de alto nivel de operación Go Catastral

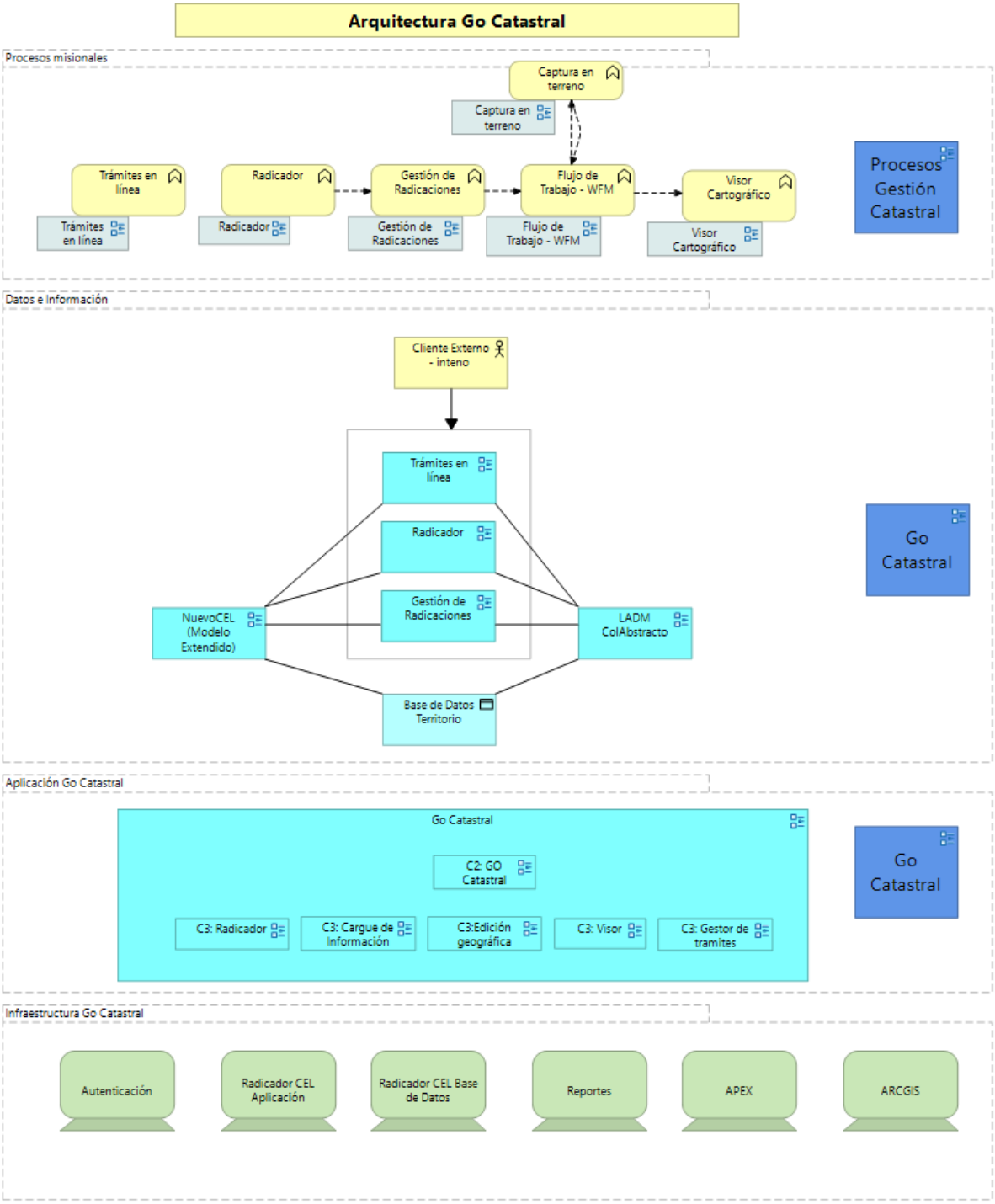


Ilustración 22. Modelado dominio de uso y apropiación Go Catastral

Para la ejecución de este plan se crearon artefactos de diverso tipo: diagramas, catálogos y documentos los cuales se encuentran en dos sitios:

1. El repositorio de Arquitectura Empresarial en Sharepoint: Arquitectura-TI - Inicio (sharepoint.com)

Arquitectura de Datos

2. La herramienta de Arquitectura Empresarial que ha utilizado la entidad en el año 2023: Archi

Sincronizada con GITLAB a través del proyecto con URL:
http://10.35.116.152/arquitecturaempresarial/uaecd2023

7.3.2 Gobierno componentes de información

Desde la Gerencia de tecnología desde el 2021 para fortalecer el gobierno y la gestión de datos se propusieron y socializaron dos modelos, a partir de los lineamientos de la Política de Gobierno Digital:

- Gobierno de datos abiertos de la UAECD
- Gobierno de datos de la UAECD

Estos documentos se encuentran disponibles en la siguiente ubicación:

https://catastrobogotacol.sharepoint.com/:f:/s/GerenciaTecnologa-GOBIERNODIGITAL/EuH4w7iWuKxDtYy80Xvs9vsBBp20VFpGgdrKFomIrZ5uGw?e=NnIYQK

En el 2023 se elaboró un documento que describe el estado de Gobierno de Datos actual en la Gerencia de Tecnología de la UAECD y en particular para los procesos de conservación y actualización catastral, el cual se encuentra en la siguiente ubicación:

As-is Gobierno de Datos Sept 2023.docx

7.3.3 Catálogos de componentes de información

Durante la vigencia 2023, se realizó revisión y actualización del catálogo de componentes de información en los siguientes ítems:

- Inclusión diccionarios de datos Actualización y Conservación Catastral: NuevoCEL y Levantamiento
- Se actualiza la información de los Activos de Información
- Se actualiza el repositorio de datos

El catálogo de componentes de información encuentra ubicado en el siguiente enlace:

Catálogo Componentes Información V6-20231206.xlsx

7.3.4 Servicios intercambio de información

En el Catálogo de Componentes de Información se encuentra relacionado los servicios de intercambio de información de la UAECD.

Durante la vigencia 2022 se realizó la medición del nivel de madurez de interoperabilidad el cual arrojó un puntaje global de 3,8. Siguiendo los lineamientos de MINTIC y con el acompañamiento de su grupo técnico, se evaluaron criterios en los cuatro dominios (organizacional, politico-legal, semántico y técnico, con el siguiente resultado:

Dominio	Resultado 3,875	Lineamiento	Criterio	Nivel	Descripción
Dominio Organizacional	**4**	**LI.IOP.OG.04**	**Liderazgo del Marco de Interoperabilidad**	2	Existen varias personas responsables de los servicios de intercambio de información
		LI.IOP.OG.05	**Cultura organizacional**	1	La entidad no promueve una cultura de intercambio de información mediante comunicaciones internas, campañas o actividades ni capacita al recurso humano en temas de interoperabilidad
		LI.IOP.OG.01 LI.IOP.OG.02 LI.IOP.OG.03	**Adecuación de procesos**	4	La entidad tiene documentados sus procesos y están actualizados y tienen documentadas las necesidades de intercambio de información

Dominio político legal	**4**	**LI.IOP.LG.01 LI.IOP.LG.02**	**Normatividad para el intercambio de información**	4	La entidad intercambia información, cuenta con todos los acuerdos para el intercambio de información con otras entidades y existe normatividad para algunos servicios de intercambio
		LI.IOP.LG.03	**Manejo de la información confidencial y personal**	4	La entidad conoce y aplica la normatividad vigente relacionada con el manejo adecuado de la información confidencia y personal en todos los servicios de intercambio de información.
Dominio semántico	**4,5**	**LI.IOP.SM.01 LI.IOP.SM.04 LI.IOP.SM.06 LI.IOP.SM.03**	**Lenguaje común de intercambio de información**	5	La entidad conoce el lenguaje común de intercambio y lo utiliza en todos los servicios de intercambio de información
		LI.IOP.SM.02 LI.IOP.SM.05	**Documentación de los servicios de intercambio**	4	La entidad cuenta con la documentación de algunos servicios de intercambio de información.
Dominio técnico	**3**	**LI.IOP.TE.01**	**Uso de servicios ciudadanos digitales**	1	La entidad no ha implementado el servicio ciudadano digital de interoperabilidad para el intercambio de información.
		LI.IOP.TE.07	**Diseño funcional de los servicios web**	4	La entidad identificó las necesidades de intercambio de información mediante requerimientos funcionales y la tiene todas las caracterizaciones de los servicios con requerimientos funcionales y no funcionales. La caracterización de algunos de los servicios tienen en cuenta el estándar del lenguaje común de intercambio de información
		LI.IOP.TE.07	**Diseño técnico de los servicios**	3	La entidad tiene documentada parcialmente la información de entrada y de salida de cada uno de sus servicios y se encuentra actualizada. Esta información incluye parcialmente los tipos de dato que se utilizan en los servicios de intercambio de información. La caracterización de sus servicios no incluye los casos de prueba documentados.
		LI.IOP.TE.07	**Pruebas de los servicios web**	3	La entidad ha ejecutado y tiene documentado los resultados de los casos de prueba para los servicios de intercambio de información de los procesos misionales de la entidad.
		LI.IOP.TE.07	**Despliegue de los servicios web**	3	La entidad tiene desplegados algunos de sus servicios en la PDI

		LI.IOP.TE.02	**Infraestructura tecnológica para el intercambio de información**	4	La arquitectura de la infraestructura tecnológica de la entidad ha sido adaptada para las necesidades específicas de intercambio de información, sin embargo, no existe ninguna documentación que soporte las decisiones tomadas.

7.3.5 Calidad de componentes de información

En el 2023, se realizó análisis y diagnóstico de la efectividad de los procesos y procedimientos de calidad de datos que se incluyeron en el documento de As Is de gobierno de datos para revisión por parte de la gerencia, sobre el proceso de actualización y conservación con enfoque multipropósito.

7.4 SISTEMAS DE INFORMACIÓN

A continuación, se describe la situación actual del dominio de Sistema de Información en cuanto a la gestión del ciclo de vida de los sistemas de información de la Unidad Administrativa Especial de Catastro Distrital.

7.4.1 Arquitectura de Sistemas de Información

La Gerencia de Tecnología cuenta con un documento que contiene la Arquitectura Tecnológica de Referencia, que fue actualizada en el 2022 y tiene como función principal la definición de los principios arquitectónicos, las guías estructurales y los lineamientos de desarrollo que deben cumplir los Sistemas de información al interior de la Unidad Administrativa Especial de Catastro Distrital.

La Arquitectura Tecnológica de Referencia - ATR tiene como función principal definir los principios arquitectónicos, las guías estructurales y algunos lineamientos de desarrollo que deben cumplir los Sistemas de Información al interior de la Unidad Administrativa Especial de Catastro Distrital - UAECD. En consecuencia, cuando se defina, diseñe y construyan sistemas de información con base a la arquitectura de referencia se asegura una construcción ordenada, minimizando riesgos, con costos controlados, con un enfoque sobre los principales problemas de negocio a resolver por la UAECD. Donde cada elemento constitutivo del sistema en construcción sea flexible, extensible, adaptable y con una adecuada especialización. Finalmente, la arquitectura se orienta para brindar una adecuada automatización de los procesos de negocio de la UAECD.

Para mayor información sobre la Arquitectura Tecnológica de Referencia se pueden consultar los siguientes documentos en sharepoint en el equipo de Gobierno Digital, canal ATR – arquitectura Tecnológica de Referencia, en el siguiente enlace:

Arquitectura-TI - General - Todos los documentos (sharepoint.com)

- 03 GT_Arquitectura Tecnológica de Referencia_V3.0_2022_documento_base.docx. Este corresponde al documento base de la ATR.
- 04 GT_ATR_V1.0_2022_Implementación de la ATR para Sistemas de Información Ge.docx. Este documento contiene la información del componente geográfico.
- 02 Estrategia de Evolución de la Arquitectura Tecnológica de Referencia.pptx. Este documento corresponde a la evolución que ha tenido la ATR.

Adicionalmente, durante el 2022 se inició la estandarización de la documentación de los sistemas de información, para ello se adoptó el **modelado C4** y los artefactos resultantes hacen parte del repositorio de arquitectura empresarial ARCHI; teniendo en cuenta que el modelado C4 es iterativo e incremental, dentro del ejercicio realizado en el caso de Go Catastral se llegó hasta el nivel C3, por lo tanto, se recomienda que para el 2023 se modele hasta el nivel C4, el cual es el nivel de código. Para poder dar cumplimiento con este objetivo, se debería incluir dentro de los contratos las obligaciones relacionadas con el apoyo al modelamiento de la arquitectura de los Sistemas de Información, hasta llegar al nivel C4.

Para los sistemas de información SIIC, Catastro en línea y Go Catastral el avance logrado correspondió a nivel C3, todos los demás se encuentran pendientes.

A continuación, se presenta un ejemplo de las vistas en el modelado C4:C1: El sistema visto como una caja negra y solo se visualiza las relaciones con el exterior:

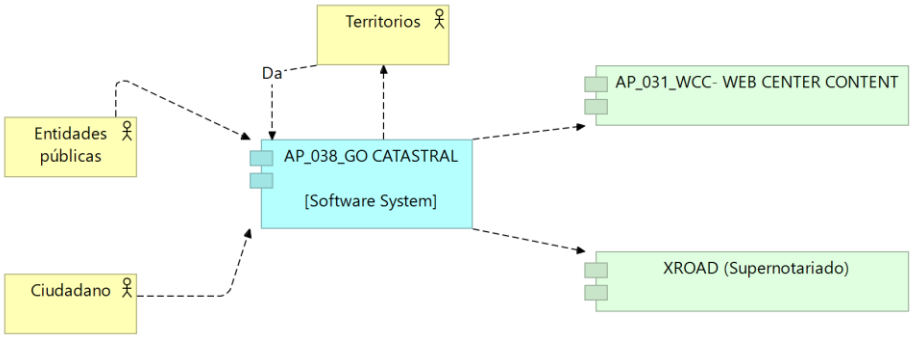


Ilustración 23. Vistas modelado C4 ejemplo

C2: Se pueden visualizar los principales componentes internos

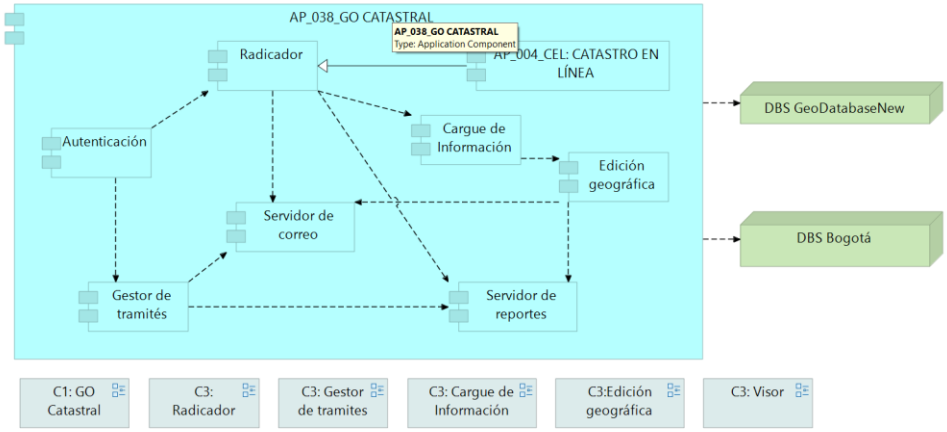


Ilustración 24. Vistas modelado C2 ejemplo

Para este ejemplo desde C2 se puede navegar a diagramas de nivel tres:

- C3: Radicador
- C3: Gestor de tramites
- C3: Cargue de Información
- C3: Edición geográfica
- C3: Visor

Como resultado de las mesas de trabajo realizadas con los equipos de desarrollo de los Sistemas de Información, se documentó la arquitectura, la cual se encuentra ubicada en el siguiente sitio:

https://catastrobogotacol.sharepoint.com/sites/PETI-ArquitecturaSistemasInformacion-2022/Documentos%20compartidos/Forms/AllItems.aspx?id=%2Fsites%2FPETI%2DArquitecturaSistemasInformacion%2D2022%2FDocumentos%20compartidos%2F2%2E%20Ejecuci%C3%B3n%2FArchimate&viewid=54f98e9e%2Dc947%2D45e7%2Daf2b%2Db625cca52665

7.4.2 Catálogo de Sistemas de Información

Actualmente Catastro dispone de un catálogo de sistemas de información actualizado en el 2023; sin embargo, este es un instrumento dinámico que requiere una revisión y actualización de forma periódica. Se definió en Sharepoint en el sitio de la Subgerencia de Ingeniería de Software un repositorio para la consulta y/o modificación del catálogo.

El catálogo de sistemas de información puede ser consultado por todos los funcionarios de la Gerencia de Tecnología y sus subgerencias y por el momento sólo lo pueden editar y/o modificar, los líderes técnicos y el Subgerente de Ingeniería de Software.

7.4.3 Documentación técnica y funcional de los Sistemas de Información

En el 2022, la documentación técnica y funcional bajo el gobierno de la Gerencia de Tecnología se organizó y dispuso en el sitio de la Gerencias de Tecnología en los siguientes enlaces:

- Manuales de Usuario (sharepoint.com)
- Documentación Técnica (sharepoint.com)

Adicionalmente, se implementaron los siguientes documentos:

- La guía de estilo y usabilidad que se puede consultar en: Guía de Estilo y Usabilidad de los Sistemas de Información.docx

- Un documento que contiene los requerimientos para el despliegue de ambientes de desarrollo, este documento se encuentra ubicado en el sitio Sharepoint de la Subgerencia de Ingeniería de Software: Requerimientos para despliegue ambientes de desarrollo.xlsx.

  https://catastrobogotacol.sharepoint.com/:x:/r/sites/SubgerenciaIngenieriaSoftware/Shared%20Documents/General/Sistemas_Informacion/Requerimientos%20para%20despliegue%20ambientes%20desarrollo.xlsx?d=wd22fecc9453043489ea5e01cb65a658e&csf=1&web=1

- Durante la vigencia 2022 se implementó el documento técnico de desarrollo seguro, el cual puede ser consultado en la siguiente ruta: Documento_Tecnico_Desarrollo_Seguro_final.doc

Con relación a la documentación de la instalación de los ambientes de desarrollo de los aplicativos, se logró obtener la documentación de los siguientes aplicativos: Tienda virtual, CEL, FOCA, SiCapital, CT, Go Catastral y LPC. Quedó pendiente la documentación de cabida y linderos.

7.4.4 Ciclo de vida de los Sistemas de Información

Actualmente sobre el ciclo de vida de los sistemas de información:

- Las versiones de los aplicativos misionales de la UAECD se encuentran en versiones de software Oracle que ya no cuentan con soporte por parte del proveedor. Es necesario que Infraestructura actualice las versiones del software base a unas versiones que cuenten con soporte actualizado por parte de Oracle. Posteriormente, por el grupo de ingeniería de software se debe realizar los desarrollos y pruebas necesarias para desplegar los códigos fuentes en estos servidores y asegurar su funcionamiento.

- Los aplicativos de Go Castastral se encuentran licenciados con software Oracle, tales como su base de datos y su generador de reportes usando FORMS and Reports

- En la UAECD se tienen como gestor de documentos dos aplicativos: uno de Oracle que se llama WCC (Web Content Center) e INFODOC.

- Todos los aplicativos administrativos de la UAECD se encuentran desplegados con el software que se heredó de la Secretaría de Hacienda el cual es SICAPITAL

- Para nuevos desarrollos se implementó un procedimiento para realizar pruebas de vulnerabilidad y poder determinar si el software es seguro o tiene fallas de seguridad.

- Para interoperabilidad se está trabajando en conjunto con la Agencia Nacional Digital a través de XROAD con los cuales se tienen dos servicios implementados: Superintendencia de Notariado y Registro y Caja de Vivienda Popular.

7.4.5 Mantenimiento y soporte de los sistemas de información

Para el desarrollo, mantenimiento y soporte de software o de los sistemas de información, la Gerencia de Tecnología cuenta con una metodología, la cual se encuentra plasmada en los siguientes procedimientos que fueron actualizados durante la vigencia 2022 con la nueva cadena de valor de la UAECD: "Desarrollo de Sistemas de Información", "Gestión mesa" y "Cambios y liberaciones" que hacen parte del Sistema de Gestión Integral (SGI) publicado en la Intranet y cuyo objetivo y alcance son:

PROCEDIMIENTO	CÓDIGO	OBJETIVO	ALCANCE
DESARROLLO DE SISTEMAS DE INFORMACIÓN	GDT-PR-06	Desarrollar, poner en producción y realizar mantenimientos a los sistemas de información desarrollados por la Subgerencia de Ingeniería de Software y que soportan la operación de la Unidad.	Inicia con la recepción de un orden de cambio viabilizada y aprobada que involucra un nuevo desarrollo o un mantenimiento a un Sistema de Información existente, y finaliza con la puesta en productivo y el cierre de esta orden de cambio.
GESTIÓN MESA	. GDT-PR-04	Atender las solicitudes (incidentes y requerimientos) registradas a través de la herramienta tecnológica de mesa de servicios de TI, de acuerdo con el catálogo de servicios de TI, cumpliendo con lo establecido en los Acuerdos de Niveles de Servicio.	Inicia con el registro de las solicitudes relacionadas con el catálogo de servicios de TI, y finaliza con alguna de las siguientes actividades: a. La solicitud cerrada. b. La validación de la base de conocimiento y en los casos que se requiera la actualización de la base de conocimiento. c. El seguimiento y análisis de la gestión de solicitudes confirmando la correcta prestación del servicio de TI o la necesidad de registrar un problema en la herramienta tecnológica de mesa de servicios de TI a

			través de la gestión de problemas o el envío de las notificaciones correspondientes al usuario o al analista de la mesa de servicios de TI.
PROCEDIMIENTO CAMBIOS Y LIBERACIONES	GDT-PR-07	Asegurar que los cambios sobre los recursos tecnológicos sean notificados, registrados, evaluados, autorizados, priorizados, planificados, ejecutados, probados, documentados, y dispuestos en producción de manera controlada con el fin de reducir incidentes, interrupciones severas, y reprocesos asociados al cambio, en el marco de las mejores prácticas.	Inicia con la generación en la mesa de servicios de una solicitud de cambio en una aplicación o base de datos o infraestructura, adjuntando a esta los formatos de solicitud de cambio correspondiente en formato Word, Excel o PDF según sea el caso y finaliza con la verificación de la ejecución e impacto del cambio o con el registro de la solicitud para actualización de la base de datos de configuración y/o catálogo de servicios de TI. .

Los procedimientos mencionados contienen los lineamientos relacionados con la realización de las pruebas de usuario y su respectiva aprobación para paso a producción.

Todos los soportes relacionados con los desarrollos implementados quedan registrados en la mesa de servicio de TI y ubicados en la orden de cambio correspondiente: ahí quedan entre otros, la viabilidad, la historia de usuario, los documentos de análisis y diseño y las guías de uso del aplicativo o desarrollo realizado, el guion de pruebas y el acta de paso a producción.

Se cuenta con un soporte técnico a disposición de los usuarios, donde a través de la Mesa de servicio de TI se atienden todas las solicitudes relacionadas con el catálogo de servicios de TI.

La Mesa de Servicios tiene como objetivo proporcionar un canal de comunicación para que los usuarios soliciten y reciban servicios técnicos estandarizados y predefinidos de acuerdo con Catálogo de Servicios de TI.

A través de Mesa de Servicios los usuarios puedan realizar sus solicitudes vía WEB, si por alguna falla técnica, no es posible registrar la solicitud por este medio, el usuario puede realizar el registro vía

correo electrónico, si el correo electrónico igualmente presenta fallas técnicas, la solicitud la puede realizar telefónicamente (extensiones 7777 - 7776 - 7746).

Una vez recibida la solicitud, el Operador de la Mesa de Servicios lo clasifica para ser gestionado de acuerdo con el tipo de solicitud (Incidente o Requerimiento). La Mesa de Servicio proporciona al usuario un mecanismo amigable para realizar y hacer seguimiento a las solicitudes registradas.

La prestación del servicio se realiza por niveles, de la siguiente manera:

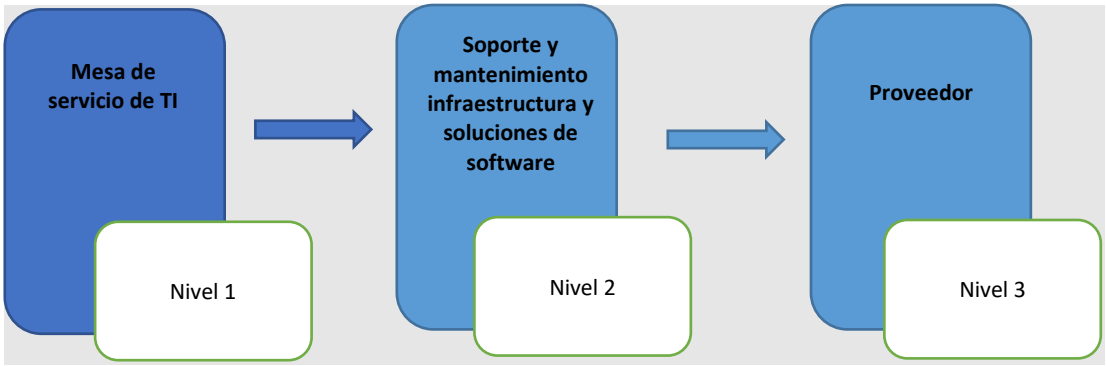


Ilustración 25. Niveles de soporte

a. **Nivel 1:** Este es el nivel de soporte inicial, responsable de las solicitudes básicas del usuario. Es sinónimo de soporte de primera línea, es donde se reúne toda la información del usuario y se categoriza y prioriza la solicitud mediante el análisis de los síntomas. Cuando se analizan los síntomas, es importante para el técnico de soporte identificar qué es lo que el usuario está intentando llevar a cabo de forma que no se pierda tiempo. Una vez que se ha logrado identificar el problema, el analista de primer nivel puede comenzar a prestar la verdadera asistencia de forma ordenada. En este grupo habitualmente manejan incidentes simples de resolución sencilla.

b. **Nivel 2:** El soporte de segundo nivel lo realizan personas especializadas en redes de comunicación, sistemas de información, sistemas operativos, bases de datos, entre otras.

c. **Nivel 3:** El soporte de tercer nivel lo brindan los proveedores con los cuales la Unidad tiene contratos en donde se especifica las características y condiciones en las que se debe prestar el servicio de acuerdo con lo establecido en el catálogo de servicios de TI, a este nivel se recurre cuando los analistas de primer y segundo nivel no cuentan con las herramientas ni recursos especializados para la atención de una solicitud, en este caso el analista de segundo nivel responsable del servicio solícita y hace seguimiento a la atención de las solicitudes realizadas al proveedor.

La Gerencia de Tecnología cuenta con una metodología para el desarrollo, mantenimiento y soporte de software o de los sistemas de información, la cual se encuentra plasmada en los procedimientos que se encuentran dentro del proceso "Gestión y Desarrollo de las TICs" del Sistema de Gestión Integral (SGI) publicado en la Intranet: mantenimiento de aplicaciones, soporte de aplicaciones y gestión de cambios y liberaciones.

7.5 INFRAESTRUCTURA DE TI

A continuación, se describe la situación actual del dominio de Infraestructura de TI en cuanto a la gestión del ciclo de vida de la infraestructura de TI de la Unidad Administrativa Especial de Catastro Distrital.

7.5.1 Gestión de la operación de la infraestructura tecnológica

La Gerencia de Tecnología gestiona la operación y el soporte de la infraestructura tecnológica para garantizar la estabilidad de la operación de TI y responder acorde al plan de capacidad, a través de procesos establecidos de administración y operación de Infraestructura tecnológica, teniendo en cuenta las buenas prácticas.

El proceso relacionado con la gestión de la operación de la infraestructura tecnológica corresponde a el "Proceso Gestión y desarrollo de las TIC", el cual se describe en el numeral "6.2.1.1.3 Gestión y desarrollo de las TIC" [GG1]. El proceso inicia con la formulación de la planeación estratégica de TI, continua con la recepción y atención de requerimientos de usuarios para desarrollar las actividades estratégicas definidas, y finaliza con el seguimiento y mejora a los planes establecidos.

La descripción detallada de este proceso, subproceso, procedimientos, instructivos y plantillas, pueden ser consultados en el Sistema de Gestión Integral – SGI, publicada en la Intranet institucional. Dentro de los procedimientos establecidos en este proceso, el procedimiento asociado directamente a la operación de la infraestructura tecnológica se denomina GDT-PR-05 "Procedimiento Gestión de la Infraestructura Tecnológica"

7.5.2 Capacidades de la infraestructura tecnológica

Infraestructura de centro de datos

A nivel de centro de datos, la UAECD aloja sus equipos de cómputo principales en un centro de datos administrado por la Secretaría Distrital de Hacienda. Este centro de datos fue diseñado para que varias entidades del nivel distrital pudieran alojar sus propios equipos de cómputo permitiéndoles contar con un sitio confiable que cumpliera con todas las características de un centro de datos de nivel III, no obstante lo anterior, la administración actual de la Secretaria Distrital de Hacienda ha manifestado la no factibilidad económica de dar continuidad a este servicio dados los altos costos de mantenimiento y/o renovación tecnológica por lo que en el término de corto plazo la UAECD deberá realizar el traslado de sus capacidades de cómputo ya sea a servicios tercerizados de centro de datos o a servicios de cómputo en una nube pública.

La unidad dispone de 3 centros de cableado ubicados en los pisos 2, 11 y 12, los cuales cuentan con un circuito eléctrico con red eléctrica regulada y normal, sistemas de aire acondicionado tipo mini-split. Dichos centros de cableado están soportados con 4 UPS del fabricante PowerSun adquiridas en el año 2016 (dos UPS de 40 KVA) y en el año 2019 (dos UPS de 30 KVA), 3 aires acondicionados marca YORK y BLueLINK adquiridos en el año 2018.

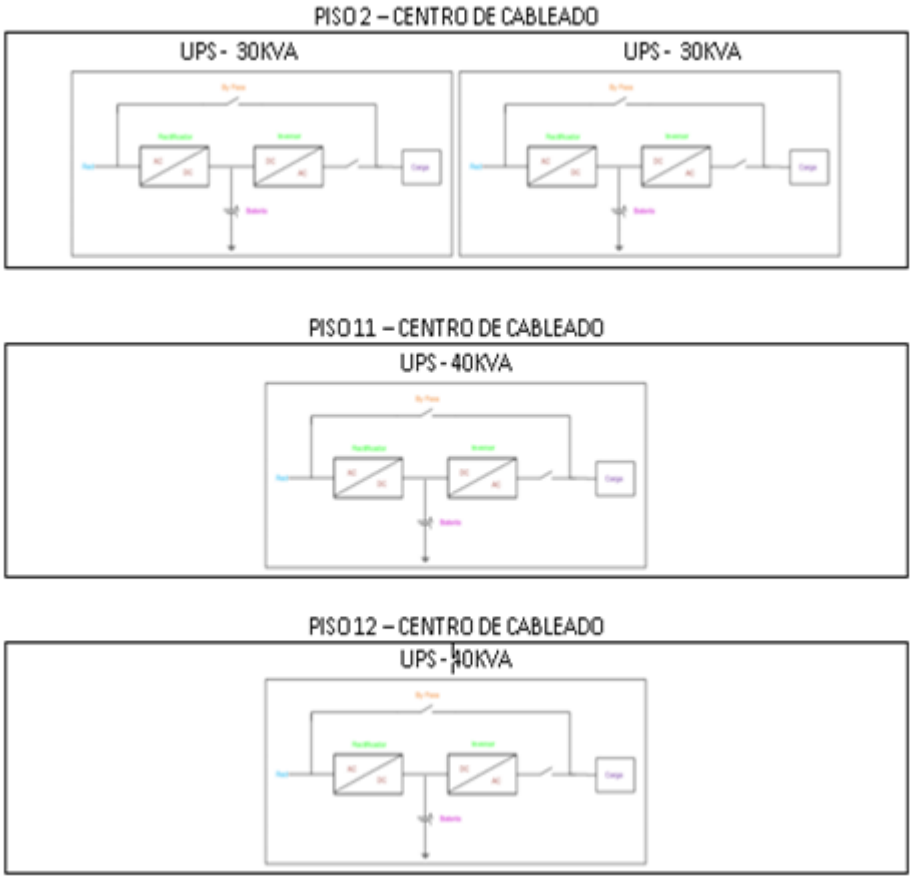


Ilustración 26. Infraestructura de centro de datos

Infraestructura de Conectividad

La UAECD cuenta con una red LAN configurada en anillo entre los diferentes pisos donde operan sus funcionarios, esta red LAN cuenta con un backbone a 20 Gbps (excepto en el piso 12, ya que la conexión entre el switch de distribución y switch core del centro de cableado del piso dos es de 10 Gbps), que permite contar con un ancho de banda eficiente y redundante para la comunicación de los diferentes pisos con los switches de core y equipos de seguridad firewalls (los cuales cumplen la función de enrutamiento o capa 3).

La siguiente ilustración, muestra la conexión LAN física entre los diferentes pisos donde opera la UAECD. Cada conexión o enlace se realiza a través de 2 Fibras OM4 con capacidad de 10Gbps

(excepto lo mencionado en el párrafo anterior), la conexión en anillo permite contar con un esquema de redundancia a nivel de conexiones físicas. La Red LAN esta segmentada por VLANs, lo que ayuda a la gestión y seguridad de las redes, teniendo VLAN diferentes para redes de usuarios, servidores de bases de datos (diferentes entre cada ambiente), servidores de capa media (diferentes entre cada ambiente), aplicaciones balanceadas, etc.

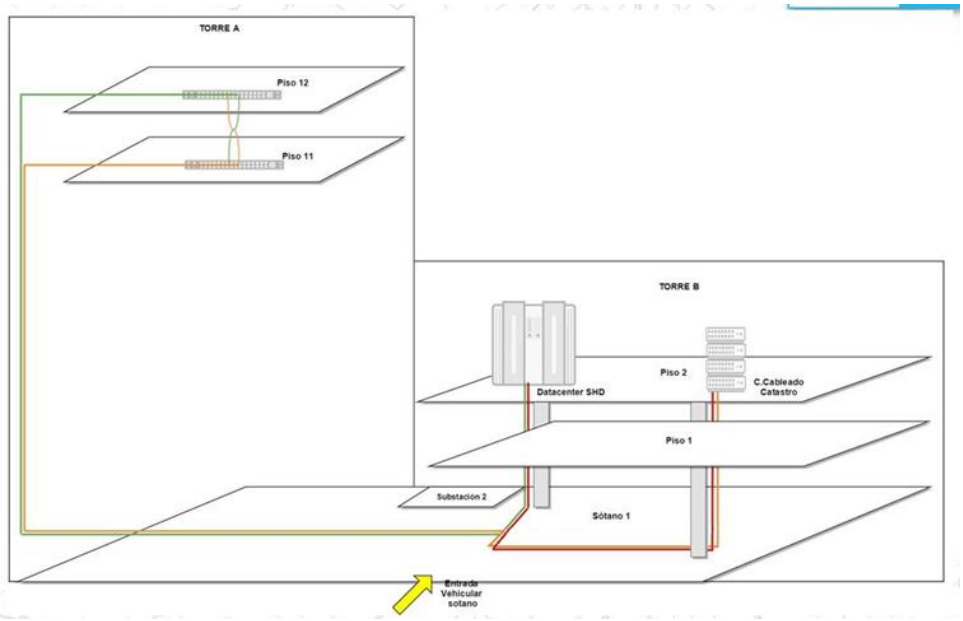


Ilustración 10. Infraestructura de Conectividad

La red LAN se encuentra distribuida y organizada de manera jerárquica (Core, Distribución y. Acceso), a través de ésta se realiza la distribución del tráfico entre los usuarios finales y aplicaciones de la UAECD. La solución está conformada por equipos DELL y Hewlett Packard – Aruba los cuales soportan la comunicación entre las capas de Distribución y Acceso de la red. Se encuentran instalados en los diferentes pisos de las sedes de la entidad garantizando la conexión de los puestos de trabajo de los usuarios finales. Su arquitectura se compone de la siguiente manera:

Los switches Dell fueron adquiridos en la vigencia 2015, los cuales permiten la conexión de dispositivos críticos para la Entidad como los son balanceadores, firewall, servidores, canales dedicados, internet y los switches de distribución y acceso, estos dispositivos permiten la conectividad a los servicios de TI tales como el correo corporativo, internet y sistemas de información de la UAECD, permitiendo que los funcionarios puedan ejecutar sus actividades.

Para este componente, la UAECD cuenta con una infraestructura distribuida de la siguiente manera:

a. Dos (2) switches Dell modelo S4048-ON-01-FE-72 ubicado en el centro de cableado del piso 2 de la torre B.
b. Dos (2) switches Dell modelo S4048-ON-01-FE-72 ubicado en el Data Center principal.
c. Un (1) switch Dell modelo S4048-ON-01-FE-72 ubicado en el centro de cableado del piso 11 de la torre A.
d. Un (1) switch Dell modelo S4048-ON-01-FE-72 ubicado en el centro de cableado del piso 12 de la torre A.
e. Un (1) Switches Dell modelo X1026 ubicados en el centro de cableado del piso 2 de la torre B (en stop).
f. Un (1) Switches Dell modelo X1026 ubicados en la tienda Catastral del piso 1 de la torre B (supercade).

Los switches HP Aruba fueron adquiridos en la vigencia 2017 (en su mayoría), con garantía, soporte y mantenimientos por un (1) año, como también se adquirió el software de gestión de los equipos activos de red denominado IMC y el cual también requiere contar con actualizaciones, soporte y mantenimiento. Para este componente, la UAECD cuenta con una infraestructura distribuida de la siguiente manera:

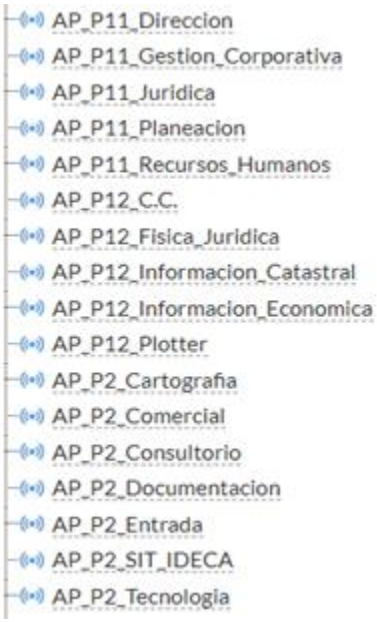
a. Siete (7) switches Aruba modelo 2930M ubicado en el centro de cableado del piso 2 de la torre B.
b. Un (1) switch Aruba modelo 2930F ubicado en el centro de cableado del piso 2 de la torre B.
c. Un (1) switch Aruba 2920 ubicado en el centro de cableado del piso 2 de la torre B.
d. Un (1) switch Aruba modelo 2930F ubicado en el Data Center de Hacienda.
e. Cuatro (4) switches Aruba modelo 2930M ubicado en el centro de cableado del piso 11 de la torre A.
f. Seis (6) switches Aruba modelo 2930M ubicado en el centro de cableado del piso 12 de la torre A.
g. Tres (2) switches Aruba modelo 1920S ubicado en el piso 2 de la torre B.
h. Un (1) switch Aruba modelo 1920S ubicado en el centro de cableado del piso 2 de la torre B (en stop).
i. Tres (3) switches Aruba modelo 1920S ubicado en el piso 1 de la torre B.

Desde la adquisición de los activos de red, se ha contratado anualmente los servicios de mantenimiento y garantía extendida, por lo anterior, es necesario mantener los switches Dell y Aruba cada año con la garantía directa de fabricante y contar con el soporte necesario para su operación, por esta razón la entidad dentro del plan anual de adquisiciones contemplo las líneas de contratación que permitan cumplir con la meta de contar con el 100% del hardware, software y conectividad que soporte la operación de la entidad y realizar la renovación de la garantía incluido

el soporte técnico y mantenimientos que requieren los switches y el software de gestión IMC, por el término de un (1) año.

El cableado estructurado que se encuentra instalado en la sede del CAD cumple con la normatividad y está certificado en debida forma al momento de su instalación (hace más de 10 años). No obstante, no se cuenta con un contrato de soporte y mantenimiento vigente, lo cual es necesario para atender las necesidades que han surgido y vayan surgiendo.

La red WIFI se soporta con una solución basada en productor Fortinet la cual está conformada por una controladora y varios APS, permitiendo realizar la configuración y administración de la solución. Los componentes de la solución son:



SSID 4

WiFi_CONTRATIS	CONTRATISTAS (WiFi_CONTRATIS)	Tunnel	WPA2 Enterprise	always	Up	8
WiFi_INVITADOS	INVITADOS (WiFi_INVITADOS)	Tunnel	Captive Portal	always	Up	10
WiFi_USUARIOS	FUNCIONARIOS (WiFi_USUARIOS)	Tunnel	WPA2 Enterprise	always	Up	8

Ilustración 27. Componentes red WIFI

Se cuenta con un Access Point en stop ubicado en el centro de cableado del piso 2.

Con respecto a la red WAN la Unidad cuenta con una red MPLS administrada por el proveedor ETB la cual presta el servicio de conectividad a las diferentes sedes o puntos de atención a los

ciudadanos, ubicados en 5 Supercades (20 de Julio, Bosa, Américas, Suba y CAD). De igual forma, para la prestación de servicios en línea al ciudadano y a otras entidades y el acceso de los funcionarios de la Unidad a internet, se cuenta con un canal de internet dedicado sin re-uso 1:1.

Estos servicios cuentan con los siguientes anchos de banda:

SEDE	ANCHO DE BANDA
Supercade 20 de Julio	2M
Supercade Bosa	2M
Supercade Américas	6M
Supercade Suba	2M
Supercade Manitas	2M
Supercade CAD	6M
INTERNET	200M

De igual forma, se cuenta con un mecanismo de redundancia de los canales de conectividad que mitiga el riesgo de pérdida de conexión de una de las sedes o conexión a internet si falla el canal principal de conexión.

El siguiente diagrama muestra la configuración de conectividad LAN y WAN de la UAECD

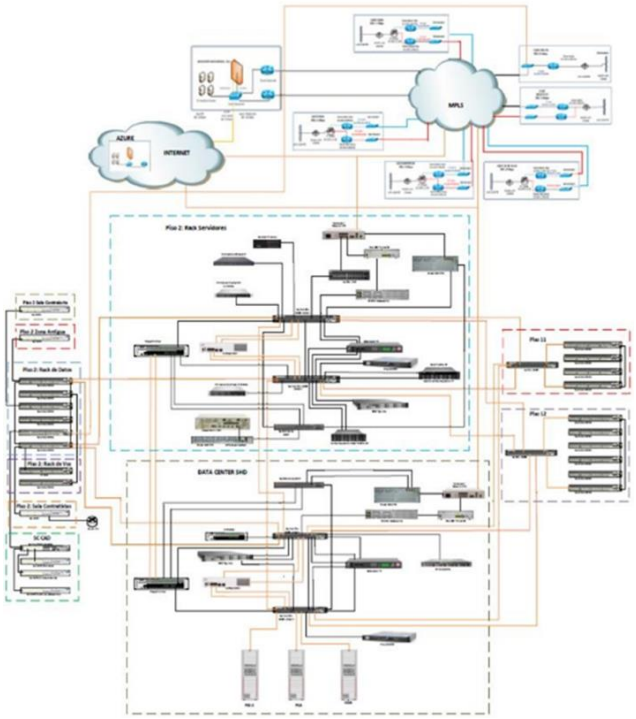


Ilustración 28. configuración de conectividad LAN y WAN de la UAECD

Para ofrecer conectividad a las sedes de Catastro Multipropósito, se cuenta con canales de internet (sin redundancia) dedicado administrado por el proveedor ETB el cual presta el servicio de conectividad a las diferentes sedes, se cuenta con canales de internet dedicado sin re-uso 1:1.

Estos servicios cuentan con los siguientes anchos de banda:

SEDE	ANCHO DE BANDA
Armenia	50M
Santa Rosa	50M
Palmira	50M
Cartagena	100M

Se retiro el canal de internet de la sede Cundinamarca, suministrando los siguientes equipos en stop; tres switches D-LINK modelo DGS-1510-52X, dos Access point D-LINK modelo DAP-2682 y una UPS marca Powest de 3 KVA, estos se encuentran en el centro de cableado del piso 2.

También se cuenta con los siguientes dispositivos que se encuentran prestando servicio en la sede de Catastro Multipropósito de Cartagena; un switch D-LINK modelo DGS-1510-52X, cinco switches

D-LINK modelo DGS-1210-26, una UPS Powest de 3 KVA y cuatro reguladores Electronic Digital de 5 KVA.

De los dispositivos mencionados, a continuación, se relaciona la obsolescencia:

Cantidad	Marca	Dispositivo	Modelo	Obsolescencia
6	HPE	Switch	1920S 24G 2SFP PPoE+ 185W	30/11/2025
1	Aruba	Switch	2920 48G POE	31/12/2023
18	Fortinet	Access Point	FAP-421E	Ya no cuentan con actualización de firmware
6	DELL	Switch	S4048	28/02/2025
2	DELL	Switch	X1026	28/02/2025

Al momento de realizar el presente informe, se cuenta con los siguientes contratos de mantenimiento para los dispositivos de conectividad:

Contrato	Objeto	Proveedor	Terminación
477-2021	Prestación de servicios de telefonía IP con comunicaciones unificadas y canales de comunicaciones para la operación de la UAECD	ETB S.A. E.S.P.	Hasta agotar recursos
1518-2022	Prestación de servicios de garantía, soporte y mantenimiento para los equipos activos de red de la UAECD. Lote 2: Adquirir la garantía, soporte y mantenimiento para los switches DELL	REDCOMPUTO LIMITADA	Diciembre 29 de 2023
851-2023	Prestación de servicios de soporte técnico incluido mantenimientos preventivos y correctivo para las UPS de la UAECD	CM & M SOLUCIONES ELECTROMECANICAS SAS	Agosto 31 de 2024
835-2023	Prestación de servicios de garantía soporte y mantenimiento para los equipos activos de red marca Hewlett Packard - Aruba de la UAECD	LATTITUDE CORP SAS	Julio 20 de 2024

Infraestructura de Procesamiento y Almacenamiento

Plataforma ON-PREMISE: PCA

La plataforma de virtualización Oracle PCA cuenta en la actualidad con la siguiente cantidad de nodos físicos de computación:

1. 10 nodos X5-2
2. 6 nodos X6-2.

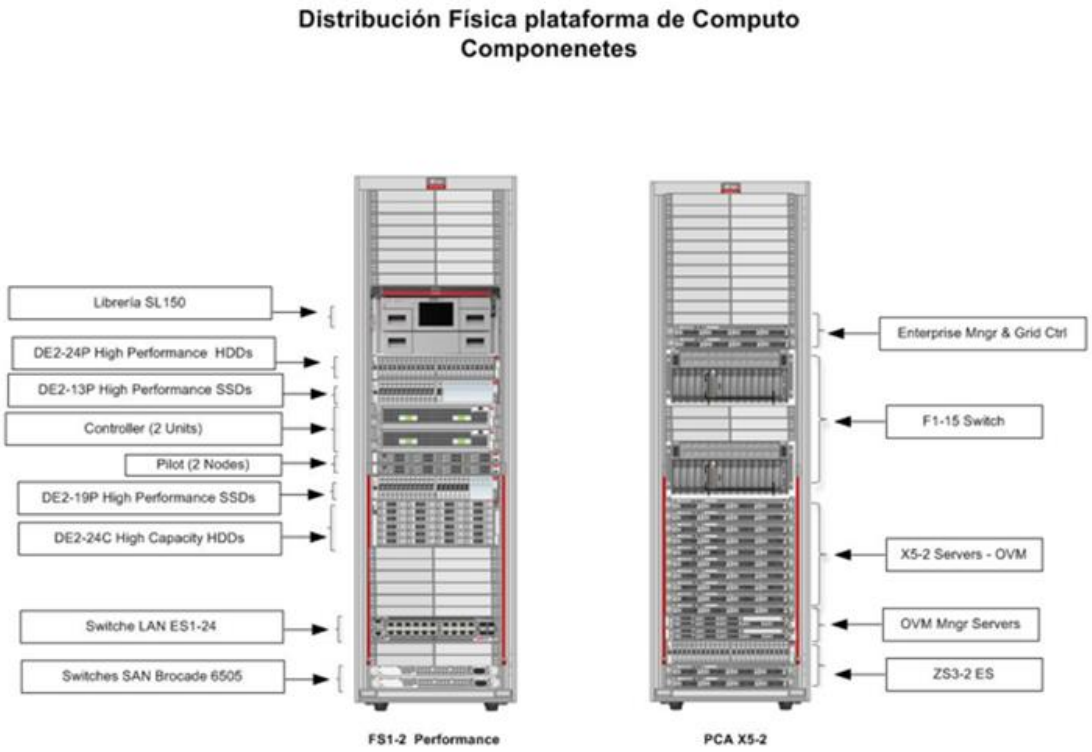


Ilustración 29 . La plataforma de virtualización Oracle PCA

En relación con el sistema de almacenamiento, se dispone de una plataforma FS1-2 (Flash Storage System), compuesta por:

1. 2 pilotos (Activo/pasivo).
2. 2 controladoras.
3. 8 drives enclosures.
4. grupos de discos.

A continuación, se registra el almacenamiento actual usado y disponible por tipo de almacenamiento:

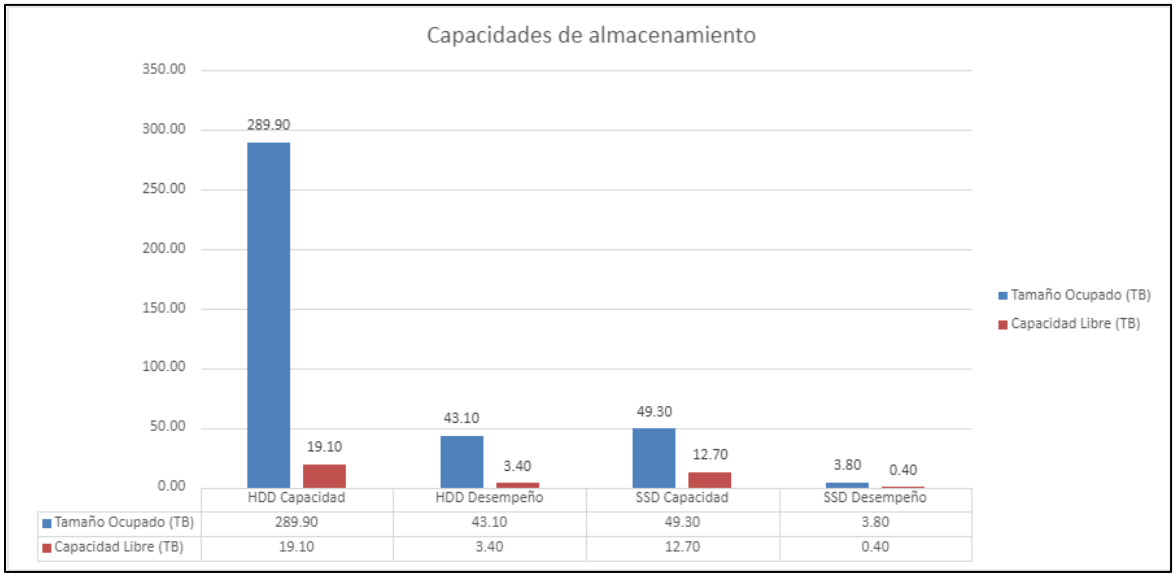


Ilustración 30. Almacenamiento actual PCA

Actualmente el sistema PCA, se encuentra en estado total de degradación, sin prestar servicios lógicos a causa de fallas físicas presentadas en todos los componentes de hardware que componen la PCA. Los daños actuales se presentan en: nodos de cómputo, sistema de almacenamiento, redes de almacenamiento y sistemas de administración.

Algunos de los daños encontrados incluyen los siguientes componentes:

Ubicación Disco	Tamaño	Numero Parte / Modelo	Descripción	Disk Group	Enclosure
Drive 23	9.9 Tb	H7210A521SUN010T	Disco de capacidad	DG 12	07
Drive 19	1.2 Tb	H1T1812SFSUN1.2T	Performance Disk	DG 14	08

Drive 23 – Disco de 10Tb

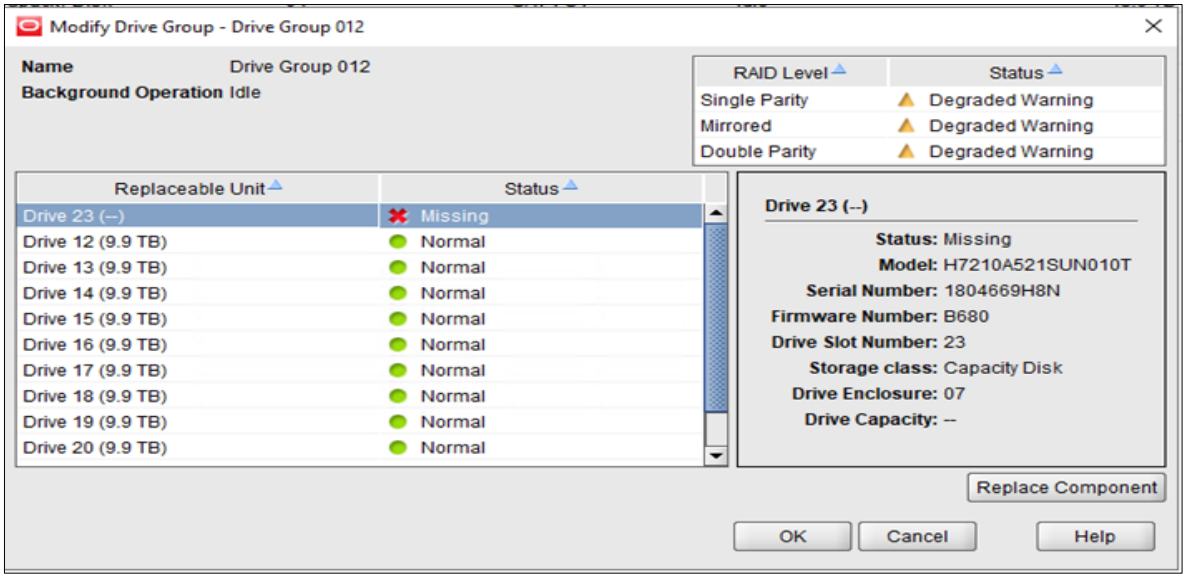


Ilustración 31. Estado actual disco 23

Drive 19 – Disco de 1.2Tb

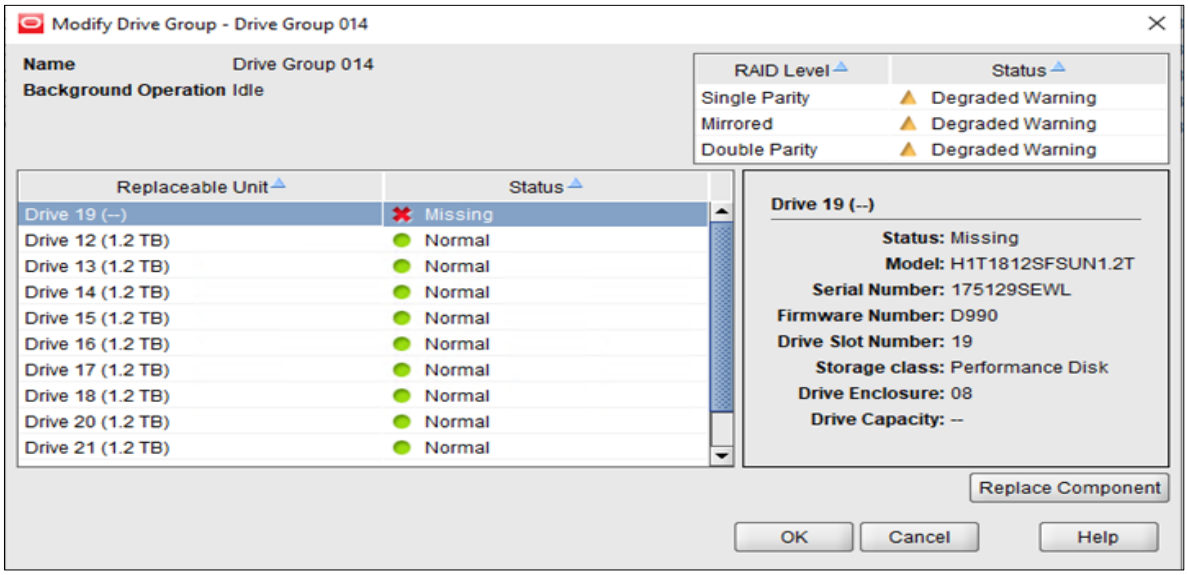


Ilustración 32. Estado actual disco 19

Registro de fallos de los discos

Drive Enclosures		
Name	Comment	Overall
Enclosure 07	SAS 10 TB (Capacity HDD)	Warning
Enclosure 08	SAS 1.2 TB (Nearline HDD)	Warning
Enclosure 01	SSD 400TB (slc)	Normal
Enclosure 02	SSD 1.6 TB (Mlc)	Normal
Enclosure 03	SAS 900 (perf Hdd)	Normal
Enclosure 04	SAS 4TB (capacity Hdd)	Normal
Enclosure 05	SAS 3.2 TB (perf SSD)	Normal
Enclosure 06	SAS 3.2 TB (perf SSD)	Normal

Ilustración 33. Registro de fallos de discos PCA

Fallo en el Switch Infiniband

Uno de los switches de acceso al almacenamiento se dañó completamente, y no es posible su recuperación. A partir de lo cual, no es posible acceder al almacenamiento a través de los paths correspondientes de este switch.

Degradando completamente el acceso a los datos de los servidor virtuales alojados allí.

Controller 02	Normal			
Slot 5	Normal			
Port 1	Not Connected	FC	21:00:00:0E:1E:27:A5:B1	--
Port 0	Not Connected	FC	21:00:00:0E:1E:27:A5:B0	--
Slot 1	Normal			
Port 0	Not Connected	FC	21:00:00:0E:1E:27:A7:C0	--
Port 1	Connected	FC	21:00:00:0E:1E:27:A7:C1	16 Gbps
Slot 4	Normal			
Port 0	Not Connected	FC	21:00:00:0E:1E:27:98:50	--
Port 1	Connected	FC	21:00:00:0E:1E:27:98:51	16 Gbps

Controller 01	Normal			
Slot 1	Normal			
Port 0	Not Connected	FC	21:00:00:0E:1E:27:92:C0	--
Port 1	Connected	FC	21:00:00:0E:1E:27:92:C1	16 Gbps
Slot 5	Normal			
Port 0	Not Connected	FC	21:00:00:0E:1E:27:7B:90	--
Port 1	Not Connected	FC	21:00:00:0E:1E:27:7B:91	--
Slot 4	Normal			
Port 0	Not Connected	FC	21:00:00:0E:1E:27:93:00	--
Port 1	Connected	FC	21:00:00:0E:1E:27:93:01	16 Gbps

Ilustración 34. Estado del acceso a servidores virtuales por fallo switch infiniband

Sistema de almacenamiento ZS3-ES (NAS)

Se registra falla en el procesador. De acuerdo con la revisión realizada por el proveedor Oracle, en este modelo de servidor no es posible reemplazar el procesador, se debe cambiar el servidor completo, ya que la CPU esta soldada a la tarjeta madre.

Controladora 2

Status

Overall Status: Service Required Total Problem Count: 1

Subsystem	Status	Details		Inventory	
Processors	Service Required	Processor Architecture: Processor Summary:	x86 64-bit Two Intel Xeon Processor E5 Series	Processors (Installed / Maximum):	2 / 2

Processors

View processor information from this page.

Health: Service Required

Health Details: P0 (CPU 0) is faulty.
See the Open Problems page for more information.

Architecture: x86 64-bit

Summary Description: Two Intel Xeon Processor E5 Series

Installed CPUs: 2

Maximum CPUs: 2

CPUs

CPU #	Health	Health Details	Location	Maximum Clock Speed	Total Cores	CPU Details
CPU 0	Service Required	An internal fault on a processor has occurred. See the Open Problems page for more information.	P0 (CPU 0)	2.100 GHZ	8	Details

Ilustración 35. Estado actual controladora 2

Cajones de discos

Fallo en el disco de 838 Gb.

Disk Shelves 1516NM401M Disk Slot Fan PSU

Back to overview

BACK FRONT

ID	MFR/MODEL	RPM	SIZE	TYPE
HDD 0	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 1	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 2	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 3	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 4	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 5	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 6	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 7	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 8	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 9	HITACHI/H109090SESUN900G	10000	838G	Spare [A]
HDD 10	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 11	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 12	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 13	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 14	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 15	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 16	HITACHI/H109090SESUN900G	10000	838G	Spare
HDD 17	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 18	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 19	HITACHI/H109090SESUN900G	10000	838G	Data
HDD 20	HGST/HSCAC2DA6SUN200G	--	186G	Log
HDD 21	HGST/HSCAC2DA6SUN200G	--	186G	Log
HDD 22	HGST/HSCAC2DA6SUN200G	--	186G	Log
HDD 23	HGST/HSCAC2DA6SUN200G	--	186G	Log

Ilustración 36. Fallo en disco

Clúster de almacenamiento en estado de fallo a causa de la caída de la controladora 2.

Active Problems Total: 6 1-6

DATE	DESCRIPTION	TYPE	PHONED HOME
2023-6-5 11:53:51	SMART health-monitoring firmware reported that a disk failure is imminent.	Major Fault	2023-6-5 12:01:58
2023-5-10 09:37:13	The cable between serial port 1 of this controller and serial port 0 of the other controller is down.	Critical Fault	2023-5-10 09:39:58
2023-5-10 09:37:13	The cable between serial port 0 of this controller and serial port 1 of the other controller is down.	Critical Fault	2023-5-10 09:39:58
2023-5-10 09:37:08	The cable between the Ethernet ports of each controller is down.	Critical Fault	2023-5-10 09:39:58
2023-4-1 10:50:09	There has been a non-recovered medium read error.	Critical Fault	2023-4-1 10:54:51
2023-4-1 10:49:17	There have been excessive recovered medium read errors on this disk.	Major Fault	2023-4-1 10:49:51

Problem Details MARK REPAIRED

Description: SMART health-monitoring firmware reported that a disk failure is imminent.
Type: Major Fault
Impact: It is likely that the continued operation of this disk will result in data loss.
Affected components: **100%** 1516NM401M: HDD 15 **(out of service)**
Manufacturer: HITACHI
Model number: H109090SESUN900G
Serial number: 001929A6G89W W8G6G89W
Revision: A7E0
Automated response: A hot-spare disk may have been activated.
Recommended action: If you are a qualified service person, detailed information on this problem can be found at http://support.oracle.com/msg/DISK-8000-0X If you are a qualified service person, detailed information on this problem can be found at http://support.oracle.com/msg/DISK-8000-0X
Event time: 2023-6-5 11:53:51
Unique Identifier: ed95bc77-062e-6586-c4e3-d87ecdc02009
Phoned home: 2023-6-5 12:01:58

Ilustración 37. Estado cluster de almacenamiento

La ocupación actual del almacenamiento en el dispositivo ZFS está en el *96.4%*, situación que conlleva a que no se cuente con el espacio necesario para realizar recuperación alguna.

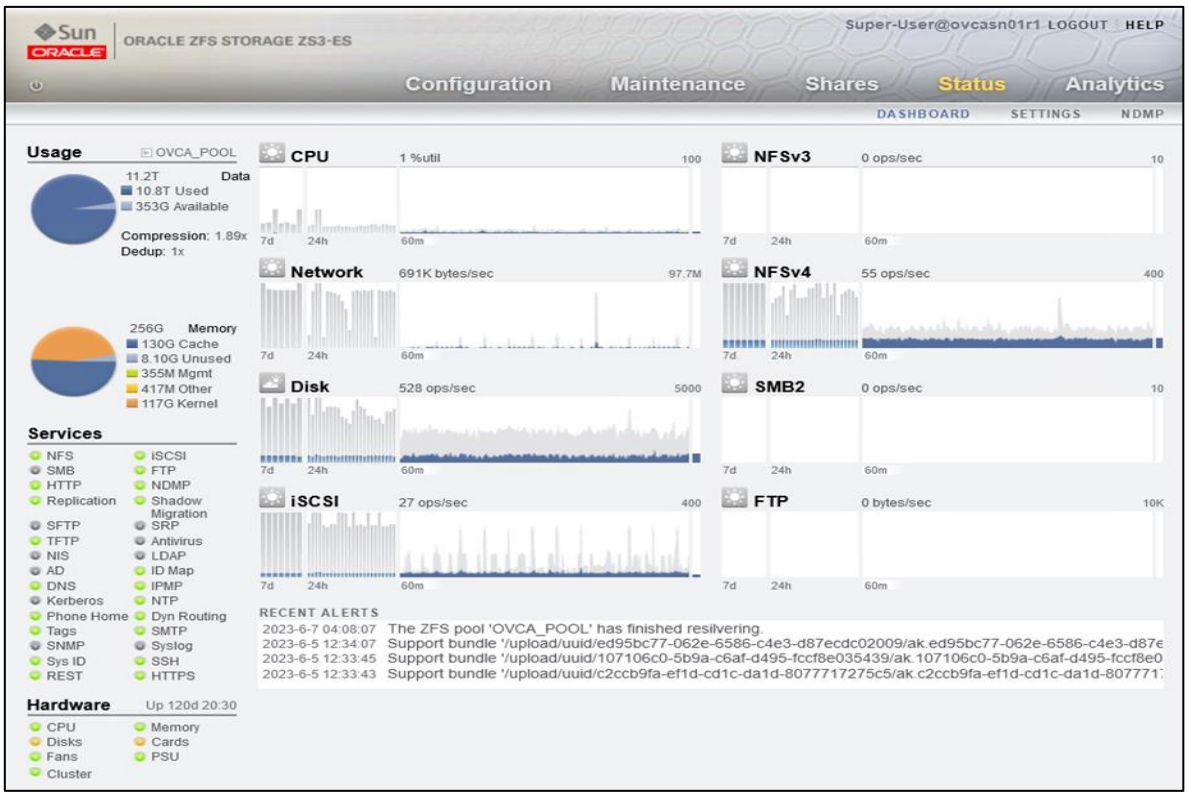


Ilustración 38. Ocupación actual almacenamiento ZFS

Sistema de virtualización PCA (Private Cloud Appliance).

El sistema de virtualización usado de la actual PCA se llama *OVM Manager*, el cual fue descontinuado por el proveedor Oracle en el año 2020.

(ver: https://blogs.oracle.com/virtualization/post/announcing-oracle-vm-3-extended-support)

Nodo físico de PCA en estado de error.

Sin acceso actualmente a la administración del nodo. Se registran con fallas en la memoria RAM del nodo.

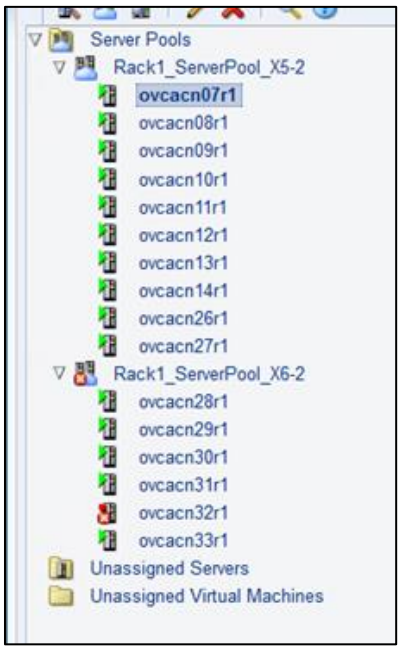
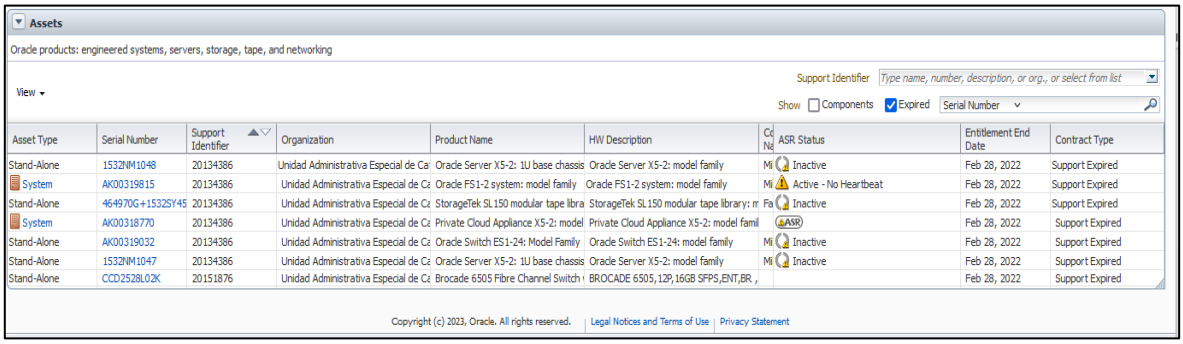


Ilustración 39. Fallas de memoria RAM del Nodo FCA

El contrato de soporte para el sistema de virtualización de la PCA finalizó el día 28 de febrero de 2022, tal como se evidencia en el portal web de soporte de Oracle: *My Oracle Support*.



Assets

Oracle products: engineered systems, servers, storage, tape, and networking

View

Support Identifier: Type name, number, description, or org., or select from list

Show: Components, Expired, Serial Number

Asset Type	Serial Number	Support Identifier	Organization	Product Name	HW Description	ASR Status	Entitlement End Date	Contract Type
Stand-Alone	1532NM1048	20134386	Unidad Administrativa Especial de Ca	Oracle Server X5-2: 1U base chassis	Oracle Server X5-2: model family	Inactive	Feb 28, 2022	Support Expired
System	AK00319815	20134386	Unidad Administrativa Especial de Ca	Oracle FS1-2 system: model family	Oracle FS1-2 system: model family	Active - No Heartbeat	Feb 28, 2022	Support Expired
Stand-Alone	464970G+1532SY45	20134386	Unidad Administrativa Especial de Ca	StorageTek SL150 modular tape libra	StorageTek SL150 modular tape library: m	Inactive	Feb 28, 2022	Support Expired
System	AK00318770	20134386	Unidad Administrativa Especial de Ca	Private Cloud Appliance X5-2: model	Private Cloud Appliance X5-2: model famil	ASR	Feb 28, 2022	Support Expired
Stand-Alone	AK00319032	20134386	Unidad Administrativa Especial de Ca	Oracle Switch ES1-24: Model Family	Oracle Switch ES1-24: model family	Inactive	Feb 28, 2022	Support Expired
Stand-Alone	1532NM1047	20134386	Unidad Administrativa Especial de Ca	Oracle Server X5-2: 1U base chassis	Oracle Server X5-2: model family	Inactive	Feb 28, 2022	Support Expired
Stand-Alone	CCD2528L02K	20151876	Unidad Administrativa Especial de Ca	Brocade 6505 Fibre Channel Switch	BROCADE 6505,12P,16GB SFPS,ENT,BR ,		Feb 28, 2022	Support Expired

Copyright (c) 2023, Oracle. All rights reserved. | Legal Notices and Terms of Use | Privacy Statement

Ilustración 40. Contrato virtualización PCA con Oracle

Plataforma ON-PREMISE: CLÚSTER HYPER-V

La infraestructura On-Premise cuenta con dos servidores Oracle X-5 (Prowingest01 y Prowingest02) que conforman el clúster de Hyper-V. En este se encuentran alojadas algunas máquinas virtuales que proveen los siguientes servicios productivos:

- Directorio Activo, DNS y DHCP
- Data Protector
- Servidor Licencias ArcGIS On-Premise y AutoCAD.
- RELAY de correo electrónico.
- LPC (Línea de Producción Cartográfica).
- PERNO
- Terminal Server
- Veeam Backup
- WSUS

Ambos servidores presentan un alto grado de obsolescencia y degradación, dado que al igual que la plataforma de la PCA no cuentan con soporte activo de mantenimiento, y a la fecha hay algunos módulos de memoria RAM y CPU con fallas en ambos servidores.

Plataforma de Nubes Públicas

La UAECD tiene desplegado actualmente servicios en las nubes de *Microsoft Azure* y *OCI (Oracle Cloud Infrastructure*), en las cuales se usa: Infraestructura como servicio (IAAS), plataforma como servicio (PAAS) y software como servicio (SAAS).

De acuerdo con lo anterior, se cuenta a la fecha con *71 servidores* en la nube de OCI (Oracle Cloud Infraestructure) y *49 servidores* en la nube de Azure.

Nube de Azure

Servicios de Catastro e IDECA desplegados en nube la Azure

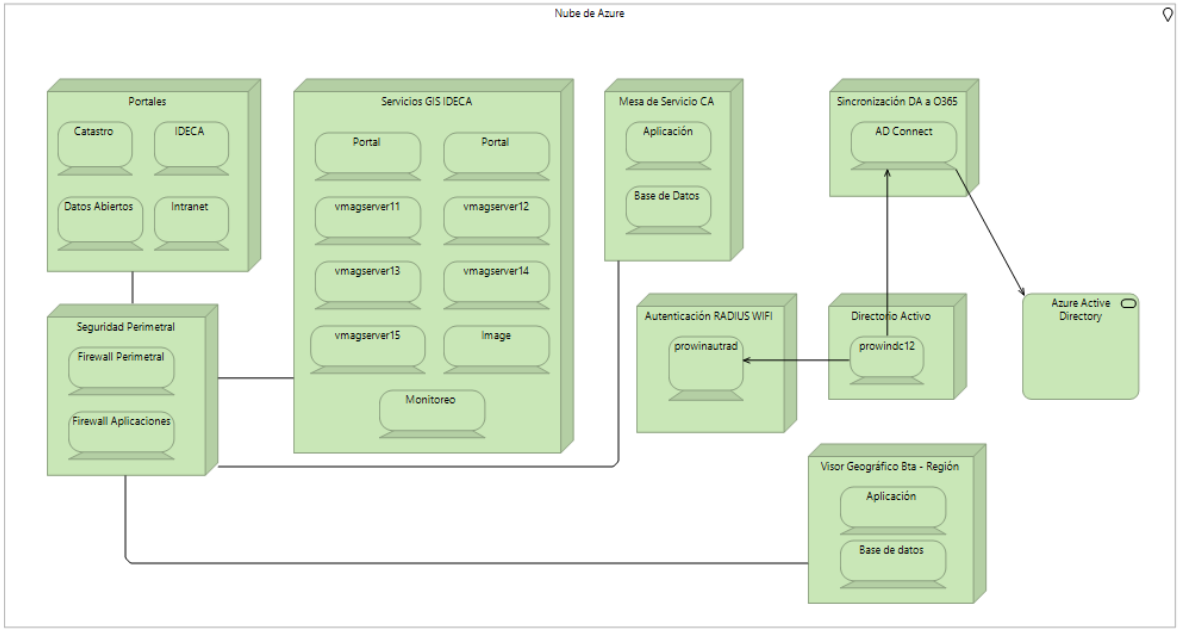


Ilustración 41. Servicios de Catastro e IDECA desplegados en nube la Azure

Los servicios desplegados en esta nube son:

- Mapas Bogotá
- Analítica IDECA
- Aplicaciones
- Catastro
- Desarrollo económico
- Gestión publica
- Imágenes
- Mapa de referencia
- movilidad
- Ordenamiento territorial
- Recreación y deporte
- Salud
- Servicios públicos
- Topografía

- Portales Web

  - Catastro

- Go-Catastral
- IDECA
- Intranet
- Mapas Bogotá
- Datos abiertos.

- Otros servicios

  - Mesa de servicio
  - Azure Active Directory
  - Visor geográfico Bogotá- Región

Nube de OCI

NUBE ORACLE CLOUD INFRAESTRUCTURE (OCI)

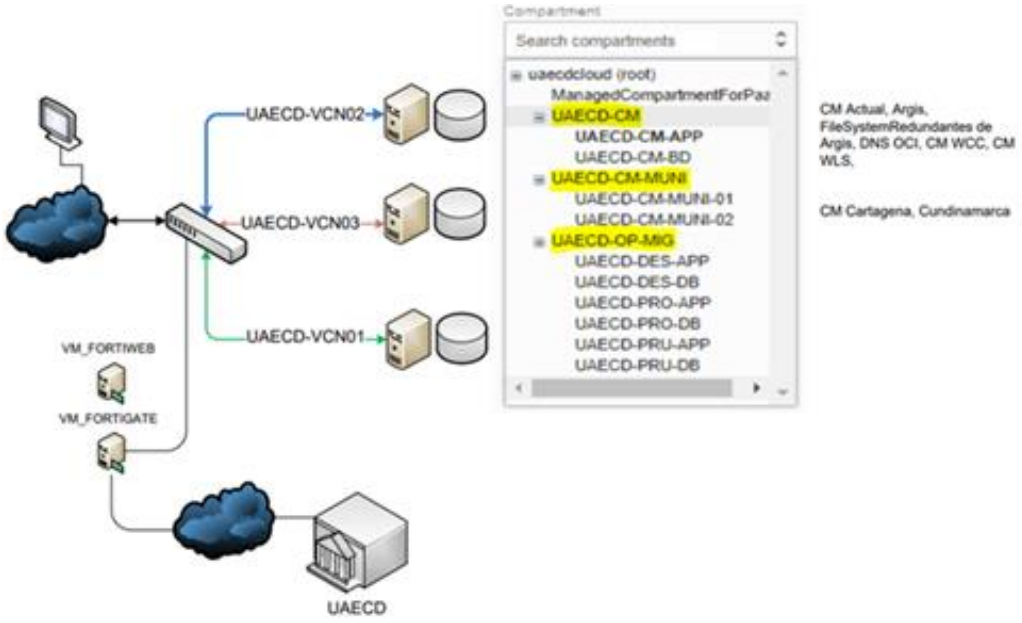


Ilustración 42. NUBE ORACLE CLOUD INFRAESTRUCTURE (OCI)

Los servicios desplegados en esta nube son:

- Catastro multipropósito:

  - Radicador y gestor de convenios.
  - Plataforma ArcGIS: Visores cartográficos de los convenios.
  - Base de datos geográficas.

- Servicios Misionales y Administrativos:

  - WCC
  - Catastro en línea (CEL).
  - Tienda Virtual
  - FOCA
  - CISA
  - SIIC
  - Avalúos Comerciales
  - Captura en Terreno (CT)
  - SICapital
  - InfoDOC
  - IsoDOC
  - Bases de datos misionales y administrativas.

Nube de OCI: Discovery

En la actualidad se encuentra en proceso la ejecución de una serie de jornadas de Discovery en la nube de OCI. Esta actividad se viene realizando en conjunto con especialistas de Oracle con quienes se ha identificado y verificado el estado actual de los servicios de: red, almacenamiento, computo, seguridad, base de datos y demás aprovisionados en esta nube. Esto último con el fin de identificar oportunidades de mejora, así como llevar a cabo los ajustes del caso sugeridos en una serie de recomendaciones técnicas que han surgido como resultado de este proceso de descubrimiento y verificación de los servicios actuales.

Plan de Recuperación de Desastres (DRP)

En la actualidad el único plan de recuperación de desastres con el que cuenta la entidad es realizar la recuperación de los servicios tecnológicos, misionales y administrativos mediante la restauración de las copias de respaldo programadas a los discos duros virtuales o sistemas de archivos de los servidores que alojan estos servicios. No se cuenta en el momento con ninguna otra infraestructura desplegada en nube u On-Premise dedicada exclusivamente al DRP.

El ambiente de productivo actual se encuentra en la nube OCI en la región ubicada en Ashburn (Virginia) y la estrategia del plan de recuperación ante desastres – DRP es el siguiente:

BASES DE DATOS:

- La base de datos misional se encuentra sincronizada en línea (réplica) en nube en la misma región.
- Las demás bases de datos (administrativa, geográfica, WCC) cuentan con copias de respaldo o backups de la información que reposa en los servidores, así mismo dichas copias se almacenan en la misma región donde reposa el ambiente productivo.

SERVIDOR OCI-AZURE:

- En cuanto a los servidores de aplicaciones se están guardando carpetas específicas en nube para no tener que recuperar todo el disco.
- Se están haciendo copias de los discos de los servidores OCI-AZURE con periodicidad semanal y de manera manual (scritps), lo cual no es buena práctica, dado que, si se pierde un archivo, se requiere recuperar todo el disco y no sólo el archivo. Adicionalmente los RTO y RPO son demasiado altos, pudiendo ocasionar impactos negativos a la entidad.

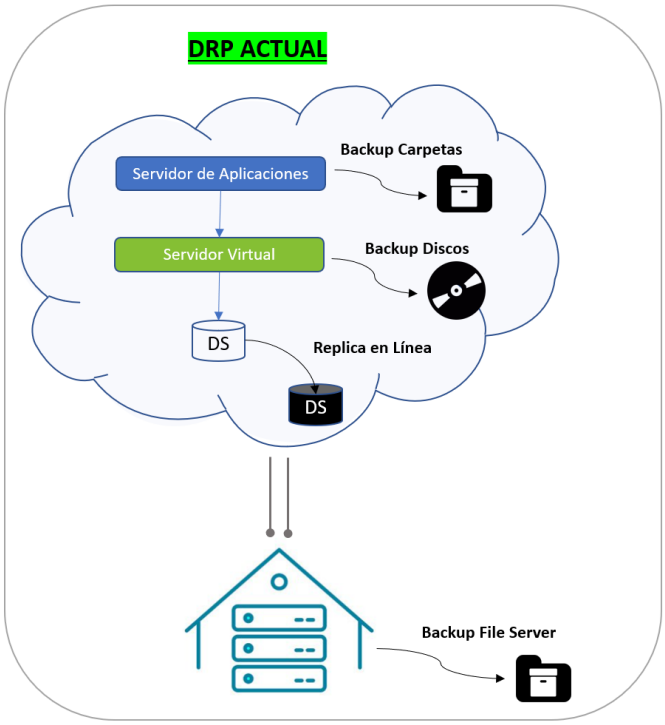


Ilustración 43. DRP Actual

Consideraciones actuales para tener en cuenta:

- **OFFICE 365 CORREO Y SHAREPOINT:**
  - Actualmente con los servicios de Microsoft Office 365 se obtienen acuerdos de niveles de servicio relacionado con la disponibilidad de la infraestructura y los servicios (no los datos), por lo que a pesar de que ofrece redundancia de datos no existe protección ante la pérdida de datos, borrado accidental o malicioso, cifrado de datos etc.
  - Sharepoint online permite la retención de documentos eliminados, pero sólo funciona si el usuario se da cuenta de la necesidad de recuperar sus datos dentro del tiempo ofrecido por el servicio de O365. Permite la recuperación de la papelera de reciclaje del usuario en un plazo de 30 días y de la papelera de reciclaje de la colección de sitios en un plazo de 93 días.
  - Office 365 sólo permite la disponibilidad de la información borrada durante un corto periodo de tiempo, pero en ningún caso es una solución de backup.
  - En cuanto a los buzones de correo, sólo los que tienen la funcionalidad de “Archive” pueden generar backups.
- **WCC-PCA:**

- En la PCA aún reposa información del WCC y pesa aproximadamente 6 terabytes, a esta información no se le está haciendo backup actualmente y es requerido hacerlo antes de que se dañe la PCA.
- La información que está almacenada es requerida por las áreas misionales para dar contestación a diferentes requerimientos de entidades y usuarios, como lo ha manifestado la Subgerencia de Información Económica quienes señalan que requieren contar diariamente con la información de años anteriores al 2018, para responder temas como revisión de avalúos, censo y plusvalía.
- El principal riesgo es que se pierda la información por daño en la PCA y por no contar con un espacio adecuado para mantenerla actualmente.

- **FILE SERVER AZURE:**
  - En la nube Azure se aprovisionó un servidor para el file Server que anteriormente se encontraba on-premise, el cual se le entregó a la Subgerencia de Información Física y Jurídica (Edgar Estevens Español Morales), a este servidor se ele están realizando copias de respaldo actualmente.
- **FILE SERVER UBICADO EN EL SERVIDOR DE BACKUPS:**
  - El file Server on-premise está ubicado actualmente en el servidor de backups que se habilitó de forma temporal. Este file server es temporal debido a que se el Sharepoint será el repositorio oficial.
  - Con relación al backup (7 teras), este se generó en el mismo sitio, lo cual es un riesgo.

Infraestructura de Servicios de Red y Autenticación

Controladores de Dominio

La entidad cuenta con un clúster de tres controladores de dominio que satisfacen la demanda actual de las peticiones de autenticación propias de los sitios, aplicaciones, servidores, vpn y usuarios.

Estos se encuentran alojados de acuerdo con la siguiente relación de sitios:

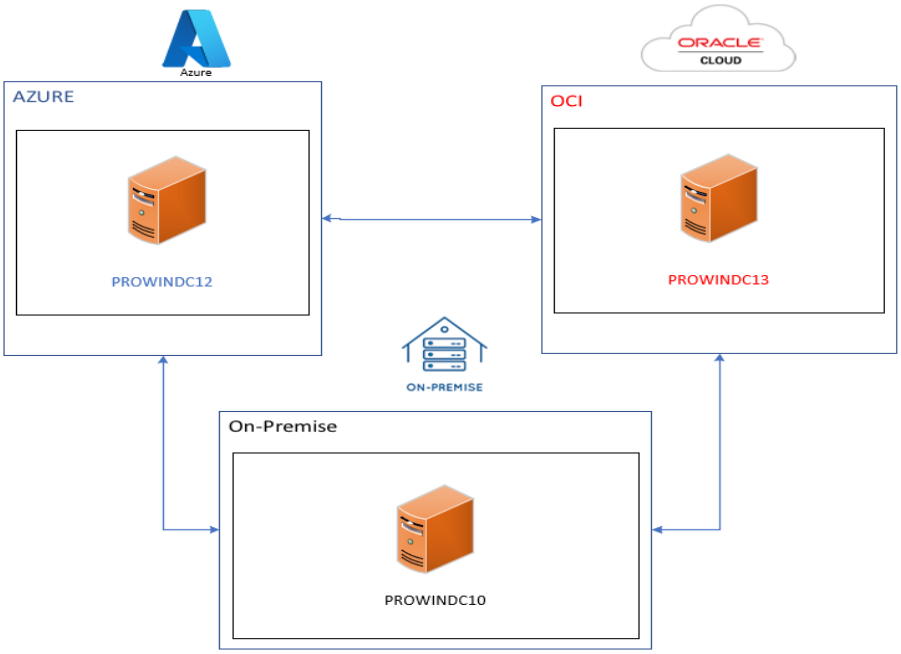


Ilustración 44. Controladores de Dominio

DNS

De manera homónima en relación con el número de controladores de dominio previamente indicado, se cuenta con la misma cantidad de servidores DNS (tres). Estos tres servidores tienen asignado el rol de servidores DNS (Domain Name System), lo cual facilita el balanceo de carga en términos de la resolución del nombre de Dominio para los diferentes sitios, aplicaciones, servidores, vpn y usuarios, tal como se mencionada en el anterior apartado.

Zona	Total
Búsqueda Directa	9
Búsqueda Inversa	18

DHCP

En relación con la asignación de direccionamiento dinámico de direcciones IP, la entidad cuenta en su infraestructura con un solo servidor DHCP (PROWINDC10), a partir del cual se define la asignación del direccionamiento IP. Este último cuenta con la siguiente cantidad de ámbitos para cada pila del protocolo IP:

Pila IP	Total Ámbitos
IPv4	18
IPv6	6

Plataforma Office 365

Actualmente la entidad cuenta con el siguiente licenciamiento de Office 365, adquirido en el presente año:

LICENCIAMIENTO OFFICE 365		
LICENCIA	**CANTIDAD**	**FECHA DE EXPIRACION**
Microsoft Defender for Office 365 (Plan 1)	1252	29/02/2024
Exchange Online Archiving for Exchange Online	291	29/02/2024
Office 365 E1	702	29/02/2024
Office 365 E3	550	29/02/2024
Power BI Pro	6	29/02/2024
Project Plan 3	20	29/02/2024
Visio Plan 2	20	29/02/2024

Infraestructura de Sistemas de Bases de Datos

Actualmente la UAECD cuenta con una arquitectura de Bases de datos desplegada sobre cuatro motores: Oracle, SQL Server, MySQL y Postgresql, para entregar servicios de datos a los sistemas de

información y aplicaciones que los diferentes usuarios de la Entidad utilizan, cubriendo de esta manera los ambientes de producción y desarrollo. El ambiente productivo se encuentra desplegado en OCI y Azure, el ambiente de desarrollo está desplegado sobre OCI.

La tabla siguiente presenta el inventario general de bases de datos de la Entidad por Ambiente y Plataforma desde la perspectiva de motor, soporte extendido por parte del fabricante y cantidad de bases de datos desplegadas, es concluyente que la Entidad cuenta con un total de bases de datos desplegadas, de estas 3 están desplegadas en versiones de motores que ya no están soportadas por el fabricante y para las demás se establece un panorama de al menos dos años de soporte.

Tabla. Inventario general de BDD de la Entidad

Ambiente	Plataforma	Motor	Versión release –	Soporte extendido **	Cantidad BDD's desplegadas
Producción	Azure	SQLServer	2016 (SP2)	2022	2
		MySQL	6	N/A	2
		PostgreSQL		N/A	1
	OCI	Oracle	11.1	2020	2
			12.2	2024	6
			19C	2024	20
				SUBTOTAL	36
Desarrollo	OCI	Oracle	12.2	2024	1
			19C	2024	2
				SUBTOTAL	3
Pruebas	OCI	Oracle	12.2	2024	1
	Azure	SQLServer	2016 (SP2)	2022	1
				SUBTOTAL	2
TOTAL BDD					41

**Información obtenida de https://www.oracle.com/us/assets/lifetime-support-technology-069183.pdf

** https://learn.microsoft.com/es-es/lifecycle/products/sql-server-2016

Fuente: Catálogo de Bases de Datos de la UAECD

En OCI se encuentran desplegadas bases de datos que soportan la misionalidad de la entidad y la parte administrativa. En la siguiente tabla se entrega el detalle de los servicios de datos desplegados por ambiente y servidor.

Se cuenta con 36 bases de datos en el ambiente productivo, en la parte Misional de destaca la información del SIIC, foca (antiguo y nuevo), la base de datos histórica de consulta, también se soporta la información geográfica y mapas. En parte administrativa y financiera se soporta la información relacional del gestor documental WCC, el ERP de SiCapital (Cordis - Correspondencia Distrital, Perno - Personal y nomina, Limay - Libro mayor Contabilidad, Sisco - Sistema de Contratación, Sai - Sistema de inventarios, Sae -Sistema de ingresos y elementos de consumo), Interfaces (Opget - Ordenes de pago y tesorería, Predis – Presupuesto y PAC), el sistema de facturación (SFV) y los sistemas paramétricos y de terceros I y II (SHD, SIT y TRC).

Para soportar la operación de Catastro multipropósito Go Catastral la cual es la marca que identifica los servicios de gestión catastral con enfoque multipropósito, que ofrece la Unidad Administrativa Especial de Catastro Distrital (UAECD) a las entidades territoriales, se cuenta con 54 instancias de Base de Datos en nube Oracle, en las diferentes ciudades como son: Santa Rosa, Palmira, Armenia, Cartagena, Cundinamarca (Anapoima, Apulo, Facatativá, Guatavita, Tocaima). Además, se cuenta con las bases de datos de pandora (soporte al proyecto para traer la data de IDARTES a Catastro) y mapas pro en la nube Oracle.

Tabla. Bases de Datos de OCI (Catastro Multipropósito)

Ambiente	DBSystem	BDD
Producción	GeoDatabaseNew/ catmulti	WCCPROD AMCOMD12 PNMSTARO REPOREPO PNMSROSA ARMENIAQ STAROSAC PALMIRAV REPOWLS

	DBSystem_cundi-ctg / cmcundi	FACATGDB CNDQUIPL CNDTIBIR CNDTIBCY CNDANAPO CNDSNANT CNDANLAI CNDAPULO CNDGUATA CNDSUBCH CNDTOCAI CARTGENA CNDFACAT
Pruebas	GeoDatabaseNew	CMBOGOTA CARTGENA PRUSROPR PRUSROSA LADMCOL
	DBSystem_cundi-ctg	PRUMIGRA cmcundi_pdb1

Fuente: Catálogo de Bases de Datos de la UAECD

Infraestructura de Capa Media

Capa Media ArcGIS

Ambiente OCI

- Arcgis Portal 10.8.1
- Arcgis Webadaptor 10.8.1
- ArcGIS Data Store 10.8.1
- Arcgis server 10.8.1
- Arcgis monitor 10.8.1
- Arcgis License Manager 2020.1
- Arcgis server Desktop 10.8
- ArcGIS Pro 2.6
- ArcGIS Work Flow Manager 10.8

Ambiente Azure

- Arcgis Portal 10.8.
- Arcgis Webadaptor 10.8
- Arcgis server 10.8
- Arcgis monitor 10.8
- Arcgis server Desktop 10.8
- ArcGIS Pro 2.6
- ArcGIS Pro 3.2

Onpremise

- Arcgis License Manager 2022.1

Capa Media ArcGIS

Actualmente no tenemos servidores obsoletos, se recomienda es aumentar las caracteristicas del Hardware y actualizacion de los sietemas y/o componentes de ArcGIS (ArcGIS Server, portal, webadaptor, data store, etc.

Capa Media Web Logic

Hoy día la arquitectura de capa media está conformada de la siguiente manera:

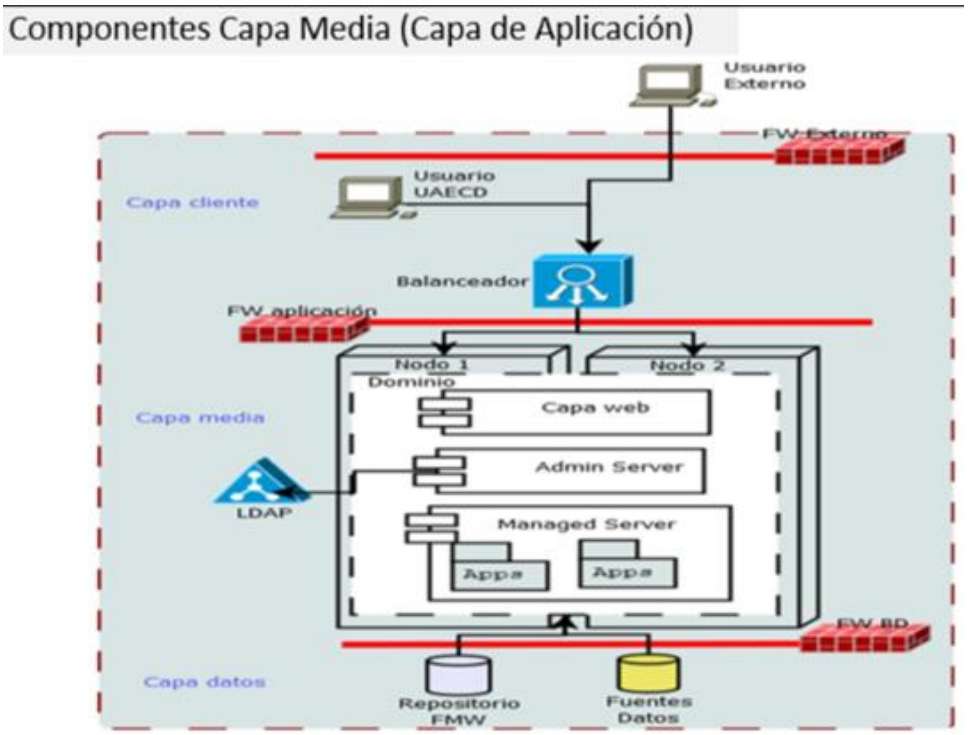


Ilustración 45. Infraestructura Capa Media

La infraestructura de Capa Media consta de:

1. Servidores en nube. 23 servidores de producción y 7 servidores de pruebas. La siguiente grafica detalla la arquitectura de Capa Media.

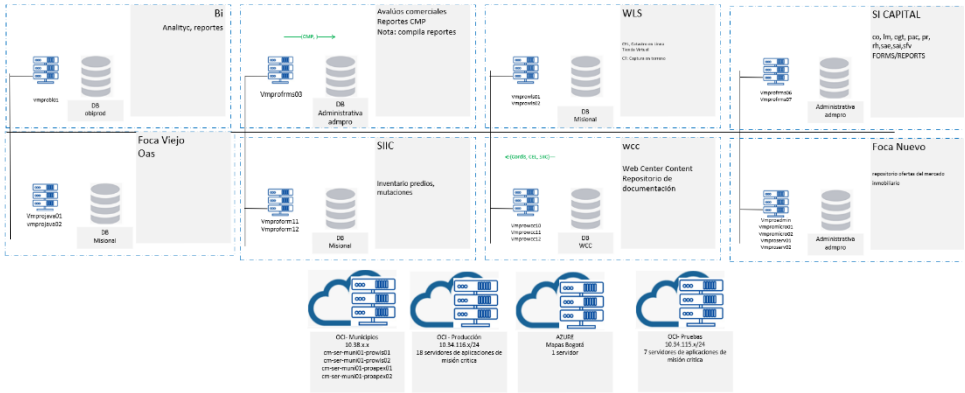


Ilustración 46. Servidores en nube

Las aplicaciones desplegadas son:

1. **SIIC - Sistema Integrado de Información Catastral.**
    1. Sistema misional de Catastro Distrital, diseñado para mantener actualizado el inventario de predios del Distrito Capital, manejo de nomenclatura, radicación de trámites de los ciudadanos, entre otros.
2. **SI CAPITAL - Sistema de Información Administrativo.**
    1. Es una herramienta informática integrada por componentes administrativos, financieros, tributarios y pensionales.
    2. SFV, TRC, Predis, Cordis, facturación, libro mayor, Perno nomina, etc.
    3. ERP (Enterprise Resource Planning).
3. **CEL – Catastro en Línea**
    1. A través de los Servicios en línea los ciudadanos y/o diferentes usuarios podrán generar certificados catastrales y certificados de poseer o no vivienda y en general conocer la información de su predio.
4. **Tienda Virtual:**
    1. portal para venta de servicios: mapas, información alfanumérica catastral, manzanas.
5. **Corec:**

    1. Sistema de consulta predial del ejército para asuntos de la vivienda militar.

6. **APEX:**
    1. Aplicación para el manejo de aplicaciones de avaluos comerciales.
7. **CT: Captura en terreno**
    1. Se usa para mantener actualizado el Censo Predial
8. **Servicios de interoperabilidad:**
    1. **VUC:** Ventanilla Única del Constructor.
9. **BI (generador de reportes)**
10. **Foca Viejo – OAS:**
    1. Ofertas Inmobiliarias para tramite de cálculo de avalúos
11. **WCC: Web Center Content**
    1. Repositorio de documentación.
12. **Foca Nuevo:**
    1. repositorio ofertas del mercado inmobiliario (para cálculo de avalúo anual)
13. **Avalúos Comerciales y reportes**

Capa Media ArcGIS

En la entidad se cuenta con un sistema de ArcGIS Enterprise, que es el software fundacional del SIG y es la base técnica de las funciones de representación cartográfica, visualización, análisis y administración de datos. Se trata de la columna vertebral de la ejecución del conjunto de aplicaciones Esri y sus propias aplicaciones personalizadas. La colaboración y la flexibilidad son elementos claves de ArcGIS Enterprise y le permiten organizar y compartir su trabajo en cualquier dispositivo en todo momento y lugar.

Los cuatro componentes de ArcGIS Enterprise cooperan entre sí para proporcionar una completa funcionalidad de representación cartográfica en la red, explotación de imágenes, manejo de datos en tiempo real, análisis de lotes de gran volumen y ciencia de datos espaciales:

ArcGIS Server potencia la representación cartográfica y el análisis en su SIG, también con varios roles de servidor especializados, y se escala dinámicamente para soportar el tráfico.

El portal de ArcGIS Enterprise es el nodo central en el que los usuarios crean, comparten y administran mapas, aplicaciones y datos espaciales y los comparten con sus colaboradores.

ArcGIS Data Store proporciona almacenamiento de datos para el servidor de alojamiento utilizado con su implementación.

ArcGIS Web Adaptor integra ArcGIS Server y Portal for ArcGIS con sus servidores web existentes y su infraestructura de seguridad de su organización.

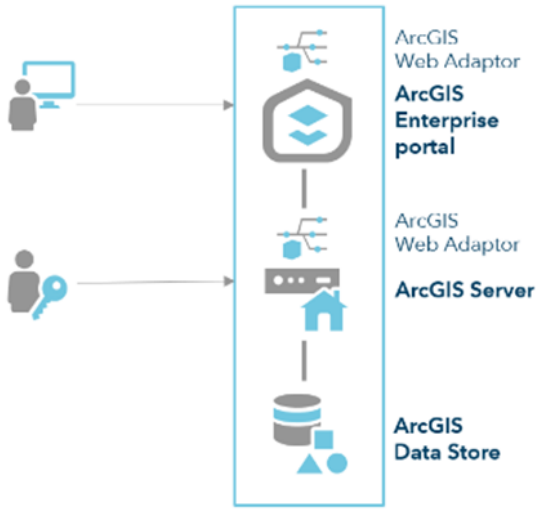


Ilustración 47. Componentes de ArcGIS Enterprise

Actualmente la entidad cuenta con tres (2) ambientes de Arcgis Enterprise con sus respectivos portales para ArcGIS, Azure y OCI a continuación, se describen los diferentes sistemas

OnPremise

En Onpremise se tiene un (1) servidor de licencia de ArcGIS encargado de suministrar licencias a Catastro Bogotá, a continuación, se describen las cantidades actuales.

Tipo Licencia	Total
ArcGIS pro advanced	2
City engine	5
Desktop advanced	225
3D analyst desktop	20
3D analyst pro	10
arcstorm	225
arcstormEnable	225
Data Interoperability Desktop	3
Data Interoperability pro	3
Data reviewer	90
Data reviewer pro	10
Geostatical Analyst Desktop	5
Geostatical Analyst pro	10
Plotting	225
Production Mapping	100
Publisher	6
Spatial Analyst Desktop	20
Spatial Analyst Pro	10
TIFFLZW	225
Workflow Manager	100
Workflow Manager Pro	11

Portal Azure

Compuesto por once (8) servidores distribuidos de la siguiente forma:

- Un (1) servidor de Portal.
- Un (1) servidor de Web Adaptor, encargado de distribuir las cargas.

- Tres (2) servidores en clúster de Arcgis Server.
- Dos (2) servidores en clúster de otros servicios.
- Un (1) servidor de ArcGIS Image.

Son los encargados de soportar la operación de catastro Bogotá en nube. Así mismo se encargan de contener todos los servicios de Mapas Bogotá expuestos a entidades externas y para consumo interno de los usuarios.

Además, se tiene un (1) servidor de Arcgis Monitor para realizar el correspondiente monitoreo de todos los servers de Enterprise, se monitoreo tanto servicios como Hardware del sistema.

Portal OCI

Compuesto por servidores distribuidos de la siguiente forma:

- Dos (2) servidores de Portal.
- Dos (1) servidores de Hosting site.
- Dos (1) servidores de parcel.
- Dos (1) servidores de Image.
- Dos (2) servidores de Data Sore Relacional.
- Dos (2) servidores de Data Sore Cache.

Son los encargados de soportar la operación de Catastro Multipropósito en todos los Territorios.

En OCI también se cuenta con un (1) servidor de licencia de ArcGIS encargado de suministrar licencias a CM, a continuación, se describen las cantidades actuales

Tipo Licencia	Total	Disponible
Pro Advanced	260/780	780
Data reviewer	260/780	780
Workflow Manager	260/780	780

Así mismo se cuenta con 260 licencias de Creator y 40 de Viewer en Portal, a continuación, se hace una descripción de las características de las cuentas

Creator: los Creators pueden crear y editar contenido como, por ejemplo, mapas y aplicaciones, realizar análisis espaciales utilizando las herramientas de análisis, recopilar datos y colaborar y compartir contenido para su uso en aplicaciones. Los Creators tienen acceso a una selección de

aplicaciones, pueden ver el contenido creado por otros miembros de la organización y pueden administrar usuarios y contenido de la organización. El tipo de usuario Creator es una buena opción para especialistas en SIG, administradores de activos, periodistas de datos y otros creadores de contenido y colaboradores.

Viewer: los Viewers pueden ver los elementos que otros usuarios de ArcGIS comparten con ellos y pueden acceder a una selección de aplicaciones. Este tipo de usuario es ideal para miembros de una organización que necesitan ver contenido de ArcGIS en un entorno seguro. Viewers no pueden crear, editar, compartir ni realizar análisis en elementos ni datos.

ArcGIS Online

Por otro lado, también se cuenta con dos (2) portales de Arcgis Online, unos para IDECA y otro para Catastro Bogotá la cual es una solución de representación cartográfica y análisis basada en la nube. Se utiliza para crear mapas, analizar datos, compartir y colaborar.

ArcGIS Online incluye todo lo necesario para crear mapas web, crear escenas web 3D, crear aplicaciones web y crear notebooks. A través de Visor de mapas, Map Viewer Classic y 3D Scene Viewer, se puede acceder a una galería de mapas base y estilos inteligentes para explorar y visualizar los datos. También tiene acceso a plantillas y widgets para crear aplicaciones web que puede publicar en ArcGIS Online. Es muy fácil compartir contenido con usuarios de dentro y fuera de la entidad. Se Pueden configurar grupos privados y solo por invitación, o grupos públicos abiertos a todo el mundo. También puede entablar colaboraciones con otras organizaciones para compartir y trabajar fácilmente con el contenido de la otra.

ArcGIS Online también brinda diferentes tipos de licencias de ArcGIS Pro Basic, estándar y Advance el cual es a aplicación SIG de escritorio profesional con plenas funcionalidades de Esri. Con ArcGIS Pro, se puede explorar, visualizar y analizar datos, crear mapas 2D y escenas 3D.

También cuenta con Los tipos de usuario determinan el acceso a las aplicaciones incluidas y las licencias complementarias compatibles como los son:

Creator: los Creators pueden crear y editar contenido como, por ejemplo, mapas y aplicaciones, realizar análisis espaciales utilizando las herramientas de análisis, recopilar datos y colaborar y compartir contenido para su uso en aplicaciones. Los Creators tienen acceso a una selección de aplicaciones, pueden ver el contenido creado por otros miembros de la organización y pueden administrar usuarios y contenido de la organización. El tipo de usuario Creator es una buena opción para especialistas en SIG, administradores de activos, periodistas de datos y otros creadores de contenido y colaboradores.

Editor: Editors pueden ver y editar datos en mapas y aplicaciones de ArcGIS que otros usuarios de ArcGIS compartan con ellos. Este tipo de usuario es ideal para usuarios que necesitan acceder y editar datos compartidos con ellos y se incluye acceso a una selección de aplicaciones.

Mobile Worker: los Mobile Workers pueden ver y editar datos que otros usuarios de ArcGIS hayan compartido con ellos y tener acceso a una selección de aplicaciones. Este tipo de usuario es ideal para usuarios que principalmente interactúen con contenido de ArcGIS a través de aplicaciones de campo.

Viewer: los Viewers pueden ver los elementos que otros usuarios de ArcGIS comparten con ellos y pueden acceder a una selección de aplicaciones. Este tipo de usuario es ideal para miembros de una organización que necesitan ver contenido de ArcGIS en un entorno seguro. Viewers no pueden crear, editar, compartir ni realizar análisis en elementos ni datos.

Infraestructura de seguridad informática

Actualmente la UAECD cuenta con una infraestructura de seguridad informática, que permite la protección de la información y de los componentes informáticos que generan estos datos, información primordial estratégicas y misionales de la Entidad. Esta infraestructura de seguridad permite asegurar la autenticación, confidencialidad y disponibilidad de la información, además de asegurar el cumplimiento a los lineamientos en temas de seguridad de la información.

A continuación, el esquema general de la infraestructura de seguridad informática de la UAECD.

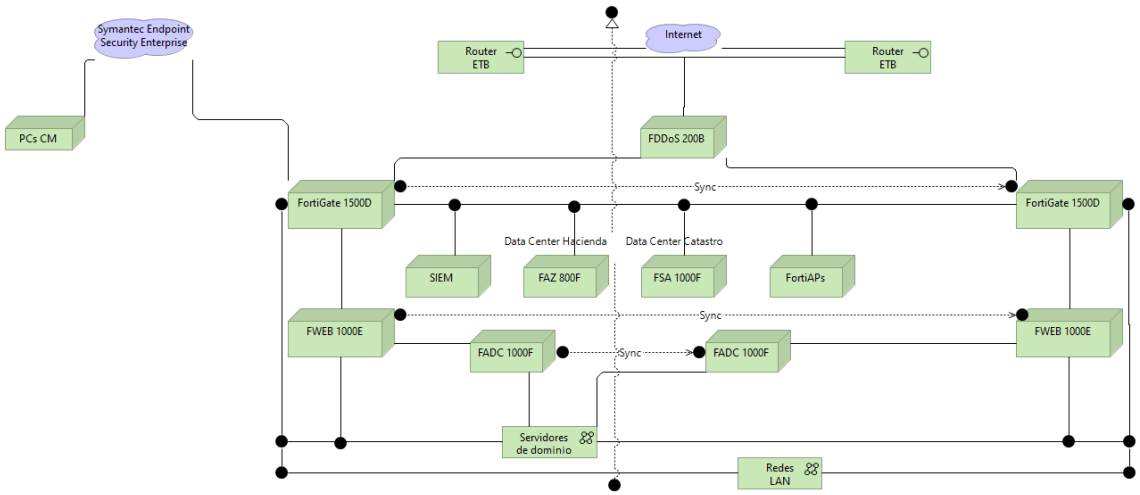


Ilustración 48 Esquema de Seguridad Informática UAECD

En la gráfica anterior nótese que los Servidores de Dominio que se mencionan aún subsisten en On-Premise, son algunos controladores de dominio, DNS y NTP. Esto debido a la contingencia de paso a la nube OCI por daño de la PCA de junio de 2023, por tal razón los servidores de aplicaciones y bases de datos, casi que en un 99% están ya en dicha infraestructura de nube.

De acuerdo con las amenazas que exponen y evolucionan frecuentemente, se mantiene una infraestructura que previene en un alto grado estas amenazas, apoyados con procedimientos, procesos y recurso humano, se encuentra conformada por los siguientes componentes:

- FIREWALL

El firewall es un dispositivo de seguridad el cual tiene funcionalidad controlar el tráfico entre diferentes redes mediante políticas de acceso, su función es permitir o denegar las conexiones entre las diferentes redes estableciendo un control a nivel de capa de red y de transporte.

El firewall implementado en la UAECD es de próxima generación, que cuenta con funcionalidades más avanzadas utilizando controles en todas las capas del modelo OSI, así que permite filtrar tráfico a nivel de dispositivo, autenticación de usuarios, perfiles de seguridad como IPS, WebFilter, Application Filter y como gateway VPN.

La Unidad cuenta con dos (2) Firewalls físicos en la infraestructura de la UAECD, que permiten la creación de hasta 10 firewalls virtuales o VDOMS. De acuerdo con las necesidades de la Unidad, se crearon 4 firewalls virtuales: Aplicaciones, Interno, Base de Datos y Perimetral, cada uno encargado de mantener políticas de acuerdo con su función.

La unidad cuenta con un Firewall virtualizado en Azure, el cual protege la infraestructura con que cuenta la UAECD en la nube de Microsoft y un Firewall virtualizado en Oracle Cloud Infrastructure OCI, el cual protege las infraestructuras de Catastro Multipropósito y DRP.

Los firewalls se encuentran distribuidos de la siguiente manera:

a. Dos (2) firewalls Fortigate 1500D, uno ubicado en el centro de cableado de la UAECD del piso 2 de la torre B. y el otro en el centro de Cómputo de Hacienda, piso 2.

c. Un (1) firewall FortiGate FGT-VM04 ubicado en la nube Azure.

c. Un (1) firewall FortiGate FGT-VM04 ubicado en la nube de Oracle Cloud Infrastructure - OCI.

- FIREWALLS DE APLICACIÓN

El firewall de aplicación es una plataforma de propósito específico, para proteger las aplicaciones WEB de todos los vectores de ataque y amenazas hacia la capa de aplicación, puede detectar vulnerabilidades a nivel de aplicación y proteger mediante análisis especifico, métodos, y controles.

Actualmente la Unidad cuenta con dos plataformas Firewall de Aplicación en alta disponibilidad para la protección de las aplicaciones WEB soportadas en la infraestructura on premise de la entidad, así como también, se cuenta con un Firewall de Aplicación para la protección de las aplicaciones WEB soportadas en la infraestructura de Azure y en la infraestructura Oracle (OCI) de la UAECD.

a. Un (1) firewall de aplicaciones Fortiweb 1000E ubicado en el centro de cableado del piso 2 de la torre B.
b. Un (1) firewall aplicaciones Fortiweb 1000E ubicado en el data center del piso 2 de la torre A.
c. Un (1) firewall Fortiweb FWB-VM04 ubicado en la nube Azure.
d. Un (1) firewall Fortiweb FWB-VM04 ubicado en la nube OCI.

Próximamente el balanceo de aplicaciones que se hace en los Forti ADCs on-Premise, se hará en los propios WAFs de OCI debido al paso de nube que tuvo que hacer la Entidad en junio de 2023 por contingencia de la PCA.

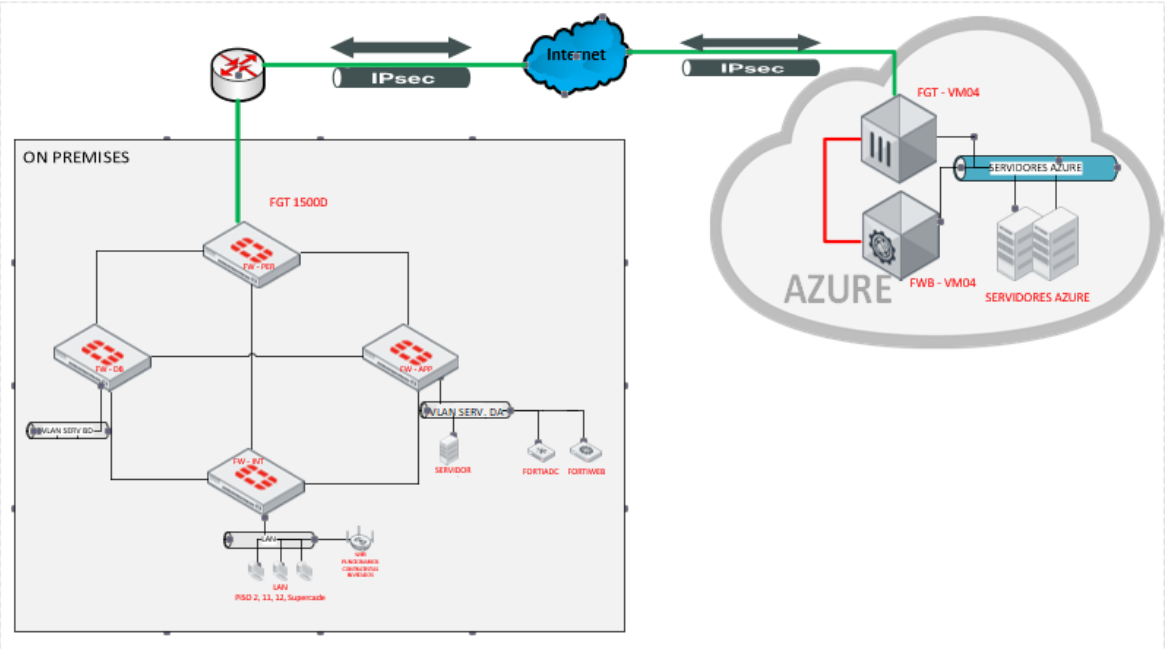


Ilustración 49. Esquema de Seguridad Informática UAECD en Azure

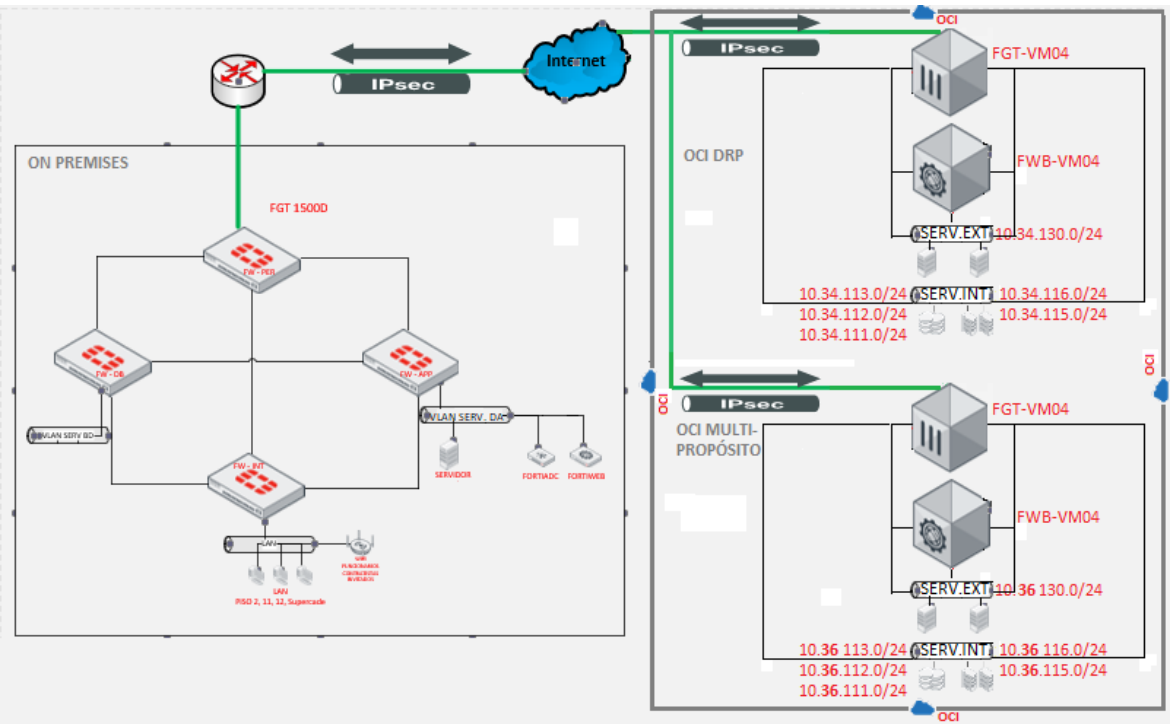


Ilustración 50. Esquema de Seguridad Informática UAECD en OCI

SIEM

La plataforma SIEM nos permite realizar dos actividades claves que apoyan la seguridad de la UAECD, es el monitoreo de red que permite preventivamente detectar comportamientos anormales en las plataformas de la infraestructura tecnológica y los servicios soportados, el segundo es el monitoreo y correlación de eventos de seguridad que ayudan a evidenciar de forma preventiva situaciones de riesgo, como accesos no autorizados, comportamientos anómalos, intentos para aprovechar vulnerabilidades mediante la recolección, tratamiento y análisis de los eventos generados por los activos de información de la Entidad.

La UAECD cuenta con una plataforma virtual SIEM, que está implementándose en la nube OCI, la cual será configurada para recolectar los eventos de los equipos de infraestructura tecnológica de la UAECD. Actualmente la entidad, cuenta con 150 licencias para monitorear diferentes activos de configuración como: equipos de red, servidores (Linux y Windows), equipos de seguridad informática, entre otros.

- ANTIVIRUS

La UAECD cuenta dentro de su arquitectura de seguridad con el software de antivirus SYMANTEC/BROADCOM, el cual fue adquirido el 18 de agosto de 2011 mediante contrato de

compraventa 389 de 2011 y cada año se ha venido renovando y actualizando. El antivirus es la herramienta cuyo objetivo es detectar y eliminar los virus que se puedan atacar la red de la Unidad en los equipos de usuario final o servidores en los sistemas operativos actuales, este sistema de antivirus no solo busca detectar los virus sino bloquearlos, desinfectar y prevenir su reproducción en otras máquinas, son capaces de reconocer malware, spyware, rootkits entre otros. La actual consola de administración del antivirus está en la nube de Symantec.

- BALANCEADORES DE CARGA

Un balanceador de carga propende por el equilibrio de tráfico de carga de los diferentes servidores de una entidad, que generalmente prestan al mismo servicio. El balanceo de carga tiene como objetivo optimizar el uso de recursos, mejorar el rendimiento, disminuir los tiempos de respuesta, proporcionar redundancia y evitar la sobrecarga de cualquier servidor individual. El uso de múltiples componentes con balanceo de carga en lugar de un solo componente aumenta la fiabilidad y la disponibilidad a través de la redundancia.

Dentro de sus funciones actuales en la UAECD, los balanceadores se configuran con direcciones IPs virtuales a manera de servidores virtuales, los cuales distribuyen las conexiones entre diferentes servidores físicos o “pool members” según la configuración establecida con el fin de tener disponibilidad en el acceso a las aplicaciones y el enmascaramiento de los recursos de los servidores físicos como puertos e IPs internas, garantizando la seguridad de los mismos ya que lo visible hacia internet o extranet es solo el servidor virtual.

Como se muestra en la Ilustración del esquema de seguridad informática UAECD los balanceadores de carga FortiADCs intervienen en la capa de aplicaciones actualmente, realizando balanceo a las aplicaciones de ambientes de producción, pruebas y desarrollo.

Próximamente este balanceo se hará en los propios WAFs de OCI debido al paso de nube que tuvo que hacer la Entidad en junio de 2023 por contingencia de la PCA.

- SISTEMA ANTI DDoS

Los ataques de denegación de servicio distribuido (DDoS) son una subclase de los ataques de denegación de servicio (DoS). Un ataque DDoS involucra múltiples dispositivos en línea conectados, conocidos colectivamente como botnet, que se utilizan para abrumar un sitio web objetivo con tráfico falso.

La Entidad cuenta con un FortiDDoS, que es una plataforma de mitigación de DDoS que inspecciona el 100 % de todo el tráfico DNS en ambas direcciones, para protegerse contra todo tipo de ataques DDoS dirigidos hacia o desde servidores DNS. Valida más de 30 parámetros diferentes en cada paquete DNS hasta 12 millones de consultas/segundo.

- SISTEMA Sandbox

Un sandbox es un entorno de prueba aislado que permite a los usuarios ejecutar programas o abrir archivos sin afectar la aplicación, el sistema o la plataforma en la que se ejecutan. Los desarrolladores de software usan sandboxes para probar nuevos códigos de programación. Los profesionales de la ciberseguridad usan sandboxes para probar software potencialmente malicioso.

La Entidad cuenta con FortiSandbox, que es una herramienta de detección que funciona mejor junto con las capacidades de cumplimiento de las capacidades de prevención de amenazas establecidas, como un firewall de última generación (NGFW) o un sistema de gestión unificada de amenazas (UTM), así como una puerta de enlace de correo electrónico seguro o una plataforma de protección de punto final.

- VERSIONES DE SOFTWARE

A continuación, se presentan las versiones actuales de los equipos de seguridad informática y el deber ser, situación que se actualizará en el mantenimiento preventivo del 6 de diciembre de 2023.

APPLIANCE / SOLUCIÓN	VERSIÓN ACTUAL	VERSIÓN IDEAL ESTABLE
Fortigate Azure	7.0.10	7.0.13
Fortigate OCI	7.0.10	7.0.13
Fortigate On-Premise	7.0.10	7.0.13
FortiAnalyzer	7.2.2	7.2.4
FortiWeb Azure	7.0.3	7.0.9
FortiWeb OCI	7.0.5	7.0.9
FortiWeb On-Premise	7.0.5	7.0.9
FortiSandbox	4.2.3	4.2.6
FortiDDoS	5.5.1	5.7.1
FortiADC	7.0.5	7.2.3
FortiAP	6.4.9	6.4.9
FortiGSLB	23.4	23.4

- RIESGOS ALTOS

La Entidad carece de un SOC (Centro de Operaciones de Seguridad) que tiene por fin supervisar y responder a amenazas de seguridad en tiempo real, utilizando tecnologías avanzadas y análisis de

datos para proteger una infraestructura. Tampoco cuenta con un SOAR (Automatización y Orquestación de Respuesta de Seguridad) que es una plataforma que automatiza y coordina las acciones de respuesta a incidentes de seguridad, mejorando la eficiencia operativa y permitiendo una gestión más rápida y efectiva de las amenazas. Ambos desempeñan un papel crucial en fortalecer la postura de seguridad de una organización. La implementación de estas soluciones recae directamente sobre las directivas que deberían ser conscientes de la utilidad de las mismas y destinar los recursos para su implementación.

En lo relativo a la arquitectura de nube OCI, hasta que no se rediseñe esta, habrá ciertas máquinas que pueden ser vulnerables por no estar integradas en la visibilidad del sistema de logs del FortiAnzalyzer y protección de firewalls en general. Esto porque el paso de On-Premise a nube fue intempestivo y se tuvo que volver el DRP, producción.

La entidad llevó a cabo, en el año 2022, un contrato de consultoría especializada en análisis de vulnerabilidades y ethical hacking. Este contrato tuvo como objetivo principal la identificación de vulnerabilidades mediante pruebas de Ethical Hacking, tanto en entornos externos (activos expuestos a internet) como internos. Estas pruebas se realizaron sobre los activos de información de la UAECD, tal como se detalla en la Tabla de Activos de Información por analizar.

El propósito fundamental de estas acciones fue evaluar el estado de seguridad de la información almacenada y procesada a través de la plataforma tecnológica de la entidad, abarcando tanto el hardware como el software. Se utilizaron herramientas especializadas para llevar a cabo la revisión de vulnerabilidades, con el objetivo de identificar de manera oportuna posibles fuentes de incidentes de seguridad.

Tabla. Tabla de Activos de Información por analizar

Activo de Información	Cantidad	Análisis de Vulnerabilidades	Ethical Hacking
Directorio Activo	1	X	X
Bases de Datos de Oracle	3	X	X
Aplicativos expuestos en internet	3	X	X
Aplicativos locales (WEB)	2	X	X
Firewall	4	X	X
Componentes activos de seguridad	5	X	X

Componentes activos de la red	15	X	X
Servidores con S.O Windows	70	X	X
Servidores con S.O Linux	90	X	X
Computadores de Usuarios Finales	150	X	
Portal Web (Por dominio)	4	X	X
Servidor de Impresión	1	X	X
Impresoras	20	X	
Red Wifi	1	X	X

En la fase inicial de la consultoría, se identificaron vulnerabilidades en los activos de información de la Subgerencia de Infraestructura Tecnológica, clasificadas según su criticidad:

Critica	Alta	Media	Baja
24	**123**	**339**	**102**

Una vez halladas estas vulnerabilidades, se realizó una remediación y un retest para validar que el plan de trabajo fuera efectivo se realizó un retest, obteniendo como resultado:

Critica	Alta	Media	Baja
22	**105**	**323**	**102**

Después de llevar a cabo y aplicar los planes de remediación en las diversas capas de la (SIT), se ha identificado lo siguiente:

En primer lugar, algunas vulnerabilidades no podrán ser abordadas, ya que las aplicaciones instaladas en varios servidores son de tipo Legacy. En consecuencia, no es posible actualizar la versión, ya que esto afectaría el correcto funcionamiento de la aplicación.

Critica	Alta	Media	Baja
3	**6**	**9**	**0**

Por otro lado, se han identificado vulnerabilidades que actualmente están siendo sometidas a análisis por las capas correspondientes. Por lo que se está evaluando detalladamente los planes a implementar.

Critica	Alta	Media	Baja
10	7	55	0

Cloud Security Assessment – Microsoft

La UAECD realizó una Evaluación de Seguridad para los servicios de la nube Azure y Office 365, llevada a cabo por expertos de Microsoft. Este análisis abarcó la evaluación de pilares fundamentales, tales como identidad, dispositivos, datos, aplicaciones, infraestructura y redes.

Los resultados de la evaluación revelaron el estado actual de los pilares examinados, siendo:

Pilar	Hallazgos	Nivel de riesgo
Identidad	• Usuarios con actividad de riesgo. • Alertas de seguridad activas en niveles medios y altos. • Falta de controles de seguridad avanzados.	Alto
Dispositivos	• Dispositivos con Riesgo de Ransomware. • Uso de Sistemas Operativos fuera de Soporte.	Medio
Datos	• Archivos con Malware dentro de las carpetas de usuarios. • •No herramienta de DLP.	Alto
Aplicaciones	• Uso de aplicaciones con niveles de permisos altos. • Software instalado con niveles críticos de vulnerabilidades.	Alto
Infraestructura	• Uso de Sistemas Operativos fuera de Soporte. • Controles de acceso básicos a la capa de infraestructura.	Medio
Redes	• Puertos administrativos expuestos accesos no autorizados.	Medio

Infraestructura de Sistema de Copias de Respaldo

La UAECD cuenta con una librería de backups (componente físico), mediante la cual se asegura la disponibilidad de la Información realizando copias de respaldo de ésta en cinta magnética utilizando las herramientas de software HP Data Protector y Veeam Backup (componentes lógicos), los cuales permite fortalecer la capa de seguridad transversal que soporta todos los componentes de la infraestructura. En resumen, los componentes del sistema de copias de respaldo son:

- Componente Físico: Librería StorageTek SL 150 Firmware Version 3.72
- Componente lógico: Software DATAPROTECTOR v 10.60
- Componente lógico : Software Veeam Backup v11

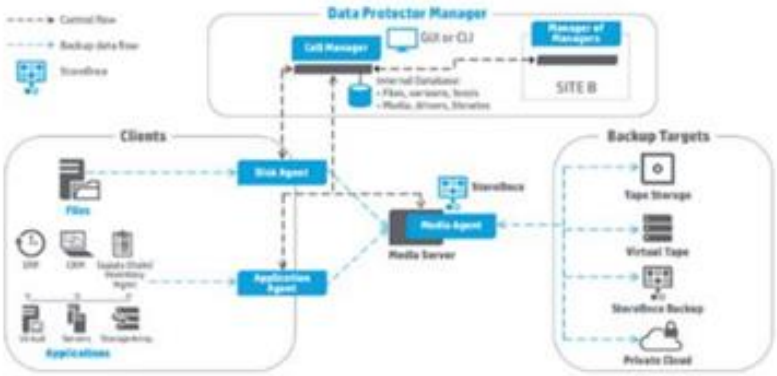


Ilustración 51. Infraestructura de Sistema de Copias de Respaldo

No contar con esta herramienta podría materializar el riesgo de pérdida de información por la ocurrencia de fenómenos imprevistos como desastres naturales, incendio y terrorismo, lo que afectaría el cumplimiento normal de los objetivos misionales de la UAECD por estas razones, se hace indispensable contar con el soporte técnico y mantenimiento preventivo y correctivo de las herramientas de gestión de copias de respaldo de los activos de información de la UAECD y de esta manera garantizar a todos los usuarios internos y externos, la disponibilidad y la continuidad en la prestación de los servicios tecnológicos.

7.5.3 Inventario de la infraestructura tecnológica

Durante la vigencia 2021, se realizó para la actualización del inventario de infraestructura, las siguientes acciones:

- Ajuste del procedimiento de gestión de configuración, cuyo objetivo es realizar el registro, actualización y/o eliminación de la información de los recursos tecnológicos de la Unidad en la base de datos de configuración – CMDB (Por sus siglas en inglés Configuration Management Database), en el marco de las mejores prácticas de ITIL® (Information Technology Infrastructure Library)
- Depuración del inventario de infraestructura de TI
- Dos actualizaciones (Mayo y Septiembre) de los recursos tecnológicos en la CMBD, teniendo en cuenta los atributos definidos en el inventario inicial del 2020. Para este ejercicio estableció una estructura de familia y clases de recursos tecnológicos, con un(os) responsable(s) por cada componente. Dicha estructura fue la siguiente:

Clase	Responsable
Servidores	Eibin Fabian Acosta y Milton tovar
Capa media	Hermes Ramirez A, Jairo Iván Monroy, Aldemar Guzmán, Mauricio García, William Tarazona.
Bases de datos	Monica Chacon, Carlos Vivas y Jorge Blanco
Redes y comunicaciones, switches, sw de redes	Alexander Gutierrez y Jhon Mack
Seguridad informática	José Ignacio Saavedra y Luisa Barragán
UPS	Alexander Gutierrez y Jhon Mack
Aires acondicionados (los del centro cableado)	Pablo Pacacira y Sergio Peña

Adicionalmente, se dispone de un documento que relaciona el uso de tecnologías emergentes en los servicios que se están implementando en catastro multipropósito, el cual se encuentra ubicado en:

https://catastrobogotacol.sharepoint.com/:f:/s/GerenciaTecnologa-GOBIERNODIGITAL/EtjfvhYsDV9Hh7aiXTs819IB8CxXlNLq54ciF_TN49_L1A?e=nx7HWQ

En el 2022 se continuo la actualización teniendo en cuenta las nuevas instalaciones de Catastro Multipropósito Territorial.

7.5.4 Recuperación y disponibilidad en la Operación

d. Redundancia y alta disponibilidad.

La infraestructura tecnológica de la UAECD cuenta con un esquema de redundancia y alta disponibilidad a nivel de los componentes que soportan los principales servicios de la Unidad, en este sentido, se cuenta con esquemas de alta disponibilidad a nivel de: Firewalls, Switches de Core, Balanceadores de carga, bases de datos e infraestructura de virtualización para procesamiento.

Adicionalmente, los servicios críticos se soportan, siempre, sobre más de un servidor virtualizado, generando un único servidor virtual para la prestación del servicio a través del balanceador de cargas, esta configuración proporciona un esquema de redundancia a nivel de las aplicaciones, permitiendo continuar con la prestación de un servicio a pesar de que exista alguna falla o mantenimiento en uno de los componentes que lo integran.

e. Recuperación ante desastres.

La UAECD cuenta con mecanismos de recuperación de la infraestructura de TI a través de un PLAN DE RECUPERACION ANTE DESASTRES (DRP) mediante un Centro Alterno de Procesamiento el cual está disponible en la NUBE mediante un contrato con la firma ORACLE. Igualmente cuenta con un plan de copias de respaldo cuya ejecución está de acuerdo con la periodicidad identificada por los dueños de los datos y de los administradores de plataforma. Además, se cuenta con un tercero que facilita el almacenamiento y transporte seguro de las copias de respaldo a un sitio externo de la entidad.

f. Escalabilidad

La UAECD cuenta con una infraestructura tecnológica de servidores que se soportan sobre una plataforma de virtualización, lo cual permite realizar la asignación o redistribución de recursos de cómputo a nivel de servidores de forma ágil; de esta forma es posible: crear nuevos servidores virtuales a partir de plantillas definidas, aumentar o disminuir los recursos de cómputo asignados a los servidores existentes de acuerdo con la demanda de los servicios que estos soportan y eliminar servidores que ya no estén en uso para liberar los recursos utilizados.

Adicionalmente, los recursos asignados a la plataforma de virtualización (servidores físicos y almacenamiento) se pueden incrementar fácilmente expandiendo la capacidad de cómputo con la que actualmente se cuenta mediante la introducción de nodos de cómputo y capacidad de almacenamiento, adicional al hardware existente, sin que sea necesario realizar una migración o reconfiguración de los servicios tecnológicos.

g. Monitoreo

La unidad cuenta con un sistema de monitoreo el cual permite controlar el uso adecuado de los componentes de la infraestructura tecnológica a través de la herramienta FortiSiem controlando los umbrales definidos en cada elemento de la IT

Toda la Infraestructura tecnológica cuenta con soporte y mantenimiento de sus componentes a través de contratos con terceros el cual renueva anualmente garantizando así la disponibilidad de todos los componentes de la infraestructura

Las políticas, procesos, procedimientos e indicadores relacionadas con la continuidad y disponibilidad de la operación se describen en los siguientes numerales de este documento:

- POLÍTICA DE COPIAS DE RESPALDO Y RECUPERACION
- Proceso Gestión Integral del Riesgo – Subproceso Gestión de Continuidad
- Gobierno de TI en el Sistema de Gestión de Continuidad de Negocio – SGCN
- Indicadores de gestión del Subprocesos Gestión de continuidad de la Información

La programación mantenimientos preventivos de los recursos tecnológicos para la vigencia 2020 se encuentra publicado en el repositorio: Gerencia de Tecnología/Gobierno Digital/1. Arquitectura/Modelo de Gestión y Gobierno de TI/Dominio de Gobierno de TI.

7.5.5 Disposición de residuos tecnológicos

Dentro de la responsabilidad que tiene Catastro Bogotá con la protección y preservación del medio ambiente, y en cumplimiento de los postulados constitucionales y legales que regulan su manejo, tiene definida la política ambiental aplicable en todos los niveles de la organización y en los procesos de su cadena de valor a desarrollar, así como las siguientes buenas prácticas:

Política ambiental de Catastro Bogotá

La Política Ambiental de la Unidad se encuentra articulada e integrada a la Política del Sistema de Gestión Integral: establece el compromiso de prevención de la contaminación, mitigación y/o compensación de los impactos ambientales y la protección del medio ambiente.

Plan Institucional de Gestión Ambiental PIGA

El Plan Institucional de Gestión Ambiental - PIGA "Es el instrumento de planeación que parte del análisis de la situación ambiental institucional, con el propósito de brindar información y argumentos necesarios para el planteamiento de acciones de gestión ambiental que garanticen primordialmente el cumplimiento de los objetivos de Ecoeficiencia establecidos en el Decreto 456 de 2008, entre otras acciones ambientales que contemplen las entidades y aporten al cumplimiento en su totalidad de los objetivos ambientales establecidos en el Plan de Gestión Ambiental – PGA establecido para el Distrito Capital." (Secretaría Distrital de Ambiente SDA-2016).

Por lo anterior, la Unidad Administrativa Especial de Catastro Distrital – UAECD en razón de la implementación del Plan Institucional de Gestión Ambiental – PIGA, ha llevado a cabo un ejercicio de planificación que parte de un análisis descriptivo e interpretativo de la situación ambiental de la entidad, su entorno, condiciones ambientales internas y de la gestión ambiental en su área de influencia para plantear los programas, proyectos, metas y asignación de los recursos que permitan alcanzar objetivos de Ecoeficiencia y mejoramiento ambiental; y a su vez propender porque el plan, sea un instrumento de consulta para los servidores de la entidad, la comunidad en general, y a su vez ofrezca a las autoridades ambientales y de control los elementos necesarios para llevar a cabo sus acciones de control y seguimiento.

Programa para la Gestión de residuos tecnológicos:

La Unidad Administrativa Especial de Catastro Distrital – UAECD, es la entidad oficial encargada de las actividades relacionadas con la formación, conservación y actualización del inventario de los bienes inmuebles situados dentro del Distrito a partir del estudio de sus elementos físico, económico y jurídico; es por ello que en su quehacer adquiere y hace uso de múltiples elementos tecnológicos, como es el caso de equipos de cómputo y sus periféricos, que una vez finalizada su vida útil se convierten para la entidad en residuos tecnológicos, también denominados residuos de aparatos eléctricos y electrónicos; motivo por el cual se requiere hacer una gestión ambientalmente adecuada de los mismos, la cual se inicia desde el mismo proceso de planeación de las adquisiciones, hasta la entrega a título gratuito de los equipos en de uso o dado el caso la entrega a gestor ambiental autorizado para procesos de aprovechamiento, valorización, reciclaje y/o disposición final.

Aunado a lo anterior y dados los grandes retos que tiene la ciudad en cuanto a la Gestión Integral de Residuos de Aparatos Eléctricos y Electrónicos - RAEEs, se dispone del Programa para la Gestión de los Residuos Tecnológicos de la UAECD, con el fin de que obre como directriz para la implementación de acciones que propendan por la gestión ambiental adecuada de estos residuos.

El Programa para la Gestión de los Residuos Tecnológicos generados por la Unidad Administrativa Especial de Catastro Distrital – UAECD, busca realizar la gestión ambientalmente adecuada y el manejo integral de los residuos tecnológicos en su componente, equipos de cómputo, procurando su minimización, reutilización, aprovechamiento, tratamiento, reciclaje y/o disposición final de éstos, mediante la implementación de compras sostenibles, cumplimiento de criterios de sustentabilidad ambiental, uso adecuado de los equipos adquiridos para prolongar su vida útil, mediante esquemas de mantenimiento, reparación y reúso de los mismos; y promoviendo en los colaboradores de la entidad el cumplimiento de sus responsabilidades como consumidores conllevando a un adecuado manejo de los residuos tecnológicos tanto internos como externos.

El documento que describe el programa para la Gestión de los Residuos Tecnológicos se encuentra en el siguiente enlace: https://www.catastrobogota.gov.co/sobre-catastro/gestion-ambiental

El documento consta de capítulos, los cuales conducen paso a paso por los procesos que debe cumplir un consumidor ambiental y socialmente responsable por la adquisición de equipos tecnológicos.

7.5.6 Implementación del Protocolo de Internet versión 6 (IPv6)

En el 2021, la Gerencia de Tecnología terminó el proceso de implementación de adopción de la transición y coexistencia del nuevo protocolo de internet versión 6, para cada uno de los servicios de infraestructura de la Unidad Administrativa Especial de Catastro Distrital, sin afectar el funcionamiento de los servicios en producción, mediante el mecanismo de Dual Stack.

7.6 USO Y APROPIACIÓN

Con el fin de fortalecer el uso y apropiación de TI en el 2023 se definió y ejecutó el plan de comunicaciones de la Gerencia de Tecnología con el siguiente alcance:

1. Estrategia de TI: PETI, Visión TI, Misión TI, Objetivos Estratégicos TI, Políticas de TI, Plan de Transformación Digital, Sitio de la Gerencia de Tecnología, Metodología de la Gerencia de Proyectos y herramientas de apoyo
2. Mesa de Servicios de TI: Catálogo de servicios de TI, conceptos y alcances de la Mesa de Servicios de TI, encuestas de satisfacción, indicadores generales de atención y de satisfacción, base de conocimiento, guía de gestión de accesos de servicios de TI
3. Seguridad de la Información: importancia del Sistema de Gestión de Seguridad de la Información, política general de seguridad, responsabilidades de usuarios y jefes, activos de

información, riesgos /eventos/incidentes de seguridad digital/información, compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología, generación de estándar de contraseñas, mecanismos de cifrado para la protección de datos personales, reportes de alertas o tips de seguridad de la información

4. Continuidad del Negocio: importancia del Sistema de Gestión de Continuidad del Negocio de la Unidad, política de continuidad del negocio, roles y responsabilidades, manual de continuidad de negocio, procedimientos e instructivos, tips y recomendaciones de continuidad del negocio

Adicionalmente, se realizaron las siguientes encuestas:

- Nivel de conocimiento y entendimiento de la Estrategia de TI liderada por la Gerencia de Tecnología
- Nivel de uso y aprovechamiento de los documentos de conocimiento de interés general publicados en la Mesa de Servicios de TI
- Nivel de uso del sitio de la gerencia de tecnología

También se rediseño el sitio de la Gerencia de Tecnología para facilitar el acceso a su información y así avanzar en la estrategia de uso y apropiación de TI. También, con el propósito de apoyar la gestión y transferencia de conocimiento entre los funcionarios y contratistas de la UAECD, para lo cual unificamos e integramos información y documentación organizada y clasificada de la Gerencia de Tecnología, a través de tres (3) secciones:

1. Organización y equipos de trabajo de la Gerencia de Tecnología
2. Proyectos y Plan Estratégico de Tecnologías de la Información - PETI
3. Datos e indicadores resultado de nuestra gestión

Para los nuevos funcionarios de la UAECD, en las jornadas de inducción se divulgaron los siguientes temas relacionados con el proceso “Gestión y de desarrollo de las TICs”

1. Gerencia de Tecnología: Funciones, procesos y procedimientos, Catálogo de servicios de TI
2. Subgerencia de Ingeniería de software: Funciones, Sistemas de información y misionales, Sistemas administrativos y de apoyo
3. Subgerencia de Infraestructura Tecnológica; Funciones, Innovación en Infraestructura Tecnológica
4. Gobierno Digital: Evolución y transformación digital, Política de Gobierno Digital, Arquitectura empresarial, Portafolio de proyectos PETI
5. Mesa de Servicios TI
6. Sistema de Gestión de Continuidad del Negocio
7. Subsistema de Gestión de Seguridad y Privacidad de la

Información- Principios de seguridad de la información: Activos de información, Riesgos de seguridad de la información, Políticas de Seguridad de la Información, Suscripción de acuerdos de confidencialidad

7.7 SEGURIDAD DE LA INFORMACIÓN

Con el fin de establecer el estado actual de seguridad de la información de la Unidad, se tomó como referencia el último instrumento (vigencia octubre 2023) para la identificación de la línea base de seguridad de la Unidad. En la siguiente tabla y gráfica se indica el estado actual de implementación de seguridad en la Unidad.

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	82	100	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	88	100	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	89	100	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	81	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	80	100	**GESTIONADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	82	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	85	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	85	100	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	79	100	**GESTIONADO**
A.15	RELACIONES CON LOS PROVEEDORES	80	100	**GESTIONADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	97	100	**OPTIMIZADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	64	100	**GESTIONADO**
A.18	CUMPLIMIENTO	83	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**84**	**100**	**OPTIMIZADO**

Ilustración 52. Brechas Seguridad de la Información

De acuerdo como se muestra en la tabla anterior, la evaluación de efectividad de los controles de los dominios relacionados con criptografía, adquisición, desarrollo y mantenimiento de sistemas de información, relación con los proveedores y aspectos de seguridad de la información de la gestión de la continuidad del negocio que corresponden al 29% de los dominios se encuentran en un nivel gestionado, lo que indica que los controles que se han implementado se monitorean y se realiza medición de éstos.

Por otra parte, el 71% de los dominios (10), que corresponden a las políticas de seguridad de la información, organización de la seguridad, seguridad de los recursos humanos, gestión de activos, control de acceso, seguridad física y del entorno, seguridad de las operaciones, seguridad de las comunicaciones, gestión de incidentes de seguridad de la información y cumplimiento se encuentran en un nivel optimizado, que indica que las buenas prácticas se siguen y automatizan.

Finalmente, y como resultado de la evaluación de la efectividad de los controles, la Unidad se encuentra actualmente en un nivel de madurez general optimizado con un porcentaje del 84%, el cual corresponde de acuerdo con las métricas definidas por el Ministerio de Tecnologías de la Información y las Comunicaciones a que se mantiene un proceso de mejoramiento continuo, retroalimentando cualitativamente el modelo.

En el periodo 2020-2023 se implementaron controles de tipo administrativos y técnicos con el fin de cerrar brechas que se tenían en seguridad la información en la Unidad para fortalecer el Modelo de Seguridad y Privacidad de la información (Sistema de Gestión de seguridad y privacidad de la información). A continuación, se detallan los logros principales.

- ✓ Definición de la política de seguridad y privacidad de la información mediante resolución 732 de 2020.
- ✓ Definición de la política de teletrabajo.
- ✓ Definición de roles y responsabilidades de seguridad y privacidad de la información.
- ✓ Mejoramiento del proceso de gestión de activos de información.
- ✓ Mejoramiento del proceso de gestión de riesgos de seguridad de la información el cual quedo alineado a los riegos de la entidad, conforme con la Guía versión 5 del DAFP.
- ✓ Seguimiento al plan de seguridad y privacidad de la información, incluidos instrumento de seguimiento y generación de nuevos indicadores.
- ✓ Fortalecimiento de los controles de seguridad de la información en la gestión de proyectos
- ✓ Mejoramiento de los procesos de concientización y sensibilización de seguridad y privacidad de la información.
- ✓ Definición de los procesos de organización, etiquetado y gestión de permisos de la información de los procesos.
- ✓ Uso y manejo de la información en repositorios en nube.
- ✓ Fortalecimiento de la infraestructura debido al proceso de gestión de vulnerabilidades y ethical hacking contratado.
- ✓ Implementación de control de ofuscamiento de datos a nivel de bases de datos.
- ✓ Mejoramiento en la documentación generada del proceso de seguridad de la información.
- ✓ Implementación de controles de cifrado.
- ✓ Fortalecimiento del control de borrado seguro de datos.
- ✓ Seguimiento al cumplimiento de los lineamientos de seguridad y privacidad de la información.
- ✓ Fortalecimiento al proceso de gestión de datos personales.
- ✓ Identificación de requerimientos de una herramienta o solución tecnológica que permita gestionar los riesgos de seguridad de la información.
- ✓ Definición inicial de un tablero de control para el seguimiento en la ejecución del plan del Sistema de Gestión de Seguridad de la Información (SGSI)
- ✓ Evaluación de soluciones o nuevos controles de seguridad para evitar la pérdida o fuga de información.
- ✓ Fortalecimiento de controles asociados al dominio de Desarrollo Seguro para el levantamiento de requerimientos técnicos y pruebas no funcionales de seguridad.
- ✓ Fortalecimiento de los controles implementados.
- ✓ Fortalecimiento de la cultura de seguridad de la información.

8 SITUACIÓN OBJETIVO (TO BE)

A continuación, se describe el deber ser o la situación deseada en materia de gestión de TI de la Unidad Administrativa Especial de Catastro Distrital, teniendo en cuenta el Modelo de Gestión y Gobierno de TI de cada uno de los dominios del Marco de Referencia de Arquitectura Empresarial de la Política de Gobierno Digital buscando avanzar a la transformación digital de la entidad.

Se describen las mejoras propuestas con el fin de lograr un modelo de gestión de TI más efectivo, controlado y alineado con las nuevas apuestas estratégicas de la institución, del nuevo Plan Distrital de Desarrollo y de su entorno (sectorial o territorial), con énfasis en lo relacionado con la puesta en operación de los servicios de Catastro Multipropósito tanto en Bogotá como en todo el país, buscando desarrollar una gestión que genere valor a la institución con el aprovechamiento y el buen uso de las tecnologías de la información, en cuanto a contribuir al mejoramiento de su gestión apoyando los procesos para alcanzar una mayor eficiencia y transparencia en su ejecución y brindando información objetiva y oportuna para la toma de decisiones en todos los niveles y a todos los grupos de interés.

8.1 ESTRATEGIA DE TI

8.1.1 Planeación Estratégica de TI

La estrategia de TI debe publicarse y divulgarse permanentemente a través de un plan de comunicación unificado que contemple lo relacionado con la gestión de TI, la operación de TI y el Plan Estratégico de Tecnologías de la Información de la Gerencia de Tecnología

Adicionalmente, se debe continuar con la planeación estratégica siguiendo el modelo de arquitectura empresarial definido en el 2022 y actualizado en el 2023, a nivel corporativo para que se puedan construir las visiones de arquitectura de la totalidad de procesos de negocio que componen la cadena de valor de la UAECD priorizando los procesos de Go Catastral.

Adicionalmente, se deben tener en cuenta las siguientes recomendaciones asociadas a la planeación estratégica de TI y el modelo de arquitectura empresarial:

- La práctica de AE debe ser a nivel institucional no es un objetivo solo de la Gerencia de TI
- Desde la cadena de valor y el mapa de capacidades en versión TO BE (por construir) se deben identificar el listado de brechas corporativas, para ello es recomendado definir en las distintas

dependencias los involucrados que pueden aportar en la construcción de los ejercicios de arquitectura empresarial.

- Actualmente la arquitectura misional no cuenta con brechas propias por consiguiente se debe iniciar ese trabajo a partir del modelamiento de los procesos de negocio en Archimate y sus relaciones con los motivadores, las capacidades, los sistemas de información, la infraestructura y los datos de la UAECD

8.1.2 Servicios de TI

Se recomienda actualizar el catálogo de servicios de TI para facilitar su entendimiento y continuar su socialización.

8.1.3 Directrices y estándares para la gestión de la gobernabilidad de TI

Se deben formalizar y socializar as siguientes nuevas políticas de la Gerencia de Tecnología

- Política de continuidad del negocio
- Políticas de gestión de recursos y servicios tecnológicos
- Políticas de gestión de software
- Política de gestión de proyectos con TI

8.1.4 Tablero de control de TI

Se deben mantener actualizados los tableros de control de la Gerencia de Tecnología y revisar si se pueden automatizar para extraer los datos desde las fuentes originales de información.

8.2 GOBIERNO DE TI

8.2.1 Procesos de Gestión de TI

Se debe garantizar el control periódico en la ejecución del presupuesto de inversiones y gastos de operación de las TIC, incluyendo análisis de costo beneficio posterior a las contrataciones, así como

el análisis del desempeño y capacidad del personal interno y externo de las TIC para evaluar si se cuenta con el personal suficiente e idóneo para hacer una mejor gestión de TI.

Se debe continuar con la optimización y automatización de la gestión de accesos a las diferentes aplicaciones/sistemas de información y servicios de TI administrados por la Gerencia de Tecnología priorizando la delegación de los mismos en el caso que sea viable.

Adicionalmente, con el fin de adoptar las nuevas tecnologías que se están adquiriendo en la entidad, las nuevas necesidades de Catastro Multipropósito y sus nuevos clientes, se deben revisar, mejorar y automatizar los procesos y procedimientos relacionados con gestión de TI y seguridad de la información, incluyendo el paso de Catastro Bogotá al modelo de Catastro Multipropósito.

8.2.2 Planeación, ejecución y gestión de proyectos de TI

Con el fin de mejorar la planeación, ejecución y seguimiento a la gestión de proyectos de TI (Tecnologías de la Información) se propone consolidar y aumentar la adopción de la metodología de gestión de proyectos de TI, desarrollada de acuerdo con lo establecido en la Política de Gobierno Digital, específicamente lo descrito en el Modelo de Gestión de Proyectos TI, de la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Teniendo en cuenta los avances en la implementación de la metodología de gestión de proyectos de TI, realizados durante el 2022 y 2023 y con el fin darle continuidad, así como de mejorar en nivel de madurez se propone lo siguiente:

1. Actualizar metodología de gestión de proyectos teniendo en cuenta los avances realizados en la vigencia 2023 y el Modelo de Gestión de Proyectos de TI - MGPTI, publicado en el mes de mayo de 2023.
2. Continuar mejorando el nivel de madurez en la aplicación y adopción de la metodología en la gestión de proyectos TI, teniendo en cuenta los resultados de la encuesta del nivel de adopción realizada en diciembre del 2023
3. Incluir en la metodología la aplicación de metodologías agiles en la gestión de proyectos de TI.

Se recomienda continuar avanzando en el nivel de madurez de uso y apropiación de la metodología de gestión de proyectos de TI, teniendo en cuenta las conclusiones y recomendaciones de le encuesta realizada en la primera semana del mes de diciembre del presente año, la cual se realizó con el propósito de medir el nivel de madurez de el uso y apropiación de dicha metodología.

8.3 INFORMACIÓN

A nivel de Información, para el año 2024, la UAECD se propone la adopción de los lineamientos de la versión 3 del Marco de Referencia de Arquitectura Empresarial publicado en noviembre de 2022.

El Marco de Referencia de Arquitectura Empresarial del Estado Colombiano (MRAE), se encuentra compuesto por tres modelos: el Modelo de Arquitectura Empresarial (MAE), el Modelo de Gestión y Gobierno de TI (MGGTI) y el Modelo de Gestión de Proyectos de TI (MGPTI), que guían la aplicación de un enfoque de Arquitectura Empresarial que facilite la articulación entre la estrategia y planeación institucional, el modelo operativo y gestión de la entidad, y la gestión de TI.

8.3.1 Arquitectura

La arquitectura de información describe la estructura e interacción de la información y los recursos que permiten su administración. La definición de una arquitectura de información busca determinar los datos e información clave para las entidades, estableciendo cómo obtenerlos, organizarlos y distribuirlos de manera que faciliten el desarrollo de la misión de las entidades de manera eficiente.

Los lineamientos de **Arquitectura de Información** que se deben cumplir son los siguientes:

LINEAMIENTO	NOMBRE	DESCRIPCIÓN
MAE.LI.AI.01	Flujos de información	Las entidades de la administración pública deben definir un modelo de gobierno que gestione las políticas, responsabilidades, decisiones y métricas para ejercer autoridad sobre la información.
MAE.LI.AI.02	Arquitectura de Información	Las entidades de la administración pública deben modelar, describir y mantener actualizada la arquitectura de información que habilite la generación de información de valor para el desarrollo de la misionalidad.
MAE.LI.AI.03	Intercambio de Información entre entidades del Estado	Las entidades de la administración pública deben identificar la información a compartir, definir servicios que habiliten el intercambio y diseñar la arquitectura de información que permita los intercambios; teniendo en cuenta para ello el uso del Marco de interoperabilidad y su Lenguaje común de intercambio.

MAE.LI.AI.04	Modelo de Información Institucional	Las entidades de la administración pública deben contar con un Modelo de Información Institucional acordado con los interesados, que proporcione una vista común y coherente de la información; sirviendo como base y guía para cualquier modelo de datos particular o proyecto de datos que se desarrolle.

8.3.2 Gobierno

Por su parte, el Modelo de Gestión y Gobierno de TI permite generar las capacidades institucionales de TI que se requieren para prestar servicios de TI a los usuarios de cada entidad mediante el uso adecuado de las tecnologías de la información y las comunicaciones.

El dominio de Gestión de Información del MGGTI contiene los elementos para orientar a las entidades en la gestión del ciclo de vida de los componentes de información.

A nivel de **Gestión y Gobierno de la Información** los lineamientos que se deben cumplir son los siguientes:

LINEAMIENTO	NOMBRE	DESCRIPCIÓN
MGGTI.LI.GI.01	Gobierno de la información	Las entidades de la administración pública deben definir un modelo de gobierno que gestione las políticas, responsabilidades, decisiones y métricas para ejercer autoridad sobre la información.
MGGTI.LI.GI.02	Gestión de la calidad de los datos	Las entidades de la administración pública deben definir y desarrollar una estrategia para diagnosticar, medir, monitorear y establecer acciones que permitan contar con información de calidad para la toma de decisiones.
MGGTI.LI.GI.03	Gestión de documentos electrónicos	Las entidades de la administración pública deben establecer un programa para la gestión de documentos y expedientes electrónicos.
MGGTI.LI.GI.04	Marco de Referencia Geoespacial	Las entidades de la administración pública deben adoptar las directrices y lineamientos encaminados a facilitar los procesos de gestión geoespacial, de acuerdo con lo definido en el Marco de Referencia Geoespacial.
MGGTI.LI.GI.05	Publicación de los servicios de intercambio de información	Las entidades de la administración pública deben exponer sus servicios de intercambio de información a través de la Plataforma de Interoperabilidad del Estado colombiano.

MGGTI.LI.GI.06	Acuerdos de intercambio de información	Las entidades de la administración pública deben establecer Acuerdos de Nivel de Servicio (ANS) que permitan el intercambio de información de calidad entre sus dependencias o con otras instituciones.
MGGTI.LI.GI.07	Uso del código postal colombiano	Las entidades de la administración pública deben en el diseño de sus componentes de información identificar aquellos a los que se les deba aplicar el código postal.
MGGTI.LI.GI.08	Explotación de datos	Las entidades de la administración pública deben seleccionar técnicas analíticas que les permitan tomar decisiones en base a información de calidad.

8.3.3 Catálogo de componentes de información

Se debe continuar con la actualización del Catálogo del componente de información teniendo en cuenta la migración realizada a la nube de los sistemas de información y aplicaciones que operaban on-premise

Sobre las posibles herramientas analizadas para facilitar la actualización del catálogo de componentes de información se debe revisar la viabilidad de adquirirlas e implementarlas.

8.4 SISTEMAS DE INFORMACIÓN

8.4.1 Catálogo de Sistemas de Información

Teniendo en cuenta que se realizó una actualización completa del catálogo de sistemas de información de la UAECD debido a toda la migración que se realizó de la infraestructura que estaba en tierra y ahora se encuentra desplegada en la nube, este nuevo catálogo de sistemas de información se va a publicar y desplegar en el SharePoint de la gerencia de tecnología.

Para garantizar la actualización del catálogo de sistemas de información, se recomienda:

- Analizar la viabilidad de llevar el Catálogo de Sistemas de Información en la CMDB.
- Con el fin de dar solución a los resultados y recomendaciones del diagnóstico realizado sobre los sistemas de información y los servicios web, se requiere contar con profesionales especializados en desarrollo de servicios web e interfaces.
- Contar con profesionales de desarrollo encargados de realizar la documentación técnica y de usuario faltante.

8.4.2 Ciclo de vida de los sistemas de información

Se deben actualizar las versiones de los aplicativos misionales de la UAECD que se encuentran en versiones de software Oracle que ya no cuentan con soporte por parte del proveedor, para lo cual es necesario que Infraestructura actualice las versiones del software base a unas versiones que cuenten con soporte actualizado por parte de Oracle y posteriormente, por el grupo de ingeniería de software se debe realizar los desarrollos y pruebas necesarias para desplegar los códigos fuentes en estos servidores y asegurar su funcionamiento.

Se debe realizar un análisis de impacto para la migración de los aplicativos de Go Castastral que se encuentran licenciados con software Oracle, tales como su base de datos y su generador de reportes usando FORMS and Reports, a un motor de base de datos de software libre como lo es POSTGRES y un generador de reportes como JASPER Reports

Se debe utilizar como gestor de documentos oficial el WCC (Web Content Center) de Oracle y migrar todas las series documentales del INFODOC a esta herramienta.

Se debe realizar un análisis institucional donde se tomen decisiones sobre los siguientes aplicativos que soportan la operación de Catastro Bogotá, dado que se encuentran obsoletas las herramientas de desarrollo sobre las que están construidos:

- SICAPITAL
- SIIC (Sistema de Información Catastral)
- LPC (Línea de Producción Caratográfica).
- CT (Captura en Terreno)

Para los sistemas SIIC, LPC y CT se recomienda evaluar el uso o adecuación de Go Catastral por estar implementado en el modelo LADM-COL, que integra la información alfanumérica y geográfica. Se hace necesario definir un proyecto con un equipo de talento humano diferente, dado que el mismo recurso humano que hace el soporte y mantenimiento no podría hacer esta actividad.

Para nuevos desarrollos se debe aplicar el procedimiento nuevo de pruebas de vulnerabilidad y así poder determinar si el software es seguro o tiene fallas de seguridad.

Se debe mantener la interoperabilidad a través de XROAD con los cuales se tienen dos servicios implementados: Superintendencia de Notariado y Registro y Caja de Vivienda Popular y se recomienda analizar la necesidad de implementar nuevos servicios en ambas vías.

Se debe contar con recursos humano para las tareas de adecuación, ajuste y mantenimiento de los sistemas de información.

8.4.3 Arquitectura de Sistemas de Información

Durante la vigencia 2023 se realizó una revisión del documento propuesto como ATR y se logró definir y realizar un análisis donde se identifica que ese documento es un ATS. Por parte de la subgerencia de ingeniería de software se realizaron unas recomendaciones entre ellas que en este documento se de línea a través de la gerencia de tecnología y poder contar con profesionales especializados en Arquitectura de Software para poder definir y actualizar este documento para la vigencia 2024.

Teniendo en cuenta que en el software ARCHIMATE y con ayuda del Arquitecto de datos de la gerencia de tecnología se avanzó en el modelo de arquitectura de datos del sistema de gestión catastral "Go Catastral" logrando así complementar la documentación de este aplicativo misional y poder detectar mejoras o procedimientos que pueden ir evolucionando con el tiempo.

Al respecto, se recomienda, a partir de los artefactos de arquitectura de los sistemas de información actualizados en el 2023, seguir completando y validando, integrados en ARCHIMATE para facilitar su consulta y actualización, teniendo en cuenta las nuevas implementaciones de Catastro Multipropósito – Go Catastral en los territorios y Bogotá.

8.4.4 Soporte y mantenimiento de Sistema de Información

Con el fin de disponer de la documentación necesaria para las actividades de soporte y mantenimiento se debe continuar con la actualización, organización y acceso a la documentación técnica y funcional a partir de la publicada en el micrositio de la Gerencia de Tecnología en el siguiente enlace:

Subgerencia de Ingeniería de Software (sharepoint.com)

Teniendo en cuenta la cantidad de requerimientos y solicitudes que se generan en la puesta en operación de Catastro Multipropósito se debe contar con más recurso humano dedicado a soporte y mantenimiento, incluyendo profesionales dedicados a realizar pruebas de software a los sistemas de información nuevos o que han sido ajustados, usando buenas prácticas. Así como, fortalecer capacidades en desarrollo de software en java, appex y desarrollo de componentes geográficos.

Se debe realizar una valoración de las necesidades de nuevas funcionalidades de sistemas de información estableciendo prioridades y recurso humano con el que se cuenta para su atención, con el fin de establecer los que desarrollos que pueden ser atendidos en la vigencia 2024.

Para el caso de Go Catastral, se debe seguir fortaleciendo sus funcionalidades y realizar la evaluación de las alternativas que permitan responder a las nuevas versiones del modelo LADM-COL y a los ajustes relacionados con la madurez del sistema de información

Para el caso de la incorporación de Bogotá en el modelo LADM-COl, se debe implementar interoperabilidad entre los aplicativos SIIC y LPC con los modelos LADM con el fin de manejar un único estándar para el intercambio de información

Realizar una evaluación del uso de las nuevas tecnologías disruptivas, como blockchain, Inteligencia Artificial y Machine Learning.

8.5 INFRAESTRUCTURA DE TI

8.5.1 Capacidades de infraestructura tecnológica

Con el fin de mantener y mejorar los servicios tecnológicos gobernados y gestionados por la Gerencia de Tecnología, se proponen las siguientes acciones:

Conectividad

Para poder mantener y mejorar el servicio de conectividad se debe:

- Contar con alta disponibilidad en los switches (DELL) de distribución ubicados en los centros de cableado del piso 11 y 12.
- Revisar el ciclo de vida de los switches de la entidad para realizar las renovaciones pertinentes.
- Contar con un contrato de mantenimiento de cableado estructurado que permita solventar las necesidades y crecimiento de la entidad.
- Mantener vigentes los contratos de mantenimiento para los switches de UAECD y las UPS, ya que con esto se tendría soporte para mantener operativos los dispositivos.
- Aumentar la planta de personal de la capa de redes (proporciona redundancia y respaldo en caso de que uno de los ingenieros no esté disponible), es necesario tener personal calificado en planta que pueda continuar con el conocimiento y la disponibilidad para atender requerimientos, incidentes, contratos, entre otros.

Sistemas de Procesamiento y Almacenamiento

ON-PREMISE: Nueva solución de virtualización

Dado el alto grado de obsolescencia y fallas de las plataformas tecnológicas físicas actuales de la PCA (más de 7 años), que actualmente se utiliza solo para mantener el Backup del File Server y el WCC y considerando que no es procedente invertir recursos adicionales, se plantea la siguiente alternativa enfocada en proveer continuidad a los servicios que requiere actualmente la entidad en el ambiente On-premise:

Adquirir una nueva solución con menores capacidades para virtualización de algunos servicios, almacenamiento y librería de back ups que permita contar con una plataforma tecnológica de última generación que garantice el óptimo funcionamiento y respaldo de los servicios. Esto implica invertir en la adquisición, implementación y soporte técnico de la solución.

Esta propuesta consiste en una nueva infraestructura de hiperconvergencia (HCI) que combina servidores y almacenamiento en una plataforma distribuida con software inteligente que crea bloques de construcción flexibles los cuales sustituyen a una estructura tradicional compuesta por servidores separados, redes de almacenamiento y cabinas de almacenamiento. Más concretamente, esta nueva solución combina elementos de hardware avanzados con una capa de software distribuido que elimina los habituales puntos débiles presentes en la infraestructura de virtualización tradicional y complementan los servicios que se tienen dispuestos en la nube.

En consecuencia, la solución propuesta debe contar con las siguientes características técnicas mínimas para garantizar una la escalabilidad tanto vertical como horizontal, así como un óptimo desempeño y alta disponibilidad:

- 3 servidores físicos con procesadores Intel de última generación (versiones platinum) con 48 cores por cada CPU física.
- Cada servidor debe tener 1.4 TB de memoria RAM.
- Almacenamiento total usable en discos de tecnología SSD NVMe con al menos 200 TB.
- Tarjetas de red con conectividad de 10 GB por cada servidor en un esquema redundante y en alta disponibilidad.
- Sistema de virtualización de última generación, compatible con escalabilidad a nubes públicas (OCI y Azure), que sea compatible con sistemas de copias de respaldo comerciales como Veeam Backup.

Esquema de la solución propuesta

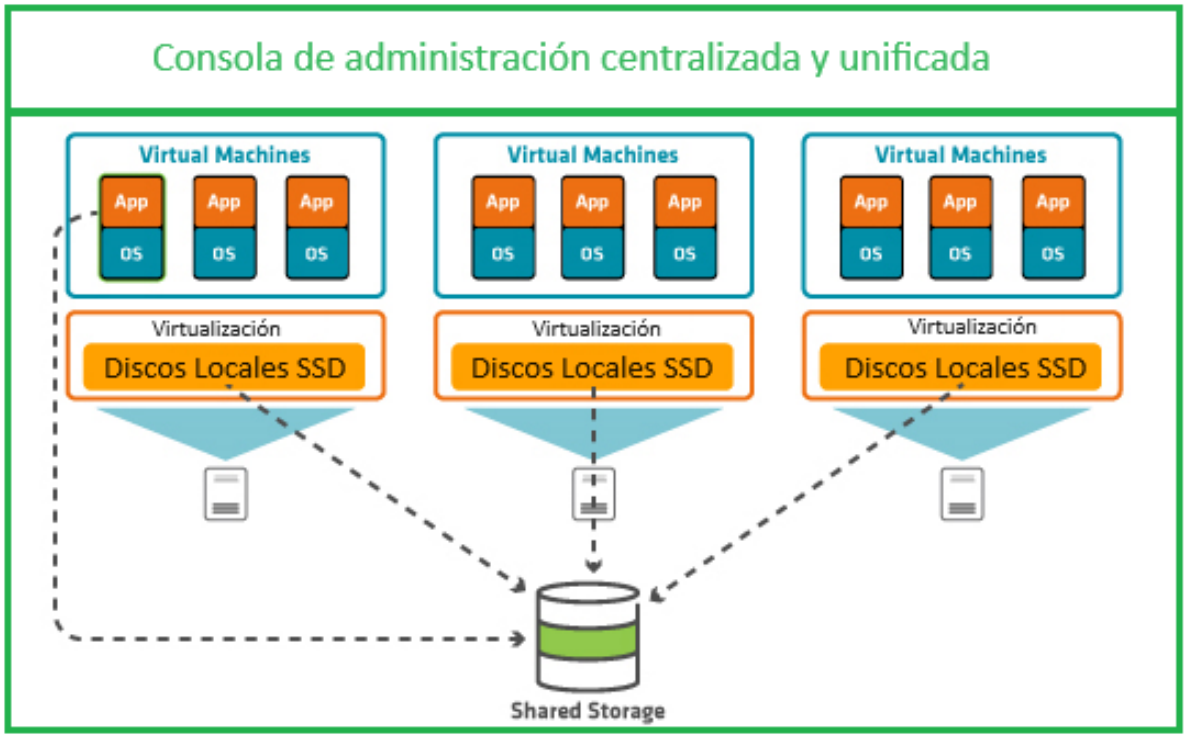


Ilustración 53. Esquema solución virtualización

NUBES PÚBLICAS

En lo referente a la estrategia de servicios en Nube, la UAECD está basada en herramientas y servicios provistos por Microsoft Azure y OCI (Oracle Cloud Infrastructure), principalmente se usan servicios de infraestructura como servicio (IAAS), plataforma como servicio (PAAS) y software como servicio (SAAS). Uno de los objetivos a desarrollar es el de mantener los servicios en nube enunciados manteniendo sus niveles de disponibilidad, confiabilidad y seguridad establecidos en los ANS del Acuerdo Marco de Conectividad IV.

Por otra parte, se hace necesario implementar a corto plazo medidas tendientes a **mejor el control de los costos** desarrollando un modelo de información que permita optimizar la asignación de los recursos y que tenga como factores determinantes para dicha gestión mecanismos de prevención, detección y corrección. De forma general se debe buscar: a) Identificar recursos que no se estén usando y eliminarlos para que los costos bajen. b) Elegir el tamaño correcto de los recursos. No aprovisionar más de lo que se necesita. c) Revisar los modelos de compra y las opciones que ofrecen

los proveedores de nube con el fin de pagar menos por los recursos d) Validar las características de los servicios con el fin de optimizar el costo de los servicios, e) Actualizar o migrar la arquitectura de la aplicación hacia servicios contenerizados o serverless que permitan hacer lo mismo que una máquina virtual, pero con menos recursos. f) Identificar patrones del servicio con el fin de brindar las capacidades requeridas en picos inesperados de carga o disminuir cargas cuando no se requiera el servicio.

Plan de Recuperación de Desastres (DRP)

Hace algunos años atrás este plan fue implementado en la nube de OCI donde se aprovisionaron en aquel entonces servicios tecnológicos, misionales y administrativos básicos mediante IAAS (Infraestructura como servicio) y PASS (Plataforma como servicio) con los mínimos recursos posibles para que la entidad pudiera operar; sin embargo, fue necesario ajustar esa infraestructura de DRP y convertirla en el nuevo ambiente productivo, migrando de tierra a nube los servicios que estaban pendientes, así como configurar y repotenciar los servicios que ya estaban en nube para garantizar el óptimo funcionamiento de esos sistemas de información y servicios implementados allí. Lo anterior, se llevó a cabo en razón a los problemas de funcionamiento de la plataforma de virtualización y almacenamiento On-premise (PCA y FSS) presentados hace algunos meses que comprometieron la disponibilidad y funcionamiento de los servicios productivos que funcionaban en On-Premise hasta entonces.

Dado el panorama actual, donde gran parte de los servicios productivos están desplegados en nube, se plantea realizar el aprovisionamiento de una infraestructura exclusiva para el DRP en nube, a partir de lo cual la actual infraestructura productiva aprovisionada en la región de Ashburn (USA) sea transformada en la infraestructura del DRP, y los servicios productivos sean migrados a otra región geográfica como: Colombia, o bien, una región cercana que permita obtener un menor tiempo de respuesta (baja latencia) respecto al actual, así como un costo razonable para cada uno de los servicios desplegados en nube.

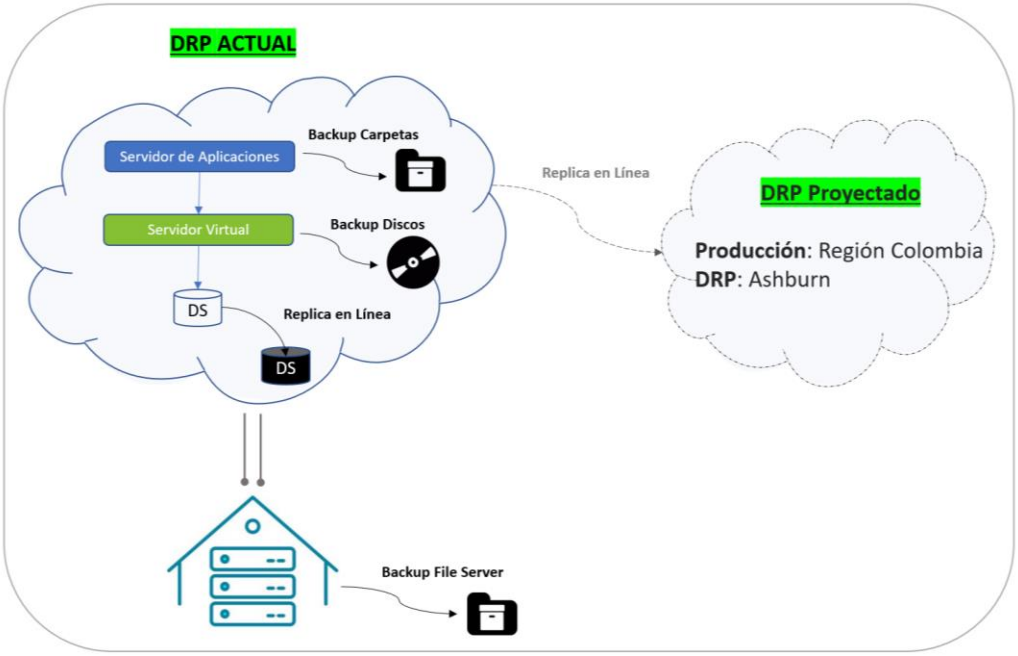


Ilustración 54. Propuesta DRP

Para ello es indispensable que se garanticen a futuro los recursos presupuestales necesarios para los contratos de nube, contratistas y demás proveedores, con el fin de contar con los recursos necesarios para planear, diseñar, implementar, probar y mantener el futuro DRP que permita a la entidad llevar a cabo una recuperación ágil de su operación en caso tal de acontecer un evento de este tipo.

De acuerdo con lo anterior, se requiere tener en cuenta la realización de las siguientes actividades:

- Proyecto de migración de la nube ubicada en la región de Ashburn a Colombia o a la región que se defina. Donde Colombia quedaría como la región principal y Ashburn como el DRP.
- En el DRP poder contar con una réplica (sincronización en línea) de las bases de datos misional, administrativa, geográfica y del WCC.

Recomendaciones y aspectos a tener en cuenta en el plan de recuperación de desastres – DRP:

- La Alta Dirección de la UAECD debe garantizar los recursos humanos y financieros a la Gerencia de Tecnología para que pueda prestar correctamente sus servicios tecnológicos cuando se produzca una interrupción en las operaciones de los Servicios de TI según las necesidades del Plan de Recuperación ante Desastres (DRP).
- Como parte del plan de recuperación de desastres (DRP) y para minimizar los riesgos de pérdida de información y afectación de los procesos críticos del negocio se recomienda

contar con la herramienta Veeam Backup, la cual se integra con Microsoft 365 permitiendo capacidades de backup, recuperación, protección contra ransomware y continuidad del negocio al proteger los datos críticos, eliminando el riesgo de perder datos de SharePoint Online, OneDrive y Microsoft Teams. Así mismo Veeam Backup for Microsoft 365 proporciona RPO (punto objetivo de recuperación) más bajos y permite la generación de backups incrementales, diferenciales y poder contar con datos históricos. Con esta herramienta es posible realizar copias automatizadas de las bases de datos, evitando la manualidad, simplificando las tareas y reduciendo los tiempos que toma realizar una copia de seguridad.

- Por otro lado, es importante considerar un proyecto al interior de la Gerencia de Tecnología que evite la obsolescencia tecnológica y los riesgos que esto conlleva:
    - Como en el caso de la actualización de las máquinas que cuentan con sistema operativo Linux 5, 6 y 7, los cuales son muy viejos y no cuentan con soporte. Estas máquinas actualmente cuentan con backup full e incremental programado de manera semanal.
    - Migración de Infodoc al WCC, dada la obsolescencia de Infodoc.
    - Aunque el aplicativo de nómina Perno se migró a la nube, el liquidador está en un sistema operativo 2008 y no es posible realizar su migración. Actualmente el aplicativo Perno se encuentra en proceso de migración de WebLogic 10G a 12C.

- Como parte de los riesgos de estar en la nube están las vulnerabilidades a ciberataques, por lo tanto, se recomienda la implementación de por lo menos un doble factor de autenticación o autenticación en dos pasos, pero para mayor protección se recomienda implementar un factor de autenticación multifactor.
- Actualmente el aplicativo Pandora se encuentra en los servidores de Idartes, debido a un convenio suscrito por parte de la Oficina Asesora de Planeación con ellos. Actualmente están en proceso de migración, pero hasta tanto no se encuentre en el gobierno de la Gerencia de Tecnología, no es posible incluirlo en el plan de recuperación de desastres.
- Es importante sacar un backup de la información del WCC que aún reposa en la PCA, que debido a la falta de espacio disponible no ha sido posible realizarlo. Esta información es requerida por las áreas misionales para dar contestación a diferentes requerimientos de entidades y ciudadanos.

Servicios de RED y Autenticación

Directorio Activo: Controladores de Dominio

Se requiere aprovisionar un segundo controlador de dominio en On-Premise para generar alta disponibilidad y balanceo de carga en este servicio. La instalación y configuración de este nuevo servidor está sujeto a disponibilidad de una nueva infraestructura de virtualización y almacenamiento On-premise en la que cuenten con óptimos y suficientes recursos de hardware (CPU, RAM y Almacenamiento) a partir de los cuales pueda ser instalado y configurado el servidor propuesto. Con la implementación de este segundo controlador se puede satisfacer de forma adecuada la demanda de las peticiones de autenticación propias de los sitios web, aplicaciones, servidores, vpn y usuarios.

Distribución de los controladores de dominio por sitio

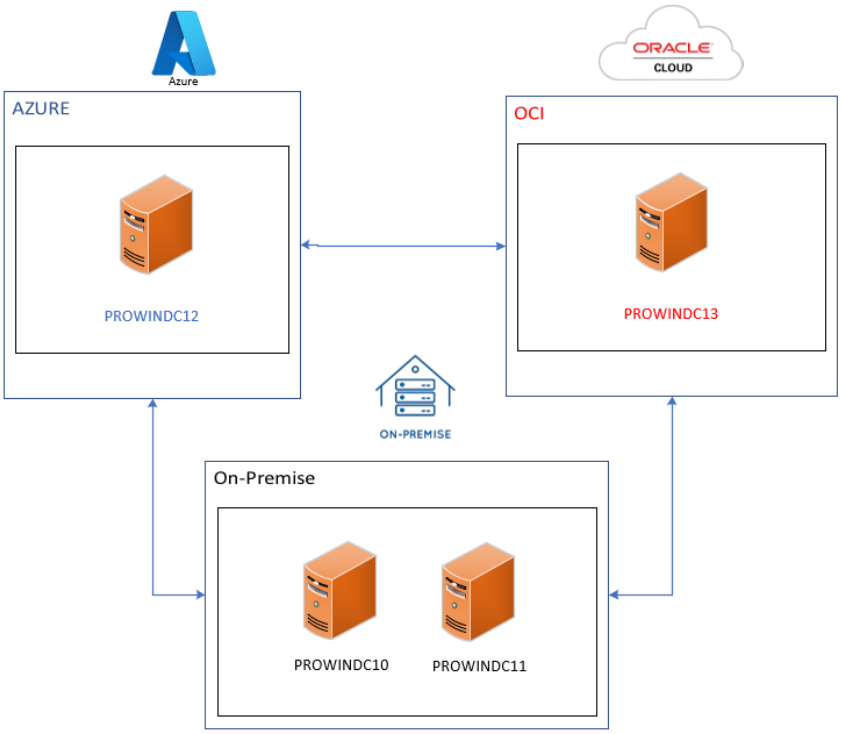


Ilustración 55. Distribución controladores de dominio

Directorio Activo: SSPR (Self-Service Password Reset)

Se requiere implementar un servicio que permita realizar el cambio de la contraseña para las cuentas de Office 365 en línea. Lo anterior, en razón a que en la actualidad no hay ningún mecanismo que permita cambiar la contraseña en línea luego de iniciar sesión en Office 365. Esta

situación es crítica, ya que existe un alto porcentaje de usuarios que al laborar fuera de las instalaciones de la entidad no cuentan con un equipo de cómputo asignado en la red LAN de catastro donde puedan cambiar la contraseña. Por tanto, al no cambiarse con cierta frecuencia o regularidad hay un riesgo informático latente en la cual los atacantes pueden obtener acceso a estas credenciales estáticas.

Por lo anterior, es de suma importancia implementar SSPR, un servicio licenciado de Microsoft que permite a los usuarios de la entidad que sin importar donde estén ubicados geográficamente puedan cambiar la contraseña en línea cada cierto tiempo, sin necesidad de desplazarse hasta las instalaciones de la entidad para cambiar su contraseña. Bajo la situación actual de teletrabajo, y en razón a que se cuenta con contratistas en regiones geográficas remotas debido a la atención de los convenios de catastro Multipropósito, SSPR se convierte en una herramienta fundamental para cumplir con esta buena práctica de seguridad (cambiar la contraseña con cierta frecuencia) enfocada en mitigar el riesgo de acceso no autorizado a las cuentas corporativas de los usuarios.

La imagen siguiente describe el flujo habitual para el cambio de contraseña de un usuario, en donde este último inicia sesión en su cuenta de Office 365 desde cualquier lugar remoto, luego accede al servicio de SSPR, allí cambia su contraseña y de forma automática este cambio se actualiza en los servidores de directorio activo de On-premise y Azure Active Directory.

Flujo del cambio de contraseña para un usuario de Office 365 usando SSPR.

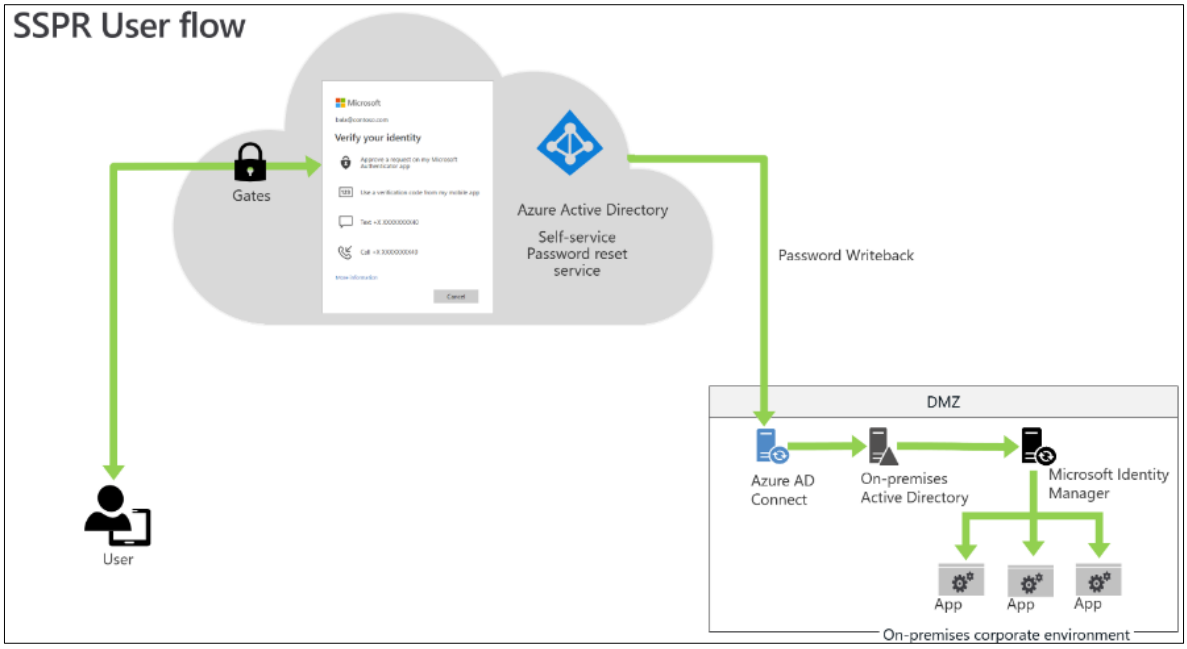


Ilustración 56. Flujo de cambio de contraseña

Fuente: https://learn.microsoft.com/en-us/entra/identity/authentication/howto-sspr-deployment

DNS

En relación con el sistema de resolución de nombres de dominio, se mantendrá el número actual de servidores (tres controladores de dominio). Esto en razón, a que este clúster cuenta con los recursos suficientes para satisfacer de forma eficaz y eficiente la provisión de este servicio. No se considera un crecimiento horizontal para este recurso tecnológico. De igual forma, el incremento en el número de zonas de búsqueda directa e inversa esta dado por la demanda actual del servicio.

DHCP

Se requiere aprovisionar un segundo servidor de DHCP en On-Premise para generar alta disponibilidad del servicio:

- PROWINDC10 (Servidor Actual)
- PROWINDC11 (Nuevo servidor a aprovisionar).

La instalación y configuración de este nuevo servidor está sujeto a disponibilidad de una nueva infraestructura de virtualización y almacenamiento On-premise en la que cuenten con óptimos y suficientes recursos de hardware (CPU, RAM y Almacenamiento) a partir de los cuales pueda ser instalado y configurado el servidor propuesto.

Office 365: Licenciamiento

En cuanto al licenciamiento de Office 365 y el esquema de colaboración, la unidad debe revisar si mantendrá la misma cantidad de licencias adquiridas en esta plataforma para el año 2024 toda vez que varios convenios de Catastro Multipropósito pueden estar llegando a su fecha de finalización y el número de contratistas que está actualmente laborando para los convenios y las diferentes dependencias de la entidad puede sufrir modificaciones.

Office 365: MFA (Múltiple Factor de Autenticación)

Dado el panorama actual relacionado con los riesgos informáticos asociados a la vulneración de las credenciales de los usuarios que conlleva a la perdida de la confidencialidad, integridad y disponibilidad de la información en plataformas y servicios como Office 365, se ha venido realizando inicialmente la implementación del MFA para las cuentas de los usuarios administradores en las plataformas: Office 365, nube de Azure y nube de OCI. Sin embargo, se hace necesario como segunda instancia, implementar esta funcionalidad en las cuentas de los usuarios finales, con el fin

de robustecer las medidas de seguridad frente a ataques informáticos que busquen obtener acceso a estas.

Inicio de sesión en Office 365 con MFA usando mensajes de texto.

Ilustración 57. Inicio de sesión con MFA

La implementación requiere de una planeación y esfuerzo coordinado entre los administradores de Office 365, el primer nivel de mesa de servicio y las diferentes dependencias, de tal manera que la entidad adopte progresivamente esta nueva funcionalidad entendiendo sus beneficios e importancia para la seguridad de la información.

Office 365: Licenciamiento herramienta Back Ups buzones críticos

Se hace necesario realizar la adquisición de una herramienta para la creación y restauración de copias de respaldo para los buzones de correo críticos para la entidad, como, por ejemplo:

- soportecel@catastrogota.gov.co
- tiendavirtualuaecd@catastrobogota.gov.co
- agendaaunclic@castrobogota.gov.co
- contactenos@catastrobogota.gov.co
- Otras.

Lo anterior, en razón a que este tipo de buzones con gran transaccionalidad generan un alto volumen de almacenamiento, y teniendo presente que cada uno cuenta con un espacio limitado en su buzón y archivado, es insuficiente para almacenar todo el histórico de los mensajes. Esta situación es crítica, teniendo en cuenta que es necesario respaldar el contenido de estos buzones debido a que de ello depende la contestación de tutelas, temas de orden jurídico y administrativo para la entidad.

Por otra parte, no es viable realizar la generación de PST para cada uno ellos, en razón a que dado el panorama actual de On-Premise donde la infraestructura se encuentra en un alto nivel de obsolescencia, fallos y sin espacio de almacenamiento, allí no hay lugar alguno donde alojar este tipo de archivos.

Sistemas de Bases de Datos

Para garantizar la operación de la capa de base de base de datos, se debe:

- Aumentar las capacidades de ASM para cada BDSystem
- Actualizar periódicamente junto con el proveedor las versiones del DBSystem y las versiones de motor de base de datos.
- Crear el ambiente de DRP para las bases de datos de la Entidad
- Programar junto con el proveedor las tareas de assessment y mantenimientos preventivos de las bases de datos
- Contar con ambiente para verificación de procesos de restauración de copias de seguridad.
- Contratar recursos humanos con experiencia en administración y mantenimiento de bases de datos Oracle.
- Contratar soporte extendido con los fabricantes.

Capa Media

Capa Media Web Logic

Para mejoramiento de Capa media se deben validar las siguientes iniciativas:

1. Levantamiento de información para definir nuevo diseño y arquitectura de la infraestructura.
2. Migrar la infraestructura actual de OCI a Data Center en Colombia.

3. Instalación y configuración de clúster para Servidor de Reportes
4. Migrar servidor de nómina a OCI.
5. Actualización de Java en servidores WLS.
6. Migrar a WLS 14.1 OAS a WebLogic:
    1. Foca Viejo
7. Migrar a WLS 14.1 las siguientes aplicaciones
    1. CT, Captura en terreno
    2. Tienda Virtual
    3. Catastro en Linea
    4. APEX
    5. Foca Nuevo
    6. WCC
    7. BI
8. Migrar a WLS 12.2.1.4.0
    1. Servidores de Forms y Reports
9. Solucionar warning presentes en las consolas de las aplicaciones, luego del parchado.
10. Implementación herramienta de Monitoreo.
11. Implementación de DRP entre nubes
12. Implementar seguridad acceso a servidores por medios de llaves de seguridad.

Capa Media ArcGis

Para garantizar la operación de capa media en cuanto a ArcGIS, se debe:

En el Ambiente OCI

- Actualmente el ambiente de ArcGis en OCI para Catastro Multipropósito esta con una sola maquinas en los sistemas, esto se redujo por temas de presupuesto, pero es recomendable que todos estén en alta disponibilidad con el fin de brindar servicio sin interrupciones. Además, es conveniente es hacer una actualización del portal de Catastro Multipropósito a una versión 10.9 o posterior.

En el ambiente Azure

- Actualmente se cuenta con un ambiente de Azure, donde reposa el portal que soporte la operación de Bogotá, es recomendable dejar en cluster todos los sistemas y aumentar las características de Hardware a todos los Server, que no se ha podido realizar por temas de presupuesto con el fin de tener un sistema estable y prestar un servicio sin interrupciones.

Además, es conveniente es hacer una actualización del portal de azure a una versión 10.9 o posterior.

Infraestructura de seguridad informática

Con el objetivo de garantizar la alta disponibilidad de los diferentes equipos de seguridad, se debe tener en cuenta que la entidad se debe orientar a:

- Contar con alta disponibilidad del firewall de aplicaciones de la nube de Azure.
- Contar con alta disponibilidad del firewall de aplicaciones de la nube de OCI.
- Fortalecer la capacidad de monitoreo de activos en la plataforma SIEM, logrando una mejor cobertura de toda la infraestructura de Servidores, Bases de datos, aplicaciones, equipos de red y quipos de seguridad informática con que cuenta la entidad.

Assesment Microsoft

El 15 de febrero de 2022 Microsoft emitió las siguientes conclusiones sobre un assessment hecho sobre la plataforma Office 365 de Catastro. Cabe resaltar que todas y cada una de ellas no pueden simplemente ejecutarse así no más, en particular hay que ser cuidadoso con los parches para que una actualización no genere incompatiblidades con las aplicaciones.

He aquí la hoja de ruta planteada:

Roadmap

Rubro	Nivel de Riesgo	Problema	Tiempo máximo de remediación	Accionable
Identidad	Alto	• Usuarios con actividad de riesgo. • Alertas de seguridad activas en niveles medios y altos. • Falta de controles de seguridad avanzados.	45 días.	• Despliegue de componentes de seguridad (MFA y Acceso condicional) • Monitoreo de usuarios con actividad sospechosa.
Dispositivos	Medio	• Dispositivos con Riesgo de Ransomware. • Uso de Sistemas Operativos fuera de Soporte.	45 días.	• Actualizar todos los sistemas operativos con los parches de seguridad más recientes por medio de directivas.
Datos	Alto	• Archivos con Malware dentro de las carpetas de usuarios. • Ataques de Phishing y malware.	60 días.	• Reforzar administración de información almacenada y depurar los riesgos. • Desplegar directivas de protección contra amenazas de correo electrónico y fugas de información.
Aplicaciones	Alto	• Uso de aplicaciones con niveles de permisos altos. • Software instalado con niveles críticos de vulnerabilidades.	60 días.	• Remover o actualizar todos los componentes que presentan vulnerabilidades.
Infraestructura	Medio	• Uso de Sistemas Operativos fuera de Soporte. • Controles de acceso básicos a la capa de infraestructura.	150 días.	• Realizar la actualización de los servidores a la ultima versión disponible. • Migrar infraestructura obsoleta a nuevas versiones.
Redes	Medio	• Puertos administrativos expuestos accesos no autorizados.	30 días.	• Generar bloqueo de IP´s dentro de los NSG

Ilustración 58. Hoja de ruta Assesment Microsoft

De los temas anteriores, todos salvo el tema de identidad requieren tener un licenciamiento active directory p2, que no tiene actualmente la Entidad para poder atenderlas.

Con referencia a la identidad, se implementó el múltiple factor de autenticación o token para actividades relativas a sharepoint, accesos al email de outlook, etc. Si bien la funcionalidad opera bien, ha sido objeto de algún rechazo por parte de los usuarios ya que infortunadamente algunos ni siquiera tienen el buen hábito de revisar el correo.

Recomendaciones DataSec / Fortinet

Debido al cambio de On-Premise a nube, este tándem sugiere las siguientes recomendaciones en las que se concuerda con la misma capa de seguridad informática de la Entidad:

- Eliminar los equipos FortiWeb On-Premise pues ya no hay servicios que se publiquen desde On-Premise.
- Eliminar el equipo FortiDDoS pues ya no hay servicios expuestos que se publiquen desde On-Premise.
- Eliminar el balanceo que hace el FortiADC y pasarlo a los FortiWeb de OCI que tienen esa misma característica.

- Potenciar el actual FortiGate de OCI pues la carga de la operación pasó a este firewall y ya no está en el FortiGate On-Premise. Se está analizando pasar a 8 CPUs, actualmente cuenta con 2.
- Eliminar en el FortiGate de OCI el vdom de DRP. Actualmente en OCI hay dos ambientes, multipropósito y producción, por simplicidad en la administración, se está analizando en dejar en el FortiGate de OCI uno sólo.

Plan de Seguridad Informática:

Las principales acciones sugeridas para mejorar la seguridad informática incluyen:

- Implementar el SIEM en la nube de OCI obteniendo los mayores beneficios. No sólo debe recuperarse las funcionalidades con que se contaba en On-Premise como informes de disponibilidad, alertas y dashboards sino que: las alertas deben ser selectivas en los emails para no abrumar con cientos de emails a los administradores de cada capa; los operadores deben familiarizarse y todos los días monitorear los dashboards; las transacciones sintéticas o monitoreos de URLs deben funcionar de la mejor manera pues no eran confiables en la solución anterior; hay que aprovechar los agentes avanzados en las máquinas windows, esto para justificar la existencia de la segunda máquina collector SIEM en OCI. Todo esto depende de los costos en la nube OCI pues DataSec, el proveedor e implementador solicitó unos recursos mínimos que se han venido ampliando gradualmente y es muy posible que vuelva a pedir crecimiento en los mismos, lo que puede originar costos significativos para la Entidad.
- Se va a implementar un plan de múltiple factor de autenticación para acceso a las VPNs de la Entidad, On-Premise y OCI. Esto debe ser discutido con el área de seguridad de la información para que su conocimiento y apoyo en la divulgación. El plan se implementará de manera granular, primero la SIT, luego la Gerencia de Tecnología y luego toda la organización.
- La implementación de un SOC y un SOAR le dará a la Entidad mayor visibilidad y previsión ante los ataques informáticos; y también automatización en la respuesta a los mismos, respectivamente.
- Ahora, finales de 2023, que Oracle va a abrir un centro de datos de nube en Bogotá, toda la infraestructura se pasará de Ausburn a Bogotá para eliminar los retardos en las respuestas a las aplicaciones, aspecto del que se han quejado los usuarios, mayormente los del sistema SIIC. Al migrar el container de Ausburn a Bogotá, se debe aprovechar para un rediseño de arquitectura de red y seguridad y no solamente pasar de un lado al otro. Una vez se migre a Bogotá, debe considerarse otro container en una locación lo más cercana a Bogotá, para preparar allí el DRP y hacer un ejercicio de implementación del mismo, el cual será

dispendioso, demandará esfuerzos de todas las capas de infraestructura y significará un costo. Si bien se entiende que no tiene sentido pagar por un DRP que no se estará usando hasta cuando no suceda una eventualidad, el área de infraestructura sí debería tener un guión de qué habría que hacer para disparar el DRP en OCI si se cae la sede o container principal, Bogotá. La Entidad debe contemplar los aspectos financiero, contractual y técnico, lo cual demanda que esté en cabeza no sólo de la Gerencia de Tecnología sino del Director de Catastro y el Comité de Continuidad del Negocio.

- No se cuenta con una sala de crisis ni con un grupo de respuesta a incidentes ante la eventualidad de un ataque exitoso de seguridad informática. Esto no debería recaer en los mismos administradores sino tener un equipo aparte o si se quieren utilizar los ingenieros de planta y contratistas, no sólo se debería capacitárseles sino aprovisionar recursos para dar respuesta a un incidente a través de dicha sala de crisis o cuarto de pánico.

8.5.2 Arquitectura de infraestructura tecnológica

Con el fin de fortalecer la gestión, identificación y descripción de las capacidades de servicios claves de la infraestructura tecnológica se debe:

- Fortalecer la gestión de la arquitectura de TI con el fin de mejorar la gestión de la plataforma tecnológica con mayor la mayor eficiencia, optimización y transparencia
- Adicionar indicadores relacionados con monitoreo de uso, disponibilidad y capacidades de la infraestructura de TI, realizando análisis periódicos con los resultados del monitoreo para la identificación de mejoras, adicionales a los indicadores de disponibilidad de la infraestructura que actualmente se reportan mensual y trimestralmente.
- Fortalecer el equipo de trabajo y sus capacidades con profesionales especializados en arquitectura de infraestructura de TI o fortalecer las capacidades de los ingenieros del área.
- Documentar y mantener las arquitecturas que representan todos los elementos de infraestructura de TI que soportan la operación de la UAECD, integrados a ARCHIMATE y la CMDB que facilite su consulta y actualización, teniendo en cuenta las nuevas implementaciones de Catastro Multipropósito – Go Catastral en los territorios y Bogotá.

8.5.3 Sistema de Copias de respaldo

Con el fin de crear arquitecturas resilientes, se debe realizar una copia de seguridad de los datos, las aplicaciones y los entornos operativos (definidos como sistemas operativos configurados con

aplicaciones) para cumplir los requisitos de los objetivos de punto de recuperación (RPO) y de tiempo de recuperación (RTO).

Se debe identificar los distintos servicios en los que residen sus datos en la aplicación. Asegurando la funcionalidad de copia de seguridad de cada servicio y de diseñar la aplicación que la rodea.

Identificar todos los datos de los servicios de almacenamiento en la nube (NVMe local, almacenamiento de bloques, archivos y objetos) que requieren copia de seguridad y realice copias de seguridad manuales o automáticas.

Revisar y considerar lo siguiente para su almacenamiento en la nube:

Oracle Cloud Infrastructure dispositivos NVMe conectados localmente

- Algunas unidades de instancia de Oracle Cloud Infrastructure incluyen dispositivos NVMe asociados localmente. Estos dispositivos proporcionan una latencia extremadamente baja, un almacenamiento en bloque de alto rendimiento. Oracle Cloud Infrastructure no protege estos dispositivos; son dispositivos individuales instalados localmente en la instancia. Es su responsabilidad proteger y gestionar la durabilidad de los datos en estos dispositivos.

- Hay tres modos de fallo principales que debe tener en cuenta al proteger los dispositivos NVMe locales:
    - Fallo de un dispositivo NVMe
    - Pérdida de la instancia o el dominio de disponibilidad
    - Corrupción o pérdida de datos por error de aplicación o usuario

- Puede mitigar el fallo de un dispositivo NVMe en Linux mediante el uso de Local Volume Manager (LVM) para reflejar el dispositivo. Los otros dos requieren implementar un método de copia de seguridad.

Oracle Cloud Infrastructure Block Volumes

- El servicio de volumen en bloque permite aprovisionar y gestionar de forma dinámica volúmenes de almacenamiento en bloque. Todos los volúmenes tienen durabilidad incorporada y se ejecutan en hardware redundante dentro de un único dominio de disponibilidad. Proporciona funciones integradas para realizar copias de seguridad de los datos en Oracle Cloud Infrastructure Object Storage. Puede utilizar las copias de seguridad

para la continuidad del negocio y la recuperación ante desastres. Están disponibles las siguientes opciones de copia de seguridad:

- Copias de seguridad programadas automatizadas y basadas en políticas, con la opción de incrementales o completas. Las políticas están predefinidas o definidas por el usuario.
- Copias de seguridad manuales bajo demanda, con una selección de incrementales o completas. Las copias de seguridad manuales no tienen ningún período de retención asociado y se almacenan indefinidamente.

Sistemas de base de datos de Oracle Cloud Infrastructure

- Los sistemas de Oracle Cloud Infrastructure Database proporcionan métodos para crear copias de seguridad de sus bases de datos en Oracle Cloud Infrastructure Object Storage, Oracle Database Zero Data Loss Autonomous Recovery Service o en un disco local.

  - Copia de seguridad automática

Al activar la función Copia de seguridad automática, puede elegir entre Autonomous Recovery Service o Object Storage como destino de copia de seguridad. Autonomous Recovery Service ofrece una recuperación sin pérdida de datos con protección de base de datos en tiempo real, utiliza un paradigma de copia de seguridad incremental para siempre y realiza automáticamente la validación de recuperación. Esto ayuda a garantizar que la base de datos esté siempre protegida y lista para la recuperación. El almacenamiento de objetos crea copias de seguridad incrementales diarias y completas semanales. Ambos destinos permiten definir un período de retención para las copias de seguridad y gestionar el programa de copias de seguridad.

  - Copias de seguridad según la demanda
  - Puede crear una copia de seguridad de la base de datos en cualquier momento, a menos que la base de datos asuma el rol en espera junto con Oracle Data Guard. Cuando el almacenamiento de objetos es el destino de copia de seguridad, las copias de seguridad bajo demanda son copias de seguridad completas y permanecen en el almacenamiento de objetos incluso después de que la base de datos haya terminado. Cuando el servicio de recuperación autónomo es el destino, las copias de seguridad a demanda son incrementales y se conservan según el período de retención.

- También puede utilizar Oracle Recovery Manager (RMAN) para gestionar las copias de seguridad de los sistemas de base de datos en su propio almacenamiento de objetos.

- Copia de Seguridad de Disco Local
- Las copias de seguridad se almacenan localmente en el área de recuperación rápida del sistema de base de datos. No es un enfoque recomendado porque proporciona baja durabilidad y si el sistema de base de datos deja de estar disponible, la copia de seguridad también no está disponible.

8.5.4 Administración de la operación

Con el fin de garantizar la disponibilidad y continuidad de los servicios tecnológicos se debe disponer de monitoreo NOC/SOC (Análisis de Vulnerabilidades / Ethical Hacking / Pruebas de Ingeniería Social). Para esto es necesario evaluar en la vigencia 2024 el recurso, dado que por restricciones en el presupuesto fue necesario retirarlo del PAA.

Adicionalmente, automatizar los procedimientos de operación de la infraestructura tecnológica incluidos los planes de mantenimiento, diagnósticos y resolución de incidentes así como la atención de requerimientos.

8.6 USO Y APROPIACIÓN

Para el 2024 se debe actualizar el plan de comunicaciones de la Gerencia de Tecnología incluyendo las recomendaciones resultado de las encuestas

Adicional a la ejecución del plan de comunicaciones se recomienda hacer un día de tecnología en que se puedan exponer lo que hace la Gerencia de Tecnología.

Se debe fortalecer el uso y aprobación del sitio de la Gerencia de Tecnología aprovechando sus redes en Yammer

Para las jornadas de inducción a los nuevos funcionarios se recomienda hacer la presentación desde el sitio de la Gerencia de Tecnología, el cual se debe mantener actualizado e incluir más información de interés según las sugerencias de los usuarios.

8.7 SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta que la implementación del Modelo de seguridad y privacidad de la información se establece dentro del ciclo de mejoramiento continuo del sistema de gestión de seguridad y privacidad de la información, se debe continuar con:

- ✓ Implementación de una herramienta o solución tecnológica que permita gestionar los riesgos de seguridad de la información.
- ✓ Implementación de un tablero de control para el seguimiento en la ejecución del plan del Sistema de Gestión de Seguridad de la Información (SGSI)
- ✓ Evaluación e implementación de solución para evitar la pérdida o fuga de información.
- ✓ Implementación de controles de seguridad en el ciclo de Desarrollo Seguro
- ✓ Revisión y fortalecimiento de controles de seguridad a nivel de infraestructura tecnológica.
- ✓ Fortalecimiento de la cultura de seguridad de la información.
- ✓ Los procesos de análisis de vulnerabilidades.

Adicionalmente y para mejorar el MSPI, se requiere:

- ✓ Automatizar el proceso de gestión de activos de información.
- ✓ Fortalecer la implementación de desarrollo seguro en los sistemas y portales de la Unidad.
- ✓ Fortalecer el proceso de gestión incidentes mediante la contratación del NOC/SOC.
- ✓ Verificación permanente del cumplimiento de los controles existentes.
- ✓ Actualización del modelo de seguridad conforme con la norma ISO 27001:2022.

Por último, se sugiere el fortalecimiento del equipo de seguridad de la información, el cual debería estar compuesto mínimo por:

- ✓ 1 oficial de seguridad de la información
- ✓ 1 profesional de apoyo con experticia en estrategia, definición de políticas y lineamientos, gestión de activos de información y riesgos de seguridad de la información.
- ✓ Profesional/técnico apoyo en la ejecución y verificación de controles de seguridad de la información.

9 HALLAZGOS Y BRECHAS

Los hallazgos y brechas identificados a partir de la situación actual con el fin de lograr mejoras en la gestión de TI, se relacionan a continuación:

ID	BRECHA
BreCGG01	Hace falta formalizar y socializar las nuevas Políticas de la Gerencia de Tecnología
BreCGG02	Hace falta consolidar y completar la documentación en Archimate de los diferentes dominios
BreCGG03	Hace Falta fortalecer el sitio de la GT como un instrumento de gestión y transferencia de conocimiento para facilitar el uso y aprovechamiento de las TIC
BreCGG04	Están pendientes por solucionar recomendaciones de MinTIC sobre la evaluación del FURAG de la Política de Gobierno Digital
BreCGG05	Hace falta consolidar la optimización de la Gestión de accesos
BreCGG06	Está pendiente por completar la ejecución del plan de transformación digital 2023-2024
BreSEG01	Se debe continuar con el fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) teniendo en cuenta los lineamientos vigentes de gobierno digital.
BreSEG02	Hace falta fortalecer nuevos controles de seguridad en el ciclo de Desarrollo Seguro
BreSIS01	Está pendiente evaluar el grado de obsolescencia de las herramientas de desarrollo de los Sistemas de Información
BreSIS02	Hace falta definir un plan de gestión y transferencia del conocimiento para la actualización de los Sistemas de Información
BreSIS03	Hace falta revisar funcionalidades y requerimientos actuales de los Sistemas de Información para implementar mejoras
BreSIS04	Se debe continuar fortaleciendo la interoperabilidad de sistemas misionales frente al modelo LADM COL
BreITI01	Está pendiente la actualización de la infraestructura tecnológica que aún presenta obsolescencia (seguridad, sistemas operativos, firewall, UPS, aire acondicionado, switches), incluyendo optimización de costos y capacidades en la nube
BreITI02	Hace falta actualizar la documentación del inventario de infraestructura en Archimate

ID	BRECHA
BreITI03	Hace falta mejorar la gestión de copias de respaldo
BreITI04	No se dispone de herramientas para el monitoreo tipo NOC/SOC
BreITI05	Hacen falta pruebas del Plan de Recuperación de Desastres (DRP) de servicios de TI

10 PORTAFOLIO DE PROYECTOS DE TI

10.1 Identificación de proyectos de TI

Teniendo en cuenta los avances logrados al 2023 de las brechas y proyectos definidos, para el 2024 se realizaron los siguientes cambios del portafolio de proyectos:

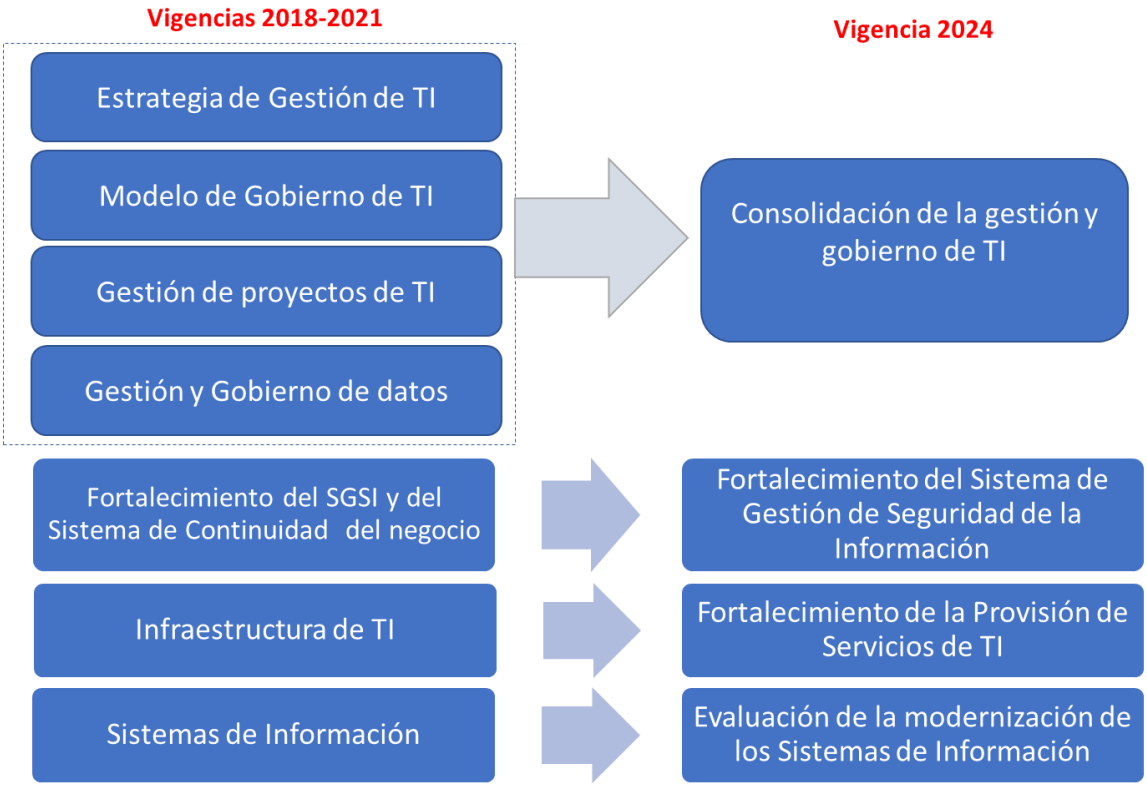


Ilustración 59. Nuevo portafolio de proyectos 2024

El portafolio de proyectos propuesto describe la ruta de implementación de la estrategia e iniciativas propuestas en el PETI para el 2024. No obstante, la Unidad Administrativa Especial de Catastro Distrital evaluará y decidirá la viabilidad de implementación de estos en virtud del presupuesto asignado a la Gerencia de Tecnología y de las prioridades de la nueva dirección de la UAECD.

10.1.1 Gestión y Gobierno de TI

Id del proyecto	**PR01**
Nombre del proyecto	**Consolidación de la gestión y gobierno de TI**
Objetivos del proyecto	1. Formalizar y socializar las nuevas Políticas de la Gerencia de Tecnología 2. Consolidar y completar la documentación en Archimate de los diferentes dominios. 3. Fortalecer el sitio de la Gerencia de Tecnología como un instrumento de gestión y transferencia de conocimiento para facilitar el uso y aprovechamiento de las TIC 4. Solucionar recomendaciones de MinTIC sobre la evaluación del FURAG de la Política de Gobierno Digital 5. Consolidar la optimización de la Gestión de accesos 6. Completar la ejecución del plan de transformación digital 2023-2024
Procesos de la entidad impactadas con el proyecto	1. Proceso GESTIÓN Y DESARROLLO DE LAS TIC
Brechas cerradas con el proyecto	BreCGG01, BreCGG02, BreCGG03, BreCGG04, BreCGG05, BreCGG06
Productos	1. Nuevas Políticas de la Gerencia de Tecnología formalizadas y socializadas 2. Documentación de arquitectura empresarial en Archimate actualizada. 3. Sitio de la Gerencia de Tecnología actualizado y socializado 4. Recomendaciones de MinTIC sobre la evaluación del FURAG de la Política de Gobierno Digital priorizadas, viabilizadas y resueltas 5. Optimización de la Gestión de accesos realizada 6. Plan de transformación digital de la vigencia 2024 ejecutado y socializado
Estimación de esfuerzo y tiempo	1 año

Estimación de costos de inversión	$194,340,000
Estimación de costo anual de operación	$0
Recursos requeridos	1. Líder de Gobierno Digital 2. Profesional experto en Gobierno Digital y Transformación Digital. 3. Profesionales especializados arquitectura empresarial y misional, arquitectura de datos, arquitectura de software y arquitectura de infraestructura

10.1.2 Sistema de Gestión de Seguridad de la Información (SGSI)

Id del proyecto	**PR02**
Nombre del proyecto	Fortalecimiento del Sistema de Gestión de Seguridad de la Información
Objetivos del proyecto	1. Fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) teniendo en cuenta los lineamientos vigentes de gobierno digital. 2. Fortalecer con nuevos controles de seguridad el ciclo de Desarrollo Seguro.
Procesos de la entidad impactadas con el proyecto	1. Proceso GESTIÓN Y DESARROLLO DE LAS TIC
Brechas asociadas con el proyecto	BreSEG01, BreSEG02
Productos	1. Sistema de Gestión de Seguridad de la información (SGSI), actualizado de acuerdo con los lineamientos vigentes de Gobierno digital. 2. Controles definidos para el fortalecimiento del ciclo de desarrollo seguro.
Estimación de esfuerzo y tiempo	1 año
Estimación de costos de inversión	$94,198,000
Estimación de costo anual de operación	$0
Recursos requeridos	1. Oficial de Seguridad 2. Profesional de apoyo con experticia en estrategia, definición de políticas y lineamientos, gestión de activos de información y riesgos de seguridad de la información.

10.1.3 Sistemas de Información

Id del proyecto	**PR03**
Nombre del proyecto	**Evaluación de la modernización de los sistemas de información**
Objetivos del proyecto	1. Evaluar el grado de obsolescencia de las herramientas de desarrollo de los Sistemas de Información. 2. Definir un plan de gestión y transferencia del conocimiento para la actualización de los Sistemas de Información. 3. Revisar funcionalidades y requerimientos actuales de los Sistemas de Información para implementar mejoras 4. Fortalecer la interoperabilidad de sistemas misionales frente al modelo LADM COL
Procesos de la entidad impactadas con el proyecto	1. Proceso GESTIÓN Y DESARROLLO DE LAS TIC
Brechas cerradas con el proyecto	BreSIS01, BreSIS02, BreSIS03, BreSIS04
Productos	1. Informe del grado de obsolescencia de las herramientas de desarrollo de los Sistemas de Información. 2. Plan de gestión y transferencia del conocimiento definido para la actualización de los Sistemas de Información. 3. Relación de funcionalidades y requerimientos actuales de los Sistemas de Información priorizados y viabilizados 4. Interoperabilidad de sistemas misionales frente al modelo LADM COL realizada
Estimación de esfuerzo y tiempo	1 año
Estimación de costos de inversión	$0
Estimación de costo anual de operación	$0
Recursos requeridos	Equipo de Trabajo (subgerencia de Ingeniera de Software)

10.1.4 Infraestructura de TI

Id del proyecto	**PR04**
Nombre del proyecto	**Fortalecimiento Provisión de Servicios de TI**

Objetivos del proyecto	1. Actualizar la infraestructura tecnológica que aún presenta obsolescencia (seguridad, sistemas operativos, firewall, UPS, aire acondicionado, switches), incluyendo optimización de costos y capacidades en la nube. 2. Actualizar la documentación del inventario de infraestructura en Archimate. 3. Mejorar la gestión de copias de respaldo 4. Disponer de monitoreo NOC/SOC para garantizar la disponibilidad y continuidad de los servicios tecnológicos. 5. Continuar las pruebas del Plan de Recuperación de Desastres (DRP) de servicios de TI
Procesos de la entidad impactadas con el proyecto	1. Proceso GESTIÓN Y DESARROLLO DE LAS TIC
Brechas cerradas con el proyecto	BreITI01, BreITI02, BreITI03, BreITI04, BreITI05
Productos	1. Infraestructura tecnológica actualizada que aún presenta obsolescencia (seguridad, sistemas operativos, firewall, UPS, aire acondicionado, switches), incluyendo optimización de costos y capacidades en la nube. 2. Documentación del inventario de infraestructura actualizada en Archimate. 3. Gestión de copias de respaldo mejorado 4. Herramienta de monitoreo NOC/SOC implementada. 5. Pruebas del Plan de Recuperación de Desastres (DRP) de servicios de TI realizadas.
Estimación de esfuerzo y tiempo	1 año
Estimación de costos de inversión	$188,674,500
Estimación de costo anual de operación	$0
Recursos requeridos	1. Equipo de trabajo (subgerencia de Infraestructura tecnológica) 2. Soporte especializado para el Plan de Continuidad del Negocio de TI 3. Arquitecto de tecnología de la UAECD.

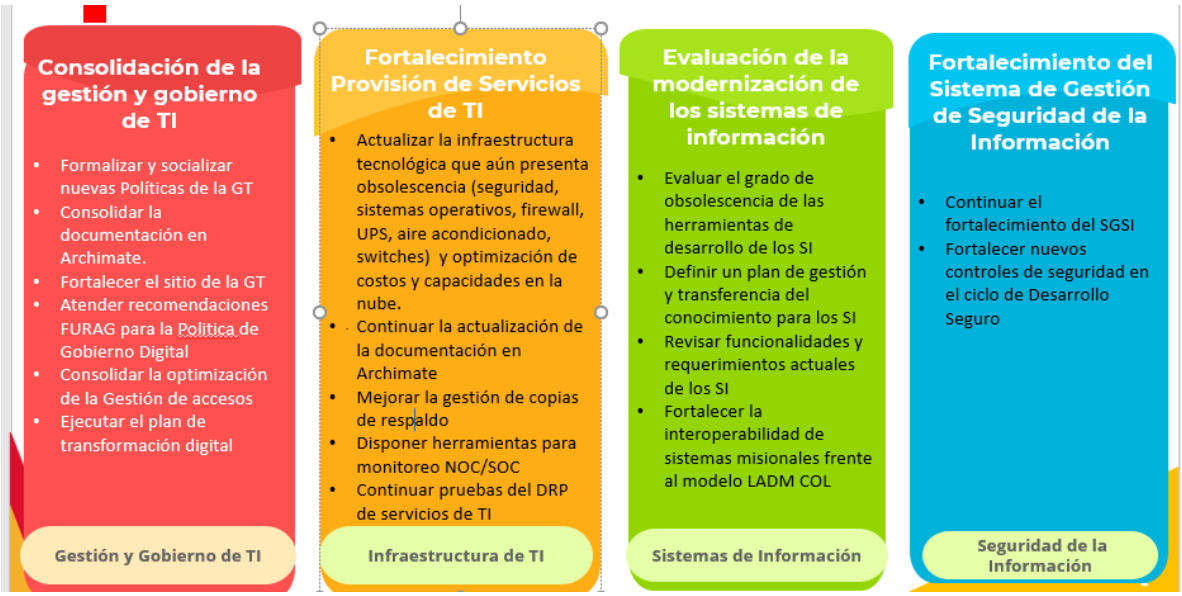
10.2 Hoja de Ruta y Presupuesto

A continuación, se describe la ejecución de los proyectos en una línea de tiempo para el último año de ejecución del Plan Estratégico de Tecnologías de la Información – PETI 2021-2024 , con base en la estimación de esfuerzo, tiempo y el presupuesto asignado a la Gerencia de Tecnología.

NOMBRE DEL PROYECTO	2024												COSTO PROYECTO
	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	
Consolidación de la gestión y gobierno de TI													$194,340,000
Fortalecimiento del Sistema de Gestión de Seguridad de la Información													$94,198,000
Evaluación de la modernización de los sistemas de información													$0
Fortalecimiento Provisión de Servicios de TI													$188,674,500
TOTAL PROYECTOS TI													**$477,212,500**
LÍNEAS DE GASTOS	**2024**												**COSTO 2024**
Infraestructura TI / Servicios Tecnológicos - Funcionamiento												$3,474,046,787	$3,474,046,787
Licenciamiento - Funcionamiento												$346,812,575	$346,812,575
Infraestructura TI /Servicios Tecnológicos - Inversión												$8,742,127,575	$8,742,127,575
Licenciamiento - Inversión												$712,407,425	$712,407,425
Talento Humano - Inversión												$1,082,365,000	$1,082,365,000
TOTAL COSTO OPERACIÓN TI												**$14,357,759,363**	**$14,357,759,363**
PRESUPUESTO INVERSIÓN													$10,536,900,000
PRESUPUESTO FUNCIONAMIENTO													$3,820,859,363
PRESUPUESTO TOTAL													$14,357,759,363

Ilustración 60. Hoja de Ruta y Presupuesto PETI 2023-2024

Las actividades de la hoja de ruta generales, cuyos cronogramas se detallarán en el primer trimestre del 2024 para avanzar en el cierre de las brechas de cada uno de los proyectos del PETI, son las siguientes:



Sobre la hoja de ruta y el presupuesto descrito, de debe tener en cuenta:

- En la línea de tiempo de ejecución del último año de ejecución del PETI, se presupuestó solo el costo del recurso humano especializado de apoyo a la Gerencia de Tecnología para Gobierno Digital, Transformación Digital, Seguridad y Privacidad de la Información, Continuidad del Negocio y Arquitectura empresarial. Este costo se incluyó en la versión inicial de presupuesto y se está definiendo si queda o no incluido en el presupuesto de inversión de Talento Humano, dado los recortes presupuestales. En el caso que en la priorización no quede alguno de los recursos requeridos el alcance del proyecto se reducirá.

- El presupuesto corresponde a la última versión enviada a la Oficina Asesora de Planeación de la UAECD del año 2023, en el mes de diciembre, para la prestación de los servicios TI por parte de la Gerencia de Tecnología, sobre el cual se deben tener en cuenta las siguientes consideraciones:

    - El presupuesto solicitado por la Gerencia de Tecnología ha sido ajustado por la Oficina Asesora de Planeación de la UAECD de la siguiente manera debido a restricciones presupuestales, impactando al alcance de los proyectos del PETI y el riesgo de la prestación continua de los servicios tecnológicos:

Versión Presupuesto	Talento Humano	Servicios Tecnológicos	Totales

Presupuesto solicitado (julio 2023)	$ 3,344,703,500.00	$ 29,088,141,905.00	$ 32,432,845,405.00
Presupuesto aprobado (diciembre 2023)	$ 1,082,365,000.00	$ 13,275,394,362.00	$ 14,357,759,362.00
Diferencia	$ 2,262,338,500.00	$ 15,812,747,543.00	$ 18,075,086,043.00

- Según el presupuesto asignado para la vigencia 2024, fue necesario disminuir el recurso humano de prestación de servicios en un 60% aproximadamente, lo que causa impacto directo en la ejecución del PETI y la prestación de los servicios de TI que brinda la Gerencia de tecnología, así:

  1. La capa Argis se queda sin soporte y Capa media con un solo recurso para su gestión
  2. Se aceptarán pocas órdenes de cambio por temas de recurso humano (solo con funcionarios de planta)
  3. El aplicativo Go Catastral no contará ni con personal de planta ni contratistas
  4. No se cuenta con soporte en horarios extendidos ni fines de semana
  5. Se comprometen los acuerdos de niveles de servicio definidos en el portafolio de servicios de TI
  6. No se realizaría monitoreo de las plataformas
  7. Se priorizaría la solución de incidentes
  8. Dificultades para la realización de los contratos que vencen el primer trimestre (ELA, licencias Microsoft, licencias Oracle, nube OCI, nube Azure).
  9. Cancelar vacaciones funcionarios de planta
  10. Las actividades de Gobierno Digital y Arquitectura Empresarial y seguridad de la información con baja gestión.
  11. Incumplimiento de las metas definidas en el proceso de planeación.
  12. Perdida de personal especializado (contratistas con el conocimiento de la infraestructura, sistemas de información de Bogotá y CM)
  13. Incumplimiento para generar archivos XTF y RIC en los primeros meses del año

11 PLAN DE COMUNICACIONES DEL PETI

A continuación, se relacionan los medios de comunicación y actividades que se utilizarán para la divulgación y adopción del PETI en la Unidad Administrativa Especial de Catastro Distrital, cuya implementación se realizará de forma integrada con la estrategia de uso y apropiación, la cual corresponde a uno de los proyectos propuestos en el PETI.

MEDIOS	ACTIVIDAD	FORMATOS	PERIODICIDAD	GRUPO DE INTERES
Portal Web	Reemplazar la versión del PETI publicada en la sección de transparencia y acceso a la información pública del portal institucional.	Documento PDF	Tan pronto sea aprobado y cada vez que se actualice (mínimo una vez al año)	Ciudadanos
Intranet	Publicar un resumen del PETI y el documento completo. Publicar en video y/o presentación que explique la importancia del PETI para Catastro	Documento PDF Video o presentación	Cada vez que se actualice (mínimo una vez al año)	Funcionarios de Planta Contratistas
Red social Institucional	Elaborar piezas gráficas y contenidos para promocionar el PETI. Informar la aprobación y publicación del PETI Publicar noticias y novedades de los avances en la implementación del PETI de interés de los servidores públicos.	Mensajes y/o Pieza gráfica	Trimestralmente	Funcionarios de Planta Contratistas
Boletín Institucional	Informar la aprobación y publicación del PETI Publicar noticias y novedades de los avances en la implementación del PETI.	Pieza gráfica	Trimestralmente	Funcionarios de Planta Contratistas

MEDIOS	ACTIVIDAD	FORMATOS	PERIODICIDAD	GRUPO DE INTERES
Correo institucional	Informar la aprobación y publicación del PETI Enviar noticias y novedades de los avances en la implementación del PETI.	Mensajes y/o Pieza gráfica	Mensualmente	Funcionarios de Planta Contratistas
Eventos de socialización	Informar del alcance del PETI y los proyectos estratégicos. Informar sobre noticias y novedades de los avances en la implementación del PETI	Presentación	Semestral	Funcionarios de Planta Contratistas
Carteleras	Publicar noticias y novedades de los avances en la implementación del PETI.	Pieza gráfica	Trimestralmente	Funcionarios de Planta Contratistas
Encuestas	Medir el nivel de entendimiento, adopción e importancia del PETI	Encuesta en línea	Semestral	Funcionarios de Planta Contratistas
Sesiones de Inducción	Presentar el PETI y su importancia para Catastro	Sesiones Virtuales y/o presenciales	Cada vez que se programe una inducción	Funcionarios de Planta Contratistas
Redes sociales	Enviar noticias y novedades de los avances en la implementación del PETI.	Mensajes y/o Pieza gráfica	Trimestralmente	Ciudadanos

MEDIOS	ACTIVIDAD	FORMATOS	PERIODICIDAD	GRUPO DE INTERES
Informes de gestión	Informar avances del PETI y su impacto en Catastro	Documento con logros y avances en PDF	Cada vez que lo soliciten	Funcionarios de Planta Contratistas