



CRA



ARQUITECTURA EMPRESARIAL

Arquitectura de Servicios Tecnológicos

**COMISIÓN DE REGULACIÓN DE AGUA POTABLE
Y SANEAMIENTO BÁSICO**

Tabla de contenido

1. ARQUITECTURA DE SERVICIOS TECNOLÓGICOS	4
1.1. ARQUITECTURA DE TI - SITUACIÓN ACTUAL	7
.....	7
1.2. DIRECTORIO DE SERVICIOS TECNOLÓGICOS	8
1.2.1. Servidores físicos y virtuales	8
1.2.2. Dispositivos de almacenamiento	12
1.2.3. Dispositivos de comunicaciones	13
1.2.4. Otros equipos del centro de datos	14
1.2.5. Equipos de cómputo usuarios finales	14
1.2.6. Dispositivos de impresión	15
1.3. CATÁLOGO DE SERVICIOS DE TI	15
1.4. ELEMENTOS PARA EL INTERCAMBIO DE INFORMACIÓN	19
1.5. PLAN DE GESTIÓN DE SERVICIOS DE TI	22
1.5.1. Gestión de la capacidad	22
1.5.2. Gestión de la seguridad	25
1.5.3. Gestión de la disponibilidad	29
1.5.4. Gestión de continuidad	32
1.6. ACCESO A SERVICIOS EN LA NUBE	40
1.7. TECNOLOGÍA VERDE	42
2. OPERACIÓN DE LOS SERVICIOS TECNOLÓGICOS	42
2.1. ALTA DISPONIBILIDAD DE LOS SERVICIOS TECNOLÓGICOS.....	42
3. SOPORTE DE LOS SERVICIOS TECNOLÓGICOS	43
3.1. MESA DE SERVICIO	46
4. GESTIÓN DE LA CALIDAD Y LA SEGURIDAD DE LOS SERVICIOS TECNOLÓGICOS	48
4.1. ANÁLISIS DE RIESGOS.....	48
5. ARQUITECTURA DE TI - SITUACIÓN OBJETIVO	50
5.1. ANÁLISIS DE BRECHAS.....	51
6. REFERENCIAS	55

Histórico de revisiones

Fecha	Versión	Descripción	Autor
24/04/2019	1.0	Definición inicial de la Arquitectura de Servicios Tecnológicos de la CRA de acuerdo con el MRAE de MinTIC.	Oficina Asesora de Planeación y TIC
10/07/2019	1.1	Ajustes al ítem soporte de los servicios tecnológicos y acceso a los servicios en la nube.	Oficina Asesora de Planeación y TIC
31/07/2019	2.0	Ampliación de los puntos relacionados con el Plan de Gestión de Servicios de TI, Políticas de seguridad de la información, elementos para el intercambio de información y procedimientos de respaldo.	Oficina Asesora de Planeación y TIC
31/10/2019	2.1	Actualización de los datos de almacenamiento relacionados en gestión de la capacidad.	Oficina Asesora de Planeación y TIC

1. Arquitectura de servicios tecnológicos

Como un ámbito del Dominio de servicios tecnológicos del MRAE, la Arquitectura de Servicios Tecnológicos busca apoyar la definición y diseño de la Arquitectura de la infraestructura tecnológica que se requiere para soportar los Sistemas de Información y el portafolio de servicios de una entidad. En este sentido, el presente documento expone la situación actual y la situación objetivo de la infraestructura tecnológica de la CRA, indispensable para el cumplimiento de sus funciones.

También es importante para la elaboración de este ejercicio recalcar que de acuerdo con la Guía General de Adopción del Marco de Referencia de Arquitectura Empresarial de MinTIC¹ (2015) las guías elaboradas y utilizadas para apoyar la adopción de este Marco tienen un objetivo centralmente orientador para las entidades públicas y así deben ser entendidas. De este modo, MinTIC aclara que *“es importante que las instituciones tengan presente que la adopción del Marco de Referencia de AE es un proceso continuo en el cual, por medio de ejercicios de Arquitectura Empresarial enfocados en resolver necesidades específicas, las instituciones van incorporando gradualmente las buenas prácticas de gestión que se enuncian en el Marco de Referencia. **A medida que una institución avanza en el desarrollo de los ejercicios de AE su nivel de madurez en el uso del mismo es cada vez mayor**”* (subrayado y en negrilla por fuera de texto). Esto último permite a la entidad avanzar de acuerdo a lo planeado en el PETI, en función de su disponibilidad presupuestal y de su recurso humano.

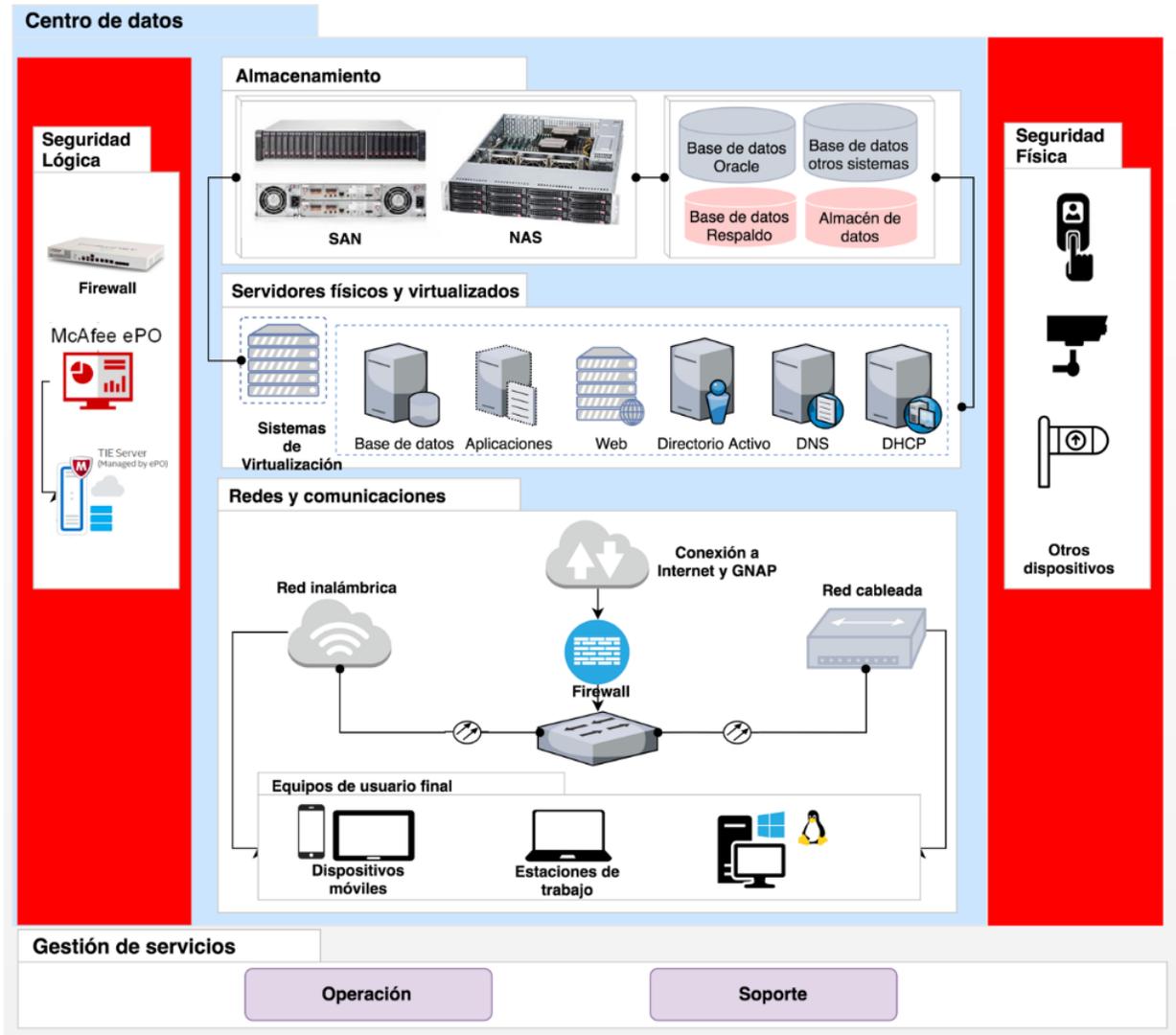
Al respecto también se pronuncia la Guía para la construcción del PETI (2019) *“Al ser documentos prácticos deben tomarse como una orientación o buena práctica más no como una obligatoriedad (...) Adicionalmente, la metodología también puede ser ajustada con base en el criterio profesional de los responsables de su implementación mediante el uso de mejores prácticas en Arquitectura Empresarial, Gerencia de Proyectos de TI, Gestión y Gobierno de TI (...)”*

Sin embargo, es importante señalar que la siguiente Arquitectura de servicios tecnológicos, busca entre otros aspectos, describir el plan de capacidad donde se identifiquen las capacidades actuales de los servicios tecnológicos y se logre contar con herramientas para proyectar las capacidades futuras requeridas para un óptimo funcionamiento de los servicios de la entidad, lo que no implica que en la actualidad no se gestionen eficientemente los servicios para responder a los usuarios internos y externos de la entidad. De igual forma la Arquitectura busca consolidar el directorio de servicios tecnológicos y la definición de su arquitectura haciendo uso de un esquema en la nube.

De acuerdo con lo anterior, es preciso describir inicialmente la Arquitectura de Referencia de los servicios tecnológicos de la CRA, la cual está conformada por cinco capas (centro de datos, Infraestructura de almacenamiento y procesamiento, redes y comunicaciones, gestión de servicios y seguridad lógica y física) que se detallan a continuación:

¹ https://mintic.gov.co/arquitecturati/630/articles-9434_Guia_Proceso.pdf

Gráfico 1. Arquitectura de referencia servicios tecnológicos

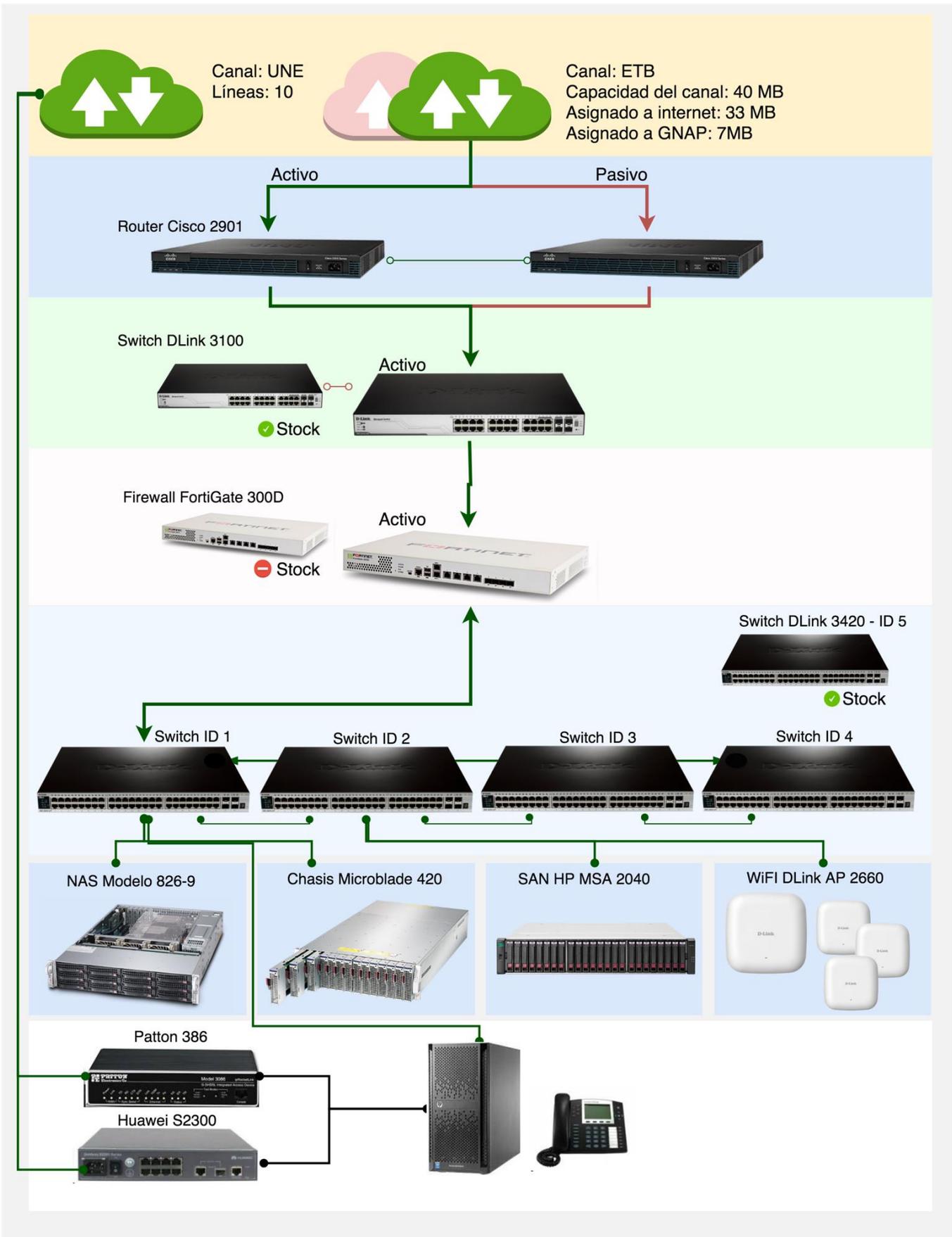


Fuente: Elaboración propia con base en información suministrada por la CRA

Capas	Descripción
Capa 1. Centro de Datos	La primera capa comprende el Centro de Datos, donde se concentra y aloja toda la infraestructura de procesamiento, almacenamiento, comunicaciones y componentes que garantizan su funcionamiento y operación (aires acondicionados, UPS, entre otros).
Capa 2. Infraestructura de almacenamiento y procesamiento	La segunda capa está compuesta por la infraestructura de almacenamiento y de procesamiento. Como parte del sistema de almacenamiento la entidad tiene implementado los dispositivos tipo SAN y NAS. El procesamiento se gestiona por medio de los sistemas de virtualización como VmWare,

Capas	Descripción
	<p>OracleVM y Hyper-V. Actualmente los servidores se encuentran clasificados en los siguientes grupos:</p> <ul style="list-style-type: none"> • <i>Servidores de aplicaciones:</i> alojan aplicaciones y lógica de los sistemas internos de la entidad. • <i>Servidores de bases de datos:</i> alojan los motores de datos con información estructurada. • <i>Servidores de infraestructura:</i> aloja la información no estructurada y servicios relacionados con la gestión de la infraestructura de TI.
<p>Capa 3. Redes y comunicaciones</p>	<p>La tercera capa comprende los aspectos relacionados con los servicios de redes que posibilitan las comunicaciones entre la plataforma tecnológica con los grupos de interés internos y externos de la entidad.</p>
<p>Capa 4. Gestión de servicios</p>	<p>En la cuarta capa se encuentra la gestión de servicios de TI que comprende la operación y el soporte de los servicios tecnológicos, orientados a que los procesos, las personas y la tecnología estén alineados a la estrategia global de la entidad, así como también a las necesidades, prioridades y disponibilidad de recursos tecnológicos requeridos.</p> <p>Todo esto para brindar servicios a las diferentes áreas de negocio internas y externas de la organización que están dotadas de las herramientas necesarias para acceder a todos los recursos informáticos disponibles, desde estaciones de trabajo, servicios de impresión, dispositivos móviles y periféricos en general.</p>
<p>Capa 5. Seguridad lógica y física</p>	<p>La seguridad lógica hace referencia a todos los mecanismos de control de acceso a los recursos informáticos basados en identificación de usuario y todos los permisos asociados a su rol al interior de la entidad. Incluye también todas las medidas de protección contra ataques internos y externos que puedan vulnerar la protección de la información. La seguridad lógica es provista por una empresa externa que provee como mecanismo de control un dispositivo Firewall. La seguridad física por su parte, se refiere a todos los controles que impiden y persuaden a las personas no autorizadas a ingresar a zonas restringidas y controladas (biométricos, cámaras de seguridad, entre otros controles).</p>

1.1. Arquitectura de TI - situación actual



De acuerdo con el MinTIC, los Servicios Tecnológicos constituyen uno de los dominios del marco de referencia de arquitectura de TI que define estándares y lineamientos para la gestión de la infraestructura tecnológica que soporta los sistemas y los servicios de información, así como los servicios requeridos para su operación. De este modo, la situación actual de la arquitectura de servicios tecnológicos, consolida las vistas y artefactos relacionados con las necesidades que la CRA busca solucionar por medio de la definición de la arquitectura empresarial. En este sentido, esta comprende la definición de la infraestructura tecnológica, la gestión de la capacidad de los servicios de TI, la gestión de la operación, así como la gestión de los servicios de soporte.

1.2. Directorio de Servicios Tecnológicos

El Directorio de servicios tecnológicos² a diferencia de los Servicios de TI³ integran los recursos de la plataforma tecnológica (hardware y software). Estos son gestionados desde la Oficina Asesora de Planeación y TIC por medio del Grupo TIC. Estos se describen a continuación.

1.2.1. Servidores físicos y virtuales

La Arquitectura de Servidores configurada en la CRA, se encuentra diseñada bajo una solución tipo microblade multinodo en un esquema de alta disponibilidad con balanceo de carga. Esta permite por medio de los sistemas de virtualización gestionar la demanda de nuevos servicios y crecer en la medida en que las capacidades y necesidades de las áreas lo requieran.

Los servidores se conectan a un sistema de almacenamiento tipo SAN a través de un esquema redundante de conectividad tipo iSCSI. El respaldo de datos de estos servidores está también basado en iSCSI para lograr un alto desempeño y menos tiempos en la generación de las copias de seguridad. Actualmente la entidad cuenta con los siguientes servidores físicos y virtuales:

ID	Servicio tecnológico	Tipo	Instalados	Soporta IPv6
1	Clúster VMware (3 Cuchillas)	Físico	3	Si
2	Clúster Oracle VM (3 Cuchillas)	Físico	3	Si
3	Plataforma Hyper-V (Servidor Tipo NAS - Rack)	Físico	1	Si
4	Servidor directorio activo principal (Servidor - Rack)	Físico	1	Si
5	Servidor planta Cetrex - (Servidor - Torre)	Físico	1	Si

ID	Servicio tecnológico	Tipo	Instalados	Soporta IPv6
1	Máquinas VMware	Virtuales	24	Si
2	Máquinas Oracle VM	Virtuales	3	Si
3	Máquinas Hyper-V	Virtuales	2	Si

² Pueden ser consultados a detalle en el documento "Directorio de servicios tecnológicos CRA"

³ Ver documento Catálogo de Servicios TI

1.2.1.1. Servidores virtualizados en VMWare según tipo de servidor

ID	Servidor	Tipo de servidor
1	Servidor Web (Producción)	Aplicaciones
2	Servidor Web (Pruebas)	Aplicaciones
3	Servidor JOOMLA Intranet, GLPI Mesa de ayuda	Aplicaciones
4	Servidor Controlador de dominio secundario, DHCP, DNS, FSSO Fortinet	Infraestructura
5	Servidor Web (Producción) - ORFEO	Aplicaciones
7	Servidor Web (Desarrollo) ORFEO	Aplicaciones
8	Servidor CertiCRA	Aplicaciones
9	Registros Entradas Salidas	Aplicaciones
10	Servidor Trident - Aplicativo de contabilidad de almacén - Cliente-Servidor	Aplicaciones
11	Backup Exec - Infraestructura	Infraestructura
12	Central Wi-Fi Manager	Infraestructura
13	Servidor Project Server y AD Connect Exchange Online: sincroniza cuentas de directorio activo con exchange 365 de la nube, BD Project Server 2013	Aplicaciones
14	Servidor de impresión	Infraestructura
15	Servidor administrador de Antivirus, Base de datos MySQL	Infraestructura
16	Servidor Search Engine - Buscador de Bodega de Orfeo	Infraestructura
17	Servidor Development Tools	Aplicaciones
18	Servidor Radius	Infraestructura
19	Orquestados - VMWare 6.5.2	Infraestructura

1.2.1.2. Servidores virtualizados en OracleVM según tipo de servidor

ID	Servidor	Tipo de servidor
1	SRVBDORAPROD	Infraestructura
2	SRVBDORAPRUE	Infraestructura
3	SRVBDORAREPLI	Infraestructura

1.2.1.3. Servidores virtualizados en Hyper-V según tipo de servidor

ID	Servidor	Tipo de servidor
1	Servidor de Bases de Datos (Producción) <ul style="list-style-type: none"> Oracle Database Standard Edition 12c Release 1 	Base de datos
2	Servidor de Bases de Datos (Desarrollo, Pruebas-Calidad) <ul style="list-style-type: none"> Oracle Database Standard Edition Weblogic Server 3. Oracle Business Intelligence 	Base de datos

1.2.1.4. Servidores físicos

ID	Servidor	Cluster	Sistema operativo	Tipo de servidor
1	ESXi-VMWHOST1	VMWare	ESXi-v6.5.0 VMKernel Release 5969303	Aplicaciones
2	ESXi-VMWHOST2		ESXi-v6.5.0 VMKernel Release 5969303	Aplicaciones
3	ESXi-VMWHOST3		ESXi-v6.5.0 VMKernel Release 5969303	Aplicaciones
4	ESXi-VMWHOST4	OracleVM	Oracle VM Manager, Versión: 3.4.5.1919	Base de datos
5	ESXi-VMWHOST5		Oracle VM Manager, Versión: 3.4.5.1919	Base de datos
6	ESXi-VMWHOST6		Oracle VM Manager, Versión: 3.4.5.1919	Base de datos

1.2.1.5. Sistemas operativos de servidores

ID	Sistema operativo	Tipo	Instalados	Soporta IPv6
1	ESXi	ESXi	3	Si
2	Oracle - Linux	Oracle VM	3	Si
3		Oracle Linux Server Release 6.9	4	
4		Oracle Linux Server Release 7.4 /Red Hat Enterprise Linux Server Release 7.4 (Maipo)	2	Si
5		Windows Server 2003 Standard Edition - Service P2	2	Si
6	Windows	Windows Server 2012 R2 Standard Edition	6	Si
7		Windows Storage Server	1	Si
8		Windows Server 2008 R2 Standard Edition	1	Si
9		Windows Server 2008 Standard Edition - Service P1	1	Si
10		Windows Server 2008 Standard Edition - Service P2	1	Si
11		Linux	Linux Debian	1
12	Linux CentOS Release 5.5 (final) x86_64		1	Si
13	Linux Redhat Enterprise Linux Server Release 7.1 (Maipo)		1	Si

1.2.1.6. Software y servicios alojados en servidores

ID	Software y servicios alojados en servidores	Cantidad	Soporta IPv6
1	Software de Control de Acceso Biométrico	1	Si
2	7-ZIP 9.20	2	NA
3	Apache V2.4.6	1	Si
4	Apache V2.2.15	4	Si
5	Apache V2.2.3	1	Si
6	Servidor de Administración del Wifi	1	Si
7	Consola Antivirus	2	NA
8	DNS: Microsoft	2	NA
9	FSSO Fortinet	2	Si
10	EMS SQL Manager 2005 Lite for MySQL	1	NA
11	Git 2.10.1	1	NA
12	GLPI	1	
13	HP Data Protector A.07.00	1	Si
14	HP Usb Key Utility	1	NA
15	IIS 10.0 Express	1	Si
16	Microsoft Application Request Routing	1	Si
17	Microsoft Visual Studio Express 2012	1	Si
18	Microsoft .NET Framework 4.5.1	1	Si
19	Microsoft Azure AD Connect Health Agent for Sync V3.0.68.0	1	Si
20	Microsoft Azure AD Connect Sincronization Services V1.1.613.0	1	Si
21	Microsoft SharePoint Server 2013	1	Si
22	Microsoft SQL Server 2012 R2 V10.52.4000.0	1	Si
23	Microsoft Network Monitor	1	Si
24	Mozilla Firefox 47.0.2	2	Si
25	MySQL V5.6.25	1	Si
26	Open SSL 1.0.1h Light	1	Si
27	Oracle Warehouse Builder V11gR2 - OWB Tahoe Development V11.2.0.4	1	Si
28	Oracle BI (Business Intelligent) 11G	1	Si
29	PHP 5.6.30	1	Si
30	PHP My Admin V 3.3.10.5	1	Si
31	PHP	3	Si
32	PHP(cli)	1	Si
33	PHP squeeze19	1	
34	SolarWinds Exchange Monitor	1	Si
35	Sql Server	1	Si
36	TortoiseGit	1	NA

ID	Software y servicios alojados en servidores	Cantidad	Soporta IPv6
37	Trident Enterprise	1	Si
38	Zend Server	2	NA
39	ZoneAlarm Free Firewall	1	Si
40	Zend Engine v2.3.0	1	NA
41	Weblogic Server	1	Si
42	WampServer 2.4	1	NA

1.2.2. Dispositivos de almacenamiento

La arquitectura de almacenamiento actual de la CRA se basa en una SAN de conectividad redundante con controladoras de disco de alto desempeño y con niveles de protección tipo arreglo de discos RAID 10.

La conectividad de los servidores a la SAN se realiza a través de una red iSCSI privada y dedicada exclusivamente a la SAN. Cada servidor tiene asignado doble tarjeta de red y cada una de estas se conecta a un switch que a su vez se conectan a la SAN. Actualmente la SAN tiene fuentes de poder redundantes (N+1) para que en caso de falla no se afecte el servicio.

Los switches son redundantes y se encuentran configurados para asumir la totalidad de la carga en el momento que uno de ellos presente alguna falla.

Respecto a la unidad de almacenamiento tipo NAS⁴, esta permite alojar las copias de respaldo ejecutadas por la herramienta de Backup Exec. Esta unida fue adquirida en el año 2017 y desde el principio se proyectó para prestar este servicio. Así mismo, presta el servicio de servidor de archivo; carpetas compartidas en red don disposición de uso para el usuario final.

Actualmente la entidad cuenta con los siguientes dispositivos de almacenamiento:

ID	Dispositivo	Equipos	Soporta IPv6	Función
1	SAN HP MSA 2040	Propios	Si	Bases de datos, solución Virtual Oracle VM y Vmware
2	NAS SuperMicro 826-9	Propios	Si	Windows Storage Server 2016 Standard Edition (Servidor de Archivo y servidor de Backup en Disco)

⁴ Ver en documento de Diagnostico NAS V1 CRA

1.2.3. Dispositivos de comunicaciones

ID	Relación	Equipos	Instalados	Soporta IPv6
1	Switch core y usuario final	Propios	5	Si
2	Access Point	Propios	4	Si
3	UNE - Switch UNE Huawei	Externos	1	Si
4	UNE - G.SHDL - PATTON	Externos	1	Si
5	Movistar - Firewall fortigate	Externos	2	Si
6	Router ETB	Externos	2	Si
7	Demarcador - ISCOM- ETB	Externos	2	Si

1.2.3.1. Detalle de los dispositivos de comunicación de la entidad

ID	EQUIPO	MARCA	MODELO	Puertos	ROL	Soporta IPv6
1	Switch	D-Link	DGS-3420-52P	48	Switch Stack	Si
2	Switch	D-Link	DGS-3420-52P	48	Switch Stack	Si
3	Switch	D-Link	DGS-3420-52P	48	Switch Stack	Si
4	Switch	D-Link	DGS-3420-52P	48	Switch Stack	Si
5	Switch	D-Link	DGS-3420-52P	48	Switch Standby	Si
6	Switch	SuperMicro	MBB-GEM-004	4	Switch Stack - Conexión Uno a Uno	Si
7	Switch	SuperMicro	MBB-GEM-004	4	Switch Stack - Conexión Uno a Uno	Si
8	Switch	HUAWEY	Quidway S2300	4	Conexión Canal Planta Telefónica	Si
9	Access Point	D-Link	DAP - 2600	1	Inalámbrica - AP	Si
10	Access Point	D-Link	DAP - 2600	1	Inalámbrica - AP	Si
11	Access Point	D-Link	DAP - 2600	1	Inalámbrica - AP	Si
12	Access Point	D-Link	DAP - 2600	1	Inalámbrica - AP	Si
13	Firewall	Fortinet	FortiGate 300 D	4	Seguridad Perimetral WAN/LAN	Si
14	Router	CISCO	2901	1	Conexión Red WAN	Si
15	Router	CISCO	2901	1	Conexión Red WAN - Backup	Si
16	Demarcador	Raisecom	ISCOM RAX700	4	Transceiver	Si

ID	EQUIPO	MARCA	MODELO	Puertos	ROL	Soporta IPv6
17	Demarcador	Raisecom	ISCOM RAX700	4	Transceiver Backup	Si
18	G.SHDL	PATTON	3086	1	Conexión Canal Planta Telefónica	Si

1.2.4. Otros equipos del centro de datos

ID	Tipo	Equipos	Instalados	Soporta IPv6
1	UPS	UPS-40-KVA -Tipo Torre	1	Si
2		UPS Tipo Torre - Vista 10 KVA	1	Si
3	Aires acondicionados	AIRES 1 SCHNEIDER	2	Si
4		AIRES 2 SCHNEIDER	2	Si
5		AIRES 3 SCHNEIDER	2	Si
6	DVR	DVR	1	Si

1.2.5. Equipos de cómputo usuarios finales

ID	Relación de equipos	Sistema operativo	Instalados	Soporta IPv6
1	Equipo Torre - DELL OptiPlex 390	Microsoft Windows 10 Pro 64 bits	7	Si
2	Equipo Torre - HP EliteDesk 800 G1 SFF	Microsoft Windows 10 Pro 64 bits	2	Si
3	ALL IN ONE LENOVO m700z	Microsoft Windows 10 Pro 64 bits	67	Si
4	ALL IN ONE LENOVO m700z	Microsoft Windows 8 Pro 64 bits	4	Si
5	ALL IN ONE LENOVO m800z	Microsoft Windows 10 Pro 64 bits	2	Si
6	Equipo Torre - HP 8100 SFF	Microsoft Windows 10 Pro 64 bits	2	Si
7	Equipo Torre - HP 8300 elite	Microsoft Windows 10 Pro 64 bits	2	Si
8	LENOVO T460 C5 6300 U	Microsoft Windows 10 Pro 64 bits	5	Si
9	PORTATIL HP PROBOOK 6TDY	Microsoft Windows 10 Pro 64 bits	4	Si
10	PORTATIL LENOVO 10/09 DOCKINIG STATION	Microsoft Windows 10 Pro 64 bits	1	Si
11	PORTATIL LENOVO REF. THINKPAD-X220	Microsoft Windows 10 Pro 64 bits	5	Si

1.2.6. Dispositivos de impresión

ID	Relación de equipos	Sistema operativo	Instalados	Soporta IPv6
1	Lexmark X656de	LEXMARK	3	Si
2	Lexmark T654	LEXMARK	4	Si
3	Lexmark C782	LEXMARK	1	Si
4	HP Laserjet M4345 MFP	HP	1	Si

1.3. Catálogo de servicios de TI

El Catálogo de servicios de TI es un inventario detallado de los servicios de TI que la Entidad tiene implementados y que se encuentran activos. Estos se describen a continuación.

No.	Nombre del servicio	Descripción
1	Soporte de Sistemas de Información externos (SECOP, SIIF, SUI, SIGEP)	El objeto es brindar apoyo sobre las herramientas necesarias como componentes, plugins o apps indispensables para el correcto funcionamiento de los Sistemas de Información. Además, prestar soporte con las áreas responsables en cada área donde se utilice el aplicativo, configurar y ajustar las condiciones adecuadas para el funcionamiento de la plataforma, configuración de puertos, actualización de componentes, etc.
2	Asesoría en el desarrollo e implementación de sistemas	El servicio busca a través de la gestión de proyectos tecnológicos asesorar a la CRA en el desarrollo, implementación y mejoramiento de los sistemas misionales y de apoyo, así como brindar a las unidades solicitantes alternativas de solución y riesgos asociados con la implementación de proyectos. Estableciendo un procedimiento de solicitud de requerimientos se identifican, recopilan, analizan y documentan las necesidades y expectativas de las áreas funcionales solicitantes y se genera la visión y alcance de la solución representada en requerimientos funcionales y no funcionales.
3	Desarrollo y mantenimiento de software	El servicio busca automatizar y optimizar procesos de la entidad por medio de un proceso de construcción de software, siguiendo una metodología de desarrollo por fases donde interviene el equipo de desarrollo con la unidad solicitante, con el objetivo de determinar el alcance y visión del software y trabajar colaborativamente en la definición de las fases de

No.	Nombre del servicio	Descripción
		análisis de requerimientos, diseño de prototipos, desarrollo, implementación y pruebas de aceptación del software.
4	Administración de bases de datos	Su objetivo es la gestión, mantenimiento e integridad de todas las bases de datos que integran la plataforma tecnológica de la CRA: Oracle, Mysql, Oracle Warehouse, Postgres. Comprende la administración de las estructuras y del sistema manejador de bases de datos, el aseguramiento y evaluación de base de datos, el control de accesos no autorizada para prevenir pérdida de datos y fuga de información y la atención de requerimientos de generación de reportes e informes.
5	Modelamiento bodega de datos – SINFONIA	El objeto es desarrollar estructuras de datos (bodega de datos) que permitan dar respuestas a interrogantes definidos por la Entidad mediante el uso de indicadores, sean estos datos representados por sus valores numéricos o mediante el uso de gráficas como histogramas o similares.
6	Videoconferencia	A través del servicio de videoconferencia la CRA establece conexiones privadas con entidades del sector, entidades gubernamentales e internacionales y realiza procesos de intercambio de información, presentación de proyectos, divulgación de tarifas y directrices sectoriales de forma segura, eficiente y oportuna.
7	Administración del Centro de datos	El objeto es garantizar la disponibilidad de los servicios del Centro de Cómputo conformada por las redes de comunicaciones, granja de servidores, correo electrónico e Internet, unidades de almacenamiento, Sistemas de extinción de incendios y refrigeración de aires acondicionados, UPS, entre otros.
8	Administración y configuración de servidores	El objeto es instalar, configurar y administrar la granja de servidores que soportan los servicios TI de la CRA, así como garantizar el desempeño, disponibilidad, capacidad y operación de cada uno de estos.
9	Administración de recursos de virtualización	El objeto es garantizar la funcionalidad de los servidores físicos de la solución de MicroBlade de la entidad, por medio de la gestión de software de virtualización. Responsable de gestionar la capacidad que permita la creación, instalación, configuración, monitoreo y aprovisionamiento en el almacenamiento , memoria, procesador asignados a los servidores virtuales.

No.	Nombre del servicio	Descripción
10	Administración de recursos de almacenamiento	El objeto es gestionar la capacidad de esta plataforma de TI en la cual se centraliza la información de la infraestructura tecnológica de la entidad, en sistemas de respaldo o dispositivos de almacenamiento conectados a la red local y de administrar los recursos de almacenamiento y respaldo de información como: SAN, NAS, unidades externa, entre otros.
11	Administración de recursos tecnológicos	El objeto es planear, ejecutar, soportar y gestionar las actividades relacionadas con la operación, buen uso y apropiación de los recursos tecnológicos (equipos de cómputo, portátiles, Tablet, dispositivos móviles impresoras, scanner, VideoBeams, tableros interactivos, entre otros) al interior de la CRA. Así mismo, asesorar técnicamente en el proceso de evaluación con el fin de apoyar a la Dirección en la toma de decisiones orientadas a la adquisición de las nuevas soluciones tecnológicas.
12	Mantenimiento preventivo y correctivo	El objeto es garantizar el correcto funcionamiento de los equipos y periféricos del parque informático de la Entidad, ya sea cambiando el equipo completo o alguna parte que este presentando fallas.
13	Correo electrónico institucional	El servicio permite el envío y recepción de mensajes electrónicos mediante el sistema administrador de correos Outlook, a través de la asignación de una cuenta institucional al funcionario con el siguiente formato: napellido@cra.gov.co
14	Ofimática (Microsoft Word, Excel, PowerPoint)	El objeto es mantener la suite de office actualizada con los parches de seguridad y funcionalidad que suministra el proveedor del aplicativo, bajo el licenciamiento adquirido.
15	Software Especializado (SPSS, STATA, Microsoft Project, Microsoft Project Server, Omnipage Profesional, Frontier, Autocad, Dragón and natural speaking.)	Permite mantener el correcto funcionamiento, instalación, modificación y/o actualización según se requiera bajo las licencias adquirido.
16	Configuración de Internet	El objeto es monitorear la disponibilidad del servicio. Este servicio está tercerizado y en caso de interrupción del mismo, se procede a realizar los escalamientos correspondientes ante el ISP.
17	Configuración Redes inalámbricas	El objeto es configurar y administrar los componentes de hardware y software que conforman esta solución de red.

No.	Nombre del servicio	Descripción
18	Configuración Enlaces de comunicaciones	El objeto es monitorear la disponibilidad del servicio. Este servicio está tercerizado y en caso de interrupción del mismo, se procede a realizar los escalamientos correspondientes ante el ISP.
19	Configuración Telefonía VoIP	Presta el servicio de configuración y asignación de extensión a cada puesto de trabajo. Además mensualmente se realiza UN reporte de llamadas de toda la Entidad.
20	Directorio activo (creación de usuarios)	El servicio de Directorio Activo tiene como objetivo organizar y gestionar las cuentas de usuarios, servicios de almacenamiento, estaciones de trabajo, impresoras y demás recursos de la red Windows de la CRA, así como de la definición de políticas y directrices de la red.
21	Bloqueo, desbloqueo y eliminación de servicios de red	El objeto es garantizar la ejecución de las acciones necesaria conforme al requerimiento.
22	Impresoras	El objetivo es mantener el servicio activo y mantener la continuidad del negocio y sus funcionalidades al interior de la CRA. Adicionalmente solucionar los requerimientos de servicio solicitados por los diferentes grupos de usuarios.
23	Escáners	El objetivo del servicio es mantener los equipos funcionales basado en los requerimientos solicitados.
24	Computadores de escritorio	Mantener actualizados los equipos del parque informático con el software licenciado por la Entidad y las actualizaciones pertinentes con el fin de evitar vulnerabilidades, además realizar cambios o soporte según se requiera.
25	Video beam	Mantener los equipos funcionales y con las pertinentes correctas conexiones
26	Computadores portátiles	Mantener actualizados los equipos del parque informático con el software licenciado por la entidad y las actualizaciones pertinentes con el fin de evitar vulnerabilidades, también realizar cambios o soporte según se requiera
27	Tablet	Realizar configuraciones para las tablets según sea requerido para los jefes de oficina y expertos
28	Antivirus	El objeto, como parte integral de los sistemas de seguridad perimetral, está orientado a la detección o eliminar virus informáticos orientado, software malicioso, bloqueo, desinfección de archivos y prevenir una infección de los mismo y de los sistemas de la plataforma informática. Apoya en mantener la integridad y disponibilidad de la información de cada uno de los equipos pertenecientes a la CRA.

No.	Nombre del servicio	Descripción
29	Administración de la seguridad de la Infraestructura TIC	El servicio tiene como objetivo asegurar que se cumplan las políticas de seguridad de la información de la CRA. Disponer de las herramientas necesarias para asegurar la plataforma, monitorear de forma permanente las posibles vulneraciones e intrusiones a la red.
30	Backup	El objeto prioritario es mantener la capacidad de recuperación de la información ante posibles pérdidas o necesidades de restauración de servicios y/o Información, Definiendo y aplicando las políticas de seguridad en el marco de Gobierno Digital, Seguridad de la Información.
31	Cámaras de vigilancia	El objeto es proveer un monitoreo constante al interior de la Entidad; hace parte integral de la seguridad física. Lo Anterior, permite reducir o disuadir robos y daños en propiedad privada.
32	VPN	El objetivo es ofrecer una conexión remota y segura por WEB a la red interna de la CRA desde cualquier proveedor de Internet, con el fin de poder hacer uso de los recursos internos de la CRA.
33	Biométrico	Configuración y registro de los funcionarios y contratistas de la entidad en los dispositivos de entrada/salida. Brindar reportes de los registros de las personas de la Entidad
34	Sensibilizar y capacitar en TIC	El servicio tiene como objetivo definir programas de sensibilización, capacitación y comunicación de los servicios definidos en el Catálogo de Servicios de TIC de la Comisión de Regulación de Agua Potable y Saneamiento Básico CRA.

1.4. Elementos para el intercambio de información

La Oficina Asesora de Planeación y TIC es la encargada del intercambio de información entre las distintas áreas de la CRA y las organizaciones externas. Actualmente, la CRA cuenta con un servicio⁵ de información definido con la Superintendencia de Servicios Públicos Domiciliarios para el proceso de extracción, transformación y cargue de información, el cual le permite consultar, mover datos desde las bases de datos del SUI, transformarlos y cargarlos a la base de datos del sistema SINFONIA a fin de analizarlos y generar reportes para procesos de regulación y toma de decisiones.

Para garantizar la existencia de las fuentes únicas de información, la CRA estableció desde el 06 de agosto del año 2010 un acuerdo de intercambio de información por medio del convenio interadministrativo de cooperación suscrito entre el Ministerio de Ambiente, Vivienda y Desarrollo Territorial, el Departamento Nacional de Planeación y la Superintendencia de Servicios Públicos Domiciliarios, con el objeto de *“Aunar esfuerzos entre las entidades firmantes para*

⁵ Ver en documento de Catálogo de Servicios de Información de la CRA

fortalecer y consolidar el SUI en el sector de los servicios públicos domiciliarios de Acueducto, Alcantarillado y Aseo, de forma que dicho sistema sirva como fuente de información oficial para el apoyo a los procesos de toma de decisiones propios de cada una de ellas”.

Las obligaciones de las partes firmantes y las funciones del Comité Técnico de Trabajo y Supervisión se detallan a continuación:

Convenio	Descripción
Convenio interadministrativo de Cooperación	Comisión de Regulación de Agua Potable y Saneamiento Básico, Ministerio de Ambiente, Vivienda y Desarrollo Territorial, el Departamento Nacional de Planeación y la SuperIntendencia de Servicios Públicos Domiciliarios
Obligaciones de la CRA	<ul style="list-style-type: none"> • Utilizar el SUI como medio principal para la solicitud de información a los prestadores de servicios públicos domiciliarios, sin perjuicio de las facultades que le otorga la Ley a las diferentes entidades que conforman el presente convenio, de solicitar directamente algún tipo de información de los prestadores de servicios públicos domiciliarios. • Cada entidad firmante que solicite a la Superservicios una nueva funcionalidad la apoyará con los recursos necesarios para su desarrollo bajo las directrices temáticas del Comité Técnico de Trabajo y Supervisión. El desarrollo de cada funcionalidad respetará las políticas del administrador del SUI. • Designar al personal que considere necesario para la implementación y coordinación de los desarrollos de información sectorial requeridos por las entidades, que serán construidos sobre las bodegas de datos sectoriales contenidas en el SUI. • Divulgar al interior de cada entidad los eventos de capacitación y/o entrenamiento, realizados por otras entidades que sean requeridas para el adecuado uso del SUI por parte de sus funcionarios y promover su asistencia. • Fomentar al interior de las partes del presente convenio, la utilización del SUI, como herramienta de trabajo y de análisis sectorial.

	<ul style="list-style-type: none"> • Apoyar a la Superservicios en la identificación de: requerimiento de información en el SUI, reportes para ser publicados y en general de nuevas funcionalidades e inconsistencia de información provenientes del SUI. Asimismo, las entidades mencionadas en este literal en relación con los servicios públicos domiciliarios de acueducto, alcantarillado y aseo, facilitarán a la Superservicios la información histórica de que dispongan y suministrarán las bases de datos que tengan bajo su custodia y administración, con el objeto de integrarlas al SUI.
<p>Obligaciones de la Superservicios</p>	<ul style="list-style-type: none"> • Aplicar las nuevas funcionalidades del SUI una vez desarrolladas, en particular, la paulatina incorporación de instrumentos de procesamiento y análisis de información. • Prestar asesoría técnica y profesional en desarrollo del presente convenio, en lo que respecta al diseño de la arquitectura para atender los requerimientos funcionales y de niveles de servicio de cada entidad, que se propongan en el Comité Técnico de Trabajo y Supervisión. • Atender dentro de los plazos previstos para el efecto, de acuerdo con la determinación de niveles de prioridad y dentro de los estándares de calidad, los requerimientos desarrollos de formularios, cargues masivos y reportes básicos que proponga el Comité Técnico de Trabajo y Supervisión. • Diseñar e implementar las bodegas de datos especializadas y las herramientas para el análisis sectorial, de acuerdo con lo que se conocerte en el Comité Técnico de Trabajo y Supervisión. • Coordinar las acciones necesarias para incorporar al SUI las bodegas de datos que sirvieron para el diseño y operación del reporteador de información SINFONIA, y los reportes predefinidos dentro de dicha aplicación. • Capacitar y/o entrenar gratuitamente al personal de las entidades suscriptoras de este convenio, en el adecuado uso de las herramientas del SUI.

<p>Comité Técnico de Trabajo y Supervisión</p>	<ul style="list-style-type: none"> • Identificar los requerimientos información, en materia de servicios públicos domiciliarios de acueducto, alcantarillado y aseo, que requieran las partes del presente convenio para el ejercicio sus funciones, con el fin de que sean suministrados a través del SUI. • Establecer los estándares unificados que las partes del presente convenio deberán aplicar en los procesos de definición, generación y reporte información y procesamiento de datos provenientes del SUI. • Revisar y aprobar las propuestas de modificación a los requerimientos de información existentes cuando fuere de caso. • Definir las herramientas de administración de metadatos que resulten necesarias. • Entre otras funciones
--	--

Dado que la coordinación de la ejecución del convenio interadministrativo está a cargo del Comité Técnico de Trabajo y Supervisión, y el comité se encarga de establecer los estándares unificados que las partes deben aplicar en los procesos de definición, generación, reporte de información y procesamientos de datos del SUI, es fundamental que el Comité determine para la Comisión de Regulación de Agua Potable y Saneamiento Básico, los acuerdos de nivel de servicio del convenio de intercambio de información con el fin de garantizar la oportunidad, disponibilidad y seguridad que requieran los Componentes de información al interior de la entidad.

1.5. Plan de gestión de servicios de TI

1.5.1. Gestión de la capacidad

En la CRA la Gestión de Capacidad busca asegurar que los servicios y recursos de Tecnología de la Información se vean respaldados por una capacidad de procesamiento y almacenamiento suficiente y correctamente dimensionada, que garantice que cada uno de los funcionarios de las unidades de la entidad que consumen los servicios tecnológicos puedan desempeñar de una manera eficiente sus actividades.

Como actividades relacionadas con la gestión de la capacidad, el Grupo TIC de la Oficina Asesora de Planeación, desarrolla como parte de su quehacer diario las siguientes actividades:

Actividad
Monitorear permanentemente el rendimiento de toda la infraestructura de TI de la entidad. El monitoreo se realiza conforme a los ANS establecidos en el catálogo de servicios de TI y proveedores de servicios tecnológicos externos.
Plantear y diseñar escenarios de la capacidad de la infraestructura de TI y proyectar el consumo de los recursos tecnológicos.
Evaluar el consumo de los recursos TI de la infraestructura tecnológica de la entidad. Entre estos: capacidad de procesamiento, almacenamiento, etc.
Realizar recomendaciones relacionadas con la gestión de la capacidad conforme a la monitorización de la infraestructura de TI para integrarlas al plan de adquisiciones de la Entidad.

A continuación, se detallan las capacidades actuales de los Servicios Tecnológicos de la CRA, los cuales permiten proyectar las capacidades futuras requeridas por la entidad para que cumpla con los niveles de servicio acordados con los grupos de interés.

1.5.1.1. Servidores virtualizados VMWare

Recurso	Cuchillas	Capacidad Total	Capacidad usada	Capacidad para aprovisionar	Consumo actual	Umbral
Procesamiento (GHz)	3	100,76	7,65	93,11	7,59%	75%
Memoria (GB)	3	191,68	132,95	58,73	69,36%	75%
Almacenamiento (TB)	3	8,36	4,71	3,65	56,33%	75%

Información generada el 31 de octubre de 2019

1.5.1.2. Detalle servidores virtuales VMWare

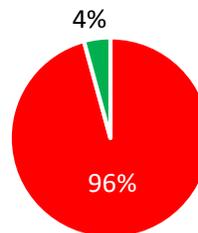
Servidor virtual	Estado	Memoria (GB)	Almacenamiento				Procesador (MHz)
			# de Disk	Cap (GB)	Cons (GB)	% Libre	
SRVAPLVCENTER	Activo	10	13	247	33,6	86%	4
SRVCCU001	Activo	3	1	70	63,0	10%	2
SRVCCU02PRUEBAS.CRAPSB.GOV.CO	Activo	2	1	63	60,9	3%	2
SRVCMS01	Activo	6	2	10	0,1	99%	4
SRVCMS01_IPv6	Inactivo	6	2	10	0,1	99%	4
SRVDC_IPv6	Inactivo	4	2	100	29,6	70%	8
SRVDC02	Activo	4	2	100	29,8	70%	8
SRVDMS01	Activo	6	3	659	395,0	40%	8
SRVDMS02	Activo	4	1	30	25,8	13%	4
SRVDMS03	Activo	2	2	30	16,5	44%	4

Servidor virtual	Estado	Memoria (GB)	Almacenamiento				Procesador (MHz)
			# de Disk	Cap (GB)	Cons (GB)	% Libre	
SRVDMS04	Inactivo	8	1	90	7,5	92%	4
srvexchange01.CRAPSB.GOV.CO	Activo	2	2	30	24,7	17%	8
SRVMVWBACK-01	Activo	16	2	6593	4807,3	27%	4
SRVMWFM	Activo	4	1	100	20,9	79%	2
SRVPMS01	Activo	8	2	178	127,0	29%	8
SRVPRINTER1	Activo	8	2	130	23,6	82%	4
SRVSEPO	Inactivo	4	1	80	34,1	57%	2
SRVSEPO1	Activo	8	1	80	0,0	100%	2
SRVSEPOTIE	Activo	16	1	182	2,7	98%	16
SRVSES01	Activo	7	1	69	36,4	47%	8
srvsinfonia01	Activo	8	1	60	57,9	3%	8
SRVSPRTG	Activo	8	1	80	40,6	49%	2
SRVSTIE	Inactivo	10	1	109	9,5	91%	0
SRVSWC-DHCP	Activo	4	1	80	35,5	55%	2
SRVWEBCRA	Activo	16	5	333	44,6	87%	4

Información generada el 31 de octubre de 2019

1.5.1.3. Almacenamiento – uso total de la SAN

Capacidad (TB)	Asignado	Libre
14,4	13,79	0,613
	96%	4%



1.5.1.4. Almacenamiento según volúmenes

Volumen	Aprovisionamiento	Raid	Capacidad (TB)	Usado	Libre	Etapas	Discos
VMWARE	2017	10 (1)	3,27	2,63	0,64	Inicial	1,2 TB
VMWARE (1)	2018	10 (3)	2,73	1,96	0,77	Ampliación	1,8 TB
VMWARE (2)	2018	10 (3)	2,36	0,12	2,24	Ampliación	1,8 TB
Análisis			8,36	4,71	3,65		
				56%	44%		

Información generada el 31 de octubre de 2019

Volumen	Aprovisionamiento	Raid	Capacidad (TB)	Asignado	Libre	Etapas	Discos
ORACLE VM	2017	10 (1)	3,38	3,38		Inicial	1,2 TB
ORACLE VM (1)	2018	10 (3)	1,2	1,20		Ampliación	1,8 TB
Análisis	2018		4,58	4,58			
				100%	0%		

Información generada el 31 de octubre de 2019

1.5.1.5. Almacenamiento – NAS

Volumen	Raid	Capacidad (TB)	Usado	Libre	% de uso	Descripción
Local disk (C:)	0	0,362	0,0986	0,2637	27%	
Backup (D:)	6	27,7	25,4	2,3	92%	Exec, Hyper-V, Servidor de Archivos y Oracle.
File (F:)	6	4,99	3,42	1,57	69%	Calidad, carpetas por unidades y público
Análisis		33,052	28,9186	4,1337		
			87%	13%		

1.5.2. Gestión de la seguridad

A través de la gestión de la seguridad se busca que la entidad cuente con una política de seguridad de la información que se encuentre alineada con las necesidades de los clientes y usuarios. Lo anterior, asegurando el cumplimiento de los estándares de seguridad, bajo criterios de confidencialidad, integridad y disponibilidad (MinTIC, 2016)

Para adelantar esta gestión, es necesario según MinTIC la definición de la política de seguridad de la información de los servicios TIC prestados a los clientes y usuarios, bajo estándares de seguridad y confidencialidad firmados entre proveedores internos y externos, su monitoreo y evaluación, hasta la supervisión, análisis y tratamiento adecuados de riesgos, vulnerabilidades e impactos en los servicios TIC.

La Comisión cuenta actualmente con el Manual de Políticas del Sistema Integrado de Gestión y Control (SIGC)⁶ aprobado por el Comité Institucional de Gestión y Desempeño en marzo de 2019, que resume las políticas que se han aprobado a lo largo de todos los Comités del Sistema Integrado de Gestión y Control como directrices generales para todos los niveles y cargos y que deben ser cumplidas por todos aquellos que realizan labores y actividades en la entidad.

Este Manual desarrolla entre otras la Política del Sistema Integrado de Gestión y Control, las Políticas del Sistema de Gestión de Seguridad de la Información, las Políticas de Buen Gobierno para la Gestión de la entidad, las Políticas de Operación Institucional, las Políticas de Gestión

⁶ Disponible en: <https://www.cra.gov.co/documents/Manual-de-politicas-del-SIGC-2019.pdf>

Documental y Cero Papel, las Políticas Generales de Defensa Judicial UAE-CRA y la Política de Prevención del Daño Antijurídico.

En relación a las Políticas del Sistema de Gestión de Seguridad de la Información, a continuación se describen cada una de estas.

Política definida en la CRA	Descripción general
Política de control de acceso a la información	Esta política se aplica a todos los funcionarios, contratistas y terceras partes que por la naturaleza de sus funciones requieren acceso a la información de la Entidad. Describe las consideraciones generales sobre la protección y el control de acceso a la información de la CRA para. evitar el acceso no autorizado a sistemas y/o servicios, y hacer que los usuarios rindan cuentas por la administración y protección de su información y sus claves.
Política de controles criptográficos	Esta política describe las consideraciones generales para asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información de la CRA. Igualmente describe las consideraciones sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida y aplica para todos los funcionarios, contratistas y terceras partes que por la naturaleza de sus funciones requieren uso de alguna técnica de protección de información mediante controles criptográficos o llaves criptográficas en la Entidad.
Política de transferencia de información	Esta política describe las consideraciones generales para mantener la seguridad de la información transferida dentro de las instalaciones de la Comisión de Regulación de Agua Potable y Saneamiento Básico entre sus diferentes dependencias o entre funcionario de la CRA y entre la CRA con cualquier otra entidad externa. Se aplica a funcionarios, contratistas y terceras partes interesadas en tener acceso a la información de la CRA.
Política de seguridad de la información con proveedores	Esta política aplica a proveedores de servicios de la CRA y contratistas y busca preservar los niveles de seguridad y privacidad de los activos de información de la CRA cuando se autorice el acceso o administración por parte de proveedores de servicios o contratos de prestación de servicios.
Política de escritorio limpio y pantalla limpia	Esta política establece los lineamientos generales para reducir los riesgos de acceso no autorizado, pérdida o daño de información en escritorios y estaciones de

Política definida en la CRA	Descripción general
	trabajo durante o fuera de las horas laborales de la Entidad. Aplica a funcionarios, contratistas y terceras partes que por la naturaleza de sus funciones deban tener acceso a estaciones de trabajo o puestos de trabajo dentro de las instalaciones de la CRA.
Política de respaldo de información	Esta política cubre a funcionarios, contratistas y terceros que por la naturaleza de sus funciones deban realizar copias de respaldo de la información institucional y define los lineamientos para la generación, administración, retención y custodia de las copias de respaldo, con el fin de preservar la disponibilidad e integridad de la información de la CRA.
Política de desarrollo seguro	Cuando la Comisión de Regulación de agua potable y saneamiento básico, desarrolle software o contrate el desarrollo de software con proveedores, deberá considerar los siguientes lineamientos generales para el desarrollo, mantenimiento y adquisición de software, con el fin de adoptar los controles de seguridad en el desarrollo del software.
Política de uso aceptable de activos de información	Esta política cubre a funcionarios, contratistas, terceras partes y todos los activos de información de la Entidad y define las pautas para realizar un uso seguro y aceptable de los activos de información de la CRA, incluyendo sus sistemas de información, estaciones de trabajo, áreas de almacenamiento de información (física o electrónica), medios de almacenamiento de información (física o electrónica), entre otros.
Política de teletrabajo	<p>Por la naturaleza de sus sistemas de información y las características de la misión de la CRA, la implementación del Teletrabajo en los términos del Decreto 1072 de 2015 a la fecha se encuentra en un ejercicio piloto. Por lo tanto, cualquier actividad formal de Teletrabajo será tramitada por los procedimientos administrativos que adopte la entidad para tal fin, cuando implemente la estrategia de Teletrabajo y una vez evaluado el ejercicio piloto. No obstante, a lo anterior, y en cumplimiento del Decreto 1072 de 2015, se crea la siguiente política para ser implementada en el momento que la entidad así lo defina.</p> <p>Esta política define las pautas generales para asegurar la información de la entidad frente a riesgos asociados al teletrabajo. Aplica a todos los funcionarios de la entidad</p>

Política definida en la CRA	Descripción general
	<p>que se encuentren autorizados para realizar actividades de teletrabajo con el pleno cumplimiento de los requisitos del Decreto 1072 de 2015, Capítulo 5 Teletrabajo.</p>
<p>Política de uso de dispositivos móviles</p>	<p>Esta política aplica a todos los dispositivos y equipos móviles de los funcionarios, contratistas o terceros de la entidad que estén autorizados para conectarse a las redes de datos de la CRA y busca garantizar la seguridad de la información cuando se administre, transmita o almacene información de la entidad en dichos dispositivos. La autorización de conexión a servicios institucionales debe ser tramitada siguiendo los procedimientos institucionales.</p>
<p>Política de protección de dispositivo propio (BYOD)</p>	<p>Esta política define las medidas necesarias para evitar que la información pública reservada o pública clasificada se vea comprometida en su integridad y confidencialidad al ser almacenada en dispositivos de propiedad de funcionarios o contratistas de la CRA.</p> <p>Esta política aplica a todos los dispositivos electrónicos personales tales como teléfonos inteligentes y tabletas, los computadores portátiles que no pertenecen la Entidad pero que son utilizados por funcionarios y contratistas para acceder o almacenar información. A estos dispositivos se les conoce comúnmente dentro del área de seguridad informática como BYOD (Bring Your Own Device).</p> <p>Como política general la Entidad no autoriza el uso de dispositivos BYOD para el tratamiento de información institucional. La Entidad determinará mediante sus procedimientos en qué momento se considera viable autorizar uso de dispositivos personales que no sean propiedad de la Entidad para el tratamiento de la información institucional.</p>
<p>Política de servicios de computación en la nube</p>	<p>El objetivo de la política de servicios de computación en la nube es mantener la seguridad de la información y de los servicios de procesamiento de información en plataformas de computación en la nube que son utilizados por la entidad, garantizando su continuidad, cumpliendo los niveles de servicio requeridos, reduciendo los riesgos legales y técnicos a niveles aceptables.</p>

Política definida en la CRA	Descripción general
	<p>Aplica para todos los servicios de computación en nube que sean utilizados o contratados por la entidad, así como a los procesos que hagan uso de dichos servicios. La autorización de uso de servicios de procesamiento de información en la nube se debe realizar a través del proceso de Gestión de tecnologías de información.</p>

1.5.3. Gestión de la disponibilidad

Con la gestión de la disponibilidad se espera asegurar que los servicios TIC estén operando cuando se requiera, determinando los requisitos de disponibilidad en estrecha relación con acuerdos establecidos, con el objeto de proponer mejoras y aumentar los niveles de disponibilidad. (MinTIC, 2016)

Para una gestión exitosa de este componente es necesario según MinTIC que la Oficina Asesora de Planeación y TIC de la CRA inicie con la determinación de los requisitos de disponibilidad de los servicios TIC, el desarrollo del plan de disponibilidad a corto y mediano plazo, el diseño del mantenimiento del servicio en operación y recuperación del mismo en caso de fallo, la elaboración de informes de seguimiento sobre disponibilidad y cumplimiento del servicio, hasta la evaluación del impacto de las políticas de disponibilidad de los servicios en la institución.

En relación a la gestión de la disponibilidad, la CRA ha diseñado un procedimiento gestión de backups y recuperación de información, con el objetivo de garantizar el resguardo de forma segura de toda la información digital que dentro del desarrollo de las funciones es importante y crítica, estableciendo mecanismos para realizar copias de seguridad y restauración, generada en cada una de las dependencias de la Comisión de Regulación de Agua potable y Saneamiento Básico – CRA.

Este procedimiento se realiza de manera automática en los servidores y equipos en los que se almacenan las bases de datos y los aplicativos de misión crítica de la Entidad.

La programación del backup se realiza a través de una herramienta informática (librería de backup) y el seguimiento lo realiza un profesional del área de Sistemas, verificando la correcta ejecución del procedimiento. En la medida en que se realice esta copia, se podrá garantizar la recuperación de la información en caso tal, en que se presenten errores en el manejo de los equipos, daño físico o cualquier eventualidad, que ponga en riesgo la seguridad de la información.

Procedimiento de backup o copias de respaldo

N°	Actividad	Descripción	Responsable	Registros
1	Identificar los elementos a los que se debe hacer Backup.	Determinar de acuerdo con el número de aplicativos y/o bases de datos y archivos para respaldo con sus tiempos de retención con el fin de Identificar todos los elementos a los que se necesitan realizar backups	Profesional Tecnologías de Información	
2	Manejo del data protector para indicarle lo que se necesita realizar backup	Indicar al data protector los files , Files Shared, BD, SO virtualizados, Archivos de configuración, Snapshots Vm	Analista de Sistemas	
3	Utilización de los mecanismos de Copias	Determinar los mecanismos de copias de respaldo según la base de datos a respaldar en la SAN Y CINTAS.	Analista de Sistemas	
4	Verifica de reportes automáticos de dataprotector	Revisar los logs de errores con la realización del backup se envía al GLPI y Correo electrónico del analista de sistemas y tecnologías de información.	Analista de Sistemas	Logs de errores del Dataprotector en \\dataprotector\grupo_sistemas\$ReportesBackups\Errores Registro GLPI Correo electrónico
5	Generación de reportes Automáticos semanalmente de Dataprotector	Generación de reportes automáticos por dataprotector semanal	Analista de Sistemas	Reporte de Dataprotector semanalmente en \\dataprotector\grupo_sistemas\$ReportesBackups\Eventos
6	Realizar una nueva copia de seguridad	Volver a realizar copia por segunda vez, si el archivo log del servidor indica error, siempre y cuando el backup sea de tipo full. Si es incremental se puede esperar el siguiente día.	Analistas de Sistemas	Logs del Dataprotector
7	Realizar por medio del dataprotector la copia a cintas.	Grabar en cintas cada 15 días el backup para entrega a custodia de medios contratados, la cinta utilizada se puede utilizar 2 veces al año.	Analistas de Sistemas	GTI-FOR03 Formato entrega y recepción de cintas
8	Rotular cintas para entrega a custodia de medios	Rotular caja de la cintas a entregar a la custodia de medios donde se indica la fecha de realizada la copia e identificación del número de la cinta dependiendo la cantidad entregada.	Analistas de Sistemas	GTI-FOR03 Formato entrega y recepción de cintas

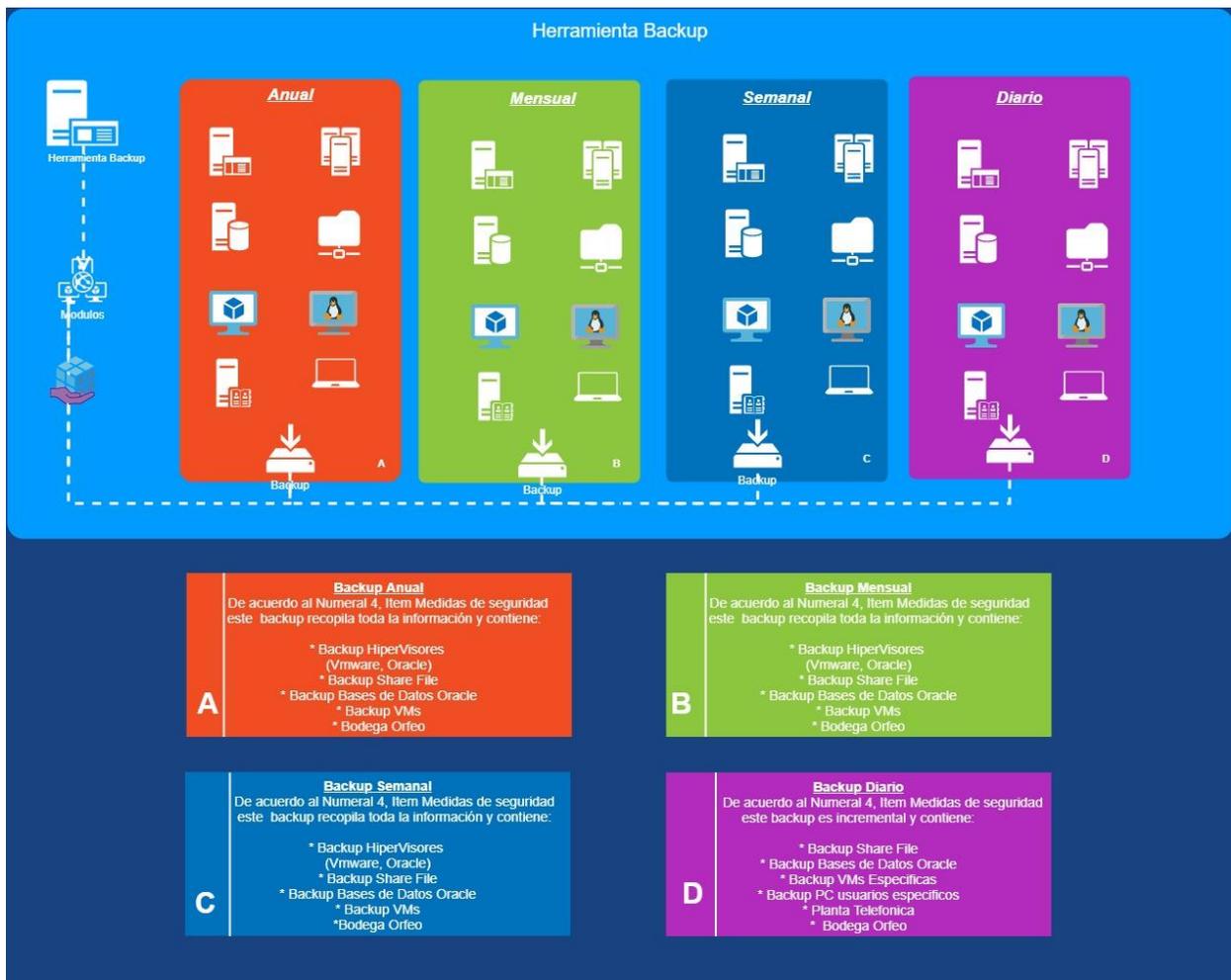
Procedimiento de recuperación de información

N°	Actividad	Descripción	Responsable	Registros
1	Recepción de la Solicitud por GLPI	Crear solicitud por medio del GLPI	Diferentes Oficinas	Registro GLPI
2	Seleccionar la opción de restore y recuperar la información.	Acceder al sistema de dataprotector y seleccionar la opción de restore donde se selecciona el origen y el destino donde quedara de nuevo información recuperada.	Analistas de Sistemas	GTI-FOR01 Formato restauración bases de datos
3	Verificar el éxito de la operación	Verificar que la operación realizada se haya restaurado sin problemas	Analistas de Sistemas	GTI-FOR02 Formato restauración de archivos

Procedimiento recuperación de bases de datos

N°	Actividad	Descripción	Responsable	Registros
1	Seleccionar la opción de restore y seleccionar la BD.	Acceder al sistema de dataprotector y seleccionar la opción de restore donde se selecciona el origen y el destino donde quedara de nuevo información recuperada.	Analistas de Sistemas	GTI-FOR01 Formato restauración bases de datos
2	Verificar que la recuperación sea exitosa	Verificar que la operación realizada se haya restaurado sin problemas.	Analista de Sistemas	GTI-FOR01 Formato restauración bases de datos
3	Recuperación de base de datos	El administrador de base de datos deberá ejecutar el manual de recuperación de base de datos. Ver Anexo	Sistemas de Información Misional	GTI-FOR01 Formato restauración bases de datos
4	Diligenciar el formato de restauración de BD	Llenar el formato de control de copias realizada	Sistemas de Información Misional	GTI-FOR01 Formato restauración bases de datos

Diagrama procedimiento creación de copias de respaldo



1.5.4. Gestión de continuidad

Con la gestión de la continuidad se busca garantizar la recuperación de los servicios de TIC en el evento de presentarse interrupciones. Para esto, se deben establecer políticas y procedimientos que eviten posibles consecuencias negativas en el negocio y ofrecer unos niveles aceptables de continuidad en el menor tiempo posible para la entidad (MinTIC, 2016)

Para avanzar en esta gestión, de acuerdo con MinTIC es preciso iniciar con el establecimiento de políticas de continuidad del servicio TIC, el análisis de los impactos generados por la interrupción de los servicios TIC, el análisis de los riesgos a los que están expuestos los servicios, la adopción de medidas de prevención de riesgos en los servicios TIC, el diseño, pruebas y revisión de planes de contingencias, hasta la formación del personal para la recuperación del servicio TIC.

Todo lo anterior se ha establecido en la CRA, a través El DRP⁷ (Disaster Recovery Plan o Plan de recuperación de desastres) el cual constituye una estrategia para garantizar la continuidad y restablecer los servicios de TI (Hardware y Software) en la Entidad.

Con la definición del DRP la entidad espera:

- Mantener la continuidad de los servicios relacionados con la TIC
- Proteger a la entidad de fallas generales en los servicios informáticos.
- Minimizar los riesgos generados por la falta de servicios.
- Garantizar el acceso de la información institucional.
- Mantener la disponibilidad de los recursos informáticos.
- Minimizar la toma de decisiones erróneas al presentarse algún desastre.
- Dar atención continua a los clientes, proveedores, accionistas, colaboradores.
- Tener capacidad de recuperación exitosa

A continuación, se expondrá el análisis para cada uno de los componentes tecnológicos de la Infraestructura de comunicaciones, almacenamiento y procesamiento de la CRA en relación con los servicios.

⁷ Ver documento Plan de Recuperación ante Desastres –DRP- de la CRA

Análisis de los componentes tecnológicos de la Infraestructura TI de la CRA

Servicio	Configuración de la infraestructura de comunicaciones				
Componente	Descripción del impacto sobre el servicio	Impacto	Probabilidad	RPO	RTO
ROUTER CISCO 2901	Al fallar ROUTER CISCO 2901 capa 3 principal, se activará de manera automática el segundo dispositivo de acuerdo a la configuración de alta disponibilidad definido. Dada esta configuración, no se verá afectada la operación y servicios de TI.	Mayor	Raro	1 min	30 min
SWITCH DLINK 3100	Al fallar el componente SWITCH DLINK 3100 capa 2, la CRA tendría una indisponibilidad de los servicios de internet, así como a los servicios TI asociados a este. Se deberá realizar por parte del Grupo TIC la conexión manual del dispositivo backup que se encuentra operativo en modalidad pasivo.	Mayor	Raro	20 min	30 min
Tansceiver Raisecom (ISCOM RAX700)	Al fallar el componente Tansceiver Raisecom (ISCOM RAX700) la CRA perdería el servicio de acceso a internet, así como los servicios asociados a este. Dado que este dispositivo se encuentra en alta disponibilidad, se activará de manera automática el segundo dispositivo de acuerdo a la configuración, por lo tanto no se verá afectada la operación y servicios de TI.	Mayor	Raro	1 min	30 min
FireWall FortiGate 300D	– El servicio de seguridad perimetral, está soportado bajo el Firewall Fortinet - Fortigate 300D, Al fallar el dispositivo, la CRA perdería el servicio de acceso a internet y a todos los servicios que dependen de este.	Mayor	Probable	2h	3h
Switch Core – DLink DGS-3420-52P	– Al fallar el componente Switch Core principal DLink DGS-3420-52P, se presentaría indisponibilidad de los servicios de procesamiento (servidores físicos y virtuales), unidades de	Mayor	Posible	1h	1h

Servicio	Configuración de la infraestructura de comunicaciones				
Componente	Descripción del impacto sobre el servicio	Impacto	Probabilidad	RPO	RTO
	almacenamiento, conexión inalámbrica, servicios de telefonía, entre otros servicios.				
Switch DLink DGS-3420-52P ID 2	Al fallar el componente Switch DLink DGS-3420-52P ID 2, se presentaría indisponibilidad de los servicios de conexión con el equipo de seguridad perimetral Firewall, la salida a los servicios de internet, conexión a la red inalámbrica, administración de UPS, administración de la consola de monitoreo del microblade, acceso al sistema de videoconferencia, al servicio de impresión, al servicio de almacenamiento SAN HP MSA 2040, al servicio de almacenamiento NAS SuperMicro 826-9 y estaciones de usuario final. Al fallar este componente, no se contaría con respaldo al Switch Core principal de acuerdo a la configuración actual.	Mayor	Probable	1h	1h
Switch DLink DGS-3420-52P ID 3	Al fallar el componente Switch DLink DGS-3420-52P ID 3, se presentaría indisponibilidad de los servicios de conexión de las terminales de trabajo de usuario final.	Mayor	Probable	1h	1h
Switch DLink DGS-3420-52P ID 4	Al fallar el componente Switch DLink DGS-3420-52P ID 4, se presentaría indisponibilidad de los servicios de conexión de las terminales de trabajo de usuario final.	Mayor	Probable	1h	1h
Switch Backup	Al fallar el componente Switch Backup, no se contaría con stock dada una indisponibilidad de alguno de los cuatro Switch DLink configurados en el Stacking actual.	Moderado	Raro	10h	3h
Red inalámbrica – Access Point DLink 2660	El servicio de red inalámbrica, está soportada bajo la controladora Central WiFi Manager de DLink, la cual administra los cuatro access point instalados en las instalaciones de la CRA. Al interrumpirse el servicio afectaría a los usuarios internos y externos que se encuentren conectados a través de dispositivos	Moderado	Probable	2h	3h

Servicio	Configuración de la infraestructura de comunicaciones				
Componente	Descripción del impacto sobre el servicio	Impacto	Probabilidad	RPO	RTO
	<p>móviles a los SSID: WCRA-CORP y CRA-INVITADOS en las áreas o salas de reuniones de la entidad.</p> <p>Si el servidor virtual que aloja la controladora WiFi Manager de DLink presenta una interrupción, afecta al servicio de red inalámbrica de la Entidad.</p> <p>Para mitigar los riesgos de acceso a la red local de la entidad a través de la red inalámbrica, la CRA configuró el servicio Radius con el objetivo de gestionar el acceso de los usuarios internos a los servicios TI. Los usuarios externos son controlados por políticas del Firewall a través del WiFi Manager de DLink.</p>				
Conexión planta telefónica – CENTREX UNE	El servidor aloja todo los servicios asociados a la planta telefónica, al interrumpirse el servicio afectaría la comunicación externa e interna de la Comisión. Asi mismo, se afectaría las líneas del PBX, y las líneas de comunicación interna entre unidades.	Mayor	Posible	2h	6h
Conexión planta telefónica – PATTON 3086	Al fallar el componente G.SHDL PATTON 3086, se perdería el servicio de conmutador virtual que gestiona las líneas telefónicas de entrada y salida de llamadas simultaneas de la CRA.	Menor	Probable	1h	1h

Servicio		Administración de recursos de almacenamiento			
Componente	Descripción del impacto sobre el servicio	Impacto	Probabilidad	RPO	RTO
SAN HP MSA 2040	<p>La SAN HP MSA 2040 gestiona el almacenamiento de las bases de datos ORACLE y las máquinas virtuales de VMWare.</p> <p>Al presentarse un daño en este dispositivo los usuarios no podrán tener acceso a la red inalámbrica, la Intranet, a los sistemas de información SINFONIA, ORFEO, tramites CCU, normatividad, Pymisis, Trident, pagos en línea, inteligencia de negocios ORACLE y consola de administración de antivirus.</p> <p>En este mismo sentido, se pierde la disponibilidad del servidor que aloja los servicios secundarios de directorio activo, DHCP, DNS y el servicio de conectividad a internet dado que se encuentra alojado también el agente FSSO.</p>	Mayor	Posible	2h	24h
NAS SuperMicro 826-9	<p>El servidor de Archivos NAS gestiona las carpetas compartidas de red que garantizan la disponibilidad de la información de cada uno de los procesos para el ejercicio de las funciones de los miembros de la CRA.</p> <p>Así mismo, este Servidor de Archivos aloja las copias de respaldo generadas por la herramienta Backup Exec Veritas de acuerdo a los esquemas definidos. La información respaldada comprende: equipos de usuario final (de acuerdo al licenciamiento), bases de datos de ORACLE, Pymisis, intranet, ORFEO, Trident y las carpetas compartidas por las áreas de la Entidad.</p> <p>Al presentarse un daño en este servidor los usuarios no podrán acceder a la información compartida y los servicios asociados perderían la capacidad de almacenar las copias de respaldo en disco.</p> <p>El servidor de Archivos NAS tiene instalado en un disco en estado sólido independiente su propio sistema operativo (Windows Server Storage 2016 Standard), donde se gestiona y administra los servicios de carpetas compartidas y el sistema de virtualización Hiper-VI donde actualmente administra las dos máquinas virtuales relacionadas con el gestor de bases de datos ORACLE.</p>	Catastrófico	Posible	2h	79h

Servicio		Administración de bases de datos			
Componente	Descripción del impacto sobre el servicio	Impacto	Probabilidad	RPO	RTO
OL72 (Freedom)-Hyper VI: Escenario de contingencia del Servidor de bases de datos ORACLE de producción de la solución OracleVM	<p>El servidor de bases de datos ORACLE: se encuentra instalado como maquina virtual sobre el servicio de virtualización Hiper-VI de Microsoft, el cual es gestionado por el sistema operativo de la NAS SuperMicro 826-9 Windows Storage 2016 Standard.</p> <p>Este servidor funciona como escenario de recuperación ante la materialización del riesgo de fallo del servidor de bases de datos ORACLE de la solución OracleVM. Este está configurado para gestionar las bases de datos de los sistemas de información SINFONIA (Oracle BI y Datawarehouse), ORFEO, Pymisys, los servicios de Weblogic server (Oracle ADF) y los trámites en línea.</p> <p>Al presentarse un daño en este servidor (estar activo como escenario de recuperación) los funcionarios y contratistas no podrán acceder al sistema misional SINFONIA (generar y extraer información por medio de Oracle BI y Datawarehouse), así como efectuar trámites de pago de contribuciones especiales y emisión de concepto de legalidad sobre Contratos de Condiciones Uniformes (CCU) por parte de las entidades contribuyentes.</p>	Menor	Posible	2h	2h
OL722 - Hyper VI: Pruebas y calidad	<p>El servidor de bases de datos ORACLE (pruebas y calidad): se encuentra instalado como maquina virtual sobre el servicio de virtualización Hiper-VI de Microsoft, el cual es gestionado por el sistema operativo de la NAS SuperMicro 826-9 Windows Storage 2016 Standard.</p> <p>Este servidor gestiona la contingencia de pagos en línea, dado que este servicio se prestaba en la infraestructura de blade que dejó de operar.</p> <p>Al presentarse un daño en este servidor quedaría fuera de operación el servicio de pagos en línea.</p>	Catastrófico	Probable	2h	80h

Servicio	Administración de recursos de virtualización				
Componente	Descripción del impacto sobre el servicio	Impacto	Probabilidad	RPO	RTO
VMWare: ESXi-VMWHOST1	Cuchilla 1. VMWHost1. (SuperMicro MBI-618R-T2), cuchilla 1 de las 3 que conforman el Cluster de la solución VMWare. Este cluster permite la administración y gestión de los recursos de la solución Vmware como són: asignación de memoria, de procesador y almacenamiento.	Mayor	Probable	2h	24h
Orquestador	Gestiona y administra el inventario de las máquinas virtuales de VMWare.	Menor	Probable	2h	8h
Vcenter Server Appliance Standard	A través de Vcenter se administran los módulos y servicios de las máquinas físicas y virtuales de VMWare de forma gráfica.	Mayor	Probable	2h	10h
Vsphere	Punto de conexión o interfaz que permite acceder a la plataforma de administración de VMWare.	Mayor	Probable	2h	10h
VMWare: ESXi-VMWHOST2	Cuchilla 2. VMWHost2. (SuperMicro MBI-618R-T2), cuchilla 2 de las 3 que conforman el Cluster de la solución VMWare. Este cluster permite la administración y gestión de los recursos de la solución Vmware como són: asignación de memoria, de procesador y almacenamiento.	Moderado	Posible	2h	12h
VMWare: ESXi-VMWHOST3	Cuchilla 3. VMWHost3. (SuperMicro MBI-618R-T2), cuchilla 3 de las 3 que conforman el Cluster de la solución VMWare. Este cluster permite la administración y gestión de los recursos de la solución Vmware como són: asignación de memoria, de procesador y almacenamiento.	Moderado	Posible	2h	12h
VMWare: ESXi-VMWHOST4	Cuchilla 1. cuchilla 1 de las 3 que conforman el Cluster de la solución Oracle VM Este cluster permite la administración y gestión de los recursos de	Moderado	Posible	2h	12h
VMWare: ESXi-VMWHOST5	Cuchilla 2. cuchilla 2 de las 3 que conforman el Cluster de la solución Oracle VM Este cluster permite la administración y gestión de los recursos de	Moderado	Posible	2h	12h
VMWare: ESXi-VMWHOST6	Cuchilla 3. cuchilla 3 de las 3 que conforman el Cluster de la solución Oracle VM Este cluster permite la administración y gestión de los recursos de	Moderado	Posible	2h	12h

1.6. Acceso a servicios en la nube

La CRA como parte de su proceso de análisis de los servicios en la nube, se encuentra evaluando qué tipo de modelo de implementación en la nube (pública, privada o híbrida) es la más acorde a los procesos de la entidad para atender las necesidades de los grupos de interés o partes interesadas.

De acuerdo a la guía de computación en la nube de MINTIC la Comisión ha estudiado los siguientes modelos de implementación de nube.

Tipo de nube	Descripción
Nube privada	La nube privada permitiría a la entidad el acceso exclusivo, el uso de la infraestructura y los recursos computacionales. Este tipo de nube puede ser administrada por la entidad o por un tercero.
Nube comunitaria	La nube comunitaria permitiría a las entidades del sector vivienda gestionar diferentes procesos acordes a los objetivos misionales, políticas de seguridad y privacidad, entre otros elementos. Este tipo de nube serviría a un grupo de entidades a diferencia de la nube privada. De igual forma que la nube privada, puede ser administrada por la entidad o por un tercero.
Nube pública	La nube pública integra la infraestructura y recursos informáticos y los pone a disposición del público en general a través de una red pública.
Nube híbrida	La nube híbrida permite a las entidades establecer dos o más nubes de acuerdo a las necesidades y procesos. Este tipo de nube permitiría que la CRA estableciera para ciertos procesos una nube privada y a su vez una nube comunitaria para el manejo de datos y aplicaciones relacionadas con el sector vivienda.

De igual forma, la entidad ha identificado qué servicios podrá adquirir de acuerdo a los modelos de servicios definidos para la contratación de servicios en la nube.

Modelo de servicios	Servicios
Software como Servicio – SaaS	<ul style="list-style-type: none">• Correo electrónico y aplicaciones de oficina• Facturación• Sistemas de Gestión y manejo de relaciones con clientes - CRM• Herramientas de Colaboración

Modelo de servicios	Servicios
	<ul style="list-style-type: none"> • Aplicaciones de gestión de contenidos • Herramientas de gestión de documentos • Finanzas • Recursos humanos • Aplicaciones de ventas • Redes de colaboración • Planificación de Recursos Empresariales (ERP)
Plataforma como servicio - PaaS	<ul style="list-style-type: none"> • Inteligencia de Negocios • Base de datos • Desarrollo y pruebas • Integración • Implementación de aplicaciones
Infraestructura como Servicio – IaaS	<ul style="list-style-type: none"> • Copia de seguridad y recuperación • Cómputo • Redes de distribución de contenido (CDN) • Gestión de servicios • Almacenamiento • Computación por lotes • Servicios tecnológicos de Internet de las cosas - IoT.

De acuerdo con las evaluaciones realizadas en relación a los servicios en la nube⁸ en el DRP en el apartado 13.6. Propuesta de sitio alternativo en esquema de computación en la nube y siguiendo las recomendaciones de MINTIC sobre la implementación de este tipo de esquemas de computación como escenarios de recuperación o sitio alternativo, la Oficina Asesora de Planeación y TIC propuso realizar la migración de servicios gradualmente e iniciar como primera fase con los componentes tecnológicos relacionados con los servicios de administración de recursos de almacenamiento (NAS y SAN), esta primera fase se establecerá como parte del PETI actual (Ver PETI 2018 - 2022) de la Entidad y su ejecución y priorización dependerá de la asignación presupuestal en el plan de adquisición de la Comisión.

Esta primera fase de implementación del sitio alternativo cuando se considere su implementación como escenario de recuperación ante un desastre, deberá seguir un modelo de nube privada en modalidad de Infraestructura como servicio.

⁸ Ver documento Plan de Recuperación ante Desastres DRP de la Comisión

1.7. Tecnología verde

En relación con la tecnología verde, la Entidad definió desde el año 2016, el Plan de manejo de los residuos de aparatos eléctricos y electrónicos - RAEE⁹ el cual busca:

- Contribuir en la prevención y reducción del impacto ambiental al interior de la CRA, administrar y gestionar el manejo de los RAEE.
- Establecer y comunicar la responsabilidad en el uso y manejo de los RAEE.
- Gestionar los riesgos en el manejo de los RAEE.
- Sensibilizar y generar mayor conciencia hacia el cuidado del Medio Ambiente.

De igual forma para contribuir con las estrategias de prevención del impacto ambiental, ha implementado acciones relacionadas con el uso eficiente del papel, la virtualización de servidores, el uso eficiente de energía, la centralización de servicios de impresión y un plan piloto de teletrabajo.

2. Operación de los servicios tecnológicos

2.1. Alta disponibilidad de los servicios tecnológicos

La Oficina Asesora de Planeación y TIC es la encargada de implementar capacidades de alta disponibilidad para las infraestructuras críticas y los Servicios Tecnológicos que afecten la continuidad del servicio de la CRA. En la siguiente tabla se relacionan los servicios tecnológicos que se encuentran en alta disponibilidad en la Comisión

Servicio tecnológico	Alta disponibilidad
ROUTER CISCO 2901	Si
SWITCH DLINK 3100	Si
Tansceiver Raisecom (ISCOM RAX700)	Si
Switch Core – DLink DGS-3420-52P	Si
Switch DLink DGS-3420-52P ID 2	Si
Switch DLink DGS-3420-52P ID 3	Si
Switch DLink DGS-3420-52P ID 4	Si
Red inalámbrica – Access Point DLink 2660	Si
Conexión planta telefónica – CENTREX UNE	Si
FireWall – FortiGate 300D	No
Conexión planta telefónica – PATTON 3086	No

⁹ Ver documento Plan de manejo de los residuos de aparatos eléctricos y electrónicos (RAEE)

3. Soporte de los servicios tecnológicos

En este apartado se describe el Catálogo de Acuerdos de Niveles de Servicio (ANS) de la CRA, teniendo en cuenta los diferentes tiempos de prestación de servicios, así como los niveles de cumplimiento para los Servicios Tecnológicos.

Categoría	Servicio	Duración del acuerdo	Nivel de cumplimiento		
			Rojo	Amarillo	Verde
Sistemas de Información	Soporte de sistemas de información externos (SECOP, SIIF, SUI, SIGEP)	2h	Rango menor a 50%	Rango entre 80% & 51%	Rango mayor a 81%
Desarrollo de Aplicaciones	Asesoría en el desarrollo e implementación de sistemas	1 semana(según requerimiento podrá cambiar de 1 a 4 semanas)	Rango menor a 50%	Rango entre 80% & 51%	Rango mayor a 81%
Desarrollo de Aplicaciones	Desarrollo y mantenimiento de software	1 semana(según requerimiento podrá cambiar de 1 a 4 semanas)	Rango menor a 50%	Rango entre 80% & 51%	Rango mayor a 81%
Bases de datos	Administración de bases de datos	1 semana	Rango menor a 50%	Rango entre 80% & 51%	Rango mayor a 81%
Bases de datos	Modelamiento bodega de datos – SINFONIA	2 semana(según requerimiento podrá cambiar de 2 a 4 semanas)	Rango menor a 50%	Rango entre 80% & 51%	Rango mayor a 81%
Apoyo virtual	Vídeoconferencia	3 días	Rango menor a 50%	Rango entre 80% & 51%	Rango mayor a 81%
Centro de Datos	Administración del centro de datos	2 días	Rango menor a 50%	Rango entre 80% & 51%	Rango mayor a 81%
Centro de Datos	Administración y configuración de servidores	2 días	Rango menor a 50%	Rango entre 80% & 51%	Rango mayor a 81%

Categoría	Servicio	Duración del acuerdo	Nivel de cumplimiento		
			Rojo	Amarillo	Verde
Centro de Datos	Administración de recursos de virtualización	3 días	Rango menor a 50%	Rango entre 80% & 51%	Rango mayor a 81%
Centro de Datos	Administración de recursos de almacenamiento	2 días	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Recursos tecnológicos	Administración de recursos tecnológicos	2 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Recursos tecnológicos	Mantenimiento preventivo y correctivo	1 -2 semanas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Sistemas de apoyo	Correo electrónico institucional	2 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Software	Ofimática	2 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Software	Software especializado (SPSS, STATA, Microsoft Project, Microsoft Project Server, Omnipage Profesional, Frontier, Autocad, Dragon and Natural Speaking.)	2 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Conectividad	Configuración de internet	2 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Conectividad	Configuración redes inalámbricas	2 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Conectividad	Configuración enlaces de comunicaciones	2 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%

Categoría	Servicio	Duración del acuerdo	Nivel de cumplimiento		
			Rojo	Amarillo	Verde
Conectividad	Configuración telefonía VoIP	4 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Conectividad	Directorio activo (creación de usuarios)	4 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Conectividad	Bloqueo, desbloqueo y eliminación de servicios de red	2 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Estación de trabajo	Impresoras	3 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Estación de trabajo	Escáners	2 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Estación de trabajo	Computadores de escritorio	4 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Estación de trabajo	Vídeo beam	1 hora	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Estación de trabajo	Computadores portátiles	4 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Estación de trabajo	Tablet	3 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Seguridad de la Información	Antivirus	4 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Seguridad de la Información	Administración de la seguridad de la infraestructura TIC	4 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Seguridad de la Información	Backup	4 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%

Categoría	Servicio	Duración del acuerdo	Nivel de cumplimiento		
			Rojo	Amarillo	Verde
Seguridad de la Información	Cámaras de vigilancia	4 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Seguridad de la Información	VPN	1 día	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Seguridad de la Información	Biométrico	2 horas	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%
Uso y Apropriación	Sensibilizar y capacitar en TIC	1 día	Rango menor a 60%	Rango entre 84% & 61%	Rango mayor a 85%

3.1. Mesa de servicio

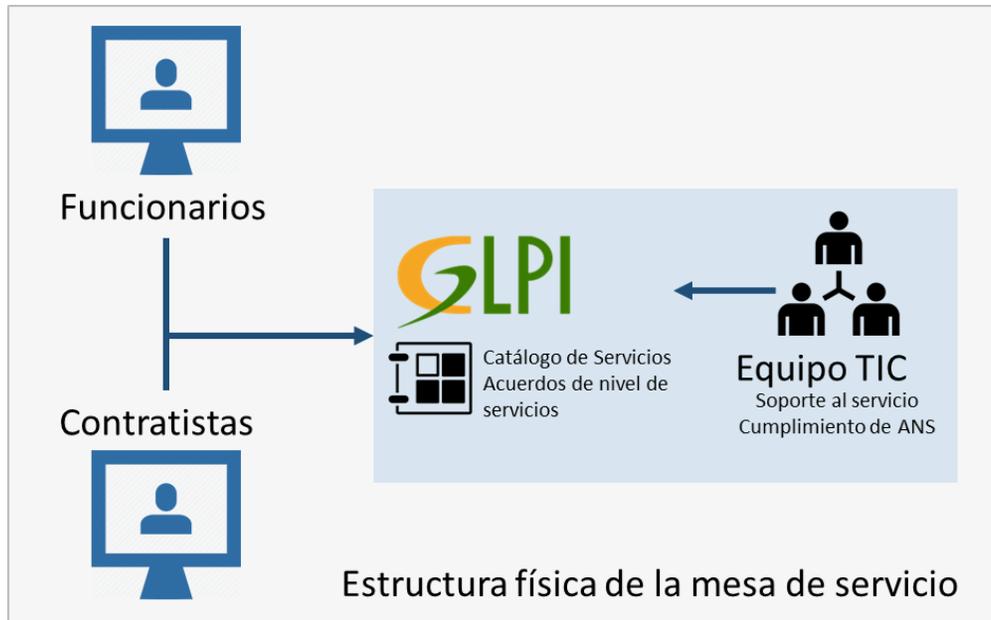
La entidad como parte de la estructura lógica de la mesa de servicio tiene implementado el sistema GLPI¹⁰, el cual está orientada a solucionar todo tipo de eventos que se presenten sobre la infraestructura tecnológica mediante la generación de tickets o casos. En la CRA, GLPI es el punto de contacto entre los Usuarios y la Oficina Asesora de Planeación y TIC.

Dentro del sistema GLPI se ha establecido el árbol de servicios donde se tiene incluido los Acuerdos de Nivel de Servicio por cada uno de estos. Los funcionarios y contratistas de la Entidad por medio de la Intranet acceden al sistema para registrar y consultar los incidentes.

En este sentido la estructura física de la mesa de servicio de la entidad es centralizada y gestionada desde la Oficina Asesora de Planeación y TIC en los horarios de funcionamiento establecidos por la Entidad.

A continuación, se relaciona la arquitectura física de la mesa de servicio:

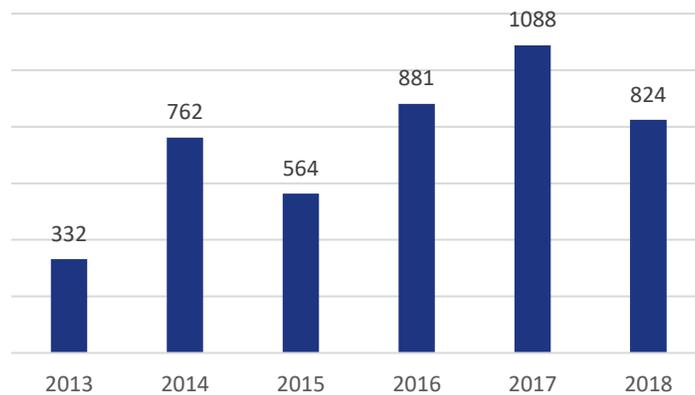
¹⁰ Sistema interno para la gestión de requerimientos, problemas e incidentes.



De acuerdo con el informe Incidencias 2015-2018¹¹, el Grupo TIC de la CRA brinda soporte a través de la mesa de servicio desde el año 2013 con la implementación del Sistema GLPI. Este sistema de software libre permite registrar y hacer seguimiento a los incidentes reportados por la indisponibilidad de los servicios tecnológicos relacionados con el catálogo de TIC.

Hasta el año 2018 se han registrado una cantidad de 4570 incidencias hasta la fecha, de los cuales se han resuelto 4500 de estos.

Periodo	Incidencias
2013	332
2014	762
2015	564
2016	881
2017	1088
2018	824



En el año 2018, los incidentes más recurrentes por categoría fueron:

¹¹ Ver documento Incidencias 2018 de la CRA

Categorías	Numero
Administracion de Usuarios de red > Creación de usuarios	70
Hardware > Impresoras	69
Software > Office > Correo Electrónico - Microsoft Outlook	60
Administracion de Usuarios de red > Bloqueo de Usuario	59
Administracion de Usuarios de red > Desbloqueo/Cambio Contraseña	43
Software > ORFEO > Otros	32
Servicios > Internet	32
Varios	30
Administracion de Usuarios de red > Desactivación de usuarios	27
Hardware > Biométrico	27

4. Gestión de la calidad y la seguridad de los servicios tecnológicos

4.1. Análisis de riesgos

Según el Mapa de Riesgos de Gestión (03) de la CRA¹², el proceso de Gestión de TIC tiene asociados los riesgos que se describen y valoran a continuación:

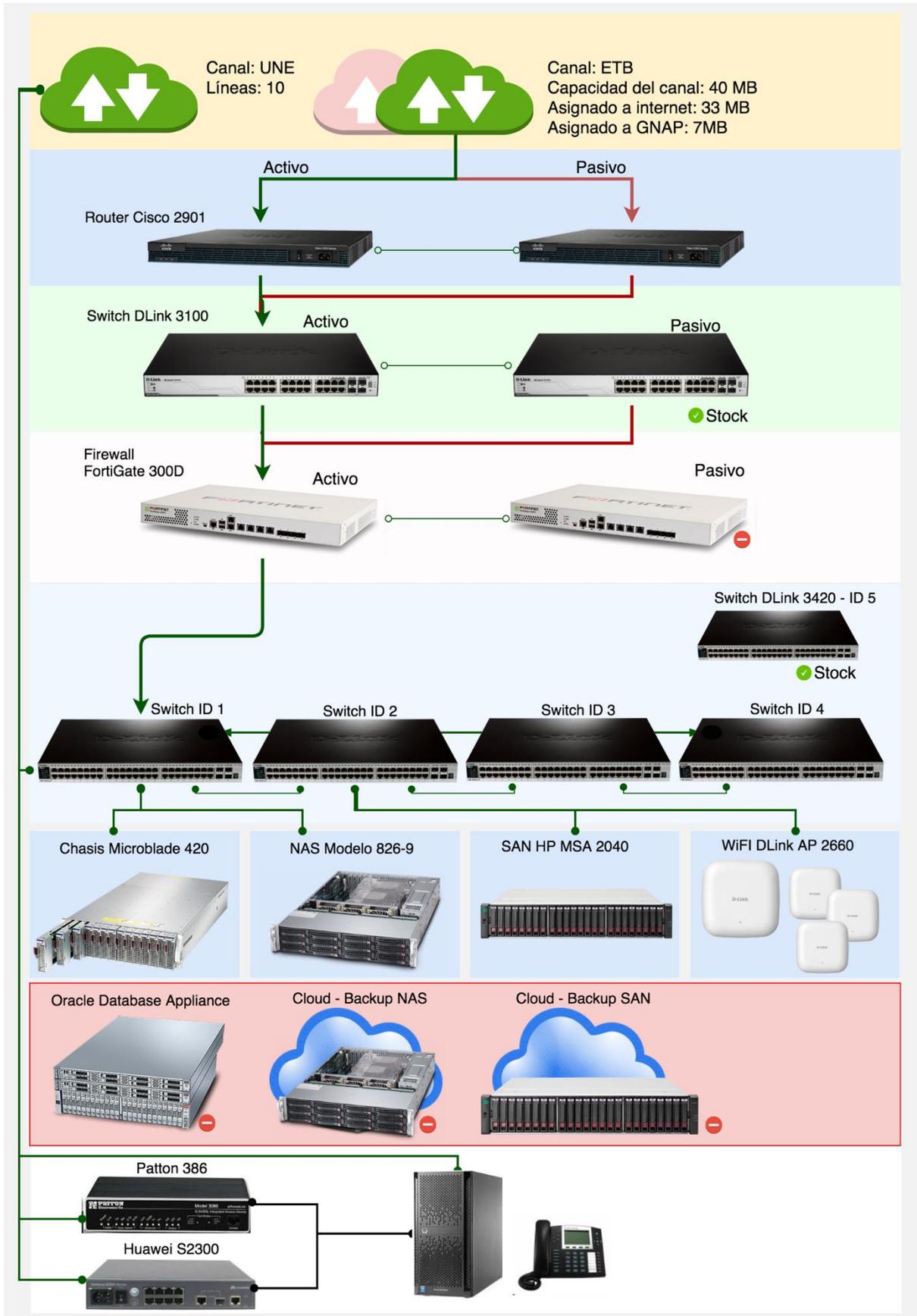


Proceso	Gestión de TIC	Oficina líder	Oficina Asesora de Planeación y TIC		
Objetivo	Implementar y mantener la plataforma tecnológica a través del desarrollo soluciones eficaces a las necesidades de los procesos misionales y administrativos para la optimización de la gestión institucional garantizando la integridad confidencialidad y disponibilidad de la información.				
Causa	Riesgo	Clase de riesgo	Nivel de riesgo		
			Inherente	Residual	
Interna	Reiterativa generación de requerimientos en	Riesgo operativo	Alto	Moderado	
• Ausencia de documentación sobre el					

¹² Ver documento DES-FOR03 Mapa de Riesgos de Gestión V03

Proceso	Gestión de TIC	Oficina líder	Oficina Asesora de Planeación y TIC		
	seguimiento y la efectividad de las actividades que dan solución a los requerimientos del GLPI.	GLPI por la misma causa, al no identificar la causa raíz de los mismos.			
	<p>Interna</p> <ul style="list-style-type: none"> Baja visibilidad del papel crítico del proceso TIC. Ausencia de lineamientos en materia de seguridad de la información. <p>Externa</p> <ul style="list-style-type: none"> Aumento de los ataques informáticos a nivel mundial. 	<ul style="list-style-type: none"> Contaminación por Malware Ataques de Ingeniería Social Alteración o pérdida de la Información. 	Riesgo de seguridad de la información	Extremo	Extremo
	<p>Interna</p> <ul style="list-style-type: none"> Fallas críticas del centro de cómputo principal. Desactualización del plan de recuperación ante desastres. <p>Externa</p> <ul style="list-style-type: none"> Fallas en los proveedores de servicio de TI críticos (esenciales). 	Pérdida e Indisponibilidad de Servicios TIC (Fallas en equipos de tecnología, errores en configuración)	Riesgo de seguridad de la información	Extremo	Extremo
	<p>Interna</p> <ul style="list-style-type: none"> Cortos eléctricos Fallas de la UPS Fallas de equipos de enrutamiento <p>Externa</p> <ul style="list-style-type: none"> Incumplimientos de los acuerdos de nivel de servicio de los proveedores. 	Caída del servicio de la internet de la entidad	Riesgo operativo	Extremo	Alto

5. Arquitectura de TI - situación objetivo



5.1. Análisis de brechas

Este análisis tiene como finalidad determinar y documentar las brechas entre la arquitectura de servicios tecnológicos actual (AS-IS) y la objetivo (TO-BE), permitiendo identificar diferencias y comparaciones entre la situación actual y la situación deseada. En este sentido, las brechas identificadas se convierten en un insumo para la identificación de iniciativas y proyectos (MinTIC, 2016).

		Situación objetivo (TO-BE)								
		Almacenamiento	Servidores	Redes y comunicaciones	Seguridad	Gestión de servicios	Catálogos de servicios	Intercambio de información	Gestión de la continuidad	Mesa de servicio
Situación actual (AS-IS)	Almacenamiento	A								
	Servidores		A							
	Redes y comunicaciones			A						
	Seguridad				A					
	Gestión de servicios					A				
	Catálogos de servicios						A			
	Intercambio de información							A		
	Gestión de la continuidad								A	
	Mesa de servicio									A
	ID Brecha		B1	B2	B3	B4	B5	B6	B7	B8
		ACTUALIZAR	A		MANTENER			M		

El anterior análisis, evidencia las brechas relacionados con los servicios tecnológicos de la CRA, los cuales deberán actualizar u optimizar para dar cumplimiento a los procesos de negocio.

Brechas identificadas relacionadas con la optimización de la infraestructura tecnológica de la entidad:

ID brecha	Nombre o componente de solución	Motivador misional que soporta	Prioridad
B1	Adquirir más almacenamiento para soportar la operación y garantizar la integridad y disponibilidad de la información y servicios	Implementar y mantener la plataforma tecnológica a través del desarrollo soluciones eficaces a las necesidades de los	Alta

ID brecha	Nombre o componente de solución	Motivador misional que soporta	Prioridad
	<p>tecnológicos (NAS y SAN) de la entidad.</p> <p>Adquirir o contratar un servicio de almacenamiento externo que garantice la disponibilidad, integridad y confiabilidad de la información contenida en la SAN HP MSA 2040.</p>	<p>procesos misionales y administrativos para la optimización de la gestión institucional garantizando la integridad confidencialidad y disponibilidad de la información.</p>	
B2	<p>Dado los análisis de capacidad realizados a los servidores físicos y virtuales de la CRA, se debe considerar la adquisición y ampliación de la Memoria RAM y almacenamiento del sistema de virtualización, que permita la capacidad para dar alcance a nueva demanda de servicios.</p> <p>Teniendo en cuenta la capacidad del Enclosure y disponibilidad de 6 cuchillas, se recomienda aprovisionar una cuchilla con las mismas características en procesador, memoria y disco duro de los Host 1, 2 y 3; con el fin de reemplazar uno de estos en el momento que se materialice el daño.</p>		Alta
B3	<p>Adquirir SWITCH DLINK 3100 capa 2 y configurar en un esquema de alta disponibilidad activo – activo. Al fallar este componente, la CRA tendría una indisponibilidad de los servicios de internet, así como a los servicios TI asociados a este. Actualmente, se debe realizar por parte del Grupo TIC la conexión manual del dispositivo de respaldo que se encuentra operativo en modalidad pasivo.</p>		Moderada

ID brecha	Nombre o componente de solución	Motivador misional que soporta	Prioridad
	Adquirir y configurar un Switch DLink DGS-3420-52P de 48 puertos + 4 puertos de administración de respaldo con el fin de garantizar el stacking dentro de la misma referencia de Switch.		
B4	<p>Contemplar en el proceso de renovación de los servicios asociados al componente firewall, un esquema de alta disponibilidad en modalidad Activo – Activo o Activo - Pasivo.</p> <p>A la fecha ante el fallo del servicio tecnológico, la entidad perdería el servicio de acceso a internet y a todos los servicios que dependen de este.</p> <p>Actualizar la política de respaldo, almacenamiento y recuperación de la información crítica de la entidad, con el objetivo de garantizar la disponibilidad e integridad de los componentes tecnológicos y servicios de almacenamiento.</p>		Alta
B5	Adquirir un contrato de soporte especializado o paquete de horas con especialista VMWare en sitio para la recuperación de toda la operación que presta la solución VMWare, dado que el contrato actual no tiene el alcance para este tipo de soporte especializado, ni capacitación especializada al especialista responsable de la gestión del servicio.		Moderada
B6	Mantener actualizado los catálogos de servicios tecnológicos y de TI y hacer medición periódica de los Acuerdos de Nivel de servicios establecidos.		Baja

ID brecha	Nombre o componente de solución	Motivador misional que soporta	Prioridad
B7	Diagnosticar la infraestructura de TI para implementar los lineamientos para la integración de la entidad al Portal Único del Estado Colombiano - GOV.CO de acuerdo a la Estrategia de Integración Digital del Estado.		Alta
B8	Evaluar la gestión de los proveedores de componentes y servicios tecnológicos de acuerdo a la prestación, implementación, garantía, cumplimiento de los ANS de los mismos, conforme a lo establecido contractualmente.		Moderada
B9	Es necesario velar para que el personal encargado de componentes y servicios de TI con mayores riesgos e impacto se encuentre debidamente capacitados para responder a las contingencias.		Alta
B10	Es determinante para la Entidad definir e implementar el proyecto planteado en el PETI 2018 – 2022, el cual tiene como objetivo definir e implementar la estrategia de gestión de servicios de TI y sus procesos, que permitan soportar la operación de los servicios tecnológicos, generar eficiencia en la prestación de los servicios y reducir costos operativos. Como parte del Proyecto de implementación del modelo de gestión de servicios de TI se busca adoptar las buenas prácticas de ITIL		Alta

6. Referencias

- MINTIC (2018) Manual de Gobierno Digital. Consultado en: https://www.mintic.gov.co/portal/604/articles-79087_recurso_1.pdf
- MINTIC (2014) G.ST.01 Guía del dominio de Servicios Tecnológicos https://www.mintic.gov.co/arquitecturati/630/articles-9277_recurso_pdf.pdf
- MINTIC (2015) Guía General de Adopción del Marco de Referencia de Arquitectura Empresarial. Consultado en: https://mintic.gov.co/arquitecturati/630/articles-9434_Guia_Proceso.pdf
- MINTIC (2018) Guía de computación en la nube. Consultado en: <https://www.mintic.gov.co/arquitecturati/630/w3-article-75554.html>
- MINTIC (2017) Generalidades del Marco de Referencia de AE para la gestión de TI. Consultado en: https://www.mintic.gov.co/arquitecturati/630/propertyvalues8158_descargable_3.pdf
- MINTIC (2017) Lineamientos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI. Consultado en: https://www.mintic.gov.co/arquitecturati/630/propertyvalues8158_descargable_1.pdf
- CRA (2018) Plan Estratégico de Tecnologías de la Información. Consultado en: <https://www.cra.gov.co/documents/PETI-2018.pdf>
- CRA (2019) Arquitectura de Negocio. Consultado en: <https://www.cra.gov.co/documents/Arquitectura-Negocios.pdf>