PLAN DE CONTINUIDAD Y DISPONIBILIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Comisión de Regulación de Agua Potable y Saneamiento Básico

INDICE DE TABLAS

Histórico de revisiones

FECHA	VERSIÓN	DESCRIPCIÓN	AUTOR
Noviembre - 2018	1.0	DRP Aprobado en el Comité Institucional de Gestión y desempeño Extraordinario Numero 5	Oficina asesora de planeación y TICS
Octubre – 2020	2.0	Verificación y ajustes al documento, de acuerdo con la infraestructura y servicios a la fecha. Se ajusta el nombre a Plan de Continuidad y Disponibilidad de las TIC, de acuerdo con la norma técnica GTC-ISO-IEC 27031	Oficina asesora de planeación y TICS
Septiembre - 2022	3.0	Verificación y ajustes al documento, de acuerdo con la infraestructura y servicios a la fecha. Se ajusta el nombre a Plan de Continuidad y Disponibilidad de las TIC, de acuerdo con la norma técnica GTC-ISO-IEC 27031	Oficina asesora de planeación y TICS

8. INTRODUCCIÓN

El plan de continuidad de procesos de negocio (BCP), es una estrategia del orden institucional, que pretende establecer los lineamientos y políticas para que el operar y la consecución de los objetivos misionales se logren pese a que se presenten situaciones de emergencia que puedan interrumpir los procesos de negocio misionales. En este orden de ideas se ha definido la estrategia del BCP que abordara únicamente el componente tecnológico de la Entidad, el cual se ha nombrado el Plan de Continuidad y Disponibilidad de las Tecnologías de la Información donde se deben integran tres aspectos principales, los cuales son:

Alta disponibilidad: Son los mecanismos para proporcionar los recursos a aplicaciones de la entidad, independientemente de los fallos locales.
Operación Continua: Se debe garantizar el funcionamiento durante un estado de emergencia.
Recuperación ante Desastres (DRP): se garantiza la manera de recuperar el centro de datos de la Entidad.

Se debe tener en cuenta que un BCP define tres componentes que lo integran, el análisis de impacto BIA, Matriz de Riesgos, DRP, estos tres componentes definen el accionar de la entidad ante una situación de emergencia la cual será activada por el grupo de tecnología y el CIO, cuando la situación lo amerite.

La entidad debe inspeccionar y hacer parte de las pruebas de los planes de recuperación de catástrofes y de continuidad del negocio del proveedor en la nube. además, integra sus planes de continuidad y recuperación con los planes de continuidad del negocio articulado con los proveedores que tienen contratos vigentes con la Entidad.

Conscientes de la presencia de posibles amenazas (externas e internas) que pueden llegar a afectar la continuidad de las actividades y servicios esenciales, con el presente documento, la CRA pretende definir el Plan de Continuidad y Disponibilidad de las Tecnologías de la Información y Comunicación, como una herramienta que le permita responder oportuna y organizadamente a situaciones que podrían interrumpir la operación regular de los procesos e impactar negativamente en el logro de los objetivos y la misión de la entidad. En este sentido, este Plan, debe responder a los procedimientos necesarios para recuperar, reanudar y restaurar la operación de los recursos, servicios y actividades en materia tecnológica, necesarios para garantizar la continuidad de las funciones críticas del negocio (ISO 22301).

Con el Plan de Continuidad y Disponibilidad de las TIC, se realiza una actualización al Plan de Recuperación de Desastres (DRP) formulado por la CRA en el 2018, entendido como la estrategia de la entidad para restablecer los servicios de TI (Hardware y Software) a su cargo. Entre los beneficios de un DRP se encuentran mantener la continuidad de los servicios relacionados con las 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, y colaboradores, y contar con una capacidad de recuperación exitosa.

La importancia que reviste este tipo de ejercicios se centra en la Continuidad del Negocio, que se refiere al proceso general de gestión que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio en caso de materializarse. La gestión de la continuidad del negocio provee un marco de trabajo para la construcción de la resiliencia organizacional (Manual de Gobierno Digital, 2019)

Este documento se encuentra alineado con las normas técnicas colombianas GTC-ISO-IEC 27031 y NTC-ISO-IEC 27001, así como con el propósito de la Política de Gobierno Digital "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital" en el cual la proactividad, entre otras cosas, alude a entidades que se anticipan, son previsivas, y mitigan riesgos.

9. GLOSARIO Y/O DEFINICIONES

Gestión de continuidad de negocio (BCM). Proceso general de gestión holístico que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio que en caso de materializarse y el cual provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor.

Plan de Continuidad de Negocio. Procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación debido una vez presentada / tras la interrupción. NOTA: Típicamente, esto incluye los recursos, servicios y actividades necesarios para garantizar la continuidad de las funciones críticas del negocio. [Fuente: ISO 22301].

Continuidad de procesos de negocio BCP: Es una estrategia del orden institucional, que pretende establecer los lineamientos y políticas para que el operar y la consecución de los objetivos misionales se logren pese a que se presenten los procesos de negocio misionales.

Análisis del impacto al negocio (BIA por sus siglas en ingles). Proceso del análisis de actividades las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. [Fuente: ISO 22300].

Nivel de Criticidad. Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

Interrupción. Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

Recuperación de desastres de tecnología y telecomunicaciones (ITCTIC). Habilidad Capacidad de los elementos de tecnología y telecomunicaciones (ITC)de las TIC de la organización para soportar sus funciones críticas a un nivel aceptable dentro de un periodo predeterminado de tiempo después de una interrupción.

Plan de recuperación de desastres de ICT LAS TIC (ICT DRP). Plan claramente definido y documentado el cual permite recuperar las capacidades de tecnología y Telecomunicaciones LAS TIC cuando se presenta una interrupción. NOTA: En algunas organizaciones es llamado el plan de continuidad de tecnología y telecomunicaciones las TIC.

Preparación de las ICT TIC para la continuidad de negocio (IRBC). Capacidad de una organización para soportar sus operaciones de negocio mediante la prevención, detección y respuesta a una interrupción, así como la recuperación de sus servicios de ICTTIC.

Objetivo mínimo de continuidad de negocio (MBCO). Mínimo nivel de productos y/o servicios que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción.

Punto objetivo de recuperación (RPO). Punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra.

Punto Tiempo objetivo de tiempo de recuperación (RTO). Periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra.

Tiempo de inactividad máximo tolerable (MTD). define la cantidad total de tiempo que un proceso de negocio puede interrumpirse sin causar consecuencias inaceptables.

Tiempo de recuperación del trabajo (WRT). determina la cantidad máxima de tiempo tolerable que se necesita para verificar el sistema y / o la integridad de los datos.

Sitio alterno. Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción.

10. OBJETIVO

Definir el Plan de Continuidad y Disponibilidad de las TIC de la CRA, a partir de la identificación de los servicios e infraestructura tecnológica crítica, así como de las estrategias y acciones que permitan garantizar la recuperación, reanudación y restauración oportuna de los servicios e infraestructura necesarios para dar continuidad a las operaciones esenciales de la Entidad, ante una posible falla o interrupción las TIC.

3.1 OBJETIVOS ESPECÍFICOS

- Realizar el Análisis de Impacto del negocio (BIA) (Business Impact Analysis) sobre los componentes TI administrados por el proceso de gestión de TI.
- Realizar el Análisis de Riesgos de Continuidad de las TIC.
- Diseñar la política de recuperación ante fallas o interrupciones acorde a las necesidades de la Comisión, de manera tal que se garantice el menor impacto posible.

11. ALCANCE

Definir el Plan de Continuidad y Disponibilidad de las TIC, basado en la norma ISO 27031:2016 y apoyadas en buenas prácticas como ISO 22301, BS 25999, para la continuidad del negocio.

12. ANÁLISIS DE IMPACTO AL NEGOCIO (BIA) SOBRE LOS COMPONENTES TIC ADMINISTRADOS POR EL PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

El Plan de continuidad está conformado por un conjunto de directrices y procedimientos, el cual tiene como finalidad que la Entidad pueda tomar las acciones pertinentes para la recuperación y restablecimiento de los servicios e infraestructuras de TI interrumpidas por situaciones de desastre o emergencias. En este sentido, el análisis de impacto del negocio como parte del plan de continuidad, se entiende como un marco conceptual sobre el cual la Comisión debe planear integralmente los alcances y objetivos, que permiten proteger la información y componentes tecnológicos críticos. Este debe tener una estrategia de continuidad de TI, que contenga los objetivos globales de la entidad, con respecto a las dimensiones de disponibilidad de datos, infraestructura tecnológica y recurso humano. El Análisis de Impacto del Negocio BIA (Business Impact Analysis) por sus siglas en inglés), es importante porque permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio. (MinTIC.2015)

Como primera actividad en la definición del Plan de Continuidad y Disponibilidad TIC, se realizó una revisión documental del plan estratégico de la entidad, el plan estratégico de TI, las políticas de seguridad de la información, las políticas de calidad, el mapa de procesos, el catálogo de servicios, entre otros documentos que permitieron una contextualización general de la Comisión y validar la articulación de la estrategia institucional con la estrategia TI.

En el mes de marzo del año 2021, los profesionales de Tecnología de la Información de la Oficina de Planeación y TIC's, realizó un ejercicio de revisión de los servicios tecnológicos conforme a las adquisiciones e implementación de tecnologías emergentes en la entidad. Como resultado del ejercicio, se realiza la actualización de los Acuerdos de Niveles de Servicios - ANS, el árbol de servicios tecnológicos y el catálogo de servicios tecnológicos; Estos tres documentos, fueron aprobados el 1 de junio de 2021 por el asesor de dirección ejecutiva con funciones de TI y socializados al interior de la entidad por medio de capacitaciones y campañas de comunicación vía correo electrónico.

Dentro del catálogo de servicios se definen entre otros, el impacto que representa cada uno de los servicios para la entidad. Entendiendo el impacto como la medida en la que un cambio, problema o incidente afecta los procesos de negocio, se clasifica en los siguientes niveles:

- **Alto:** Si la interrupción del servicio afecta de manera crítica la operación y los procesos de la entidad.
- **Medio:** Si la interrupción del servicio afecta la operación, pero no impide su uso ni afecta los procesos.
- **Bajo:** Si el servicio se ve afectado, pero no impide su uso ni afecta los procesos de la entidad.

5.1 RELACIÓN ENTRE LOS SERVICIOS DE TI Y LOS PROCESOS DE NEGOCIO

Al generar la matriz de relación entre los servicios TI y los procesos de negocio[1], que se encuentran vigentes en el sistema de calidad de la entidad. identificó que una afectación de los servicios de: *conexión a internet por red física de datos e inalámbrica, correo electrónico, herramientas colaborativas de la suite ofimática, fallos en las estaciones de trabajo física o virtuales, directorio activo*, entre otros servicios. Incidiría de manera negativa directamente a los 12 procesos de negocios de la entidad. En este mismo sentido, se identificó qué los procesos de negocio que tendrían un mayor impacto en las operaciones de: Gestión de Tecnologías de Información, Regulación General, Gestión Regulatoria y Servicio al Ciudadano.

Lo anterior, se evidencia en las siguientes tablas 1 y 2.

[1] Procesos de negocio de la CRA: Dirección estratégica, evaluación y control, gestión contable y financiera, gestión de bienes y servicios, gestión de seguimiento y mejora, gestión de TI, gestión del talento humano, gestión documental, gestión jurídica, gestión regulatoria, regulación general, servicio al ciudadano gestión de comunicaciones y gestión de cooperación internacional.

.

TABLA NO 1 RELACIÓN ENTRE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y LOS PROCESOS DE NEGOCIO. IMPACTO: ALTO

ID	Servicio	Impacto	Dirección estrategica	Evaluación y Control	Gestión contable y Financiera	Gestión de bienes y servicios	Gestión de seguimiento y mejora	Gestión de tecnologia de la información	Gestión de Talento Humano	Gestión Documental	Gestión Juridica	Gestión Regulatoria	Regulación General	Servicios al Ciudadano	Gestión de Comunicaciones	Gestión de Cooperación Internac.	Numero de procesos
1	Soporte y Mantenimiento de información Estructurada y No estructurada	Alto															4
2	Administración de bases de datos	Alto															2
3	Configuración de Equipos de computo Fisicos y Virtuales	Alto															
4	Correo electrónico Institucional	Alto															14
5	Herramientas colaborativas Suite Ofimática	Alto															14
6	Administración y configuración de servidores	Alto															1
7	Administración de recursos de virtualización	Alto															1
8	Administración de recursos de almacenamiento	Alto															1
9	Conexión cableada a rec de datos e Internet	Alto															1
10	Configuración Redes inhalambricas e Internet	Alto															14
11	Administración de la seguridad y privacidad de la Información	Alto															14
12	VPN	Alto															1
1|3	Antivirus	Alto															3
14	Control de acceso biométrico	Alto															14
15	Videovigilancia	Alto															14
16	Sensibilizar y capacitar en TI	Alto															14
17	Elaboración de Términos de referencia: contratación de productos y servicios de las TIC	Alto															4

TABLA NO 2 RELACIÓN ENTRE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y LOS PROCESOS DE NEGOCIO. IMPACTO: MEDIO Y BAJO

ID	Servicio	Impacto	Dirección estrategica	Evaluación y Control	Gestión contable y Financiera	Gestión de bienes y servicios	Gestión de seguimiento y mejora	Gestión de tecnologia de la información	Gestión de Talento Humano	Gestión Documental	Gestión Juridica	Gestión Regulatoria	Regulación General	Servicios al Ciudadano	Gestión de Comunicaciones	Gestión de Cooperación Internac..	Numero de procesos
18	Desarrollo y ajustes de sistemas de información	Medio															3
19	Soportes de sistemas de información externos	Medio															5
20	Soporte a software especializado ((SPSS, STATA, Microsoft Project, Microsoft Project Server, Omnipage Profesional, Frontier, Autocad, Dragon and natural speaking.))	Medio															14
21	Soportes de sistemas de impresoras, escaners y Video Beam	Medio															14
22	Configuración telefonia VoIP	Medio															14
23	Mantenimiento preventivo y correctivo	Medio															14
24	Videoconferencias	Medio															14
25	Administración de correosde datos e infraestructura en la Nube	Medio															1
26	Directorio activo- Gestión de usuarios	Medio															1
27	Conceptos técnicos	Medio															5

5.2 RELACIÓN ENTRE LOS SERVICIOS DE TI, EL IMPACTO Y LOS GESTORES **DEL SERVICIO.**

Dado la composición de la Oficina de Planeación y TIC de la CRA, específicamente sus funcionarios de planta, se identificaron 5 roles centrales en el proceso de Gestión de las tecnologías de la información en la entidad.

Rol	Descripción
CIO	Coordinar la formulación, implementación, evaluación y seguimiento de los lineamientos necesarios para el fortalecimiento y correcto funcionamiento de la Comisión de Regulación y Agua Potable y Saneamiento Básico en materia de Tecnologías de la Información y la Comunicación. En caso de no estar presente el CIO, asumirá el rol el Profesional Especializado Grado 22
Profesional Especializado grado 22	Definir, planear y coordinar las actividades relacionadas con el sistema de gestión de seguridad de la información y los esquemas y políticas de seguridad informática que se deban implementar a fin de asegurar la plataforma de infraestructura y de Sistemas de información, interactuando con los diferentes entes de seguridad, realizando o liderando las auditorias de seguridad de la información acorde con las normas establecidas. Asumiendo el rol de Oficial de Seguridad de la Entidad. En caso de no estar presente el Profesional Especializado Grado 22, asumirá el rol el Profesional Especializado Grado 15
Profesional Especializado grado 22	Definir, planear y coordinar las actividades relacionadas con los sistemas de información requeridos como apoyo a los procesos de Regulación y Asesoría, en cuanto dimensionamiento y asesoramiento a las áreas misionales y de apoyo de nuevas herramientas y/o sistemas de información, aseguramiento de la calidad y del soporte y mantenimiento de los Sistemas de información vigentes, soporte y manejo de los proveedores o fabricantes del software. En caso de no estar presente el Profesional Especializado Grado 22, asumirá el CIO
Profesional Especializado grado 15	Definir, planear y coordinar las actividades relacionadas con la definición, implementación del esquema de servicios tecnológicos y de mesa de ayuda, definiendo el árbol de servicios tecnológicos con todos los profesionales de TIC que hacen parte de la Oficina de Planeación y tics y velando por su atención, soporte y cumplimiento de los ANS a la Entidad. En caso de no estar

Rol	Descripción
	presente el Profesional Especializado Grado 15 asumirá el rol el Profesional Especializado Grado 22

TABLA NO 3 IMPACTO Y LOS GESTORES DEL SERVICIO
Fuente: Elaboración propia Manual de Funciones

Estos funcionarios además de gestionar los servicios asociados a su rol en TI, son los encargados de llevar a cabo los procedimientos de recuperación ante la materialización del riesgo. Si llegase a materializarse el riesgo y el funcionario no se encontrará en la entidad el tiempo de recuperación del servicio será afectado y en consecuencia la operación de los servicios y procesos de negocio relacionados con este servicio.

Teniendo en cuenta lo anterior, se realizó un análisis de los procesos de la entidad con el fin determinar la relación entre los servicios TI y el rol responsable del servicio, con el fin de determinar el efecto de la ausencia de un gestor de servicio o funcionario ante la materialización del riesgo. (Ver tabla 3).

Lo que evidencia este análisis es que el rol del CIO tiene asociado un servicio de impacto alto y un servicio de impacto medio. Por su parte el Profesional Especializado Grado 22 tiene asociado trece servicios de impacto alto y cinco de impacto medio. Así mismo, el Profesional Especializado Grado 15 tiene relación con tres servicios de impacto alto, cuatro de medio.

Tabla 3. Relación entre los servicios de TI, el impacto y los gestores del servicio.

ID	Servicio	Gestor	Impacto
1	Soporte y Mantenimiento de Información Estructurada y No Estructurada	Profesional Especializado Grado 22	Alto
2	Desarrollo y Ajustes de Sistemas de Información	Profesional Especializado Grado 22	Medio
3	Soporte de Sistemas de Información Externos	Profesional Especializado Grado 15	Medio
4	Soporte a Software Especializado	Profesional Especializado Grado 15	Medio
5	Administración de bases de datos	Profesional Especializado Grado 22	Alto

6	Configuración de Equipos de Cómputo Físicos y Virtuales	Profesional Especializado Grado 15	Alto
7	Soporte y Configuración de Impresoras, Escáner y Video Beam	Profesional Especializado Grado 15	Medio
8	Configuración Telefonía VozIP	Profesional Especializado Grado 22	Medio
9	Mantenimiento Preventivo	Profesional Especializado Grado 15	Medio
10	Correo Electrónico Institucional	Profesional Especializado Grado 22.	Alto
11	Herramientas Colaborativas	Profesional Especializado Grado 22	Alto
12	Videoconferencia	Profesional Especializado Grado 22	Medio
13	Administración del Centro de Datos e Infraestructura en la Nube	Profesional Especializado Grado 22	Medio
14	Administración y configuración de servidores	Profesional Especializado Grado 22	Alto
15	Administración de recursos de virtualización	Profesional Especializado Grado 22	Alto
16	Administración de recursos de almacenamiento	Profesional Especializado Grado 22	Alto
17	Conexión cableada a red de datos e Internet	Profesional Especializado Grado 22	Alto
18	Configuración Redes Inalámbricas e Internet	Profesional Especializado Grado 22	Alto
19	Directorio activo - Gestión de usuarios	Profesional Especializado Grado 22	Medio
20	Administración de la seguridad y privacidad de la información	Profesional Especializado Grado 22	Alto
21	Antivirus	Profesional Especializado Grado 22	Alto
22	Control de Acceso - Biométrico	Profesional Especializado Grado 15	Alto
23	VPN	Profesional Especializado Grado 22	Alto
24	Videovigilancia	Profesional Especializado Grado 22	Alto

25	Sensibilizar y capacitar en TI	Profesional Especializado Grado 15	Alto
26	Conceptos técnicos	CIO – Chief Information Officer	Medio
27	Elaboración de Términos de referencia: contratación de productos y servicios de las TIC	CIO – Chief Information Officer	Alto

TABLA NO 4 IMPACTO Y LOS GESTORES DEL SERVICIO
Fuente: Elaboración propia

13. EVALUACIÓN DEL IMPACTO (RPO-RTO-MTD-WRT) Y PROBABILIDAD

Dado que todos los servicios de TI de la CRA aún dependen de la infraestructura tecnológica alojada en el datacenter, el análisis que se desarrollará a continuación corresponde a un escenario en el cual la infraestructura sufra algún daño o materialice algún riesgo y en consecuencia afecte los servicios de TI.

En este sentido, para identificar el impacto en los servicios de TI, en relación con algún daño en los componentes tecnológicos, se realizó un proceso de evaluación con los especialistas de la Oficina Asesora de Planeación y TIC. A través de esta evaluación se identificó el impacto, el Punto de Recuperación Objetivo (RPO), el Tiempo de Recuperación Objetivo del servicio (RTO), Tiempo de recuperación del trabajo (WRT) y el Tiempo de inactividad máximo tolerable (MTD); y la probabilidad de ocurrencia en un escenario de materialización del riesgo de cada uno de los componentes tecnológicos(hardware) que hacen parte de la infraestructura de comunicaciones, almacenamiento y procesamiento (servidores) de la CRA y que pueden llegar afectar los 27 servicios de TI que fueron descritos previamente en este documento, los cuales corresponden a los definidos en el Catálogo de Servicios de TI de la entidad[2], para lo cual fue adoptada la guía para la administración del riesgo del DAFP[3], así como el Manual de Administración de Riesgo y de Oportunidades[4], donde el impacto se entiende como las consecuencias que puede ocasionar a la Entidad la materialización del riesgo, y la probabilidad como la posibilidad de ocurrencia del riesgo; que puede ser medida con criterios de frecuencia, si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado.

La evaluación del impacto y probabilidad se realiza con base al manual de administración de riesgos y oportunidades.

[2] Catálogo de servicios de TI actualizado en junio del 2022.
[3] https://www.funcionpublica.gov.co/web/eva/detalle-publicacion?entryId=34316499

[4] EVC-MAN01 Manual de administración de riesgos y oportunidades v06.docx

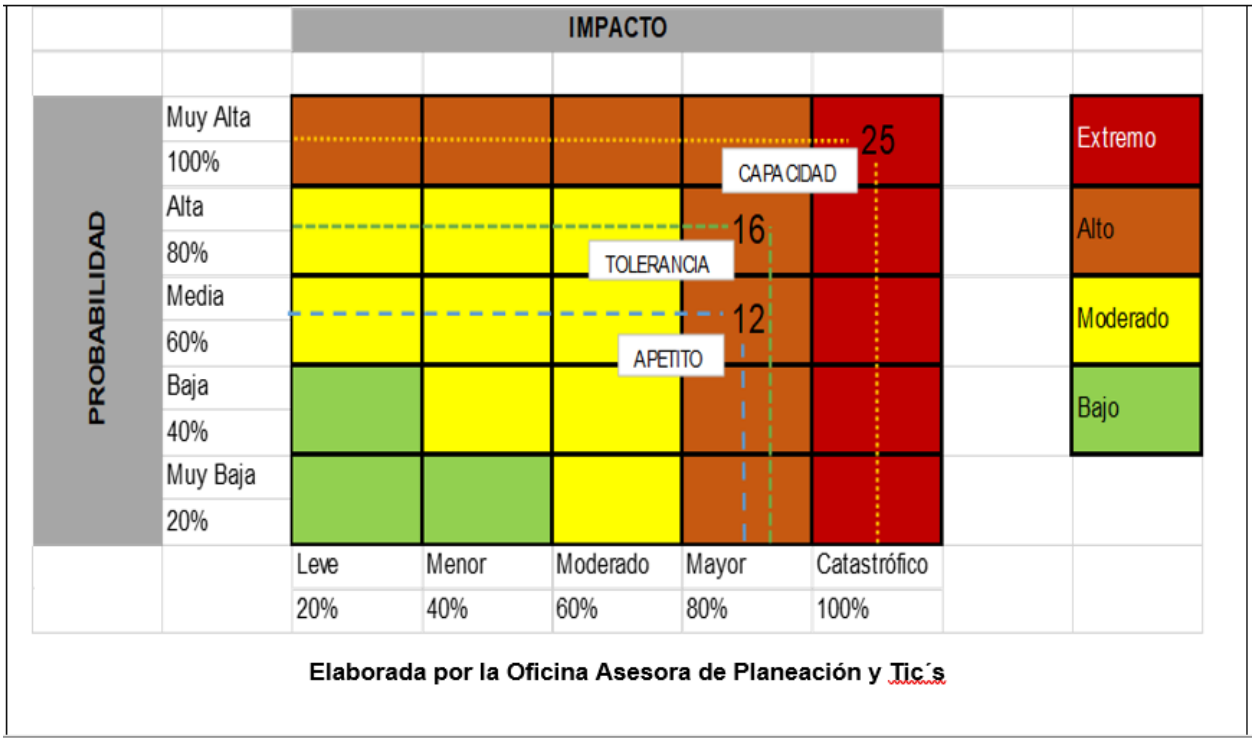
14. EVALUACIÓN DE RIESGOS

Una vez identificadas las acciones realizadas por los Especialistas de TI para mitigar el riesgo de los componentes tecnológicos de la Infraestructura TI de la Entidad, se realizó la evaluación del riesgo para cada uno de los componentes.

La evaluación de riesgos permitió comparar los resultados de la calificación del riesgo de los componentes tecnológicos, con los criterios definidos para establecer el grado de exposición de la Comisión; con esta relación de información se pudo hacer una distinción entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y así fijar las prioridades de las acciones requeridas para su tratamiento.

Para facilitar la calificación y evaluación, se elaboró el mapa de riesgos de acuerdo con la metodología propuesta del Manual de Administración de Riesgo y de Oportunidades de la CRA. El mapa facilita a la Comisión formular estrategias de mitigación para pasar los riesgos de una zona a otra, atacando ya sea la probabilidad[5] o el impacto[6].

A continuación, se presenta el mapa de riesgos adoptado que evidencia la valoración de los riesgos según su impacto y probabilidad.



Elaborada por la Oficina Asesora de Planeación y Tic´s

[5] Las categorías relacionadas con la probabilidad son Muy alta, Alta, Media, Baja, Muy baja.
[6] Las categorías relacionadas con el impacto son: Leve, Menor, moderado, Mayor y Catastrófico.

A continuación, se presenta la valoración de los riesgos según el impacto y probabilidad para cada uno de los componentes tecnológicos asociados a los servicios TI de la Comisión de Regulación de Agua Potable y Saneamiento Básico CRA.

Entendiendo la valoración como la medida en la que un cambio, problema o incidente afecta los procesos de negocio, se clasifica en los siguientes niveles:

Tabla 7. Valoración

Valoración	Descripción
Extremo	Se estima que un evento pueda ocurrir más de una vez al año en la mayoría de las circunstancias.
Alto	El evento podría ocurrir en algún momento, al menos de una vez en los últimos 2 años.
Moderado	El evento puede ocurrir en algún momento al menos de una vez en los últimos 5 años.
Bajo	El evento puede ocurrir solo en circunstancias excepcionales no se ha presentado en los últimos 5 años

Tabla 8. Evaluación según el mapa de riesgos del DAFP para la CRA

Componente	Impacto	Probabilidad	Valoración
Raisecom (ISCOM 2900/RAX700)	Mayor	Baja	**A**
FireWall–FortiGate 400E	Mayor	Media	**A**
Switch de borde Capa 3 Allied Telesis X600	Mayor	Alta	**A**
Switch Core DLink DGS-3420-52P ID 1	Mayor	Alta	**A**
Switch Dlink DGS-3420-52P ID 2	Mayor	Media	**A**
Switch DLink DGS-3420-52P ID 3	Mayor	Media	**A**
Switch DLink DGS-3420-52P ID 4	Mayor	Media	**A**
Switch DLink DGS-3420-52P ID 5	Mayor	Alta	**A**
Forti-AP	Baja	Leve	**B**
Solución Wifi-6 - FORTISWITCH M426E-FPOE	Mayor	Alta	**A**
FAZ-200F	Moderado	Media	**M**
Comunicaciones Unificadas, solución virtual 3CX	Mayor	Media	**A**
Conexión telefónica – PATTON 3086	Menor	Media	**A**
Conexión Telefónica UNE Switch S2300	Menor	Muy Baja	**A**
SAN Pure Storage FA-X10R3	Mayor	Alta	**A**
SAN HP MSA 2040	Moderado	Alta	**M**
NAS SuperMicro 826-9	Menor	Baja	**M**
Jbod Super Micro SC826 P	Menor	Baja	**M**

Componente	Impacto	Probabilidad	Valoración
Servicio Nube Publica - Azure	Mayor	Alta	**A**
ORACLE VM – ORACLE DB: Producción	Catastrófico	Media	**E**
ORACLE VM – ORACLE DB: Pruebas y calidad	Catastrófico	Media	**E**
Vcenter Server Appliance Standard	Menor	Media	**M**
VMWare: ESXi-VMWHOST1, VMWHOST2, VMWHOST3	Mayor	Media	**M**
Oracle VM Manager	Menor	Media	**M**

TABLA NO 9 EVALUACIÓN SEGÚN EL MAPA DE RIESGOS DEL DAFP PARA LA CRA

Por su parte, el RPO (Recovery Point Objective) o Punto de Recuperación Objetivo se entenderá como “la cantidad de información en términos de tiempo que la entidad está dispuesta a perder en una situación de desastre”. Adicionalmente, el RTO (Recovery Time Objective) o Tiempo de Recuperación Objetivo estará relacionado con el “tiempo que puede soportar la entidad sin el servicio. Para este caso es el tiempo que se considera en el Plan de Continuidad y Disponibilidad TIC para recuperar los servicios en un escenario de daño de los componentes tecnológicos.

A continuación, se detallará todos los dispositivos que integraran la arquitectura (ver diagrama 1, 2, 3 y 4) e infraestructura de la Entidad expondrá el análisis para cada uno de los componentes tecnológicos de comunicaciones, almacenamiento y procesamiento de la CRA en relación con los servicios.

Diagrama 1. Diseño físico de red de la Comisión.

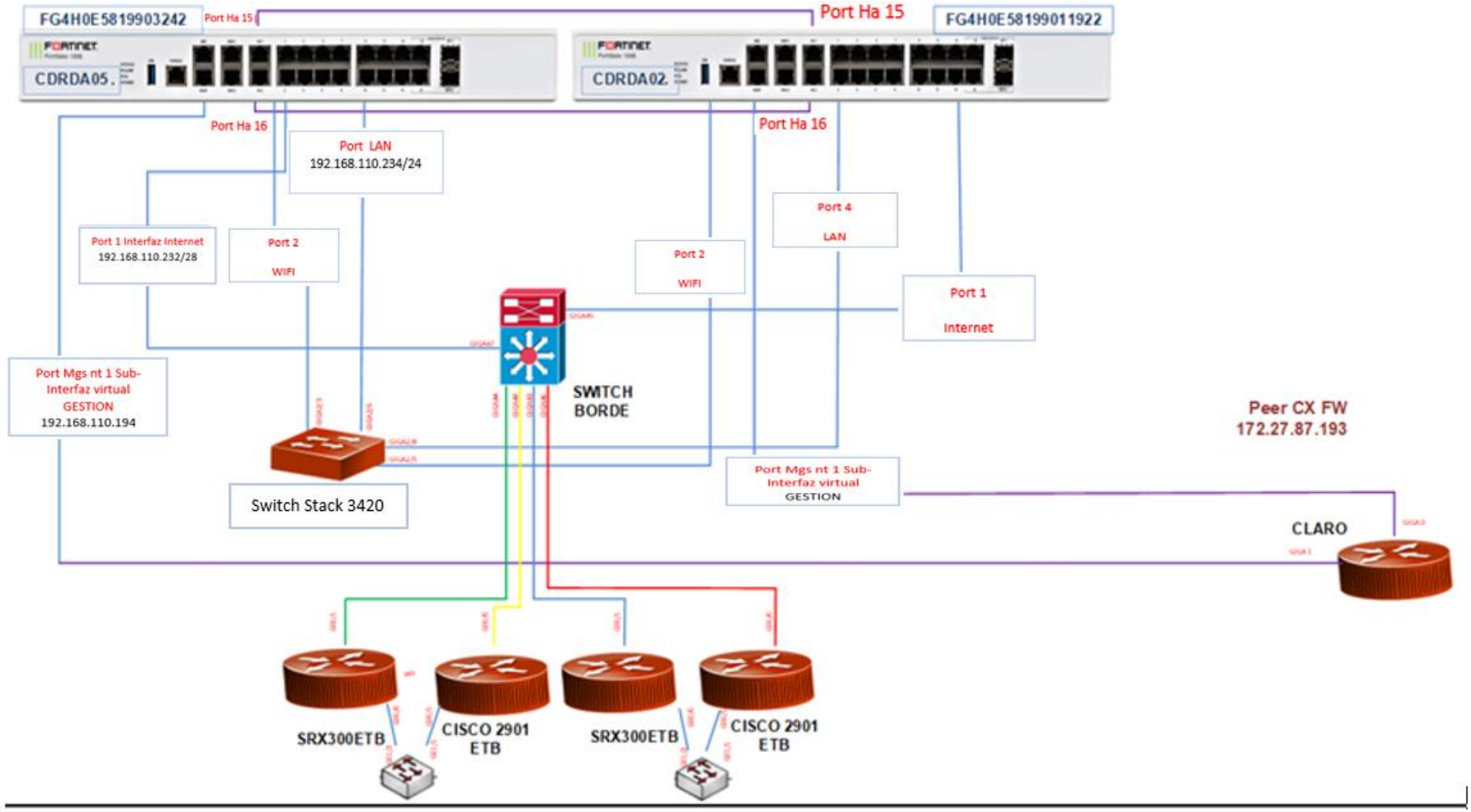


Diagrama 2. Conectividad de los componentes críticos de la entidad – (Instalaciones CRA, Cuarto Técnico, Wifi-6, Video Vigilancia).

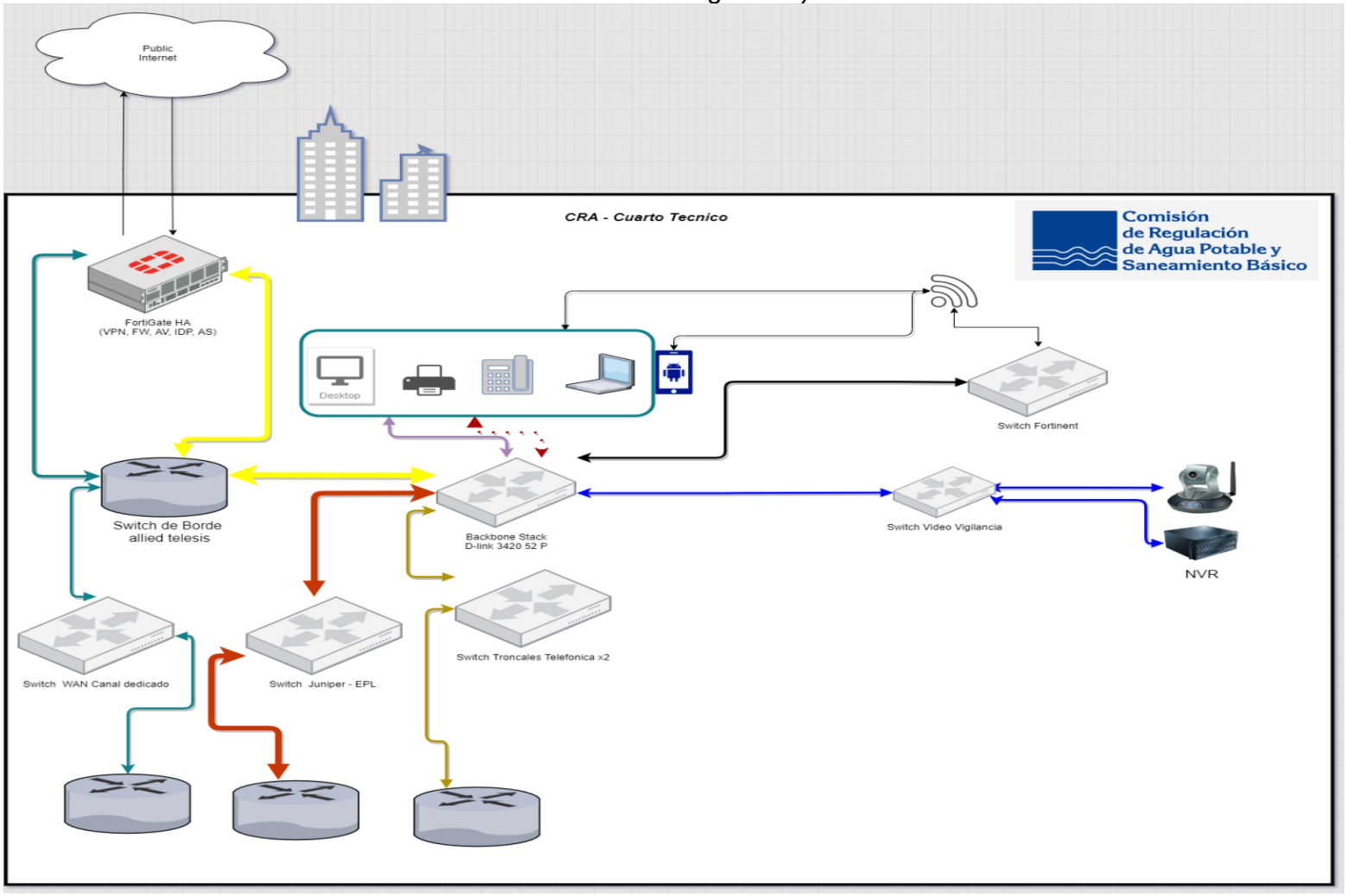
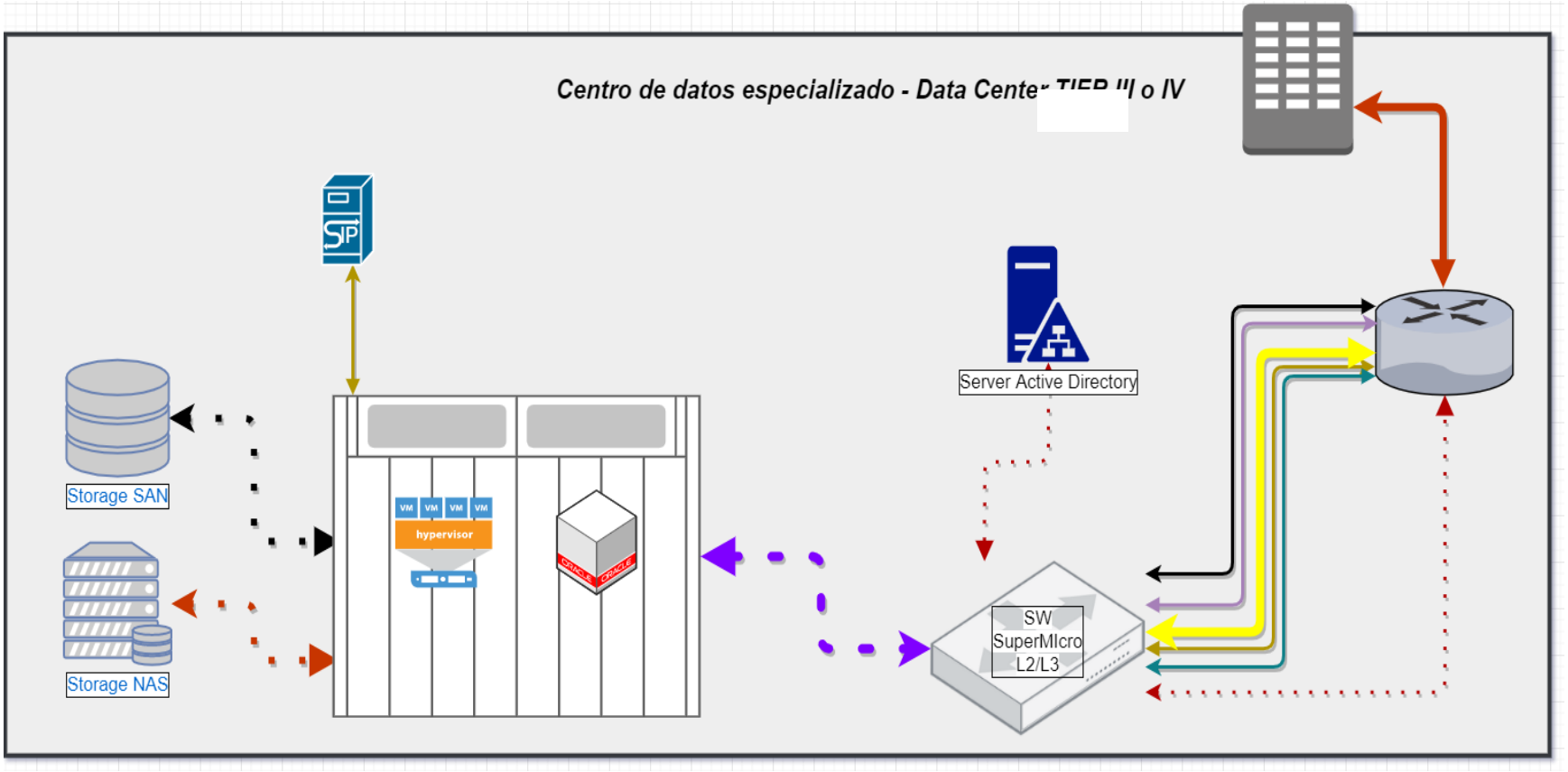
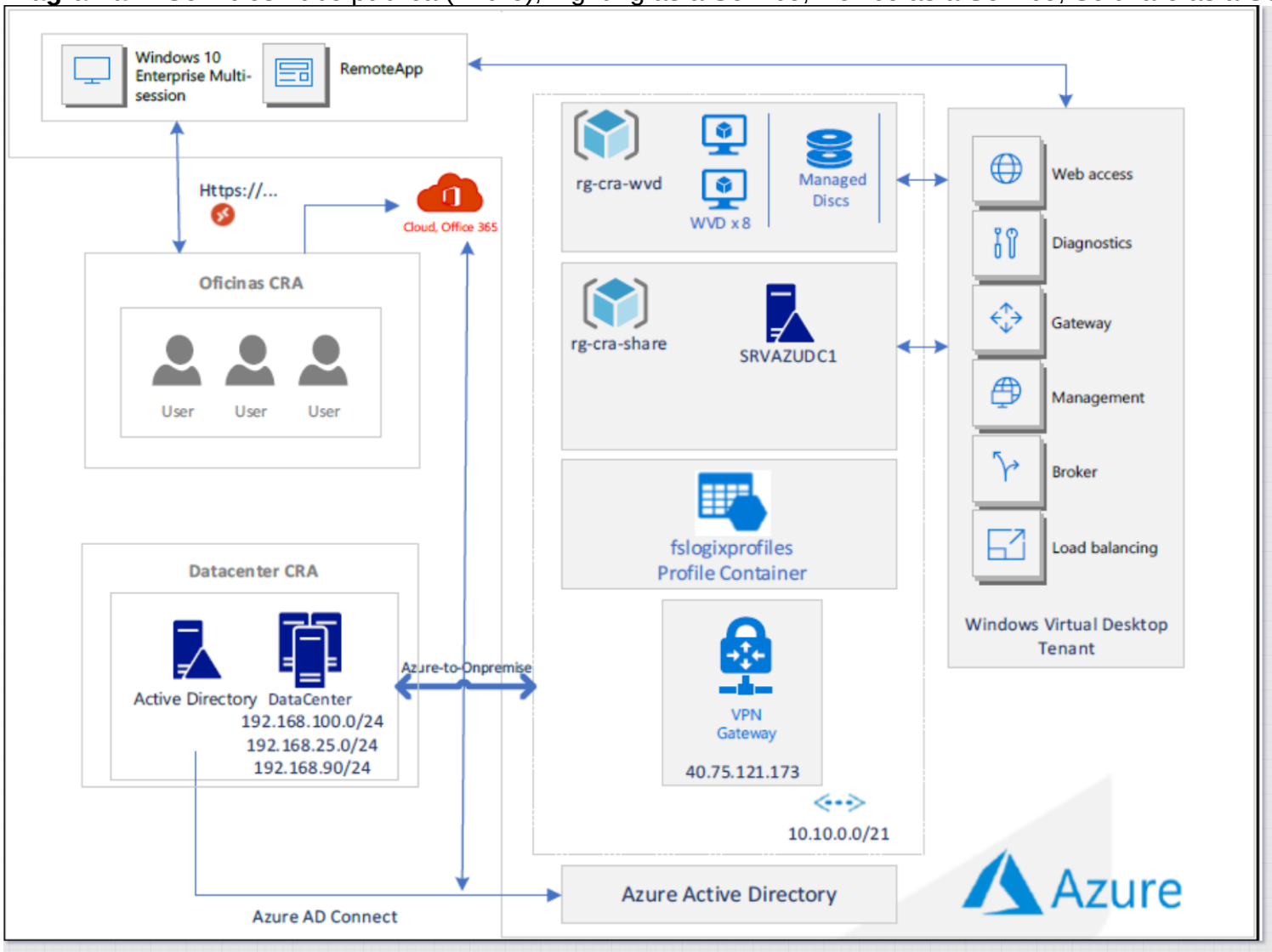


Diagrama 3. Conectividad de los componentes críticos de la entidad – DataCenter – Tier III.



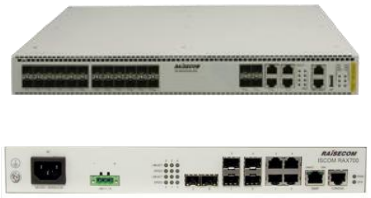
Fuente: Elaboración propia

Diagrama 4. Servicios nube publica (Azure), Lighting as a Service, Device as a Service, Software as a Service.



Fuente: Elaboración propia

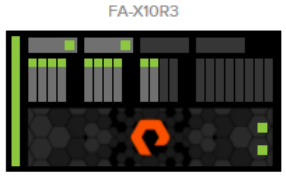
Análisis de los componentes tecnológicos de la Infraestructura TI de la CRA

Servicio						
Componente	Descripción del impacto sobre el servicio	VALORACIÓN	RPO	RTO	WRT	MTD
Raisecom (ISCOM RAX700) 	La CRA cuenta con un canal dedicado Internet redundante (Principal y Backup) al fallar el componente Rioseco (ISCOM 2900) el dispositivo Raisecom RAx 700 entra en operación conmutando de canal principal a Backup, al fallar estos dos dispositivos la CRA perdería el servicio de acceso a internet, así como los servicios asociados a este.	Alto	2h	2h	2h	4h
FireWall–FortiGate 400E 	El servicio de seguridad perimetral está soportado bajo el Firewall Fortinet - Fortigate 400E en HA, Al fallar el dispositivo, la CRA perdería el servicio de acceso a internet y a todos los servicios que dependen de este, pero al contar con la configuración en HA si falla uno de ellos el otro entra como master manteniendo el servicio en operación	Alto	2h	2h	2h	4h
Switch de borde Capa 3 Allied Telesis X600	El Swtich de borde garantiza la comunicación del canal dedicado con el Firewall, al fallar este dispositivo se presentaría perdida de los servicios hacia y desde Internet por la pérdida de comunicación entre el ISP y Firewall.	Alto	2h	2h	2h	4h
Switch Core – DLink DGS-3420-52P ID 1 	Al fallar el componente Switch ID 1 principal DLink DGS-3420-52P, se presentaría indisponibilidad en una parte de estaciones de trabajo, también se presentaría perdida en la navegación de los usuarios desde y hacia internet, el tiempo transcurrido conmuta al Switch ID 3 y restablece comunicación con el Firewall, también fallaría el canal de comunicación EPL el cual comunica con centro de datos TIER III.	Alto	1h	1h	1h	2h

Servicio						
Componente	Descripción del impacto sobre el servicio	VALORACIÓN	RPO	RTO	WRT	MTD
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 de las terminales de trabajo de usuario final.	Alto	1h	1h	1h	2h
Switch DLink DGS-3420-52P ID 3 	Al fallar el componente Switch DLink DGS-3420-52P ID 3, se presentará fallo en servicios de navegación de 25 usuarios, también se presenta perdida de gestión de los servicios de conexión a los Aires acondicionados, UPS, y respaldo en conmutación de Firewall y canal de conectividad entre puntos con el centro de datos TIER III y Troncales SIP proveedor.	Alto	1h	1h	1h	2h
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.	Alto	1h	1h	1h	2h
Switch DLink DGS-3420-52P ID 5 	Al fallar el componente Switch DLink DGS-3420-52P ID 5, se presentaría indisponibilidad de los servicios de conexión de las terminales de trabajo de usuario final.	Alto	1h	1h	1h	2h

Servicio						
Componente	Descripción del impacto sobre el servicio	VALORACIÓN	RPO	RTO	WRT	MTD
Forti-AP 	El servicio de red inalámbrica, está soportada bajo la controladora Central WiFi Manager de 431F, al fallar uno de los dispositivos los demás los respaldan, los dispositivos tienen garantía con fabrica por 3 años desde su adquisición en el 2021, también se cuenta con un AP de reserva para reemplazar por fallos, reduciendo de manera efectiva el umbral de fallo de la solución, está solución opera de manera nativa con el Firewall Fortinet por lo que los grupos de navegación, DHCP y políticas son administradas por el Firewall 400E o el que a sus veces sea reemplazado.	Bajo	2h	2h	2h	4h
Solución Wifi-6 - FORTISWITCH M426E-FPOE 	La solución de Wifi, dentro de sus componentes cuenta con un Fortiswitch M426E POE con garantía de 3 años desde su adquisición en la vigencia 2021, el dispositivo comunica la infraestructura Wireless con el Firewall 400E Fortinent por lo que los grupos de navegación, DHCP y políticas son administrados por el Firewall. Al fallar este componente se presentará falla total de la solución de wifi.	Alto	1h	1h	1h	2h
FAZ-200F 	Se cuenta con un fortianalyzer FAZ-200F con garantía de 3 años desde su adquisición en la vigencia 2021, el dispositivo cumple con el roll de compilar y analizar los datos de los equipos Fortinet. El fallo de este componente no genera afectación en los servicios.	Moderado	1h	1h	1h	2h

Servicio						
Componente	Descripción del impacto sobre el servicio	VALORACIÓN	RPO	RTO	WRT	MTD
Comunicaciones Unificadas, solución virtual 3CX 	El servidor aloja todos los servicios asociados a la planta telefónica, al interrumpirse el servicio afectaría la comunicación externa e interna de la Comisión. Así mismo, se afectaría las líneas del PBX, y las líneas de comunicación interna entre unidades.	Alto	2h	4h	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.	Alto	1h	1h	1h	2h
Conexión Telefónica UNE Switch Huawei S2300 	Al fallar el componente Huawei S2300 se perdería el servicio de conmutador virtual que gestiona las líneas telefónicas de entrada y salida de llamadas simultaneas de la CRA.	Alto	1h	1h	1h	2h

Servicio						
Componente	Descripción del impacto sobre el servicio	VALORACIÓN	RPO	RTO	WRT	MTD
Pure Storage FA-X10R3 	La SAN PURE STORAGE FA-X10R3 gestiona los almacenamientos presentados a los diferentes Hipervisores On-premise Vmware y Oracle, soportando la totalidad de servicios de la Comisión. Al presentarse un daño en este dispositivo los usuarios no podrán tener acceso a la red la Intranet, a los sistemas de información ORFEO, tramites CCU, normatividad, Trident, pagos en línea, inteligencia de negocios ORACLE y consola de administración de antivirus. 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. La herramienta cuenta monitoreo del proveedor desde su contratación, alertas tempranas, monitoreo web, móvil, cloud	Alto	2h	24h	24h	48
NAS SuperMicro 826-9 	El almacenamiento NAS SuperMicro, almacena los backups de Exchange y OneDrive de los usuarios retirados, también tiene como roll de almacenamiento de los trabajos generados por la herramienta de Backups (Exchange, SharePoint, OneDrive, Hipervisores), por otra parte, almacena la data de los sharefile antiguos antes de la migración a Sharepoint. Al presentarse un fallo en este dispositivo el funcionario administrador de la infraestructura perderá acceso a los backups de la información contenida en este repositorio.	Moderado	2h	24h	24h	12h

Servicio						
Componente	Descripción del impacto sobre el servicio	VALORACIÓN	RPO	RTO	WRT	MTD
	La NAS cuenta con arreglo de discos RAID-5 que garantiza la continuidad de servicios y reduce el umbral de fallos en la solución.					
Jbod Super Micro SC826 P 	Este dispositivo está administrado por la NAS, así mismo, este Servidor de Archivos aloja las copias de respaldo de las bases de datos de la herramienta y procedimiento de backup de la Comisión. Al presentarse un fallo en este dispositivo el funcionario administrador de la infraestructura perderá acceso a los backups de la información contenida en este repositorio. La NAS cuenta con arreglo de discos RAID-5 que garantiza la continuidad de servicios y reduce el umbral de fallos en la solución. El servidor de es un componente de almacenamiento que se comunica con la NAS a 10 GB.	Moderado	2h	24h	24h	12h

Servicio

Componente	Descripción del impacto sobre el servicio	VALORACIÓN	RPO	RTO	WRT	MTD
Servicio Nube Publica - Azure	La solución de servicios en la nube hospeda el componente de escritorio como servicio (DaaS) Zona de trabajo virtual, por otra parte, es uno de los componentes que, del plan de recuperación, los servicios críticos se replicarán activo pasivo con la herramienta de Backup. El fallo de este servicio provocará los usuarios finales no puedan acceder a la zona de trabajo virtual y se pierda acceso al sitio de recuperación. En caso de presentarse fallos en el servicio de los productos O365, como contingencia o de mitigación se deben realizar alguno de los siguientes pasos: ✓ Comprar una licencia provisional para el dominio CRA, y notificaciones. ✓ Activar las licencias de pruebas del paquete gratuito de los servicios de O365.	Alto	2h	24h	24h	48h
ORACLE VM – ORACLE DB: Producción ORACLE VM ORACLE DATABASE	**El servidor de bases de datos ORACLE (producción):** se encuentra instalado como máquina virtual sobre el servicio de virtualización Oracle VMI Este servidor gestiona las bases de datos de los sistemas de información SINFONIA (Oracle BI y Datawarehouse), ORFEO, Pymisys, los servicio de Weblogic server (Oracle ADF). Al presentarse un daño en este servidor los funcionarios y contratistas no podrán acceder al sistema misional SINFONIA, Pimisys, (generar y extraer información por medio de Oracle BI y Datawarehouse), así como efectuar trámites de pago de contribuciones especiales y emisión de	Extremo	2h	80h	24h	48h

Servicio						
Componente	Descripción del impacto sobre el servicio	VALORACIÓN	RPO	RTO	WRT	MTD
	concepto de legalidad sobre Contratos de Condiciones Uniformes (CCU) por parte de las entidades contribuyentes. Dado el esquema actual, las copias de respaldo de las bases de datos de producción sistemas mencionados se realizan de acuerdo de las horas transcurridas después de la última generación.					

Servicio						
Componente	Descripción del impacto sobre el servicio	VALORACIÓN	RPO	RTO	WRT	MTD
Vcenter Server Appliance Standard	VCenter Server es la herramienta para administración centralizada para VMware, se utiliza para administrar y gestionar máquinas virtuales, múltiples hosts ESXi dependientes desde una única ubicación centralizada	Moderado	2h	2h	2h	4h
VMWare: ESXi-VMWHOST1, VMWHOST2, VMWHOST3	Es un componente de la infraestructura de Vmware nivel inferior de la capa de virtualización, el hipervisor Los Host 1, 2 y 3, (SuperMicro MBI-618R-T2), los hosts 1 al 3 conforman el Cluster de la solución VMWare.	Moderado	2h	10h	2h	8h
Oracle VM Manager	**El servidor de bases de datos ORACLE (producción):** se encuentra instalado como máquina virtual sobre el servicio de virtualización Oracle VMI Este servidor gestiona las bases de datos de los ORFEO, sistemas de información SINFONIA (Oracle BI y Datawarehouse), Al presentarse un daño en este servidor los funcionarios y contratistas no podrán acceder al sistema de información misional si a la Base de datos de Desarrollo Pruebas y Producción Dado el	Moderado	2h	8h	4h	12h

Servicio						
Componente	Descripción del impacto sobre el servicio	VALORACIÓN	RPO	RTO	WRT	MTD
	esquema actual, las copias de respaldo de las bases de datos de producción sistemas mencionados se realizan de acuerdo de las horas transcurridas después de la última generación.					
ORACLE VM – ORACLE DB: Pruebas y calidad 	El servidor de bases de datos ORACLE (pruebas y calidad): se encuentra instalado como máquina virtual sobre el servicio de virtualización Oracle VM Al presentarse un daño es este servidor quedaría fuera de operación el servicio de Orfeo y Servicios relacionados	Extremo	2h	8h	4h	12h

TABLA NO 7 IMPACTO ANÁLISIS DE LOS COMPONENTES TECNOLÓGICOS DE LA INFRAESTRUCTURA TI DE LA CRA

Fuente: Elaboración propia componentes de la entidad

15. ANÁLISIS DE RIESGOS DE CONTINUIDAD DE LOS COMPONENTES TECNOLÓGICOS

El proceso de análisis de riesgos se determinó una vez definido en el BIA el impacto (consecuencias) y la probabilidad (posibilidad de ocurrencia de riesgo) de cada uno de los componentes tecnológicos de la infraestructura de comunicaciones, almacenamiento y procesamiento.

La definición de estos dos aspectos, permitieron orientar la clasificación del riesgo y obtener la información suficiente para establecer el nivel de riesgo y las acciones que se han implementado para mitigarlo por cada uno de los componentes tecnológicos.

En la siguiente tabla, se expondrán las acciones que han realizado los Especialistas de la Oficina de Planeación y TIC para mitigar el riesgo de fallo de los componentes tecnológicos.

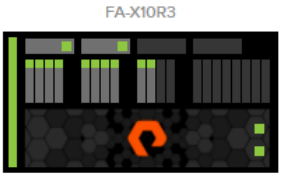
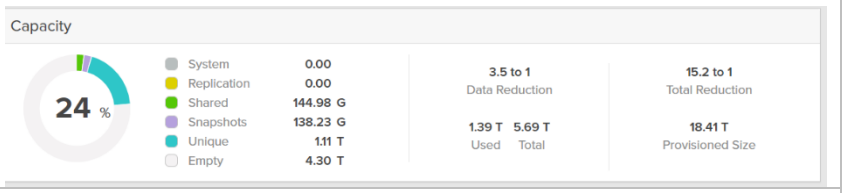
Tabla 7. Acciones realizadas por los Especialistas para mitigar el riesgo

Servicio	**Configuración de la infraestructura de comunicaciones**
Componente	Acciones realizadas por los Especialistas de TI para mitigar el riesgo
Raisecom (ISCOM RAX700)  	Para mitigar el riesgo de fallo del componente (Router Cisco ASR 900), la Comisión ha contemplado dentro de la contratación del servicio canal dedicado de internet el rango más alto dentro del acuerdo marco de precios (Oro), el cual debe garantizar el 99.8% de la disponibilidad de los servicios. Es importante tener en cuenta que el canal de internet principal y de respaldo están asociados al mismo ISP de acuerdo a los lineamientos establecidos por Colombia Compra Eficiente. En caso de fallo del canal principal el Router Back-up conmuta automáticamente, por otra parte, los demarcadores para cada router son diferentes por lo que puede tardar hasta 5 minutos en subir el servicio backup, en caso de fallo de este proceso automatizado se debe contactar al ISP para corrección dentro de los tiempos establecidos en el acuerdo marco de precios.
FireWall–FortiGate 400E 	Para dar alcance a la materialización del riesgo, se contempló contractualmente, el aprovisionamiento de un dispositivo similar el cual conforma un Cluster de Firewall garantizando la conmutación de los dispositivos en caso de fallos, conforme a los ANS establecidos.
Switch de borde Capa 3 Allied Telesis X600 	La CRA ha preparado un dispositivo de iguales o similares características, el cual entran a operar en caso de fallo. Por otra parte, se tiene contemplado adquirir stack de 6 dispositivos que permitan atención de requerimientos e

Servicio	**Configuración de la infraestructura de comunicaciones**
Componente	Acciones realizadas por los Especialistas de TI para mitigar el riesgo
	incidencias, teniendo en cuenta que el dispositivo actual no cuenta con soporte dentro del ciclo de vida del fabricante.
Switch Core – DLink DGS-3420-52P 	Para mitigar el riesgo de fallo, la entidad tiene contemplado este componente en alta disponibilidad en modalidad activo-activo. Así mismo, con el fin de minimizar riesgos asociados a la infraestructura eléctrica, se adquirió para este componente una fuente de poder externa que permita mitigar el impacto ante el daño de su única fuente de poder interna. Al materializarse el riesgo de daño del dispositivo, los profesionales de Tecnología de la Información de la Oficina de Planeación y TIC's, de la Comisión deberá proceder a la conexión física de los cables desde el teléfono a la estación de trabajo del usuario final. Por otra parte, se tiene contemplado adquirir stack de 6 dispositivos que permitan atención de requerimientos e incidencias, teniendo en cuenta que el dispositivo actual no cuenta con soporte dentro del ciclo de vida del fabricante.
Switch DLink DGS-3420-52P ID 2 	Switch ID 2: Para mitigar el riesgo de fallo, se ha configurado el Stack para que el Switch ID 1 tome el rol y gestione los servicios asociados del Switch ID 2. Al materializarse el riesgo de daño del dispositivo, los profesionales de Tecnología de la Información de la Oficina de Planeación y TIC's, de la Comisión deberá proceder a la conexión física de los cables desde el teléfono a la estación de trabajo del usuario final. Por otra parte, se tiene contemplado adquirir stack de 6 dispositivos que permitan atención de requerimientos e incidencias, teniendo en cuenta que el dispositivo actual no cuenta con soporte dentro del ciclo de vida del fabricante.
Switch DLink DGS-3420-52P ID 3 	Switch ID 3 de borde o usuario final: Para mitigar el riesgo de fallo, se ha configurado el Stack para que el Switch ID 1 y 4 tomen el rol y gestionen los servicios de conexión de las terminales de trabajo de usuario final del Switch ID 3. Al materializarse el riesgo de daño del dispositivo, los profesionales de Tecnología de la Información de la Oficina de Planeación y TIC's, de la Comisión deberá

Servicio	**Configuración de la infraestructura de comunicaciones**
Componente	Acciones realizadas por los Especialistas de TI para mitigar el riesgo
	proceder a la conexión física de los cables desde el teléfono a la estación de trabajo del usuario final. Por otra parte, el funcionario que administra la infraestructura deberá cambiar los puertos de gestión y conmutación de los servicios de EPL, Firewall y Troncales. Por otra parte, se tiene contemplado adquirir stack de 6 dispositivos que permitan atención de requerimientos e incidencias, teniendo en cuenta que el dispositivo actual no cuenta con soporte dentro del ciclo de vida del fabricante.
Switch DLink DGS-3420-52P ID 4 	Switch ID 4: Para mitigar el riesgo de fallo, se ha configurado el Stack para que el Switch ID 1 tome el rol y gestione los servicios asociados del Switch ID 4. Al materializarse el riesgo de daño del dispositivo, los profesionales de Tecnología de la Información de la Oficina de Planeación y TIC's, de la Comisión deberá proceder a la conexión física de los cables desde el teléfono al punto de datos a la estación de trabajo del usuario final. Por otra parte, se tiene contemplado adquirir stack de 6 dispositivos que permitan atención de requerimientos e incidencias, teniendo en cuenta que el dispositivo actual no cuenta con soporte dentro del ciclo de vida del fabricante.
Switch DLink DGS-3420-52P ID 5 	Switch ID 4: Para mitigar el riesgo de fallo, se ha configurado el Stack para que el Switch ID 1 tome el rol y gestione los servicios asociados del Switch ID 4. Al materializarse el riesgo de daño del dispositivo, los profesionales de Tecnología de la Información de la Oficina de Planeación y TIC's, de la Comisión deberá proceder a la conexión física de los cables desde el teléfono al punto de datos a la estación de trabajo del usuario final. Por otra parte, se tiene contemplado adquirir stack de 6 dispositivos que permitan atención de requerimientos e indecencias, teniendo en cuenta que el dispositivo actual no cuenta con soporte dentro del ciclo de vida del fabricante.
Solución Wifi-6 - Access Point FORTIAP-431F	Dentro de la solución de Wifi actual se tienen instalados 15 dispositivos y 1 de backup, la solución cuenta con garantía de 3 años desde la adquisición en 2021 y atención a requerimientos e incidentes.

Servicio	**Configuración de la infraestructura de comunicaciones**
Componente	Acciones realizadas por los Especialistas de TI para mitigar el riesgo
	La solución de Wifi se encuentra vinculada nativamente al firewall Fortinent 400E el cual se encuentra conformado por un clúster en HA por lo que adopta las políticas de navegación, perfiles y demás aspecto desde un ambiente centralizado sin generar codependencia de servidores o DHCP de las controladoras de dominio.
FAZ-200F 	Dentro de la solución de Wifi actual se tienen instalados 1 dispositivos FortiAnalyzer, la solución cuenta con garantía de 3 años desde la adquisición en 2021 y atención a requerimientos e incidentes. El FAZ-200F se encarga de recolectar y almacenar los logs de los dispositivos que conforman la solución de Wifi y Firewall al estar vinculada nativamente al firewall Fortinent 400E en caso de fallo se cuenta con un FAZ del proveedor y reportará para cambio.
Comunicaciones Unificadas, solución virtual 3CX 	El servidor virtual que hospeda la solución de comunicaciones Unificadas se encuentra respaldado por la herramienta de Backups de la entidad, garantizando restauración de data o SO en caso de fallo, la aplicación también tiene un componente de backup automático de la configuración el cual aloja en los servidores FTP configurado dentro de la infraestructura Onpremise de la Entidad.
Conexión PATTON 3086 	Actualmente ante el fallo del componente, no se cuenta con un dispositivo que soporte los servicios asociados a este componente. La Comisión ha contemplado el cambio a fibra óptica de las troncales solicitando dispositivos que garanticen alta disponibilidad de las troncales SIP.
Conexión Telefónica UNE Switch Huawei S2300 	Actualmente ante el fallo del componente, no se cuenta con un dispositivo que soporte los servicios asociados a este componente. La Comisión ha contemplado el cambio a fibra óptica de las troncales solicitando dispositivos que garanticen alta disponibilidad de las troncales SIP. .

Servicio	**Administración de los recursos de almacenamiento**
Componente	Acciones realizadas por los Especialistas de TI para mitigar el riesgo
SAN HP MSA 2040  	SAN HP MSA 2040: Para mitigar el riesgo, se configuró la SAN con redundancia en fuentes de poder y controladoras. De igual forma se definieron dos arreglos en RAID 10 para la gestión y disponibilidad de las bases de datos ORACLE y para el alojamiento de las máquinas virtuales VMWare. La solución de almacenamiento PURESTORAGE FA-X10R3 cuenta con herramienta Hardware Health encargada del monitore y reporte, preventivo, predictivo en la web, móvil y cloud. También cuenta con Snapshot de volúmenes y grupos de trabajo programados diariamente permitiendo la recuperación de volúmenes específicos en los cluster de hipervisores Vmware y Oracle, adicionalmente cuenta con arreglo de discos NVMe, Analityca, proyección de capacidades y replicación, la solución cuenta con garantía de 3 años desde su contratación en 2020 y permite actualización y ampliación con algoritmos de reducción de hasta 15.2 a 1. 
SAN HP MSA 2040 	SAN HP MSA 2040: Para mitigar el riesgo, se ha migrado el 90% la información a PureStorage FA-X10R3, al finalizar la actividad de migración se procederá procede con el apagado y RAEES del dispositivo, teniendo en cuenta que no cuenta con soporte en ciclo de vida del fabricante o soporte con partner.
NAS SuperMicro 826-9  	Para mitigar el riesgo de daño del dispositivo, se configuró la NAS con redundancia en las fuentes de poder, se definieron dos RAID 5 para la gestión y disponibilidad de las carpetas compartidas y para el espacio asignado como repositorio de back-up. Respecto a un eventual daño por sistema operativo, se cuenta con un disco duro copia del Sistema Operativo almacena las últimas configuraciones de las funcionalidades del sistema operativo de la NAS. Imagen que permitiría subir el sistema operativo con sus respectivas configuraciones, publicar las carpetas de red y minimizar los tiempos de recuperación.

Servicio	**Administración de los recursos de almacenamiento**
Componente	Acciones realizadas por los Especialistas de TI para mitigar el riesgo
Jbod Super Micro SC826 P 	El almacenamiento SuperMicro JBOD, se encuentra conectado por ISCI a la NAS en puertos de 10GB, está configurada con arreglos de discos RAID-5, al ser dependiente del SO de la NAS, se garantiza su funcionamiento con el respaldo del mismo en SSD, replica del SO.

Servicio	**Administración de Hipervisores**
Componente	Acciones realizadas por los Especialistas de TI para mitigar el riesgo

Servicio	**Administración de recursos de virtualización**
Componente	Acciones realizadas por los Especialistas de TI para mitigar el riesgo
VMWare: ESXi-VMWHOST1,2 y 3 	Para mitigar el riesgo, la solución de VMWare está configurada bajo un esquema de Cluster con las tres primeras cuchillas del Enclosure (SuperMicro MBI-618R-T2) con la misma arquitectura de hardware y software; garantizando alta disponibilidad de las máquinas virtuales a la hora de materializarse el riesgo por falla de una de las tres cuchillas.
VMWARE vmware vSphere	Para mitigar el riesgo, se tiene contemplado soporte directo con partner del fabricante una vez creado el caso desde alguno de sus canales de servicio, cuentan con ANS específicos para brindar la asistencia remota e iniciar actividades que permitan reactivar el servicio.
VMWare: OVM-VMWHOST4,5 y 6 	Para mitigar el riesgo, la solución de OVM está configurada bajo un esquema de Cluster con los tres hosts del Enclosure (SuperMicro MBI-618R-T2) con la misma arquitectura de hardware y software; garantizando alta disponibilidad de las máquinas virtuales a la hora de materializarse el riesgo por falla de una de las tres cuchillas.
OVM, ORACLE VIRTUAL MANAGER ORACLE VM	Para mitigar el riesgo, se tiene contemplado soporte directo con partnert del fabricante una vez creado el caso desde alguno de sus canales de servicio, cuentan con ANS específicos para brindar la asistencia remota e iniciar actividades que permitan reactivar el servicio.

TABLA NO 8 ACCIONES REALIZADAS POR LOS ESPECIALISTAS PARA MITIGAR EL RIESGO
Fuente: Elaboración propia a partir de la guía técnica de computación en la nube.

16. Requisitos y brechas para la continuidad del negocio de TIC

De acuerdo con los anteriores análisis, a continuación, se define unas necesidades de recursos a modo de requerimientos para la continuidad de los componentes tecnológicos de la Entidad para contemplar en el Plan Estratégico de Tecnologías de la Información según disponibilidad presupuestal.

Esto es el resultado del Análisis del Impacto del Negocio BIA y del análisis y evaluación del riesgo.

Componente tecnológico	Necesidad de recursos
Switch Core – DLink DGS-3420-52P ID 1, 2, 3, 4, 5	Contemplar la asignación presupuestal con el fin de realizar la adquisición de Stack de 6 Switches con ciclo de vida no menor a 5 años.
Switch DLink DGS-3420-52P ID 5	
Conexión telefónica –UNE	Plantear migración a troncales de fibra, que garanticen la prestación de servicio con dispositivos en alta disponibilidad, también se encuentra en proceso de análisis la implementación de una troncal SIP como servicio este cambio implicaría cambio de números se debe validar el impacto. Validar los tiempos, ANS y alcances con el contrato del proveedor, para identificar las responsabilidades tanto del proveedor como de la CRA una vez se ha materializado el riesgo.
NAS SuperMicro 826-9 - Jbod	Mantener la herramienta que garantice la generación de imágenes del disco donde se encuentra instalado el Windows Server Storage 2016 Standard, así mismo, contar con un contrato de soporte para la gestión de la NAS y JBOD o paquete de horas con especialista del partner que apoye la labor de recuperación. Finalizar proceso de depuración de información duplicada con cada una de las dependencias que permita liberar espacio en la NAS y JBOD de acuerdo con la información migrada a SharePoint. 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

Componente tecnológico	Necesidad de recursos
	los componentes tecnológicos y servicios de almacenamiento. Definir el procedimiento para la recuperación de los datos a partir de las últimas copias de seguridad generadas por los sistemas de información misionales y de apoyo, conforme a los esquemas previamente establecidos y definidos en la política de respaldo. Este procedimiento deberá contemplar la fuente, el destino, responsable y la periodicidad de ejecución.
ORACLE VM – ORACLE DB: Producción	Dar continuidad al servicio de la solución o herramienta de back-up, para mitigar el riesgo.
ORACLE VM – ORACLE DB: Pruebas y calidad	Dar continuidad al servicio de la solución o herramienta de back-up, para mitigar el riesgo.
Vsphere	Mantener 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.
ROUTER´s CISCO ASR 920	Dado que el canal de internet principal y Back-up son gestionados por el mismo ISP, se debe validar que las últimas millas vienen por fibras diferentes, garantizando la independencia al momento de realizar la conmutación de los servicios en caso de fallos.
Raisecom (ISCOM RAX700)	Realizar el estudio y viabilidad técnica para la contratación del canal Backup Plata con un ISP diferente al principal o garantizar que el proveedor actual viene por nodos y troncales diferentes, de no ser así el servicio de internet estaría sin respaldo.
Solución Wifi-6 **- Access Point FORTIAP-431F** **- FORTISWITCH M426E-FPOE** **-FAZ-200F**	Realizar estudios técnicos y viabilidad económica para adquirir FortiSwtich que permita alta disponibilidad en los servicios de conectividad, renovar garantía una vez se culminen los 3 años vigentes 2024.
• **Conexión telefónica – PATTON 3086** • **Comunicaciones unificadas, solución virtual 3CX** • **Conexión Telefónica UNE Switch Huawei S2300**	Realizar viabilidad técnica y económica para migrar las troncales SIP análogas a digitales, revisar viabilidad técnica para migrar a troncal SIP como servicio integrando servicios que permita integración con servicios de la suite de trabajo colaborativo Teams.

TABLA NO 10 REQUISITOS Y BRECHAS PARA LA CONTINUIDAD DEL NEGOCIO DE TIC

Fuente: Elaboración propia a partir de la guía técnica de computación en la nube

17. Políticas para la implementación del Plan de Continuidad y Disponibilidad de las Tecnologías de la Información PCD-TI

A continuación, se proponen algunas orientaciones generales a modo de política que posibilitaran la implementación del **PCD-TI** en la CRA.

- La Oficina Asesora de Planeación y TIC de la Comisión de Regulación de Agua Potable y Saneamiento Básico será la responsable de liderar el Plan de Continuidad y Disponibilidad TIC, definiendo las acciones a llevarse a cabo en caso de un evento que ponga en riesgo los componentes tecnológicos y en consecuencia la continuidad de los servicios de TI de la entidad. También será la encargada de hacer seguimiento a dichas actividades y velar por su cumplimiento.

- La Oficina Asesora de Planeación y TIC de la CRA deberá desarrollar planes de contingencia para cada uno de los componentes y servicios de TI que se encuentren en zonas de riesgos ALTA o EXTREMA, según el mapa y la evaluación de riesgos definidas en el PCD-TIC.

- Los planes de contingencia deberán contener procedimientos para su ejecución. Estos deberían ser revisados, actualizados y aprobados periódicamente, según sea necesario, por parte del CIO de la CRA. Así mismo, estos planes podrán asignar responsabilidades a funcionarios específicos, a fin de posibilitar la recuperación o continuidad del funcionamiento de los componentes y servicios de TI y deberán asegurar los recursos necesarios para facilitar su ejecución.

- Es necesario velar por que el personal encargado de componentes y servicios de TI con mayores riesgos e impacto se encuentre debidamente capacitados para responder a las contingencias.

18. Estrategia para la preparación de las TIC para la continuidad del negocio

Categoría	Estrategia
Gobierno de TI	Definir un equipo o rol dentro del los profesionales de Tecnología de la Información de la Oficina de Planeación y TIC's, de la entidad, encargado de la implementación efectiva del PCD-TIC a fin de apoyar la preparación de las TIC para la continuidad del negocio.

Categoría	Estrategia
	Este equipo o rol debe incluir la participación de las áreas de dirección, de los profesionales de Tecnología de la Información de la Oficina de Planeación y TIC's,, líderes de procesos y proveedores externos.
Habilidades y conocimiento	Diseñar un programa de capacitación orientado especialmente a cubrir los componentes de TI asociados a los servicios críticos de la entidad. Esto con el objetivo de fortalecer las habilidades y conocimiento de los especialistas que gestionan los componentes tecnológicos.
Tecnología	Mantener actualizada la categorización de los servicios tecnológicos, definiendo el nivel de impacto sobre los procesos de la entidad y el plan de contingencia. En la definición, se deberá determinar el Punto de Recuperación Objetivo (RPO), el Tiempo de Recuperación Objetivo del servicio (RTO), Tiempo de recuperación del trabajo (WRT) y el Tiempo de inactividad máximo tolerable (MTD), de los componentes tecnológicos o servicio TI. Implementar planes de contingencia de los componentes y servicios tecnológicos, permitiendo garantizar la restauración ante un evento que ocasione la interrupción total o parcial de los mismos por un tiempo mayor a los tiempos de recuperación definidos.
Datos	Implementar y hacer seguimiento a la seguridad de la Información de la Entidad, permitiendo la identificación de vulnerabilidades y amenazas que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información gestionada y generada por los sistemas de información internos y externos. Definir sitio alterno para soportar escenarios de recuperación de los sistemas de almacenamiento (NAS, SAN) de la entidad.
Procesos	Definir y poner en marcha los procesos de incidentes y requerimientos para la gestión de la mesa de servicios de la entidad.
Proveedores	Evaluar la gestión de los proveedores de componentes y servicios tecnológicos de acuerdo con la prestación, implementación, garantía, cumplimiento de los ANS de los mismos, conforme a lo establecido contractualmente.

TABLA NO 11 ESTRATEGIA PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO.

Fuente: Elaboración propia

19. Organización de roles y responsabilidades para la implementación del Plan de Continuidad y Disponibilidad de las Tecnologías de la Información y las Comunicaciones (PCD-TIC)

Dado que la entidad en la actualidad cuenta con un esquema de gobierno de TI, se propone para la ejecución del PCD-TIC, abordar los incidentes o temas relacionados en las reuniones periódicas de seguimiento de TI de la Oficina Asesora de Planeación y TIC. De igual forma se sugiere mantener el rol de Coordinador del PCD-TIC y de los profesionales que realicen la gestión del mismo.

- **Coordinador del Plan de Continuidad y Disponibilidad de las TIC**

  El coordinador del PCD-TIC de la CRA, actuará como canal de comunicación para la gestión del Plan y los profesionales de seguimiento de TI de la Oficina Asesora de Planeación y TIC. A través de este rol se transmitirán las decisiones acordadas en torno a las acciones, los niveles de ejecución y el estado de los componentes tecnológicos que cubre el Plan.

  El coordinador será el Oficial de Seguridad de la entidad, y en su ausencia, su delegado, será el CIO. Las actividades por realizar son las siguientes:

  - Proponer políticas y acciones para la mejora del Plan de Continuidad y Disponibilidad de las Tecnologías de la Información y las Comunicaciones.
  - Autorizar la ejecución del Plan de Continuidad y Disponibilidad de las TIC.
  - Monitorear y hacer seguimiento al cumplimiento y mantenimiento del Plan.

- **Los profesionales de trabajo para la gestión del PCD-TIC**

  Los profesionales de trabajo estarán organizados según los roles del grupo TI de la Oficina Asesora de Planeación y TIC, responsables de la ejecución de las acciones definidas dentro del mismo.

  Integrantes
  - CIO
  - Profesionales especializados
  - Analista de sistemas
  - Personal de apoyo contratado en la vigencia.

  Los profesionales de trabajo para la gestión tendrán como responsabilidades:

  - Ejecutar cada una de las acciones planeadas relacionadas con el Plan.
  - Documentar y formalizar el PCD-TIC.
  - Diseñar planes de capacitación para los funcionarios de la CRA, para que participen en la definición del PCD-TIC.

- Preparar y realizar pruebas del PCD-TIC antes y después de una contingencia.
- Programar el plan de pruebas y simulacros, de acuerdo a los planes de recuperación ante desastres y contingencias establecidos para el centro de datos y cada uno de los componentes tecnológicos de la entidad.
- Mantener actualizado el Plan de Continuidad y Disponibilidad de las TIC.
- Gestionar recursos para la ejecución del Plan de Continuidad y Disponibilidad de las TIC.

20. Plan de Continuidad y Disponibilidad de las TIC y procedimientos de apoyo

Como parte de la ejecución, se realizó una identificación de los eventos que activarían una contingencia en la Oficina Asesora de Planeación y TIC de la entidad, con el objetivo de establecer los mecanismos de mitigación de riesgos de los servicios TI clasificados de alto impacto.

Eventos	Alertas
Alarma del centro de datos de la entidad	• Alerta generada por la Herramienta de Monitoreo o personal de apoyo de infraestructura. • Alerta del Sistema de Energía Ininterrumpida UPS (modo Bypass) a la caída del fluido eléctrico del sector. • Alerta del Sistema de aire acondicionado de precisión. • Alertas generadas por el profesional de Tecnología de la Información de la Oficina de Planeación y TIC's, que hace el monitoreo del Centro de datos.
Alarma de los servidores	• Alerta LED de los componentes asociados al servidor (discos duros, fuente de poder, chasis). • Alerta en la consola de administración de Hipervisores (VmWare, OracleVm). • Alerta o mensajes de servicios en la nube publica - Azure (IaaS, DaaS, PaaS).
Alarma de las unidades de almacenamiento	• Alerta en la consola de administración de la NAS y la SAN.
Alarma de los dispositivos de comunicaciones	• Alerta LED de los componentes asociados a los dispositivos de comunicaciones. • Alerta en la consola de administración.

Eventos	Alertas
	• Alerta Herramienta de monitoreo o entornos de monitoreo de los dispositivos.
Reporte de falla de los sistemas de información misionales (SINFONIA, CCU, pagos en línea de contribuciones especiales, Chat de participación ciudadana), de apoyo (Intranet, correo institucional, ORFEO, GLPI, Trident, Pimisys, portal web) y externos (SIIF, SECOP I II, SIGEP).	• Falta de accesibilidad. • Caducidad de contraseña de usuario de dominio. • Lentitud en el procesamiento de datos. • Perdida de información. • Latencia en la red. • Errores de codificación. • Errores de integración e interoperabilidad de sistemas. • Uso incorrecto o no aplicación de la metodología de desarrollo de software de la entidad.
Reporte de falla de los servicios de comunicaciones.	• Falta de acceso. • Lentitud en el procesamiento de datos. • Perdida de gestión. • Latencia en la red. • Errores de ejecución.
Alerta por el incumplimiento contractual por parte de los contratistas que apoyan los servicios tecnológicos	
Alerta por la demora en los procesos de contratación de acuerdo a lo especificado y aprobado en el PAA	• Análisis del mercado de la solución a contratar. Definición del alcance de la solución y justificación de la necesidad en la elaboración de los estudios previos.
Alarma por la no ejecución exitosa en la generación de las copias de seguridad.	• Alerta generada por la consola de administración de la solución de Backup aprobada por la Entidad. • Tarea de Revisión diaria de la plataforma tecnológica.
Reporte de pérdida de conexión a los sistemas de bases de datos.	• Tarea de Revisión diaria de la plataforma tecnológica.
Reporte por la no notificación del sistema de mensajería ante la radicación de un trámite del sistema de apoyo ORFEO.	• Profesional, Oficina Asesora de Planeación TI
Mensajes de error y/o indisponibilidad durante la ejecución del correo institucional, sistemas de información o software especializado.	• Profesional, Oficina Asesora de Planeación TI.

Eventos	Alertas
Fallas de conectividad en los equipos de cómputo asignado a los funcionarios y contratistas de la entidad.	• Profesional, Oficina Asesora de Planeación TI.
Falla general en los equipos de cómputo asignado a los funcionarios y contratistas de la entidad.	• Profesional, Oficina Asesora de Planeación TI.
Fallo en el servicio de telefonía “comunicaciones unificadas” de la entidad.	• Profesional, Oficina Asesora de Planeación TI.
Alarma de ataques y virus informático.	• Alerta en la consola de administración del Firewall.
Alerta por el uso incorrecto de los recursos computacionales y de los sistemas de información misionales, de apoyo y externos por parte de los funcionarios y contratistas de la entidad.	• Falta de uso y aprovechamiento de los sistemas misionales. • Reporte fallo por los usuarios funcionales que consumen el servicio.
Alerta por indisponibilidad en los servicios utilizados para trabajo colaborativo (Sharepoint, OneDrive).	• Profesional, Oficina Asesora de Planeación TI.

TABLA NO 12 PLAN DE CONTINUIDAD Y DISPONIBILIDAD DE LAS TIC Y PROCEDIMIENTOS DE APOYO
Fuente: Elaboración propia

7.2 PROCEDIMIENTO PARA LA RECUPERACIÓN DEL CENTRO DE DATOS INHOUSE O EXTERNO

Al presentarse una falla en el centro de datos por un incidente catalogado como no controlable, el procedimiento a seguir es el siguiente:

- Consultar la lista de contactos los profesionales de Tecnología de la Información de la Oficina de Planeación y TIC’s de trabajo del PCD-TIC y la lista de proveedores de los componentes y servicios tecnológicos que hacen parte del centro de datos.
- Notificar al Coordinador del Plan y proveedores de los componentes y servicios tecnológicos.
- Notificar la no disponibilidad de los servicios a los usuarios, empleando los medios establecidos y disponibles.
- Diagnosticar físicamente dentro del centro de datos y a nivel lógico, el estado de los siguientes componentes tecnológicos:
    a. UPS, aires acondicionados, sistema de circuito cerrado de televisión (CCTV).
    b. Enlaces de comunicación y equipos de última Milla (Router. Transceiver).
    c. Equipo de seguridad perimetral (Firewall).
    d. Equipos de red (Stack de Switch).

e. Granja de servidores y soluciones de virtualización (VmWare, OracleVm, Hyper-V y físicos)
f. Unidades de almacenamiento NAS y SAN (Base de datos, máquinas virtuales y servidor de archivos).
g. Servicio de Comunicaciones Unificadas.

- Evaluar el nivel de daños de los componentes relacionados con el centro de datos.
- Ejecutar los escenarios de contingencia de acuerdo con el Plan de Recuperación ante Desastres.

Como parte de la evaluación de los daños relacionados con los componentes tecnológicos asociados al centro de datos, el o los especialistas responsables de la operación, deberán seguir los siguientes procedimientos para el restablecimiento de los mismos:

7.3 PROCEDIMIENTO DE RECUPERACIÓN DEL CANAL DE INTERNET

La Comisión ha contemplado dentro de la contratación un servicio de un canal dedicado de internet el rango más alto dentro del acuerdo marco de precios (Oro), el cual debe garantizar el 99.8% de la disponibilidad de los servicios.

Es importante tener en cuenta que el canal de internet principal y de respaldo están asociados al mismo ISP de acuerdo con los lineamientos establecidos por Colombia Compra Eficiente.

En caso de fallo del canal principal el Router Back-up conmuta automáticamente, por otra parte, los demarcadores para cada router son diferentes por lo que puede tardar hasta 5 minutos en subir el servicio backup, en caso de fallo de este proceso automatizado se debe contactar al ISP para corrección dentro de los tiempos establecidos en el acuerdo marco de precios.

- NIVEL 1
  Contactar telefónicamente o por medio del portal al centro de servicio del proveedor ISP y crear ticket donde se reporte la falla presentada sobre el canal de internet. Dado el impacto del componente sobre el catálogo de servicios, se debe especificar en la solicitud de reporte, que el caso se clasifique con la prioridad más alta.
  Conforme a los ANS, se debe hacer seguimiento a los cumplimientos de los tiempos de recuperación y escalamiento establecidos contractualmente con el proveedor

- NIVEL 2
  En este nivel, el proveedor, asigna a un especialista para realizar un primer acercamiento y profundizar sobre la falla presentada. Dependiendo de la falla reportada, se coordinará con el especialista de la entidad los tiempos de desplazamiento y acompañamiento del soporte en sitio, así como los trámites de acceso a las instalaciones. Dado el caso, solicitará apoyo el profesional de

Tecnología de la Información de la Oficina de Planeación y TIC's de tecnología para realizar acciones remotas.

En caso de que el proveedor ISP recupere el servicio del canal principal dentro de los ANS esperados, se inicia el proceso de seguimiento y monitoreo del comportamiento del servicio. Una vez se confirme la estabilidad del mismo, se procede a la autorización del cierre del ticket.

Si el componente no se restaura luego del soporte realizado por el especialista del proveedor, se procederá a realizar un escalamiento nivel 3.

- NIVEL 3

  En este nivel, el especialista genera informe detallando las fallas presentadas en el canal de internet y en los elementos que integran la solución (router, transceiver, corte de fibra óptica, etc).

  Para el caso de daño de los **elementos** que integran la solución, el proveedor deberá entregarlos instalados y operando de acuerdo con los ANS establecidos contractualmente.

  Si el servicio del canal principal no se recupera en los ANS esperados, se procederá a poner en operación el canal de respaldo como escenario de recuperación del canal de internet. El proveedor ISP deberá informar el tiempo estimado de entrega e instalación conforme a lo establecido contractualmente.

  Sin embargo, dado que el servicio de internet afecta servicios críticos para la operación, el CIO comunicará al interior de la Entidad, sobre el estado de la emergencia y pondrá en marcha el escenario de recuperación configurado previamente, de acuerdo al plan de contingencia establecido.

Una vez activado el escenario de recuperación, se deberá:

Acciones	Responsable	Tiempo
Realizar pruebas de acceso a los servicios asociados al canal de internet y a los medios de comunicación (página web, correo electrónico, SECOP, etc.) de la entidad.	Profesional especializado del proveedor del Firewall (ISP), y Profesionales apoyo de TIC	Durante la operación de la contingencia.
Monitorear y validar los servicios de conectividad asociados al canal de internet	Profesional, Oficina Asesora de Planeación TIC	4 horas.

Acciones	Responsable	Tiempo
Hacer seguimiento a los tiempos acordados con el ISP para la entrega e instalación de los elementos y recuperación del canal principal.	• Profesional, Oficina Asesora de Planeación TIC	De acuerdo con los ANS establecidos.
Realizar un diagnóstico del funcionamiento y desempeño del servicio de internet y los servicios que dependen del mismo.	• Profesional, Oficina Asesora de Planeación TIC	24 horas.
Solicitar el (informe del proveedor) sobre el origen del incidente y documentar el caso en GLPI, con el objetivo de mejorar el escenario de recuperación o contingencia. Nota: Formatos de calidad.	Profesional especializado del proveedor ISP y • Profesional, Oficina Asesora de Planeación TIC	24 horas.

TABLA NO 13 ACCIONES

7.4 PROCEDIMIENTO PARA LA RECUPERACIÓN DEL RAISECOM (ISCOM 2900/RAX700).

Conforme a los ANS y niveles de escalamiento establecidos contractualmente con el proveedor, el procedimiento se activa con la creación del ticket.

- NIVEL 1
  Contactar telefónicamente o por medio del portal al centro de servicio del proveedor ISP y crear ticket donde se reporte la falla presentada sobre los componentes Router Cisco ASR 920 y Raisecom (ISCOM 2900/RAX700) que permiten la conectividad desde la red local de la Entidad hacia los servicios de internet. Dado el impacto del componente sobre el catálogo de servicios, se debe especificar en la solicitud de reporte, que el caso se clasifique con la prioridad más alta.
  Conforme a los ANS, se debe hacer seguimiento a los cumplimientos de los tiempos de recuperación y escalamiento establecidos contractualmente con el proveedor.

- NIVEL 2
  En este nivel, el proveedor, asigna a un especialista para realizar un primer acercamiento y profundizar sobre la falla presentada. Dependiendo de la falla reportada, se coordinará con el especialista de la entidad los tiempos de

desplazamiento y acompañamiento del soporte en sitio, así como los trámites de acceso a las instalaciones. Dado el caso, solicitará apoyo al profesional de Tecnología de la Información de la Oficina de Planeación y TIC's de tecnología para realizar acciones remotas.

En caso de que el proveedor ISP habilite o aprovisione los componentes Router Se quita referencia Router Cisco y

Raisecom (ISCOM RAX700) dentro de los ANS esperados, se inicia el proceso de seguimiento y monitoreo del comportamiento del servicio. Una vez se confirme la estabilidad del mismo, se procede a la autorización del cierre del ticket.

Si los componentes no se restauran luego del soporte realizado por el especialista del proveedor ISP, se procederá a realizar un escalamiento nivel 3.

- NIVEL 3

  En este nivel, el especialista del proveedor ISP genera un informe detallando las fallas presentadas en los componentes Router Cisco Asr 920 y Raisecom (ISCOM 2900/RAX700).
  Para el caso de daño de los **componentes**, el proveedor deberá entregarlos instalados y operando de acuerdo con los ANS establecidos contractualmente.

  Si los componentes no se recuperan en los ANS esperados, se procederá a poner en operación el canal de respaldo como escenario de recuperación del canal de internet. El proveedor ISP deberá informar el tiempo estimado de entrega e instalación conforme a lo establecido contractualmente.

  .

  Sin embargo, dado que el fallo de los componentes, afectan directamente el servicio de internet y el acceso a los servicios críticos para la operación, el CIO comunicará al interior de la Entidad, sobre el estado de la emergencia y pondrá en marcha el escenario de recuperación configurado previamente, de acuerdo con el plan de contingencia establecido.

  Una vez activado el escenario de recuperación, se deberá:

Acciones	Responsable	Tiempo
Realizar pruebas de acceso a los servicios asociados al Router de respaldo.	Profesional especializado del proveedor ISP (Firewall) y Profesional, Oficina Asesora de Planeación TIC.	30 minutos.

Acciones	Responsable	Tiempo
Realizar pruebas de acceso a los servicios asociados al canal de internet y a los medios de comunicación (página web, correo electrónico, SECOP, etc.) de la entidad.	Profesional especializado del proveedore del Firewall profesional especializado del proveedor ISP (Firewall) y Profesional, Oficina Asesora de Planeación TIC	Durante la operación de la contingencia.
Monitorear y validar los servicios de conectividad asociados al canal de internet.	Profesional, Oficina Asesora de Planeación TIC	4 horas.
Hacer seguimiento a los tiempos acordados con el proveedor ISP para la entrega e instalación de los elementos y recuperación del canal principal.	Profesional, Oficina Asesora de Planeación TIC	De acuerdo a los ANS establecidos.
Instalar, configurar y validar en el cuarto técnico, el funcionamiento de el o los componentes Router CISCO Juniper ASR920 y Raisecom (ISCOM 2900/RAX700).	Profesional especializado del proveedor ISP (Firewall) y Profesional, Oficina Asesora de Planeación TIC	30 minutos.
Realizar un diagnóstico del funcionamiento, desempeño del servicio de internet y de los servicios que dependen del mismo.	Profesional, Oficina Asesora de Planeación TIC	24 horas.
Solicitar el minutograma (informe del proveedor) sobre el origen del incidente y documentar el caso en GLPI, con el objetivo de mejorar el escenario de recuperación o contingencia. Nota: Formatos de calidad.	Profesional especializado del proveedor ISP, profesional especializado y Profesional, Oficina Asesora de Planeación TIC	24 hora

TABLA NO 14 ACCIONES

Fuente: Elaboración propia a partir de la guía técnica de computación en la nube

7.5 PROCEDIMIENTO PARA LA RECUPERACIÓN DEL FIREWALL - FORTIGATE 400E

Conforme a los ANS y niveles de escalamiento establecidos contractualmente con el proveedor, el procedimiento se activa con la creación del ticket.

- NIVEL 1
  Contactar telefónicamente o por medio del portal al centro de servicio del proveedor del equipo de seguridad perimetral (Movistar) y crear ticket donde se reporte la falla presentada sobre el componente Firewall – FortiGate 400E. Dado el impacto del componente sobre el catálogo de servicios, se debe especificar en la solicitud de reporte, que el caso se clasifique con la prioridad más alta.
  Conforme a los ANS, se debe hacer seguimiento a los cumplimientos de los tiempos de recuperación y escalamiento establecidos contractualmente con el proveedor.

- NIVEL 2
  En este nivel, el proveedor del equipo de seguridad perimetral asigna a un especialista para realizar un primer acercamiento y profundizar sobre la falla presentada. Dependiendo de la falla reportada, se coordinará con el especialista de la entidad los tiempos de desplazamiento y acompañamiento del soporte en sitio, así como los tramites de acceso a las instalaciones. Dado el caso, solicitará apoyo al profesional de Tecnología de la Información de la Oficina de Planeación y TIC's de tecnología para realizar acciones remotas.

  En caso de que el proveedor Movistar habilite o aprovisione el Firewall – FortiGate 400E dentro de los ANS esperados, se inicia el proceso de seguimiento y monitoreo del comportamiento del servicio. Una vez se confirme la estabilidad del mismo, se procede a la autorización del cierre del ticket.

  Si los componentes no se restauran luego del soporte realizado por el especialista del proveedor Movistar, se procederá a realizar un escalamiento nivel 3.

- NIVEL 3
  En este nivel, el especialista del proveedor Movistar genera informe detallando las fallas presentadas en el Firewall – FortiGate 400E.

  Si el componente no se recupera dentro de los ANS esperados, se procederá a coordinar con el proveedor los tiempos para el aprovisionamiento de un dispositivo similar.

  Dado que el Firewall – FortiGate 400E ubicado en el centro de datos de la Entidad, no contempla un escenario de recuperación bajo un esquema de alta disponibilidad, ni un escenario de equipo de respaldo que supla el fallo del componente, el proveedor deberá según lo establecido contractualmente, reemplazar, instalar, configurar y poner en producción un dispositivo con las mismas características.

Sin embargo, dado que el componente afecta servicios críticos para la operación, el CIO convocará al Sub-Comité de TI para informar sobre el estado de la emergencia y solicitar autorización para poner en marcha el escenario de recuperación configurado previamente, de acuerdo al plan de contingencia establecido.

Una vez activado el escenario de recuperación, se deberá:

Acciones	Responsable	Tiempo
Coordinar con el proveedor del Firewall, en el menor tiempo posible, el aprovisionamiento del componente Firewall, con el fin de minimizar los tiempos de afectación de los servicios y recuperación de la operación. Nota: como parte de las recomendaciones a la entidad en la definición del Plan de Continuidad y Disponibilidad de las TIC, se contrató el componente firewall en un esquema de alta disponibilidad en modalidad Activo – Activo. Esto me permitiría minimizar los tiempos de respuesta RTO ante la materialización del riesgo.	Profesional especializado del proveedor del Firewall, Oficial de Seguridad y Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Hacer seguimiento a los tiempos acordados con el proveedor para la entrega e instalación y recuperación del componente Firewall.	Oficial de Seguridad	De acuerdo con los ANS establecidos.
Instalar, configurar y validar en el centro de datos, el funcionamiento de Firewall – FortiGate 400E.	Profesional especializado del proveedor Firewall y Profesional, Oficina Asesora de Planeación TIC	2 horas.
Realizar pruebas de acceso a los servicios asociados al Firewall – FortiGate 400E.	Profesional especializado del proveedor Firewall y Profesional, Oficina Asesora de Planeación TIC	1 hora.
Monitorear y validar los servicios de conectividad y seguridad.	Profesional, Oficina Asesora de Planeación TIC	36 horas.

Acciones	Responsable	Tiempo
Solicitar el informe del proveedor sobre el origen del incidente y documentar el caso en GLPI, con el objetivo de mejorar el escenario de recuperación o contingencia. Nota: Formatos de calidad.	Profesional especializado del proveedor Firewall y Profesional, Oficina Asesora de Planeación TIC.	24 horas.

TABLA NO 15 ACCIONES

Fuente: Elaboración propia

7.6 PROCEDIMIENTO PARA LA RECUPERACIÓN DE LA SAN PURESTORAGE

Conforme a los ANS y niveles de escalamiento establecidos contractualmente con el proveedor PURESTORAGE, el procedimiento se activa con la creación del ticket.

- NIVEL 1
  Contactar telefónicamente o por medio del portal al centro de servicio del proveedor PURESTORAGE y crear ticket donde se reporte la falla presentada sobre la unidad de almacenamiento. Dado el impacto del componente sobre los sistemas de bases de datos los cuales está aprovisionados sobre la solución de Oracle-VM y las máquinas virtuales de VMWare, se debe especificar en la solicitud de reporte, que el caso se clasifique con la prioridad más alta.
  Se debe iniciar seguimiento a los cumplimientos de los tiempos de escalamiento establecidos con el proveedor PURESTORAGE.

- NIVEL 2
  En este nivel, el especialista asignado por el proveedor PURESTORAGE realizará un primer acercamiento donde solicitará profundizar sobre la falla presentada. Así mismo, coordinará con el especialista de la entidad los tiempos de desplazamiento y acompañamiento del soporte en sitio y los tramites de acceso a las instalaciones. Dado el caso, solicitará apoyo al profesional de Tecnología de la Información de la Oficina de Planeación y TIC's de tecnología para realizar acciones remotas.

  Si el componente se restaura en este nivel, se realizarán las respectivas pruebas de funcionalidad de los servicios asociados a este.

  - Pruebas de funcionalidad
    - El especialista responsable de la gestión de las bases de datos, deberá realizar un diagnóstico sobre los motores de bases de datos una vez confirmada la estabilidad de la SAN con el fin de garantizar la integridad y

disponibilidad de los datos de los sistemas de información misionales y de apoyo.

- El especialista responsable de administrar la plataforma de virtualización VMWare, OracleVM, deberá realizar un diagnóstico sobre los servidores virtuales y la disponibilidad de los servicios configurados sobre los mismos.

Realizadas las pruebas, se inicia una fase de seguimiento con una duración de hasta tres días, para validar y garantizar el funcionamiento del dispositivo. Finalizada esta fase, se confirma la estabilidad del componente y la autorización para el cierre del ticket de servicio.

Si el componente no se restaura luego del soporte realizado por el especialista PURESTORAGE, se procede a realizar un escalamiento nivel 3.

- NIVEL 3

  En este nivel, el especialista HPE genera informe detallando las fallas presentadas en el componente SAN y en los elementos que integran la solución (fuente de poder, controladoras, discos duros, etc). Así mismo, informa a la entidad sobre la disponibilidad, tiempos de entrega e instalación de los componentes o elementos afectados.

  Para el caso de daño de los **elementos** que integran la solución, el proveedor deberá entregarlos instalados y operando en un tiempo no mayor a 24 horas.

  Tener presente que, según lo acordado con el proveedor, el servicio, el soporte y los compromisos de garantía de PURESTORAGE no cubren reclamaciones derivadas de:

  - Utilización inapropiada, inadecuada preparación del sitio o condiciones medioambientales del sitio disconformes con el Material de Apoyo aplicable.
  - Modificaciones o mantenimiento inapropiado del sistema o calibración no realizada por PURESTORAGE o autorizada por PURESTORAGE.
  - Fallos o limitaciones funcionales de cualquier software que no sea propiedad de PURESTORAGE o productos que impacten en los sistemas que reciben servicios o soporte de PURESTORAGE.
  - Programas malignos (virus, infección, gusano u otro código intencionado) no introducidos por PURESTORAGE.
  - Abuso, negligencia, accidente, daños causados por el fuego o el agua, alteraciones eléctricas, transporte por parte de la entidad u otras causas fuera del control de PURESTORAGE.

En caso de que se presente el daño total del **componente SAN Pure Storage FA-X10R3**, el proveedor PURESTORAGE deberá informar el tiempo estimado de entrega e instalación conforme a lo establecido contractualmente[7].

Sin embargo, dado que el componente afecta servicios críticos para la operación, el CIO convocará al Comité de TI para informar sobre el estado de la emergencia y solicitar autorización para poner en marcha el escenario de recuperación configurado previamente, de acuerdo con el plan de contingencia establecida.

Una vez aprobada la activación del escenario de recuperación, se deberá:

Acciones	Responsable	Tiempo
Poner en producción los servicios configurados para esta contingencia.	Profesional, Oficina Asesora de Planeación TIC.	2 horas.
Monitorear y validar la integridad de los datos procesados y generados por los sistemas de Información misionales y de apoyo.	Profesional, Oficina Asesora de Planeación TIC	Durante la operación de la contingencia.
Hacer seguimiento a los tiempos acordados con el proveedor PURESTORAGE para la entrega e instalación conforme a lo establecido contractualmente.	Profesional, Oficina Asesora de Planeación TIC.	De acuerdo con los ANS establecidos.
Re apuntar las bases de datos ORACLE desde la nueva unidad de almacenamiento a los servidores de administración de la solución clúster del Microblade.	Profesional, Oficina Asesora de Planeación TIC	1 hora.
Realizar pruebas funcionales y seguimiento, para garantizar el funcionamiento de los sistemas Þ información misionales y de apoyo.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Informar sobre el estado de la recuperación y solicitar autorización para poner en marcha la plataforma principal.	CIO.	Inmediato.

[7] Los servicios de soporte de PURESTORAGE se describen en el correspondiente material de apoyo, que contendrá la descripción de los servicios de PURESTORAGE ofertados, requisitos de elegibilidad, limitaciones del servicio y responsabilidades de la entidad, así como los sistemas soportados de la entidad.

Acciones	Responsable	Tiempo
Dar por finalizado el escenario de contingencia, detener la plataforma y generar copias de respaldo.	Profesional, Oficina Asesora de Planeación TIC.	3 horas.
Montar la copia de respaldo en la plataforma principal y validar la integridad de los datos.	Profesional, Oficina Asesora de Planeación TIC.	5 horas.
Poner en producción los servicios configurados.	Profesional, Oficina Asesora de Planeación TIC	30 minutos.
Monitorear y validar la integridad de los datos procesados y generados por los sistemas de Información misionales y de apoyo.	Profesional, Oficina Asesora de Planeación TIC TI.	3 días.
Confirmada la estabilidad del componente SAN PURESTORAGE, se procederá a la autorización del cierre del ticket de servicio.	Profesional, Oficina Asesora de Planeación TIC.	30 min.
Configurar los esquemas de copias de respaldo según la programación establecida.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Garantizar que se estén ejecutando los esquemas y generando las copias de respaldo.	Profesional, Oficina Asesora de Planeación TIC.	3 horas.

TABLA NO 16 ACCIONES

Fuente: Elaboración propia

7.7 PROCEDIMIENTO PARA LA RECUPERACIÓN DE LA NAS SUPERMICRO 826-9

Conforme a los establecido contractualmente con el proveedor SuperMicro - Evocom, el procedimiento de recuperación se activa con la creación del ticket.

- NIVEL 1
  Contactar telefónicamente o por medio de correo electrónico al proveedor de SuperMicro y crear ticket donde se reporte la falla presentada sobre la unidad de almacenamiento.
  Se debe especificar en la solicitud de reporte, que el caso se clasifique con la prioridad más alta.

- NIVEL 2

  En este nivel, el especialista asignado por el proveedor SuperMicro realizará un primer acercamiento dentro de las 4 primeras horas del reporte solicitando profundizar sobre la falla presentada. Así mismo, coordinará con el especialista de la entidad los tiempos de desplazamiento y acompañamiento del soporte en sitio y los tramites de acceso a las instalaciones. Dado el caso, solicitará apoyo al profesional de Tecnología de la Información de la Oficina de Planeación y TIC's de tecnología para realizar acciones remotas.

  Si el componente se restaura en este nivel, se realizarán las respectivas pruebas de funcionalidad de los servicios asociados a este.

  - Pruebas de funcionalidad a ejecutar por parte del especialista responsable de la infraestructura de TI.
    - Realizar un diagnóstico sobre el funcionamiento del servidor de archivos y el acceso a las carpetas compartidas en red.
    - Garantizar la integridad y disponibilidad de los datos almacenados en la NAS SuperMicro 826-9.
    - Validar que la solución de Hyper-V que gestiona los dos servidores virtuales del sistema de gestión de bases de datos ORACLE estén operativos.
    - Realizar un diagnóstico sobre los servidores virtuales y la disponibilidad de los servicios configurados sobre los mismos.

  Realizadas las pruebas, se inicia una fase de seguimiento con una duración de hasta tres días, para validar y garantizar el funcionamiento del dispositivo, finalizada esta fase, se confirma la estabilidad del componente y la autorización para el cierre del ticket de servicio.

  Si el componente no se restaura luego del soporte realizado por el especialista SuperMicro se procede a realizar un escalamiento nivel 3.

- NIVEL 3

  En este nivel, el especialista SuperMicro genera informe detallando las fallas presentadas en el componente NAS SuperMicro 826-9 y en los elementos que integran la solución (fuente de poder, discos duros, sistema operativo, etc). Así mismo, informa a la entidad sobre la disponibilidad, tiempos de entrega e instalación de los componentes o elementos afectados.

  Para el caso de daño de los **elementos** que integran la solución, el proveedor deberá entregarlos instalados y operando de acuerdo con el servicio 5x8 NBD acordado contractualmente.

En caso de que se presente el daño total del **componente NAS SuperMicro 826-9**, el proveedor SuperMicro deberá informar el tiempo estimado de entrega e instalación conforme a lo establecido contractualmente.

Sin embargo, dado que el componente afecta servicios críticos para la operación, el CIO convocará al Comité de TI para informar sobre el estado de la emergencia y solicitar autorización para poner en marcha el escenario de recuperación configurado previamente, de acuerdo con el plan de contingencia establecido.

Una vez aprobada la activación del escenario de recuperación, se deberá:

Acciones	Responsable	Tiempo
Poner en producción los servicios configurados para esta contingencia.	Profesional, Oficina Asesora de Planeación TIC.	2 horas.
Garantizar que se estén ejecutando los esquemas y generando las copias de respaldo.	Profesional, Oficina Asesora de Planeación TIC.	3 horas.
Hacer seguimiento a los tiempos acordados con el proveedor SuperMicro para la entrega e instalación conforme a lo establecido contractualmente.	Profesional, Oficina Asesora de Planeación TIC	De acuerdo con los ANS establecidos.
Contactar al centro de servicio de SuperMicro y generar ticket para apoyar el levantamiento de los servicios acorde a los ANS establecidos.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Validar el inventario y reportar los dispositivos tecnológicos afectados ante la aseguradora de la entidad.	Subdirección Administrativa y Financiera	36 horas
Instalar, actualizar y configurar el Sistema Operativo Windows Storage Server 2016 Standard.	Profesional especializado de SuperMicro y Profesional, Oficina Asesora de Planeación TIC	6 horas.
Configurar en la NAS SuperMicro 826-9 los arreglos de discos.	Profesional especializado de SuperMicro - Evocom y Profesional, Oficina Asesora de Planeación TIC.	36 horas.

Acciones	Responsable	Tiempo
Migrar la copia de respaldo de la PURESTORAGE a la NAS SuperMicro 826-9.	Profesional especializado de SuperMicro - Evocom y Profesional, Oficina Asesora de Planeación TIC.	5 horas.
Realizar pruebas funcionales y seguimiento, para garantizar el funcionamiento de la NAS SuperMicro 826-9.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Informar sobre el estado de la recuperación y solicitar autorización para poner en marcha la plataforma principal.	CIO.	Inmediato.
Dar por finalizado el escenario de contingencia, detener la plataforma y generar copias de respaldo.	Profesional, Oficina Asesora de Planeación TIC.	3 horas.
Realizar actualización de la información por medio de proceso diferencial entre la NAS SuperMicro 826-9 con la SAN PURESTORAGE.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Poner en producción los servicios configurados.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos
Monitorear y validar la integridad de los datos almacenados en la NAS SuperMicro 826-9.	Profesional, Oficina Asesora de Planeación TIC	3 días.
Confirmada la estabilidad del componente NAS SuperMicro 826-9, se procederá a la autorización del cierre del ticket de servicio.	Profesional, Oficina Asesora de Planeación TIC.	30 min.
Configurar los esquemas de copias de respaldo según la programación establecida.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.

TABLA NO 17 ACCIONES

Fuente: Elaboración propia a partir de la guía técnica de computación en la nube

Plan de contingencia establecido para la recuperación de la NAS SuperMicro 826-9

Acciones	Responsable	Tiempo
Configurar y asignar 1 Terabyte efectivo de almacenamiento en el tercer RAID 10 de la SAN HP MSA 2040	Profesional, Oficina Asesora de Planeación TIC.	2 horas.
Presentar y transferir a la solución VMWare la última copia de respaldo generada por la NAS a la QNAP.	Profesional, Oficina Asesora de Planeación TIC.	5 horas.
Entregar el software de instalación que se requiera para la recuperación de la operación.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Convertir servidor físico (Windows Storage Server 2016 Standard) a servidor virtual, empleando la herramienta VMWare Converter.	Profesional, Oficina Asesora de Planeación TIC.	24 horas.
Presentar al servidor virtualizado el espacio de almacenamiento definido en la SAN HP MSA 2040.	Profesional, Oficina Asesora de Planeación TIC.	3 horas.
Validar la configuración del servidor virtual y realizar pruebas de funcionalidad de los servicios asociados al servidor de archivos.	Profesional, Oficina Asesora de Planeación TIC.	4 horas.
Realizar un diagnóstico sobre la integridad y disponibilidad de los datos.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Realizar pruebas funcionales y seguimiento para garantizar el funcionamiento de los servicios asociados al servidor de archivos.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.

TABLA NO 18 NAS SUPERMICRO 826-9

Fuente: Elaboración propia

7.8 PROCEDIMIENTO PARA LA RECUPERACIÓN DE LA SOLUCIÓN ENCLOSURE MBE-314E-420

Respecto a la solución Enclosure MBE-314E-420 es importante considerar, que sobre esta plataforma se encuentra configurado los Cluster (OracleVM y VMWare) que administran y gestionan los servicios de bases de datos y servidores virtuales sobre los cuales se encuentran implementados los sistemas de información misionales

(SINFONIA, CCU, pagos en línea de contribuciones especiales, Chat de participación ciudadana), de apoyo (Intranet, correo institucional, ORFEO, GLPI, Trident, Pimisys, portal web) y externos (SIIF, SECOP I II, SIGEP).

Conforme a los establecido contractualmente con el proveedor SuperMicro, el procedimiento de recuperación se activa con la creación del ticket.

- NIVEL 1
  Contactar telefónicamente o por medio de correo electrónico al proveedor SuperMicro y crear ticket donde se reporte la falla presentada sobre el Enclosure (servidores blade). Dado la criticidad de la falla del componente, se deberá solicitar que la generación del caso se clasifique con la prioridad más alta.

- NIVEL 2
  En este nivel, el especialista asignado por el proveedor SuperMicro realizará un primer acercamiento dentro de las 4 primeras horas del reporte solicitando profundizar sobre la falla presentada según el contrato de soporte actual (5x8 NBD). Así mismo, coordinará con el especialista de la entidad los tiempos de desplazamiento y acompañamiento del soporte en sitio y los tramites de acceso a las instalaciones. Dado el caso, solicitará apoyo al profesional de Tecnología de la Información de la Oficina de Planeación y TIC's de tecnología para realizar acciones remotas.

  Si el componente se restaura en este nivel, se realizarán las respectivas pruebas de funcionalidad de los servicios asociados a este.

  - Pruebas de funcionalidad a ejecutar por parte del especialista responsable de la infraestructura de TI

    - Realizar un diagnóstico sobre el funcionamiento del Enclosure, servidores, máquinas virtuales y elementos (fuentes de poder, switch microblade, procesador, memoria y discos duros) que conforman la solución.
    - Validar la funcionalidad de la solución VMWare – Vcenter y conectividad con unidad de almacenamiento SAN HP MSA 2040, unidad que almacena los servidores virtuales y servicios asociados a los mismos.
    - Validar la funcionalidad de la solución OracleVM – Manager y conectividad con unidad de almacenamiento SAN HP MSA 2040, unidad que almacena las bases de datos de los misionales.
    - Realizar un diagnóstico de la integridad del motor de base de datos, servidores virtuales y la disponibilidad de los servicios configurados sobre los mismos.

  Realizadas las pruebas, se inicia una fase de seguimiento con una duración de hasta tres días, para validar y garantizar el funcionamiento del dispositivo, finalizada esta

fase, se confirma la estabilidad del componente y la autorización para el cierre del ticket de servicio.

Si el componente no se restaura luego del soporte realizado por el especialista SuperMicro, se procede a realizar un escalamiento nivel 3.

- NIVEL 3

En este nivel, el especialista SuperMicro genera informe detallando las fallas presentadas en el componente Enclosure MBE-314E-420 y en los elementos que integran la solución (fuentes de poder, switch microblade, procesador, memoria y discos duros). Así mismo, informa a la entidad sobre la disponibilidad, tiempos de entrega e instalación de los componentes o elementos afectados.

Para el caso de daño de los **elementos** que integran la solución, el proveedor deberá entregarlos instalados y operando de acuerdo con el servicio 5x8 NBD acordado contractualmente.

En caso de que se presente el daño total del componente Enclosure MBE-314E-420, el proveedor SuperMicro deberá informar el tiempo estimado de entrega e instalación conforme a lo establecido contractualmente.

Sin embargo, dado que el componente afecta servicios críticos para la operación, el CIO convocará al Comité de TI para informar sobre el estado de la emergencia y solicitar autorización para poner en marcha el escenario de recuperación configurado previamente, de acuerdo con el plan de contingencia establecido.

Una vez aprobada la activación del escenario de recuperación, se deberá:

Acciones	Responsable	Tiempo
Poner en producción los servicios configurados para esta contingencia.	Profesional, Oficina Asesora de Planeación TIC.	2 horas
Monitorear y validar el funcionamiento y rendimiento del servidor físico y plataforma de virtualización implementada para el escenario de recuperación.	Profesional, Oficina Asesora de Planeación TIC	Durante la operación de la contingencia.
Generar los SnapShot o copias de respaldo de los servidores virtualizados contemplados en el escenario de recuperación.	Profesional, Oficina Asesora de Planeación TIC.	5 horas.

Acciones	Responsable	Tiempo
Hacer seguimiento a los tiempos acordados con el proveedor SuperMicro - Evocom para la entrega e instalación conforme a lo establecido contractualmente.	Profesional, Oficina Asesora de Planeación TIC.	De acuerdo a los ANS establecidos
Instalar y realizar pruebas de funcionalidad de los elementos que integran el nuevo componente Enclosure MBE-314E-420 en el centro de datos de la entidad.	Especialista SuperMicro - Evocom y Profesional, Oficina Asesora de Planeación TIC	8 horas
Contactar al centro de servicio de SuperMicro - Evocom y generar ticket para validar la actualización del inventario de los componentes y elementos de los dispositivos adquiridos por la entidad.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Actualizar el inventario de dispositivos tecnológicos en la Subdirección Administrativa y Financiera.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Actualizar el inventario y reportar los dispositivos tecnológicos afectados ante la aseguradora de la entidad.	Subdirección Administrativa y Financiera.	36 horas.
Configurar los cluster de VMWare y OracleVM.	Profesional especializado de SuperMicro - Evocom y Profesional, Oficina Asesora de Planeación TIC.	120 horas.
Hacer la configuración de red y presentar la unidad de almacenamiento SAN HP MSA 2040 a la solución VMWare y motor de bases de datos ORACLE.	Profesional especializado de SuperMicro - Evocom y Profesional, Oficina Asesora de Planeación TIC.	8 horas.
Realizar pruebas funcionales y seguimiento, para garantizar el	Profesional, Oficina Asesora de Planeación TIC.	5 horas.

Acciones	Responsable	Tiempo
desempeño del Enclosure MBE-314E-420 y respectivos servidores virtuales.		
Informar sobre el estado de la recuperación y solicitar autorización para poner en marcha la plataforma principal.	CIO.	Inmediato.
Dar por finalizado el escenario de contingencia, detener la plataforma y generar SnapShot o copias de respaldo.	Profesional, Oficina Asesora de Planeación TIC	6 horas.
Validar qué servidores virtuales de la plataforma OracleVM deberán ser recuperados de la copia de respaldo almacenada en la NAS generados antes de la materialización del riesgo.	Profesional, Oficina Asesora de Planeación TIC.	3 horas.
Validar qué servidores virtuales de la plataforma VMWare deberán ser migrados desde el escenario de recuperación a la plataforma principal.	Profesional, Oficina Asesora de Planeación TIC.	3 horas.
Migrar los servidores virtuales de VMWare que se identificaron durante el proceso de validación. Nota: Para este proceso se debe garantizar que no se duplique en el inventario de VMWare y en el directorio activo el mismo servidor. Se sugiere tener apagados ambos servidores, antes de realizar el proceso de migración del Snapshot.	Profesional, Oficina Asesora de Planeación TIC.	1 hora x servidor.
Poner en producción la plataforma de VMWare y servidores virtualizados.	Profesional, Oficina Asesora de Planeación TIC.	2 horas.
Poner en producción la plataforma de Oracle VM y servidores virtualizados.	Profesional, Oficina Asesora de Planeación TIC.	2 horas.
Monitorear, validar el funcionamiento y rendimiento de la plataforma VMWare y OracleVM.	Profesional, Oficina Asesora de Planeación TIC de TI.	3 días.

Acciones	Responsable	Tiempo
Confirmada la estabilidad del componente Enclosure MBE-314E-420, se procederá a la autorización del cierre del ticket de servicio.	Profesional, Oficina Asesora de Planeación TIC.	30 min.
Configurar los esquemas de copias de respaldo según la programación establecida.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Garantizar que se estén ejecutando los esquemas y generando las copias de respaldo.	Profesional, Oficina Asesora de Planeación TIC.	3 horas.

TABLA NO 19 SOLUCIÓN ENCLOSURE MBE-314E-420

Plan de contingencia establecido para la recuperación de la Enclosure MBE-314E-420

Acciones	Responsable	Tiempo
Enviar a los especialistas los últimos SnapShot o copias de respaldo generadas por la plataforma VMWare y OracleVM, que se encuentran almacenadas en la NAS SuperMicro 826-9	Profesional, Oficina Asesora de Planeación TIC.	2 horas
Entregar el software de instalación de la plataforma VMWare, software de ORACLE, software especializado de gestión, entre otros que se requieran para la recuperación de la operación.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Validar la disponibilidad de hardware para la instalación y configuración de la plataforma VMware como escenario de recuperación.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Instalar y configurar servidor asignado para la instalación de la plataforma VMWare. Configurar: ○ Configuración del software Linux ESXi ○ Asignación de IP dentro del mismo segmento. ○ Actualización del Sistema operativo. ○ Instalación y configuración del Appliance – Vcenter, Vsphere y orquestador. ○ Migrar las máquinas virtuales. ○ Registrar en el inventario las máquinas virtuales migradas.	Profesional, Oficina Asesora de Planeación TIC y profesional especializado externo.	30 días.

Acciones	Responsable	Tiempo
○ Configurar en el stack central de switch DLink las rutas asociadas a las VLAN de data, el Nuevo escenario de recuperación. ○ Probar la estabilidad y desempeño del escenario propuesto. Nota: El escenario de recuperación debe contemplar los mismos controles de cambios generados en el ambiente de producción. Los cuales se garantizan con la generación de los SnapShot, que conservarían las actualizaciones de los sistemas operativos y generación de nuevas reglas en el directorio activo y demás cambios de configuraciones.		
Migrar de la NAS los SnapShot o copias de recuperación de los servidores virtuales al escenario de recuperación.	Profesional, Oficina Asesora de Planeación TIC y profesional especializado externo.	5 horas.
Realizar un diagnóstico del funcionamiento y desempeño del servidor físico y los servidores virtuales migrados.	Profesional, Oficina Asesora de Planeación TIC.	24 horas.
Realizar pruebas funcionales y seguimiento para garantizar la operación de los sistemas de información misionales y de apoyo.	Profesional, Oficina Asesora de Planeación TIC.	5 horas.
Documentar el resultado de las pruebas funcionales, de ser necesario realizar los ajustes de las actividades en el plan de contingencia. Nota: Formatos de calidad.	Profesional, Oficina Asesora de Planeación TIC.	2 horas.

TABLA NO 20 ENCLOSURE MBE-314E-420

Fuente: Elaboración propia

7.9 PROCEDIMIENTO PARA LA RECUPERACIÓN DEL STACKING Y SWITCH CORE DLINK

Conforme a los establecido contractualmente con el proveedor DLink - Evocom, el procedimiento de recuperación se activa con la creación del ticket.

- NIVEL 1

Contactar telefónicamente o por medio de correo electrónico al proveedor DLink - Evocom y crear ticket donde se reporte la falla presentada sobre uno de los componentes de red Switch que integran el Stacking para la conectividad de los componentes activos de red y equipos de cómputo de los funcionarios y contratistas de la entidad. Dado la criticidad de la falla en uno o más componentes de red, se deberá solicitar que la generación del caso se clasifique con la prioridad más alta.

- NIVEL 2

  En este nivel, el especialista asignado por el proveedor DLink - Evocom realizará un primer acercamiento dentro de las 4 primeras horas del reporte, solicitando profundizar sobre la falla presentada según el contrato de soporte actual (5x8 NBD). Así mismo, coordinará con el especialista de la entidad los tiempos de desplazamiento y acompañamiento del soporte en sitio y los trámites de acceso a las instalaciones. Dado el caso, solicitará apoyo al profesional de Tecnología de la Información de la Oficina de Planeación y TIC's de tecnología para realizar acciones remotas.

  Si el componente se restaura en este nivel, se realizarán las respectivas pruebas de funcionalidad de los servicios asociados a este.

  - Pruebas de funcionalidad a ejecutar por parte del especialista responsable de la infraestructura de TI

    - Realizar un diagnóstico sobre el funcionamiento del Stack de Switch y realizar toma de tiempos de respuesta (PING y TRACERT) entre los componentes de red, servidores y servicios de internet que conforman la solución.
    - Validar la calidad y funcionalidad de los componentes y servicios conectados[8] al Stack.

  Realizadas las pruebas, se inicia una fase de seguimiento con una duración de hasta tres días, para validar y garantizar el funcionamiento del Stack, finalizada esta fase, se confirma la estabilidad del componente y la autorización para el cierre del ticket de servicio.

  Si el componente no se restaura luego del soporte realizado por el especialista DLink - Evocom, se procede a realizar un escalamiento nivel 3.

- NIVEL 3

[8] Solución VMware, servidores virtuales, OracleVM, sistemas de Información misionales y de apoyo, servicio de internet, entre otros.

En este nivel, el especialista DLink - Evocom genera informe detallando las fallas presentadas en los componentes de red Switch DLink DGS-3420-52P, en la configuración del Stacking o en elementos que integran la solución (fuentes de poder, cables SFTP, etc). Así mismo, informa a la entidad sobre la disponibilidad para superar la emergencia, tiempos de entrega e instalación de los componentes o elementos afectados.

Para el caso de daño de los **elementos** que integran la solución, el proveedor deberá entregarlos instalados y operando de acuerdo con el servicio 5x8 NBD acordado contractualmente.

En caso de que se presente el daño de uno de los componentes de red que integran el Stacking de Switch, el proveedor DLink - Evocom deberá informar el tiempo estimado de entrega, instalación y disponibilidad del componente de acuerdo con el Stock previendo la obsolescencia tecnológica de la familia del componente.

Sin embargo, dado que el componente afecta servicios críticos para la operación, el CIO convocará al Comité de TI para informar sobre el estado de la emergencia y solicitar autorización para poner en marcha el escenario de recuperación configurado previamente, de acuerdo con el plan de contingencia establecido.

Una vez aprobada la activación del escenario de recuperación, se deberá:

Acciones	Responsable	Tiempo
Identificar el componente Switch DLink DGS-3420-52P afectado, para realizar el proceso de reemplazo.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Poner en producción el componente Switch DLink DGS-3420-52P configurado para esta contingencia. Nota: El componente deberá estar dentro del centro de datos de la entidad, plenamente identificado.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Monitorear y validar el funcionamiento y rendimiento del Stack de Switch y el componente configurado como parte del escenario de recuperación.	Profesional, Oficina Asesora de Planeación TIC.	Durante la operación de la contingencia.
Generar copia de respaldo de la configuración del Stack de Switch.	Profesional, Oficina Asesora de Planeación TIC	30 minutos

Acciones	Responsable	Tiempo
Identificar el componente Switch DLink DGS-3420-52P afectado, para realizar el proceso de reemplazo.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Hacer seguimiento a los tiempos acordados con el proveedor DLink - Evocom para la entrega e instalación del componente afectado conforme a lo establecido contractualmente.	Profesional, Oficina Asesora de Planeación TIC.	De acuerdo con los ANS establecidos.
Instalar y realizar pruebas de funcionalidad del componente instalado y del Stack de Switch en el centro de datos de la entidad.	Especialista DLink - Evocom y Profesional, Oficina Asesora de Planeación TIC.	2 horas.
Informar sobre el estado de la recuperación y solicitar autorización para poner en marcha la plataforma principal.	CIO.	Inmediato.
Contactar al centro de servicio de DLink - Evocom y generar ticket para validar la actualización del inventario de los componentes y elementos de los dispositivos adquiridos por la entidad.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Actualizar el inventario de dispositivos tecnológicos en la Subdirección Administrativa y Financiera.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Actualizar el inventario y reportar los dispositivos tecnológicos afectados ante la aseguradora de la entidad.	Subdirección Administrativa y Financiera.	36 horas.
Realizar seguimiento para garantizar el desempeño de Stack de Switch en operación.	Profesional, Oficina Asesora de Planeación TIC.	24 horas.
Solicitar informe sobre el origen del incidente y documentar el caso en GLPI, con el objetivo de mejorar el escenario de recuperación o contingencia. Nota: Formatos de calidad.	Profesional especializado del proveedor DLink - Evocom, Profesional, Oficina Asesora de Planeación TIC.	24 horas.

TABLA NO 21 STACKING Y SWITCH CORE DLINK

Fuente: Elaboración propia

21. PLAN DE CONTINGENCIA ESTABLECIDO PARA LA RECUPERACIÓN DEL STACKING Y SWITCH CORE DLINK

Acciones	Responsable	Tiempo
Validar la disponibilidad en Stock del componente Switch DLink DGS-3420-52P, para el respectivo cambio de la unidad afectada dentro del Stacking.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos
Instalar y configurar el componente Switch DLink DGS-3420-52P, de acuerdo con la posición (ID) establecido para el componente afectado. Nota: Al materializarse el riesgo de daño del Switch Core (ID 1), el especialista en la CRA deberá proceder a la conexión física de los cables de red en la misma posición y numeración de puertos del Switch ID 1 al Switch ID 5 configurado para tomar el rol de Switch Core principal.	Profesional, Oficina Asesora de Planeación TIC	4 horas
Realizar un diagnóstico del funcionamiento y desempeño del Switch DLink DGS-3420-52P y del Stacking.	Profesional, Oficina Asesora de Planeación TIC.	24 horas.
Realizar pruebas funcionales y seguimiento para garantizar la operación del Stacking.	Profesional, Oficina Asesora de Planeación TIC.	5 horas.

TABLA NO 22 RECUPERACIÓN DEL STACKING Y SWITCH CORE DLINK

8.1 PROCEDIMIENTO PARA LA RECUPERACIÓN DE LA SOLUCIÓN RED INALÁMBRICA DLINK

Conforme a los establecido contractualmente con el proveedor DLink – AconpiExpress, el procedimiento de recuperación se activa con la creación del ticket.

- NIVEL 1
  Contactar telefónicamente o por medio de correo electrónico al proveedor DLink - AconpiExpress y crear ticket donde se reporte la falla presentada sobre uno de los componentes (central wifi manager, puntos de acceso APs) de la solución de red inalámbrica empleada por los funcionarios y contratistas de la entidad. Dado la

criticidad de la falla en uno o más componentes de la solución, se deberá solicitar que la generación del caso se clasifique con la prioridad más alta.

- NIVEL 2

  En este nivel, el especialista asignado por el proveedor DLink - AconpiExpress realizará un primer acercamiento dentro de las 4 primeras horas del reporte, solicitando profundizar sobre la falla presentada según el contrato de soporte actual (5x8 NBD). Así mismo, coordinará con el especialista de la entidad los tiempos de desplazamiento y acompañamiento del soporte en sitio y los trámites de acceso a las instalaciones. Dado el caso, solicitará apoyo al profesional de Tecnología de la Información de la Oficina de Planeación y TIC's de tecnología para realizar acciones remotas.

  Si el componente se restaura en este nivel, se realizarán las respectivas pruebas de funcionalidad de los servicios asociados a este.

  - Pruebas de funcionalidad a ejecutar por parte del especialista responsable de la infraestructura de TI

    - Realizar un diagnóstico del estado de los puntos de acceso APs por medio de la controladora central wifi manager.
      - Con el diagnóstico inicial se busca:
        - Confirmar el estado de funcionamiento del servidor.
        - Validar que el central wifi manager esté operativo.
        - Confirmar que el servicio de internet esté activo.
    - Validar la conexión física del Switch DLink ID 2 por medio de la toma de tiempos de respuesta (PING) desde el servidor donde se encuentra el central wifi mánager a cada uno de los puntos de acceso APs que conforman la solución inalámbrica.
    - Validar las configuraciones de cada uno de los componentes que integran la solución de la red inalámbrica.

  Realizadas las pruebas, se inicia una fase de seguimiento con una duración de hasta tres días, para validar y garantizar el funcionamiento de la red inalámbrica, finalizada esta fase, se confirma la estabilidad de la solución y la autorización para el cierre del ticket de servicio.

  Si la solución no se restaura luego del soporte realizado por el especialista DLink - AconpiExpress, se procede a realizar un escalamiento nivel 3 con el fabricante DLink.

- NIVEL 3

  En este nivel, el especialista DLink - AconpiExpress genera informe detallando las fallas presentadas en los componentes afectados de la solución de red inalámbrica

(puntos de acceso APs). Así mismo, informa a la entidad sobre la disponibilidad para superar la emergencia, tiempos de entrega e instalación de los componentes o elementos afectados.

Para el caso de daño de los **componentes** que integran la solución, el proveedor deberá entregarlos instalados y operando de acuerdo con el servicio 5x8 NBD acordado contractualmente.

En caso de que se presente el daño de uno de los puntos de acceso APs que integran la red inalámbrica, el proveedor DLink - AconpiExpress deberá informar el tiempo estimado de entrega, instalación y disponibilidad del componente de acuerdo con el Stock previendo la obsolescencia tecnológica de la familia del componente.

Sin embargo, dado que el componente afecta el servicio de red inalámbrica, el CIO solicitará poner en marcha el escenario de recuperación configurado previamente, de acuerdo con el plan de contingencia establecido.

Una vez aprobada la activación del escenario de recuperación, se deberá:

Acciones	Responsable	Tiempo
Identificar el componente punto de acceso AP afectado, para realizar el proceso de reemplazo.	Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Cambiar el dispositivo adicional de respaldo para cubrir la zona que estaba irradiada por el AP afectado. Nota: La entidad previendo la indisponibilidad de uno de los puntos de acceso, cuenta con un dispositivo adicional para dar respuesta ante la mitigación del riesgo.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Monitorear y validar el funcionamiento de la solución y el comportamiento del punto de acceso de respaldo configurado como parte del escenario de recuperación.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Generar copia de respaldo de la configuración del Stack de Switch.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.

Acciones	Responsable	Tiempo
Hacer seguimiento a los tiempos acordados con el proveedor DLink - AconpiExpress para la entrega e instalación del componente afectado (AP) conforme a lo establecido contractualmente.	Profesional, Oficina Asesora de Planeación TIC.	De acuerdo a los ANS establecidos.
Instalar y realizar pruebas de funcionalidad del componente instalado y de toda la solución de red inalámbrica.	Especialista DLink - AconpiExpress y Profesional, Oficina Asesora de Planeación TIC.	2 horas.
Contactar al centro de servicio de DLink - AconpiExpress y generar ticket para validar la actualización del inventario de los componentes y elementos de los dispositivos adquiridos por la entidad.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Actualizar el inventario de dispositivos tecnológicos en la Subdirección Administrativa y Financiera.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos
Actualizar el inventario y reportar los dispositivos tecnológicos afectados ante la aseguradora de la entidad.	Subdirección Administrativa y Financiera.	36 horas.
Realizar seguimiento para garantizar el desempeño de la red inalámbrica.	Profesional, Oficina Asesora de Planeación TIC.	24 horas.
Solicitar informe sobre el origen del incidente y documentar el caso en GLPI, con el objetivo de mejorar el escenario de recuperación o contingencia. Nota: Formatos de calidad.	Profesional especializado del proveedor DLink -, profesional especializado y Profesional, Oficina Asesora de Planeación TIC.	24 horas.

TABLA NO 23 SOLUCIÓN RED INALÁMBRICA DLINK
Fuente: Elaboración propia

22. PLAN DE CONTINGENCIA ESTABLECIDO PARA LA RECUPERACIÓN DE LA SOLUCIÓN DE RED INALÁMBRICA

Acciones	Responsable	Tiempo
Generar copias de respaldo Firewall y configuración de los AP.	Profesional, Oficina Asesora de Planeación TIC, Profesional Claro, Profesional Proveedor	30 minutos.
Instalar físicamente el AP de respaldo de acuerdo a las recomendaciones realizadas por el proveedor, para garantizar la cobertura del área total ente el fallo de uno de los tres dispositivos que cubren la entidad.	Profesional, Oficina Asesora de Planeación TIC.	30 minutos.
Realizar un diagnóstico del funcionamiento y desempeño de la solución red inalámbrica y del AP configurado.	Profesional, Oficina Asesora de Planeación TIC.	3 días.
Realizar pruebas funcionales y seguimiento para garantizar la operación de la red inalámbrica.	Profesional, Oficina Asesora de Planeación TIC.	5 horas.

Fuente: Elaboración propia a partir

9.1 PROCEDIMIENTO PARA LA RECUPERACIÓN DEL SERVIDOR VIRTUAL 3CX QUE CONTROLA LAS COMUNICACIONES UNIFICADAS Y COMPONENTES DE RED UNE.

Nota: Tomando en cuenta que la herramienta principal de comunicaciones unificadas es 3CX, la entidad en su proceso de mejora continua y mediante el proceso de adquisición del plan Office 365 E3, empleará las bondades de este conjunto de herramienta dentro de las cuales está **Microsoft Teams,** la cual empleará como herramienta de apoyo a 3CX.

Conforme a los establecido contractualmente con el proveedor del sistema de comunicaciones unificada 3CX, el procedimiento de recuperación se activa con la creación del ticket.

- NIVEL 1
  Contactar telefónicamente o por medio de correo electrónico al proveedor 3CX y crear ticket donde se reporte la falla presentada sobre la solución virtual contratada en la nube de 3CX donde se encuentra instalada la solución. Dado la criticidad de la falla, se deberá solicitar que la generación del caso se clasifique con la prioridad más alta.

- NIVEL 2

  En este nivel, el especialista asignado por el proveedor 3CX realizará un primer acercamiento dentro de los tiempos acordados, solicitando profundizar sobre la falla presentada según lo acordado contractualmente. Así mismo, coordinará con el especialista de la entidad los tiempos de desplazamiento y acompañamiento del soporte en sitio y los trámites de acceso a las instalaciones. Dado el caso, solicitará apoyo al profesional de Tecnología de la Información de la Oficina de Planeación y TIC's de tecnología para realizar acciones remotas.

  Si el componente se restaura en este nivel, se realizarán las respectivas pruebas de funcionalidad de los servicios asociados a este.

  - Pruebas de funcionalidad a ejecutar por parte del especialista responsable de la infraestructura de TI

    - Realizar un diagnóstico sobre el funcionamiento del servicio de comunicaciones unificadas 3CX y elementos de interconexión que intervienen en el servicio.
    - Validar la funcionalidad del sistema operativo Linux y software de administración de la planta telefónica.
    - Realizar un diagnóstico a los dispositivos de conectividad PATTON y Switch UNE y conectividad con el Switch de Core.

  Realizadas las pruebas, se inicia una fase de seguimiento con una duración de hasta tres días, para validar y garantizar el funcionamiento del servicio de planta telefónica, finalizada esta fase, se confirma la estabilidad de la solución y la autorización para el cierre del ticket de servicio.

  Si la solución no se restaura luego del soporte realizado por el especialista de 3CX, se procede a realizar un escalamiento nivel 3.

- NIVEL 3 – Proveedor de Componentes de hardware de comunicaciones unificadas.

  En este nivel, el especialista de telefonía genera informe detallando las fallas presentadas en los componentes afectados de la solución (PATTON, tarjetas de comunicación, Huawei, elementos del servicio). Así mismo, informa a la entidad sobre la disponibilidad para superar la emergencia, tiempos de entrega e instalación de los componentes o elementos afectados.

  Para el caso de daño de los **componentes** que integran la solución, el proveedor deberá entregarlos instalados y operando de acuerdo con los niveles de servicios acordados contractualmente.

En caso de que se presente el daño de uno de los componentes (PATTON y UNE) que integran la solución, se solicitará al proveedor 3CX informar el tiempo estimado de entrega, instalación y disponibilidad del componente.

Dado que el servidor es una solución en modelo de nube, se contempla un escenario de recuperación bajo un esquema de restaurar una imagen instantánea, el proveedor deberá según lo establecido contractualmente, restaurar y poner en producción el servicio.

Sin embargo, dado que el fallo de uno de estos componentes afecta servicios críticos para la operación, el CIO convocará al Comité de TI para informar sobre el estado de la emergencia y solicitar autorización para poner en marcha el escenario de recuperación configurado previamente, de acuerdo con el plan de contingencia establecido.

Una vez aprobada la activación del escenario de recuperación, se deberá:

Acciones	Responsable	Tiempo
Coordinar con el proveedor de la solución de componentes de interconexión de comunicaciones unificadas, en el menor tiempo posible, el aprovisionamiento del servicio PATTON o HUAWEY con el fin de minimizar los tiempos de afectación de los servicios y recuperación de la operación.	unificadas", CIO y Profesional, Oficina Asesora de Planeación TIC.	1 hora.
Hacer seguimiento a los tiempos acordados con el proveedor de la solución de telefonía para la entrega e instalación y recuperación de los componentes.	Profesional, Oficina Asesora de Planeación TIC	De acuerdo con los ANS establecidos.
Instalar, configurar y validar en el centro de datos, el funcionamiento los componentes.	Profesional especializado del proveedor de la solución de telefonía y Profesional, Oficina Asesora de Planeación TIC.	2 horas.
Realizar pruebas de acceso a los servicios asociados a los componentes.	Profesional especializado del proveedor de la solución de telefonía y	1 hora.

Acciones	Responsable	Tiempo
	Profesional, Oficina Asesora de Planeación TIC.	
Monitorear y validar los servicios de la solución de telefonía	Profesional, Oficina Asesora de Planeación TIC.	36 horas.
Solicitar el informe del proveedor sobre el origen del incidente y documentar el caso en GLPI, con el objetivo de mejorar el escenario de recuperación o contingencia. Nota: Formatos de calidad.	Profesional especializado del proveedor de la solución de telefonía y Profesional, Oficina Asesora de Planeación TIC.	24 hora.

TABLA NO 24 COMPONENTES DE RED UNE.
Fuente: Elaboración propia

9.2 PROCEDIMIENTO PARA LA RECUPERACIÓN DE DOCUMENTACIÓN ELECTRÓNICA

El procedimiento para la recuperación de documentos electrónicos alojados en los diferentes sistemas de apoyo y misionales de la entidad, conforme a los ANS y a los niveles de escalamiento establecidos en el Catálogo de Servicios de TI de la entidad, el procedimiento se activa con la creación del ticket en la mesa de ayuda del sistema GLPI de la Oficina Asesora de Planeación y TIC.

Nivel 1.
Los usuarios afectados deberán crear un ticket de servicio a través de la mesa de ayuda de GLPI, donde se debe especificar en la solicitud que tipo de documento electrónico se requiere recuperar y desde que sistema de apoyo o misional se encontraba publicado. Una vez realizada la solicitud, se le asignará al usuario afectado un profesional de Tecnología de la Información de la Oficina de Planeación y TIC's
Nivel 2.
En este nivel el funcionario asignado para atender el servicio realizará un primer análisis de búsqueda de información en el sistema de apoyo o misional reportado y generará un reporte sobre los resultados obtenidos en su análisis. Si la documentación electrónica fue recuperada a satisfacción, se enviará el reporte generado al usuario afectado y se indicará la ubicación o enlace directo de consulta de los documentos electrónicos. Adicionalmente, se procederá al cierre del ticket en la mesa de ayuda de GLPI.

Si la documentación electrónica no fue recuperada, se procederá a un nuevo escalamiento al Nivel 3.

Nivel 3.

En este nivel, el funcionario asignado contacta al especialista o proveedor del sistema de apoyo o misional y comparte el reporte sobre los resultados obtenidos en su análisis. Dependiendo del incidente reportado, se coordinará con el especialista de la entidad los tiempos de desplazamiento y acompañamiento del soporte en sitio, así como los trámites de acceso a las instalaciones. Dado el caso, el especialista podrá solicitar apoyo al profesional de Tecnología de la Información de la Oficina de Planeación y TIC's de tecnología para realizar acciones remotas.

Si la documentación electrónica fue recuperada a satisfacción, se enviará el reporte generado por el especialista al usuario afectado y se indicará la ubicación o enlace directo de consulta de los documentos electrónicos. Adicionalmente, se procederá al cierre del ticket en la mesa de ayuda de GLPI. Si la documentación electrónica no fue recuperada, se indicará al usuario afectado los motivos de la perdida de información y se procederá a validar los lineamientos, políticas y procedimientos relacionados con la gestión de copias de seguridad de la entidad, para evitar un nuevo caso de pérdida de información.

Conforme a los niveles de escalamiento, a continuación, se describen las acciones que deben realizar los funcionarios asignados por la Oficina Asesora de Planeación y TIC para dar respuesta a los Niveles 1 y 2 descritos en el apartado anterior.

. Pasos para la recuperación de los sistemas misionales

Sistema de apoyo o misional	Pasos para la recuperación
Microsoft Sharepoint	Para restaurar los elementos eliminados por los funcionarios y contratistas, es fundamental contar con los permisos de administración requeridos para su edición. 1. Diríjase al SharePoint institucional 2. En la barra de navegación de inicio rápido de la parte inferior izquierda de la pantalla, haga clic en Papelera de reciclaje. 3. En la página Papelera de reciclaje, haga clic en el cuadro a la izquierda de los elementos o archivos que desea restaurar. 4. Haga clic en Restaurar. 5. Cuando se restaura un elemento, se restaura en la misma ubicación desde la que se eliminó. Es importante considerar que los elementos eliminados se conservan en las papeleras de reciclaje durante un período de tiempo determinado. Por SharePoint, el tiempo de retención es de 93 días. Comienza cuando elimina el elemento de su ubicación

	original. Al eliminar el elemento de la papelera de reciclaje del sitio, se incluye en la papelera de reciclaje de la colección de sitios. Permanece allí durante el resto de los 93 días y, a continuación, se elimina de forma permanente. Detalle de las papeleras: ✓ Papelera de Primer Nivel 30 Días - Usuario ✓ Papelera de segundo Nivel 93 Días - Administrador del TENANT ✓ Sitios Eliminados 30 Días - Administrador de TENANT Se invita a los funcionarios y contratistas a ver el siguiente video de apoyo realizado por el equipo de Microsoft: https://www.microsoft.com/es-es/videoplayer/embed/RE4yfx8?pid=ocpVideo0-innerdiv-oneplayer&maskLevel=20&market=es-es
Microsoft OneDrive	1. Para restaurar los documentos electrónicos eliminados por los funcionarios y contratistas, es fundamental iniciar sesión con su cuenta de Microsoft institucional. 1. En el panel de navegación, selecciona Papelera de reciclaje. 2. Seleccione los archivos o carpetas que desea restaurar señalando a cada elemento y haciendo clic en la casilla de círculo que aparece y, a continuación, haga clic en Restaurar. Es importante tener presente que los documentos electrónicos de la Papelera de reciclaje se eliminarán automáticamente después de 93 días, a menos que el administrador haya cambiado la configuración. Detalle de las papeleras: ✓ Papelera de Primer Nivel 30 Días - Usuario ✓ Papelera de segundo Nivel 93 Días - Administrador del TENANT ✓ Sitios Eliminados 30 Días - Administrador de TENANT Se invita a los funcionarios y contratistas a ver el siguiente video de apoyo realizado por el equipo de Microsoft: https://www.microsoft.com/es-es/videoplayer/embed/RWfEAH?pid=ocpVideo0-innerdiv-oneplayer&maskLevel=20&market=es-es

Sistema de Gestión Documental ORFEO (SGD) Y Sede Electrónica	Para el SGD es importante señalar que desde el CMS ningún documento se elimina quedando guardado en la carpeta bodega del servidor de producción de Orfeo, en el caso de tener alguna falla en el servidor o ataque informático, se podrá recuperar granularmente los archivos o la maquina completa, donde es importante resaltar que la entidad cuenta con un sistema de versionamiento de código la cual ayudara a recuperar código fuente de la plataforma. Como componente importante, en la base de datos se están realizando copias mediante RMAN y ExportDump Para la sede electrónica es importante resaltar que está contratado como servicio, por tal razón el proveedor cuenta con las copias de respaldo de la aplicación y base de datos.

TABLA NO 25 RECUPERACIÓN DE LOS SISTEMAS MISIONALES.
Fuente: Elaboración propia

23. PROPUESTA DEL PLAN DE PRUEBAS PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO.

El programa de plan de pruebas para la recuperación de los servicios tecnológicos de la entidad busca definir cómo se abordarán los riesgos asociados a los componentes tecnológicos críticos que integran la infraestructura tecnológica, validar que los servicios críticos de TIC se pueden mantener y recuperar de acuerdo con los acuerdos de nivel de servicios definidos con los proveedores y los tiempos estimados por el profesional de Tecnología de la Información de la Oficina de Planeación y TIC's.

En una primera instancia en el desarrollo del plan de recuperación ante desastres, la entidad ha seleccionado como parte de su plan de pruebas las siguientes simulaciones con su respectiva fecha de ejecución y responsable, para dar respuesta ante fallos a componentes asociados a servicios tecnológicos clasificados con un impacto alto.

Nro	Simulaciones	Fecha de ejecución	Responsable	Periodicidad
1	Simular la recuperación del Canal de Internet y componentes asociados (Router CISCO Raisecom) ante la materialización de falla del servicio y de acuerdo con plan de contingencia previamente establecido.	Semestre 1	Profesional, Oficina Asesora de Planeación TIC. Proveedor del servicio de Firewall y canal de internet.	1 vez al año.

Nro	Simulaciones	Fecha de ejecución	Responsable	Periodicidad
			Coordinador del Plan.	
2	Simular la falla de uno de los hosts (cuchillas) que conforman el cluster VMWare de la solución Enclosure MBE-314E-420 con el objetivo de validar la alta disponibilidad.	Semestre 2.	Profesional, Oficina Asesora de Planeación TIC. Proveedor del servicio. Coordinador del Plan.	1 vez al año.
3	Simular el daño del Switch ID 1 (Core) y configurar Switch ID 2 para que tome el control automático una vez se materialice el riesgo de falla del Switch ID 1, de acuerdo con plan de contingencia previamente establecido.	Semestre 2	Profesional, Oficina Asesora de Planeación TIC. Proveedor del servicio. Coordinador del Plan.	1 vez al año.
4	Simular el daño de un punto de acceso AP con el fin de garantizar la cobertura total de la red inalámbrica de la entidad.	Semestre 1	Profesional, Oficina Asesora de Planeación TIC. Proveedor del servicio. Coordinador del Plan.	1 vez al año.
5	Simular el escenario de recuperación ante la falla del cluster ORACLEVM el cual deberá ser configurado en la NAS SuperMicro 826-9 bajo el ambiente virtualizado de Microsoft Hyper-V.	Semestre 2	Profesional, Oficina Asesora de Planeación TIC. Profesional especializado (DBA) y proveedor externo. Coordinador del Plan.	1 vez al año.
6	Simular la recuperación de las copias de respaldo de las bases de datos ORACLE de	Semestre 2	Profesional, Oficina Asesora de	1 vez al año.

Nro	Simulaciones	Fecha de ejecución	Responsable	Periodicidad
	acuerdo con el esquema de copias de respaldo definido por la entidad.		Planeación TIC. Profesional especializado (DBA) y contratista de apoyo. Coordinador del Plan.	
7	Simular el escenario de recuperación ante la falla de las UPS del centro de datos de la entidad.	Semestre 1	Profesional, Oficina Asesora de Planeación TIC. Proveedor del servicio. Coordinador del Plan.	1 vez al año.
8	Simular el escenario de recuperación ante la falla del aire acondicionado del centro de datos de la entidad.	Semestre 1	Profesional, Oficina Asesora de Planeación TIC. Proveedor del servicio. Coordinador del Plan.	1 vez al año.

TABLA NO 26 PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO.
Fuente: Elaboración propia

Dado que la entidad en este momento se encuentra coordinando la instalación, configuración y puesta en producción del Cluster ORACLE-VM, en la solución Enclosure MBE-314E-420, el proveedor debe recrear el escenario de recuperación con el fin de validar la alta disponibilidad del cluster.

10.1 PLANIFICACIÓN DEL PLAN DE PRUEBAS

Como parte de la planificación de las pruebas preliminares del plan de pruebas, se establecieron criterios para minimizar el riesgo de incidentes como resultado de la ejecución del programa de pruebas.

Entre los criterios establecidos se contemplaron:

- Validar la documentación de las conexiones físicas de los componentes tecnológicos, antes de su desconexión. Esta actividad busca plasmar en un documento el estado actual de las conexiones físicas del componente tecnológico, con dispositivos y otros componentes asociados (Ej: El MicroBlade tiene una conexión física en el Puerto 49 del Switch Core ID 1).

- Generar copias de respaldo de las configuraciones de los componentes tecnológicos.

- Garantizar la ejecución del programa de pruebas en ambientes controlados.

- Coordinar el plan de pruebas en horarios no hábiles con el fin de minimizar riesgos de incidentes.

- Informar al coordinador del Plan de Continuidad y Disponibilidad de las TIC y a los profesionales de apoyo para la gestión del Plan de Continuidad y Disponibilidad de las TIC sobre el plan de pruebas a realizar.

- Informar a los lideres del proceso y proveedores sobre el plan de pruebas a ejecutar con el fin de alertar ante la suspensión de los servicios durante el tiempo de ejecución.

Así mismo, se consideró el diseño del formato de pruebas y registro de resultados donde se deberá registrar la descripción de la prueba a ejecutar, los objetivos, alcance, restricciones, riesgos, criterios de éxito, recursos, roles y responsabilidades, toma de tiempos o captura de datos del ejercicio y acciones de mejoras.

Formato 1. Plan de pruebas

CRA	Formato de plan de pruebas		
Componente de TI		Fecha de la prueba	
Descripción de la prueba			
Objetivo de la prueba			
Alcance			
Restricciones			
Riesgos			
Criterios de éxito			
Recursos			
Roles y responsabilidades			
Toma de tiempos			

Conclusiones de la ejecución del plan de contingencia	
Acciones de mejora	

Revisión del formato de pruebas			
Fecha	Versión	Descripción	Responsable
Elaborado por	Revisado por		Aprobado por

24. RESULTADOS DE LA PRUEBA PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO.

Prueba realizada del plan de contingencia del Cluster OracleVM como parte del proceso del PCD-TIC.

CRA	Formato de plan de pruebas		
Componente de TI	**Cluster OracleVM**	Fecha de la prueba	
Descripción de la prueba	Dado que en la solución Enclosure MBE-314E-420 se encuentra configurado el Cluster de OracleVM, para la administración y gestión de los servicios de bases de datos y servidores virtuales sobre los cuales se encuentran implementados los sistemas de información misionales SINFONIA, CCU, pagos en línea de contribuciones especiales y de apoyo Pimisys. A continuación, se pondrá en marcha el plan de continuidad diseñado como escenario de recuperación ante la materialización de fallo del Cluster OracleVM.		
Objetivo de la prueba	• Simular el escenario de recuperación ante la falla del Cluster OracleVM en la NAS SuperMicro 826-9 bajo el ambiente virtualizado Hyper-V configurado en el sistema operativo Microsoft Windows Storage Server 2016 Standard. • Garantizar el cumplimiento de los tiempos de recuperación, según los acuerdos de nivel de servicio establecidos en el Plan de Continuidad y Disponibilidad TIC . • Mantener actualizados los planes de contingencia, así como los recursos necesarios para la puesta en marcha de los escenarios de recuperación.		

CRA	Formato de plan de pruebas
Alcance	• Garantizar la operación de los servicios asociados al Cluster OracleVM en los tiempos acordados en el plan de contingencia.
Restricciones	• Almacenamiento: garantizar en la NAS SuperMicro 826-9 en la unidad de disco D:\backup 1.5TB • Memoria: garantizar 12 GB de memoria RAM para la configuración del servidor (Server I. 8GB y Server II. 4GB). • Virtualización: El Hiper-V deberá estar activo. • Configuración de red: Las IP asignadas al Server I y II se deben mantener reservadas e identificadas. • Recurso humano: Los especialistas de bases de datos y analista de sistemas deben tener conocimiento de los procedimientos y configuraciones para poner en marcha el plan de contingencia establecido para este escenario.
Riesgos	• Tecnológico: indisponibilidad de los servicios, perdida de gestión de las bases de datos de los sistemas de información SINFONIA (Oracle BI y Datawarehouse), ORFEO, Pymisys, los servicio de Weblogic Server (Oracle ADF) y los trámites en línea.
Criterios de éxito	Para la ejecución del escenario de recuperación se han establecidos los siguientes criterios: • Actualizar la documentación de las conexiones físicas de los componentes tecnológicos, antes de su desconexión. Esta actividad busca plasmar en un documento el estado actual de las conexiones físicas del componente tecnológico, con dispositivos y otros componentes asociados (Ej.: El Micro Blade tiene una conexión física en el Puerto 49 del Switch Core ID 1). • Generar copias de respaldo de las configuraciones de los componentes tecnológicos. • Garantizar la ejecución del programa de pruebas en ambientes controlados. • Coordinar el plan de pruebas en horarios no hábiles con el fin de minimizar riesgos de incidentes. • Informar al coordinador del Plan de Continuidad y Disponibilidad TIC y al profesional para la gestión del Plan de Continuidad y Disponibilidad TIC sobre el plan de pruebas a realizar. • Informar a los lideres del proceso y proveedores sobre el plan de pruebas a ejecutar con el fin de alertar ante la suspensión de los servicios durante el tiempo de ejecución.

CRA	Formato de plan de pruebas
Recursos	• Técnicos: capacidad de almacenamiento, memoria y procesamiento. • Recurso humano: disponibilidad de los profesionales de TI para la ejecución del plan de contingencia. • Gestión: Aprobación de la ejecución del plan por parte del coordinador del plan de Continuidad y Disponibilidad TIC.
Roles y responsabilidades	• Coordinador del plan de Continuidad y Disponibilidad TIC – Aprobación de la ejecución del plan de contingencia. • Los profesionales de TICS del plan de Continuidad y Disponibilidad TIC – Ejecución del plan de contingencia. • Contratistas – Apoyo en la ejecución del plan de contingencia.
Toma de tiempos	• Una vez realizada la prueba del plan de contingencia para el Cluster Oracle VM, se pudo establecer que la recuperación de la operación de los servicios asociados al Cluster Oracle VM tomó 2 horas hábiles; dado que se requirió encender las máquinas virtuales dispuestas en el escenario de recuperación, subir los servicios de ORACLE y validar la funcionalidad de los servicios asociados a este escenario de recuperación.
Conclusiones de la ejecución del plan de contingencia	• El escenario configurado como plan de contingencia, permitió recuperar la operación, disponibilidad y funcionalidad de los servicios asociados al Cluster Oracle VM. • Luego de la ejecución del plan de contingencia, se pudo garantizar que la recuperación de los servicios está dentro de los tiempos estimados en el plan de contingencia. • Dado el escenario de recuperación, se deberá continuar con la generación de los esquemas de copias de respaldo de las máquinas virtuales.
Acciones continuas	• Contrato de Servicio soporte en sitio y de partes está activo. Dar continuidad a la renovación del contrato con el fabricante y servicio de soporte con el fabricante durante el tiempo de funcionamiento de la plataforma. De la misma forma, servicio de paquetes de horas que serán empleadas por el especialista de la plataforma en el evento de falla, actualización de Firmware de la solución, mantenimiento preventivo y correctivo.

	• Socializar a los profesionales de TIC, los cambios realizados al plan de continuidad. • Actualizar el documento de Plan de Continuidad y Disponibilidad TIC , de ser necesario.

25. PROPUESTA DE DESARROLLO DE LA ESTRATEGIA DE SITIO ALTERNO PARA EL Plan de Continuidad y Disponibilidad TIC DE LA CRA

La CRA como primera actividad para la definición de su estrategia de Sitio Alterno, deberá evaluar 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 con la guía de computación en la nube[9] de MINTIC la Comisión puede optar por los siguientes modelos de implementación de nube.

25.1. Modelos de implementación de nube

A continuación, se desarrollan los tipos de nube a considerar en la estrategia de sitio alterno para el Plan de Continuidad y Disponibilidad TIC de la CRA.

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.

[9] Guía técnica versión 1.0 del 15 de mayo de 2018.

Tipo de nube	Descripción
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 hibrida permite a las entidades establecer dos o más nubes de acuerdo con 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.

Fuente: Elaboración propia a partir de la guía técnica de computación en la nube de MINTIC.

.

25.2. Modelos de servicio en la nube

De acuerdo con el servicio de TI que se requiera migrar a un esquema de computación en la nube, es importante determinar el modelo de servicio más acorde y técnicamente viable para su proceso de contratación.

De acuerdo con MINTIC los siguientes servicios deberían ser contratados para cada uno de los modelos de servicios existentes.

Modelo de servicios	Servicios
Software como Servicio – SaaS	• Correo electrónico y aplicaciones de oficina • Facturación • Sistemas de Gestión y manejo de relaciones con clientes - CRM • Herramientas de Colaboración • 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	• Inteligencia de Negocios • Base de datos • Desarrollo y pruebas

Modelo de servicios	Servicios
	• Integración • Implementación de aplicaciones
Infraestructura como Servicio – IaaS	• 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.

Fuente: Elaboración propia a partir de la guía técnica de computación en la nube de MINTIC.

25.3. Beneficios de migrar a un esquema de computación en la nube

Beneficio	Descripción
Reducción de costos de operación.	• Pagar únicamente por la capacidad o servicio que se utilice. • Reducir los costos por el no pago de licencias de Software. • Optimizar el recurso humano especializado. Se reduce la gestión y administración asociadas a actualizaciones, compatibilidad con sistema operativo, instalación, mantenimiento y soporte de equipos y servidores. • Reducir los costos en energía eléctrica. Se reduce el número de servidores físicos dentro de centro de datos.
Escalabilidad.	• Optimizar los tiempos en el despliegue de nuevos servicios o trámites. • Atender la demanda de la capacidad. Por su naturaleza el servicio es flexible y escalable.
Reducción de costos de obsolescencia tecnológica.	• Tercerizar los costos por obsolescencia tecnológica. La entidad no tendrá que preocuparse por invertir en nuevas tecnologías, únicamente se presupuesta y paga el derecho al uso de las mismas tal como servidores, licenciamiento y aplicaciones de software.
Acceso a tecnología de punta.	• Garantizar que todos los servicios contratados están operando bajo plataformas de última generación.

Beneficio	Descripción
Rápida recuperación ante desastres y fallos.	• Por la naturaleza del servicio, está orientado para la gestión de la capacidad de respaldo ante en evento de la interrupción del servicio, ofreciendo la modalidad de alta disponibilidad y continuidad de la operación para la entidad.
Transferencia y reducción de riesgos técnicos.	• Respaldo por parte del proveedor, apoyado en su mejora continua. Brinda soporte técnico en el momento que la entidad necesite implementar nuevos servicios en la nube.
Entrega rápida y flexible	• Reducir el tiempo en publicar o desplegar nuevos servicios o trámites. Así mismo, contratar las capacidades deseadas en cualquier momento y cantidad, conforme a lo demandado por el servicio (ancho de banda, capacidad de almacenamiento, procesamiento, entre otros).
Permite concentrar esfuerzos en la misión, y objetivos de la entidad.	• Transferir al proveedor las actividades de implementación, configuración y mantenimiento de la infraestructura. Esta transferencia permitirá a los integrantes de la Oficina Asesora de Planeación y TIC de la entidad, orientar más esfuerzos hacia aspectos estratégicos y de planeación que tengan un mayor impacto sobre los procesos de la misma.

Fuente: Elaboración propia a partir de la guía técnica de computación en la nube de MINTIC.

25.4. Aspectos a considerar al migrar a un esquema de computación en la nube

Aspecto	Descripción
Aprovisionamiento de servicios	La entidad al contemplar el aprovisionamiento de servicios de computación en la nube debe garantizar que sea provisto bajo demanda acorde con los acuerdos de nivel de servicios y demás condiciones contractuales, de una manera eficiente en tiempo, costo y uso de recursos.
Migración y portabilidad	La entidad debe ser consciente que a futuro puede tener que cambiar de proveedor de nube, en especial si se utilizan servicios de computación en la nube contratados a través de los Acuerdos Marco de TI. Garantizar la portabilidad de los datos entre los prestadores de servicios en el menor tiempo posible.

Aspecto	Descripción
	Acceder a toda su información y poderla migrar nuevamente a sus sistemas o a otros proveedores del servicio con total garantía de la integridad de la información y sin incurrir en costos adicionales. En relación con el ítem anterior, se deben definir cláusulas que garanticen que, al término del contrato ya sea por decisión de la entidad, del proveedor del servicio, por eventos tales como quiebra o insolvencia entre otros, toda la información suministrada por la entidad y almacenada por los proveedores pueda ser restituida a los usuarios o a terceros designados por estos, recuperada por los usuarios con herramientas provistas por el proveedor, sin contratiempos.
Escalonamiento	La entidad debe comprender que no es necesario migrar de inmediato todos los servicios de TI a la nube. Se recomienda realizar este paso gradualmente e iniciar con pequeños pasos. Se sugiere antes de migrar a servicios en la nube dar respuesta a los siguientes cuestionamientos: • ¿Qué vale la pena migrar a la nube de manera inmediata? • ¿Qué puede esperar? • ¿Qué aplicaciones es preferible mantener internas en el futuro previsible?
Seguridad y Privacidad	La entidad debe aclarar que los esquemas de computación en la nube del proveedor cuenten con las herramientas necesarias para garantizar un ambiente seguro entre usuarios. De igual forma, solicitar la política de identidad y control de acceso, basado en el mínimo privilegio. Clasificar la información de acuerdo a la ley de transparencia y acceso a la información pública (ley 1712 de 2014) y demás normatividad aplicable y vigente, con el fin de determinar qué información puede o debe llevarse a la nube.
Gestión de incidentes	Definir de manera explícita y clara el proceso o procedimiento para la gestión de incidentes en donde el proveedor de nube le informe al contratante si ha ocurrido algún incidente con el servicio o se ha puesto en riesgo la seguridad de la información.
Gestión de cambios	Establecer contractualmente la obligación de mantener actualizados los sistemas, para garantizar el correcto funcionamiento de los mismos, así como eliminar las posibles

Aspecto	Descripción
	vulnerabilidades que pueden afectar los servicios de computación en la nube prestados. Definir un procedimiento de coordinación en el mantenimiento de la infraestructura que soporta los servicios entre ambas partes para prevenir interrupciones o errores en la prestación del servicio; este procedimiento debe incluir la notificación con suficiente antelación de la realización de mantenimientos por parte del proveedor, identificando los tiempos en los que puede interrumpirse el servicio.
Asuntos legales relacionados con la residencia física de los datos.	La entidad deberá asegurarse de que siempre tendrá la propiedad y el control de su información independientemente del lugar donde se almacenen los datos.
Servicio totalmente dependiente de una conexión a internet.	Contratación de un mayor ancho de banda en la entidad e implementación de políticas de calidad de servicio o conexiones alternas, para evitar problemas en el acceso a las aplicaciones, o accesibilidad lenta que puedan poner en juego el desempeño de las aplicaciones.
Planes de continuidad del negocio (BCP) y recuperación de desastres Plan de Continuidad y Disponibilidad TIC.	La entidad debe inspeccionar y hacer parte de las pruebas de los planes de recuperación de catástrofes y de continuidad del negocio del proveedor en la nube. La entidad deberá integrar sus planes de continuidad y recuperación a los planes de continuidad del negocio y recuperación del proveedor.
Acuerdos de Nivel de servicio (ANS).	La entidad debe establecer acuerdos de nivel de servicio.
Reputación y solvencia del proveedor de servicios	Revisar la experiencia, la relación con los clientes, la estabilidad financiera del proveedor y su reputación.
Cláusulas de derechos de proveedores y limitación de responsabilidad	La entidad debe poner especial atención a aquellas clausulas incluidas en los términos de acceso a los servicios en la nube que puedan otorgar a los proveedores de servicios derechos sobre la información que pueda estar alojada en sus servidores, cualquiera que sea el propósito de ellas.
Privacidad	La entidad debe garantizar contractualmente que los proveedores de nube garanticen la protección, la recopilación, el procesamiento, la comunicación, el uso y la disposición de la información personal y de la información de identificación personal en la nube de acuerdo con la normatividad vigente.

Fuente: Elaboración propia a partir de la guía técnica de computación en la nube de MINTIC.

25.5. Aspectos para considerar en los ANS del proceso de contratación del sitio alterno bajo un esquema de computación en la nube

De acuerdo con MINTIC para la estrategia de Sitio Alterno por medio de servicios de computación en la nube, se deberán considerar acuerdos de nivel de servicio donde se detallen los siguientes aspectos:

- Controles.
- Reglamentación que cumplir.
- Medidas de protección y seguridad.
- Plazos de recuperación del servicio.
- Indicadores y forma de medición de indicadores de calidad del servicio.
- Valores mínimos aceptables de los mismos.
- Tiempos de respuesta ante una eventual falta de disponibilidad.
- Penalizaciones y el régimen de responsabilidad por los daños y perjuicios ocasionados por un incumplimiento del proveedor.
- Limitaciones al servicio o a sus garantías.
- Solicitudes de cambio.
- Gestión de incidentes.
- Regulación de la seguridad y el tratamiento de datos de carácter personal.
- Causas de terminación del servicio/contrato.

25.6. Propuesta de Sitio Alterno en esquema de computación en la nube

Una vez realizado el análisis y evaluación de riesgos de continuidad de los componentes tecnológicos de la Comisión de Regulación de Agua Potable y Saneamiento Básico CRA, se pudo identificar que los componentes relacionados con el servicio de administración de los recursos de almacenamiento ocasionarían un impacto clasificado como **catastrófico** con una probabilidad de ocurrencia **posible**, esto dado a que si se materializa el riesgo afectaría la disponibilidad e integridad de la información, así como la interrupción de servicios TI críticos de la entidad.

Por lo anterior y siguiendo las recomendaciones de MINTIC sobre la implementación de esquemas de computación en la nube como escenarios de recuperación o sitio alterno, se propone para la CRA realizar la migración de servicios gradualmente e iniciar como primera fase con los componentes tecnológicos relacionados con la infraestructura de procesamiento y almacenamiento.

Esta primera fase de implementación del sitio alterno y de acuerdo a las recomendaciones, deberá seguir un modelo de implementación de nube privada, hosting o colocation.

De igual forma, con el fin de centralizar los datos e información que producen los funcionarios y contratistas, así como, garantizar un ecosistema de trabajo virtual con acceso a sistemas, información, recursos TI y herramientas de gestión, desde cualquier dispositivo móvil y desde cualquier lugar, cumpliendo y asegurando la aplicación de las políticas de seguridad de la información de la entidad, se propone la implementación de la estrategia de Escritorios Virtuales y suite ofimática de apoyo al trabajo colaborativo.

De esta manera, se puede contribuir a facilitar la gestión de la entidad, bajo los estándares de seguridad requeridos; y se sigue fortaleciendo la gestión del conocimiento en cuanto a la captura, acceso y disponibilidad de la información.

25.7. Propuesta de Sitio Alterno en esquema de computación en la nube

Una vez realizado el análisis y evaluación de riesgos de continuidad de los componentes tecnológicos de la Comisión de Regulación de Agua Potable y Saneamiento Básico CRA, se pudo identificar que los componentes relacionados con el servicio de administración de los recursos de almacenamiento ocasionarían un impacto clasificado como **catastrófico** con una probabilidad de ocurrencia **posible**, esto dado a que si se materializa el riesgo afectaría la disponibilidad e integridad de la información, así como la interrupción de servicios TI críticos de la entidad.

Por lo anterior y siguiendo las recomendaciones de MINTIC sobre la implementación de esquemas de computación en la nube como escenarios de recuperación o sitio alterno, se propone para la CRA realizar la migración de servicios gradualmente e iniciar como primera fase con los componentes tecnológicos relacionados con la infraestructura de procesamiento y almacenamiento.

Esta primera fase de implementación del sitio alterno y de acuerdo con las recomendaciones, deberá seguir un modelo de implementación de nube privada, hosting o colocation.

De igual forma, con el fin de centralizar los datos e información que producen los funcionarios y contratistas, así como, garantizar un ecosistema de trabajo virtual con acceso a sistemas, información, recursos TI y herramientas de gestión, desde cualquier dispositivo móvil y desde cualquier lugar, cumpliendo y asegurando la aplicación de las políticas de seguridad de la información de la entidad, se propone la implementación de la estrategia de Escritorios Virtuales y suite ofimática de apoyo al trabajo colaborativo.

De esta manera, se puede contribuir a facilitar la gestión de la entidad, bajo los estándares de seguridad requeridos; y se sigue fortaleciendo la gestión del conocimiento en cuanto a la captura, acceso y disponibilidad de la información.

25.8. Fases del Plan de Recuperación ante Desastres propuesto para poner en marcha el Sitio Alterno

De acuerdo con el proceso de definición del Plan de Recuperación ante Desastres de la Comisión, a continuación, se describen las fases a realizar una vez se produzca un evento de impacto catastrófico en la entidad y se requiera declarar la emergencia por parte del Coordinador del Plan de Continuidad y Disponibilidad de las TIC, habilitar el Sitio Alterno de operación y reestablecer la operación en el centro de datos de la entidad.

Fases	Actividades
Fase 1. Declaración de la emergencia	Determinar qué clase de siniestro o incidente se está presentando.
	Comunicar al administrador del edificio donde opera la entidad, de ser necesario.
	Comunicar a los profesionales TIC, del Plan de Continuidad y Disponibilidad de las TIC que se consideren necesarios, de acuerdo con el siniestro o incidente presentado.
	Comunicar a los miembros del Comité de Tecnología de Información sobre el estado de la emergencia.
	Mantener informados a los funcionarios y contratistas de la entidad sobre la evolución de la emergencia.
	Coordinar actividades con miembros con los profesionales del Plan de Continuidad y Disponibilidad de las TIC y funcionarios relacionados con la emergencia cuando así lo exijan las circunstancias.
	Analizar los escenarios de acuerdo con la evaluación del daño.
	Establecer los controles necesarios para llevar de forma confiable las actividades del Plan de Continuidad y Disponibilidad de las TIC.
	Determinar con los profesionales del Plan de Continuidad y Disponibilidad de las TIC y proveedores de servicios tecnológicos relacionados con la emergencia, la magnitud del daño generado por el siniestro y validar si se requiere poner en marcha el Plan de Recuperación ante Desastres.
	Convocar una sesión extraordinaria del Comité de Tecnología de Información, para informar sobre el estado de la emergencia y solicitar autorización para poner en marcha el Plan de Continuidad y Disponibilidad de las TIC.
	Activar el Plan de Recuperación ante Desastres.
Fase 2. Plan para	Reunir los profesionales del Plan de Continuidad y Disponibilidad de las TIC contratistas y proveedores relacionados con la emergencia,

Fases	Actividades
operar en Sitio Alterno	para coordinar las tareas y procedimientos a desarrollar de acuerdo con el Plan de Continuidad y Disponibilidad de las TIC.
	Habilitar los servicios de comunicaciones, para activar los procesos de restauración y puesta en operación del Sitio Alterno (centro de datos o nube pública).
	Solicitar al administrador de base de datos y administrador de la infraestructura TI, las versiones más actualizadas de las copias de seguridad de los servidores virtualizados y de los sistemas de información misionales y de apoyo, para el proceso de restauración en el Sitio Alterno; en caso de pérdida de información.
	Mantener informado al Comité de Tecnología de Información del estado de la recuperación en el Sitio Alterno y generar informe diario de las acciones adoptadas.
	Coordinar actividades con los profesionales del Plan de Continuidad y Disponibilidad de las TIC y funcionarios relacionados con la emergencia cuando así lo exijan las circunstancias.
Fase 3. Operación en Sitio Alterno	Verificar que se estén llevando a cabo los procedimientos para la recuperación de los servicios tecnológicos.
	Coordinar los procesos de comunicación entre la Comisión y el Sitio Alterno.
	Coordinar los procesos de restauración de los servicios críticos de la entidad en el Sitio Alterno (centro de datos o nube pública).
	Verificar el funcionamiento, disponibilidad, integridad y confiabilidad de las bases de datos, sistemas de almacenamiento y sistemas de información críticos (misionales y de apoyo), con el objetivo de garantizar la operación de la Comisión.
	Autorizar la operación en el Sitio Alterno de las bases de datos, sistemas de almacenamiento y sistemas de información críticos.
	Verificar una vez activa la operación, que la información producida y generada sea confiable.
	Mantener informado al Comité de Tecnología de Información del estado de la recuperación en el Sitio Alterno y generar informe diario de las acciones adoptadas.
Fase 4. Restablecer operación en centro de datos de la Entidad	Coordinar actividades para reestablecer las operaciones en el Centro de Datos de la Entidad
	Coordinar la instalación y configuración de la infraestructura de comunicaciones, almacenamiento y procesamiento.
	Coordinar la instalación y configuración de sistemas de bases de datos y sistemas de información misionales y de apoyo.
	Coordinar la instalación y configuración de sistemas de bases de datos y sistemas de información misionales y de apoyo.
	Verificar el funcionamiento de las bases de datos, sistemas de almacenamiento y sistemas de información críticos (misionales y de

Fases	Actividades
	apoyo), con el objetivo de garantizar la operación en el Datacenter de la Entidad.
	Autorizar la operación en el Datacenter de la Entidad de las bases de datos, sistemas de almacenamiento y sistemas de información críticos.
	Verificar una vez activa la operación, que la información producida y generada sea confiable.
	Mantener informado al Comité de Seguridad de Información del estado de la recuperación en el Sitio Alterno y generar informe diario de las acciones adoptadas.
	Documentar el proceso de recuperación y los resultados obtenidos en la ejecución del Plan de Continuidad y Disponibilidad de las TIC.
	Determinar con los profesionales de trabajo del Plan de Continuidad y Disponibilidad de las TIC y proveedores de servicios tecnológicos relacionados con la emergencia, si se da por concluida la situación de emergencia.
	Informar al Comité de Seguridad de Información y Directivo sobre el establecimiento de las operaciones en el Datacenter de la Entidad.

26. Referencias bibliográficas

- **GTC-ISO-IEC 27031,** Tecnologías de la Información. Técnicas de Seguridad. Directrices para la preparación de la tecnología de información y las comunicaciones para la continuidad del negocio.

- **NTC-ISO-IEC 27001,** Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la seguridad de la Información (SGSI).

- **Ministerio de Tecnologías de la Información. Colombia**. Marco de Referencia de Arquitectura Empresarial para la gestión de TI. Disponible: www.mintic.gov.co/arquitecturati.

- **Ministerio de Tecnologías de la Información. Colombia**. Guía de Computación en la nube. Disponible: https://www.mintic.gov.co/arquitecturati/630/w3-article-75554.html

- **Departamento Administrativo de la Función Pública. Colombia.** Guía para la Administración del riesgo. Disponible: https://goo.gl/ijajgU

- **Ministerio de Tecnologías de la Información. Colombia**. Guía para la preparación de las TIC para la continuidad del negocio. Disponible: https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

- **Ministerio de Tecnologías de la Información. Colombia**. Guía para realizar el Análisis de Impacto de Negocios BIA. Disponible: https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

- **Documento CONPES 3995.** Política Nacional de confianza y seguridad digital https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf