PLAN DE CONTINUIDAD DEL NEGOCIO GESTIÓN TIC

2025

CONTENIDO

1. Introducción

El Plan de Continuidad del Negocio es una herramienta estratégica diseñada para garantizar la capacidad de prevenir y reaccionar eficazmente frente a incidentes que puedan interrumpir las operaciones de Canal Capital. Su propósito es asegurar la continuidad en la prestación de los servicios y el cumplimiento de los compromisos establecidos en la planeación estratégica. Este plan, desarrollado por el área de Gestión TIC, establece una serie de acciones planificadas que buscan responder de manera eficiente ante eventualidades, restablecer los servicios en el menor tiempo posible y minimizar el impacto negativo derivado de la pérdida de recursos.

2. Descripción general

2.1. Propósito

Establecer un plan de contingencia en Canal Capital para gestionar los riesgos potenciales y existentes derivados de desastres, definiendo actividades específicas respaldadas por los sistemas de información e infraestructura tecnológica disponibles, con el objetivo de garantizar la continuidad operativa y minimizar el impacto de dichos eventos.

2.2. Objetivo General

Definir las actividades preventivas, detectivas y correctivas para reaccionar de manera eficiente y reducir al mínimo, el tiempo de inactividad tecnológica y la pérdida de información ante una eventualidad que comprometa el desarrollo de las actividades cotidianas.

2.2.1. Objetivos Específicos

- Identificar las actividades críticas, los recursos y los procedimientos necesarios para llevar a cabo las operaciones durante las interrupciones prolongadas del servicio.
- Asegurar la recuperación en los servicios críticos para los grupos de valor.
- Disminuir los tiempos de interrupción de la operación de los procesos.
- Proteger los bienes e información de la entidad de manera adecuada.

3. Generalidades del plan de continuidad

El Plan de Continuidad reúne un conjunto de actividades o procedimientos que facilitarán mantener el funcionamiento de los servicios administrativos y que afectan la misionalidad de la entidad; la prestación de sus servicios se establece en tres momentos:

- **Preventivo:** Dentro de este aspecto se involucran los recursos humanos, quienes deben estar preparados en caso de presentarse un evento inesperado, y las acciones anticipadas que se puedan articular a la gestión institucional en los diferentes procesos.
- **Reactivo:** Este aspecto va dirigido a fortalecer las políticas internas y comunicarlas oportunamente para ponerlas en marcha una vez detectada la contingencia.
- **Recuperación:** Este aspecto está enfocado en las actividades a desarrollar en el momento de atender una contingencia.

4. Plan de contingencia – Área Gestión TIC

El Plan de Contingencia describe los principales procedimientos y medidas a adoptar frente a eventos que pudieran acontecer durante la operación del área de Gestión TIC, a fin de obtener una respuesta, rápida, adecuada y oportuna que pueda mitigar al mínimo el tiempo de inactividad tecnológica de Canal Capital.

En el desarrollo del plan se tiene en cuenta la información como uno de los activos más importantes de la entidad y se realiza una clasificación de los servicios informáticos que se prestan en las operaciones diarias del área, para establecer un procedimiento escrito, que indique las acciones principales para afrontar efectivamente un evento que se presente, a fin de reducir significativamente el impacto negativo en las operaciones.

4.1. Clasificación de procesos y servicios

El presente plan incluye los componentes y recursos informáticos que conforman los sistemas de información que se relacionan a continuación:

- **Datos o Información:** En general se consideran datos todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados o no estructurados.
- **Aplicaciones:** Son los programas, herramientas y medios desarrollados o adquiridos por Canal Capital.
- **Tecnología:** Incluye los equipos de cómputo como computadores de escritorio, periféricos, servidores, servidores virtuales, cableado estructurado, router, firewall, Switch, telefonía IP etc.
- **Instalaciones:** Lugares físicos de Canal Capital donde se encuentre el software.
- **Personal:** Individuos con conocimientos y experiencia específica que integran el área de Gestión TIC de Canal Capital y que dentro de sus funciones deban programar, planificar, organizar, administrar y gestionar los sistemas de información.

Aplicaciones de software

- Sistema de órdenes de pago ORDPAGO.
- Sistema de Inventario KARDEX.
- Sistema de Contabilidad SIIGO.
- Sistema de Contabilidad SIMED.
- Sistema de Nomina NOVASOFT.
- Software de Intranet.
- Software de gestión documental.
- Software de gestión contractual.
- Software de SICC/ERP/ERPC

Tecnología, infraestructura tecnológica

- Un (2) Firewall Fortinet 401E, que provee la seguridad a la red, ya que es el encargado de bloquear el acceso no autorizado a la red, IPS, WEB, APP, Antivirus, SSL, IDS, etc.
- Switch CORE principal, HP 5900 JG510A.

- Switch CORE de respaldo, HP A5120-48G JE069A.
- Servidor HP, tipo Enclosure C3000 con virtualización VmWare 6.5, contiene 54 servidores virtuales en plataformas Microsoft Windows en un 90% y plataforma linux en un 10 %.
- Servidor ThinkSystem SR630, para servicios de servidores de dominio de directorio activo (AD DS), servidor de nombre de dominio (DNS) y servidor de asignación dinámica de host (DHCP).
- Equipo de almacenamiento HP MSA 2050, donde se encuentra la data o información de los servidores virtuales.
- Servidor ThinkSystem SR630, Servidor de Backup.
- Servidor plan de recuperación ante desastres (DRP), Lenovo SR630 V2- 7Z71
- Librería HP MSL 2024, la cual cuenta con dos (2) drives de tecnología de escritura para cintas LTO-5; este es el encargado de realizar respaldo de la información a través de Backup.
- HP 1950 - JG961A con conexión en estrella con dispositivos CORES para brindar el servicio de datos y voz.
- Telefonía IP
- Aire acondicionado del centro de datos.
- UPS.

Servicios

- Canales de Internet - ISP
- Correo electrónico
- Intranet
- Telefonía IP
- Servicios de almacenamiento compartido: MSA 2050
- Backup.
- Servicio de red de área local (LAN)
- Servicio de red de área local inalámbrica (WLAN)
- Servicio de granja de servidores (VmWare)
- Servicio de canal de datos (MPLS)
- Servicio de seguridad perimetral (Firewall)
- Servicio de seguridad endpoint (Antivirus)
- Servicio de monitoreo infraestructura TIC (PRTG)
- Restauraciones.

Software

- Symantec Backup Exec 2020.
- VMWare 6.5. y 7.0
- Windows Server Data Center, standard 2016 and 2019.
- Software de inventarios Assets Invgate.
- Bitdefender Gravityzone V6.56
- Fortinet v7.2.5 build1517
- Aplicación de red Unifi 8.2.93
- Software de monitoreo PRTG Network Monitor 24.3.98.1210 x64
- Site recovery

5. Estructura Área de Gestión TIC

Dentro de las principales funciones del área de Gestión TIC está las de realizar las acciones y proyectos orientados a la consolidación de las iniciativas de Gobierno digital y seguridad digital orientadas a la disponibilidad, acceso a la información pública y seguridad de la información, así como determinar y ejecutar el plan estratégico de la entidad y aquellos proyectos TIC que desde lo administrativo impactan el buen desarrollo de la misión institucional y la continuidad del negocio.

A su vez, para mantener la operatividad de la infraestructura de red y servicios tic a usuarios finales, cuenta con ingenieros con especialidades diferentes en seguridad de la información, infraestructura de redes y comunicaciones y soporte a usuario final.

5.1. Organigrama

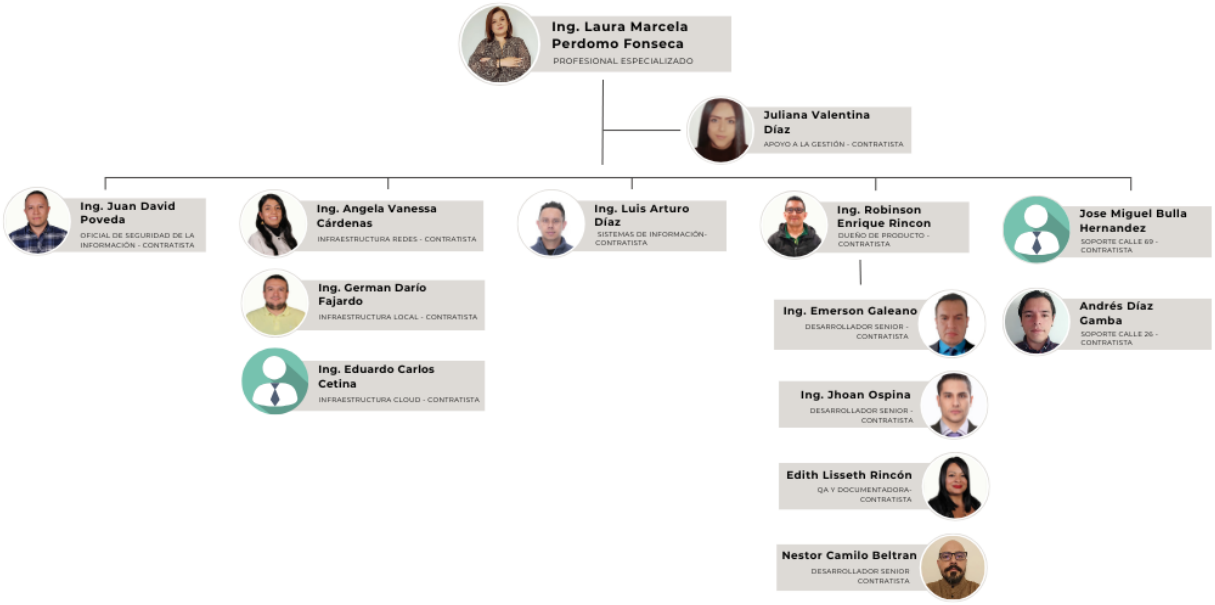

Figura 5.1 Organigrama Área de Gestión TIC

5.1.1. Condiciones Generales (Esquema General)

El Plan de Recuperación ante Desastres DRP cubre todos los aspectos de la organización que pueden verse afectados por un desastre, tales como:

- **Infraestructura tecnológica:** Servidores, sistemas de respaldo, bases de datos, redes, nube, etc.
- **Personal:** Evacuación, seguridad, asistencia médica.
- **Operaciones:** Continuidad de la producción, ventas, atención al cliente, etc.

- **Recursos físicos:** Suministros esenciales, equipos y maquinaria crítica

.

A continuación, se relacionan las diferentes definiciones de riesgos generales que pueden afectar el funcionamiento de los servicios actuales de Canal Capital y los cuales se encuentran dentro del Data Center.

Factor Riesgo	Tipo de Riesgo	Prevención y Mitigación
Bajo	Fuego: destrucción de equipos y archivos.	Extintores, detectores de humo, dos (2) Solkaflam, pólizas de seguros.
Bajo	Equivocaciones: daño a los archivos.	Copias de respaldo, Políticas de Seguridad.
Medio	Terremotos: destrucción de equipos y archivos	Seguro contra todo riesgo, Copias de Respaldo.
Medio	Fallas en los equipos: daño a los archivos.	Mantenimiento, garantía y copias de respaldo.

Tabla 5.1 Cuadro de riesgos generales

5.2. Criterios Matriz de Riesgos

A continuación, se relacionan las diferentes definiciones de riesgos generales que pueden afectar el funcionamiento de los servicios de TI actuales de Canal Capital y los cuales se encuentran en el Data Center.

Cuadro de riesgos generales

Factor Riesgo	Tipo de riesgo	Prevención y mitigación
Bajo	Fuego: destrucción de	Extintores, detectores de humo, dos
	Equipos y archivos.	(2) Solkaflam, pólizas de seguros.
	Equivocaciones: daño a los Archivos.	Copias de respaldo, Políticas de seguridad
Medio	Terremotos: destrucción de equipo y archivos	Seguro contra todo riesgo, Copias de Respaldo.
Medio	Fallas en los equipos: daño a los archivos	Mantenimiento, garantía y copias de respaldo

Tabla 5.2 Matriz de Riesgos

Se definen los criterios para los riesgos asociados a la continuidad del servicio aclarando que se atenderán y hará parte del mapa de riesgos institucional los de la dimensión 5 x 5 (5 horas al día y 5 días a la semana de lunes a viernes) y se identifiquen con nivel extremos:

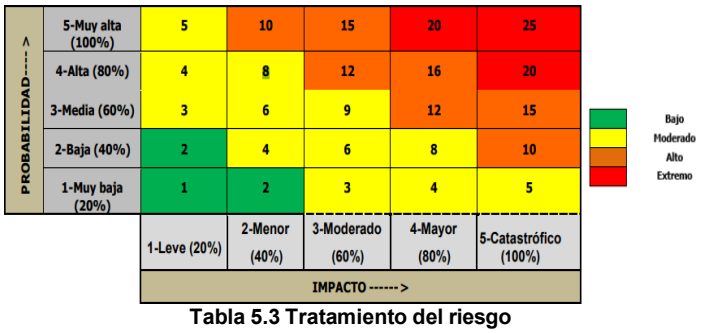

Tabla 5.3 Tratamiento del riesgo

ZONA DE RIESGO	OPCIONES DE TRATAMIENTO DEL RIESGO
Baja	Asumir el riesgo Se administrará a través de las actividades del proceso, proyecto o plan. Se debe adelantar un monitoreo semestralmente por parte de los líderes de proceso con el fin de verificar que estos riesgos no surten cambios en su aceptación que requiera la implementación de actividades de control. El reporte de su gestión se registrará en la herramienta determinada por el proceso.
Moderada	Reducir el riesgo Implementación de acciones de control preventivas que permitan reducir la probabilidad. Su monitoreo se realizará cuatrimestralmente por los líderes de proceso y sus equipos de trabajo con el fin de verificar que estas mitigan la materialización del riesgo identificado, se registrará en la herramienta determinada por el proceso.
Alta y Extrema	Manejo a través del mapa de riesgos del proceso e institucional, estableciendo acciones preventivas. Su monitoreo se realizará trimestralmente por parte de los líderes de proceso y la ejecución de esta actividad se registrará en la herramienta determinada por el proceso.

Tabla 5.4 Tratamiento de riesgo

Se relacionan las actividades que se deben realizar con el objeto de prever, mitigar o eliminar los posibles riesgos conocidos:

No	Actividad	Elementos	Resultado
1	Copias de seguridad de la información y documentos residentes en las carpetas compartidas de las diferentes áreas.	Documentos en formatos Word, Excel, PDF e imágenes.	Copias de seguridad, incremental diaria y un full semana a cinta de todos los documentos.
2	Copias de seguridad de los sistemas de información y base de datos.	Aplicaciones WEB e Intranet ERP/ERPC del Canal. Aplicaciones y bases de datos de los procesos y archivos.	Copias de seguridad, incremental diaria y un full semana a cinta de toda la información.
3	Mantener pólizas de seguros vigentes, contra todo riesgo los equipos y bienes, asegurándose por el valor real.	Equipos electrónicos, eléctricos, portátiles, móviles y equipos de comunicación.	Póliza vigente contra todo riesgo de daño y/o pérdida física por cualquier cosa.
4	Mantenimientos preventivos y correctivos de equipos de cómputo y comunicación.	Equipos de cómputo y comunicación, periféricos, sistemas eléctricos, UPS.	Contratos anuales de mantenimiento, garantías vigentes.

Tabla 5.5 Actividades riesgos generales

Estrategias de Recuperación

- Para cada tipo de desastre, se desarrollarán estrategias y procedimientos específicos, tales como:
- Recuperación de datos: Implementación de copias de seguridad diarias/semanales de los datos clave.
- Plan de contingencia para el personal: Procedimientos de evacuación y protocolos de seguridad para empleados.
- Recuperación de infraestructura tecnológica: Reemplazo o reparación de hardware y recuperación de software y bases de datos.
- Alternativas para las operaciones: Implementar estrategias de trabajo remoto o en sitios

alternativos.

5.3. Plan de Acción

El plan de acción detallado debe incluir:

- **Activación del plan:** Procedimientos para declarar una emergencia y activar el DRP.
- **Rol de los equipos de respuesta:** Establecer responsabilidades claras para los equipos de respuesta ante desastres (comunicación, tecnología, logística, etc.).
- **Recuperación operativa:** Procedimientos para restaurar operaciones clave dentro de un período específico.
- **Restauración de servicios:** Recuperación de servicios esenciales (como comunicaciones, servidores, etc.).
- **Evaluación post-desastre:** Evaluación del impacto, lecciones aprendidas y ajustes al plan.

5.3.1. Casos de Emergencia

Las actividades que se deben realizar con el objeto de prever, mitigar o eliminar los riesgos conocidos para el área de Gestión TIC. Así mismo se informa el procedimiento a seguir en el evento en que fallen equipos críticos al interior de Canal Capital.

5.3.1.1. Ausencia o falla del servicio de internet

Actualmente se cuenta con un canal dedicado de internet de 250 MB con el ISP Cirion y canal de respaldo dedicado de internet de contingencia de 100 MB, con el proveedor Liberty Networks. Para garantizar una alta disponibilidad del servicio que presta Canal Capital a la ciudadanía.

a. Garantías de conectividad:

Se cuenta con un canal principal de Internet de 250 MB y un canal de respaldo de 100 MB para garantizar la disponibilidad del servicio.

b. Posibles causas y soluciones:

Fallo del Proveedor de Servicios de Internet (ISP):

- Verificación del estado del servicio: Contactar al ISP para identificar si la falla es por mantenimiento, interrupciones o problemas técnicos.
- Consulta de incidencias: Revisar alertas emitidas por el ISP.
- Tiempos de resolución: Solicitar al ISP un estimado para la restauración del servicio.

5.3.1.2. Problemas de Hardware o Red Interna Problemas de Hardware o Red Interna

- Reiniciar equipos de red: Reinicia los routers, switches o módems para descartar problemas temporales o errores de configuración que puedan haber causado la falla.
- Verificar el estado de los cables y conexiones: Comprobar que todos los cables de red y dispositivos (módem, routers, switches) estén correctamente conectados y funcionando.
- Verificar la configuración del router: Revisar las configuraciones del router o gateway para

asegurarse de que esté recibiendo correctamente las direcciones IP, configuraciones de NAT y demás parámetros.

- Revisar los registros de eventos: Consultar los logs del router o módem para detectar posibles errores o fallos de conexión.

5.3.1.3. Problemas de Configuración de Red

- Revisar la configuración de DNS: Asegurarse de que los servidores DNS están configurados correctamente. Si es necesario, probar configurando los DNS de Google (8.8.8.8 y 8.8.4.4) o los de Cloudflare (1.1.1.1).
- Verificar la puerta de enlace predeterminada: Asegurarse de que la puerta de enlace predeterminada está configurada correctamente en los dispositivos de red.
- Revisar configuraciones de firewall o filtrado de tráfico: Verificar que el firewall de la red o el dispositivo de seguridad no esté bloqueando el tráfico saliente.

5.3.1.4. Fallo de Equipos de Acceso

- Reemplazo de hardware defectuoso: Si un dispositivo de acceso (como un router, módem o switch) está fallando, reemplazarlo por uno de repuesto si está disponible.
- Uso de equipo de respaldo: Si la organización dispone de equipos de respaldo para la conectividad, como un módem o router de repuesto, utilizarlo temporalmente mientras se diagnostica el problema.

a. Recuperación Completa:

- Restaurar configuraciones desde copias de seguridad.
- Probar conectividad global y monitorear estabilidad.

5.3.2. Fallos Específicos en Infraestructura:

5.3.2.1. Switch Core, Distribución y Acceso:

- Verificar alimentación, enlaces y configuraciones.
- Reiniciar o redirigir el tráfico si no hay recuperación inmediata.
- Utilizar switches de respaldo si el equipo está defectuoso.

5.3.2.2. Falla del Firewall:

- **Diagnóstico de la falla:** Identificar si la causa es un error de hardware, software o una configuración incorrecta. Para esto, puede ser necesario revisar los logs del firewall y realizar pruebas de diagnóstico.
- **Reinicio del firewall:** En algunos casos, un simple reinicio o restablecimiento a la configuración predeterminada puede resolver el problema temporalmente.
- **Restauración de la configuración:** Si el firewall está funcionando, pero la configuración se ha perdido o corrompido, restaurar una copia de seguridad de la configuración previa.
- **Sustitución de hardware:** Si se confirma que el fallo es de hardware, proceder a reemplazar el firewall defectuoso por uno nuevo o utilizar una solución temporal hasta

que se recupere el dispositivo original.

- **Actualización del firmware:** En caso de que la falla esté relacionada con una vulnerabilidad de seguridad, actualizar el firmware del firewall a la versión más reciente disponible.
- **Validación de la configuración:** Tras la restauración, verificar que las reglas de seguridad del firewall estén configuradas correctamente y que no haya riesgos de exposición.
- Contactar al fabricante para soporte técnico.

5.3.2.3. Falla en Servidores Virtuales:

- **Reiniciar la máquina virtual:** Intentar reiniciar la máquina virtual desde el hipervisor para descartar problemas temporales en el sistema operativo de la VM.
- **Verificar la integridad del sistema operativo de la VM:** Si la máquina virtual no arranca, acceder a la consola de la VM para diagnosticar el sistema operativo (en busca de errores en el arranque, corrupción de archivos, etc.).
- **Reparación del sistema operativo:** Si se detecta un problema en el sistema operativo (por ejemplo, corrupción de archivos), proceder con la reparación utilizando herramientas como el arranque en modo seguro o la restauración de imágenes del sistema operativo.
- **Verificación del almacenamiento:** Comprobar que el almacenamiento virtual (discos virtuales) esté disponible y sin errores. Si hay problemas con el disco, intentar reparar o recuperar los archivos dañados.

5.3.2.4. Recuperación Completa

Si la falla no puede resolverse rápidamente o si la máquina virtual está irremediablemente dañada, es necesario restaurar la máquina virtual desde una copia de seguridad.

5.3.2.5. Falla del Servicio Wi-Fi

- **Fallo del hardware:** Daños en los puntos de acceso Wi-Fi (AP), controladores o switches que gestionan la red Wi-Fi.
- **Problemas de configuración:** Errores en la configuración de los puntos de acceso, como cambios en los parámetros de red (SSID, VLAN, etc.), autenticación incorrecta, o problemas con la asignación de direcciones IP.
- **Interferencia de señal:** Interferencia externa (como dispositivos electrónicos cercanos) que afecta la señal Wi-Fi.
- **Problemas con el servidor DHCP:** El servidor que asigna direcciones IP a los dispositivos conectados puede estar fallando.
- **Problemas con el acceso al servidor de autenticación:** Si se utiliza un servidor RADIUS u otro sistema de autenticación, un fallo en el acceso o la configuración de este servidor puede interrumpir el servicio Wi-Fi.

a. Estrategia de Recuperación

A continuación, se describe un enfoque paso a paso para la recuperación del servicio Wi-Fi en

caso de fallo.

b. Respuesta Inmediata a la Falla

- **Confirmar la falla:** Verificar que la falla del Wi-Fi afecta a varios usuarios o dispositivos dentro de la organización, y no a un único dispositivo o área.
- **Realizar pruebas de conexión:** Intentar conectar diferentes dispositivos al Wi-Fi en diversas áreas para confirmar que el problema es generalizado.
- **Verificar la conectividad:** Comprobar si los dispositivos son capaces de detectar la red Wi-Fi y, si es así, si pueden obtener una dirección IP o establecer la conexión correctamente.
- **Notificar al equipo de TI:** Informar al equipo de soporte técnico, redes e infraestructura sobre la interrupción del servicio Wi-Fi. Si se cuenta con una herramienta de monitoreo de red, revisarla para obtener más detalles.

c. Comprobar el estado de los puntos de acceso:

- **Revisar las luces de los puntos de acceso (APs):** Asegurarse de que los APs estén encendidos y funcionando. Si no lo están, comprobar si hay un problema de alimentación o si el dispositivo está fuera de servicio.
- **Comprobar si los APs están sobrecargados:** Verificar si algunos APs están sobrecargados con demasiados dispositivos conectados, lo cual podría estar afectando el rendimiento o la conectividad.

d. Verificar la red interna:

- **Revisar los switches y routers:** Asegurarse de que los equipos de red que gestionan el tráfico del Wi-Fi, como switches, routers o controladores Wi-Fi, estén funcionando correctamente y que no haya interrupciones en el tráfico de red.

e. Diagnóstico y Resolución

Fallo de Hardware (Punto de Acceso Wi-Fi o Equipos de Red)

- **Reiniciar los puntos de acceso:** Si los puntos de acceso Wi-Fi no están funcionando correctamente, reiniciarlos para ver si el problema se resuelve. En algunos casos, el reinicio de los equipos puede solucionar problemas temporales de conexión.
- **Reemplazar puntos de acceso defectuosos**: Si un punto de acceso está dañado o defectuoso, reemplazarlo por uno de repuesto. Asegúrate de que los nuevos puntos de acceso estén correctamente configurados y funcionando.
- **Comprobar el controlador Wi-Fi:** Si el sistema de Wi-Fi está gestionado por un controlador central (en lugar de puntos de acceso autónomos), verificar si el controlador está operativo y realizando la gestión adecuada de los puntos de acceso.

f. Problemas de Configuración

- **Verificar la configuración de la red Wi-Fi:** Asegurarse de que el SSID (nombre de

la red) y la configuración de seguridad (contraseña, protocolo de cifrado) sean correctos.

- **Confirmar que los parámetros de red** (por ejemplo, VLAN, DNS) están configurados adecuadamente.
- **Verificar el servidor DHCP:** Asegurarse de que el servidor DHCP (si se usa) esté funcionando correctamente y que tenga suficiente capacidad para asignar direcciones IP a los dispositivos conectados. Si el servidor DHCP no está respondiendo, reiniciarlo o, si es necesario, cambiar a un servidor DHCP de respaldo.

g. Interferencia de Señal

- **Cambiar el canal de Wi-Fi:** Si la red Wi-Fi está experimentando interferencias debido a otras redes o dispositivos (microondas, teléfonos inalámbricos, etc.), cambiar el canal de la red Wi-Fi para evitar la congestión del canal. Utilizar herramientas de análisis de espectro o Wi- Fi para identificar interferencias.
- **Optimización de la colocación de puntos de acceso:** Revisar la ubicación de los puntos de acceso para asegurarse de que cubren adecuadamente las áreas de la oficina o la red, evitando zonas muertas o interferencias físicas (como paredes gruesas).

h. Problemas con el Servidor de Autenticación (RADIUS u Otros)

- **Verificar el servidor de autenticación:** Si se utiliza un servidor de autenticación (como RADIUS), comprobar que esté operativo y que los dispositivos puedan autenticarse correctamente en la red Wi-Fi.
- **Revisar las políticas de acceso:** Verificar que las políticas de acceso Wi-Fi (por ejemplo, 802.1X) no hayan cambiado o no estén impidiendo la autenticación de los usuarios.

i. Recuperación Completa

- **Restaurar configuración desde copia de seguridad**: Si la falla se debe a una pérdida de configuración o un error en la misma, restaurar la configuración de los puntos de acceso o del controlador Wi-Fi desde una copia de seguridad reciente.
- **Verificar la conectividad completa:** Una vez que los problemas se hayan resuelto, realizar pruebas de conectividad en todas las áreas de la red Wi-Fi para asegurar que todos los dispositivos puedan conectarse correctamente.
- **Monitorear la red:** Implementar monitoreo de red en tiempo real para garantizar que no haya problemas adicionales y que el servicio Wi-Fi sea estable.

j. Estrategias de Monitoreo y Prevención:

- Implementar monitoreo continuo de red para detectar problemas a tiempo.
- Mantener copias de seguridad actualizadas y equipos de respaldo funcionales.

6. Escalamiento Interno

A continuación, se relacionan los nombres y números telefónicos de los responsables del área de Gestión TIC, y los correspondientes turnos.

El Profesional Especializado de Gestión TIC, a su vez informará al Subdirector/a Administrativo/a de la entidad, los hechos y el estado actual de la situación, con el fin de que se escale la información hasta el Secretario/a General y a su vez al Gerente, y de esta manera tener informado a los directivos de los hechos ocurridos.

- **Nivel 1 – Operativo / Primera Respuesta**

  Responsables de ejecutar acciones inmediatas, diagnóstico inicial, registro del incidente y contención temprana.

Rol / Persona	Función en el BCP
Soporte Calle 69 – Jose Miguel Bulla	Soporte presencial, diagnóstico inicial de fallas en sitio.
Soporte Calle 26 – Andrés Díaz	Soporte técnico en sede, incidentes de hardware y conectividad local.
Desarrolladores Senior – Emerson Galeano, Jhoan Ospina, Néstor Camilo Beltrán	Respuesta inicial a fallas de aplicaciones, logs, errores transaccionales.
QA y Documentación – Edith Lisseth Rincón	Revisión inicial de documentación y evidencias del incidente.
Infraestructura Local – Ing. Germán Darío Fajardo	Problemas de red local, cableado, switches, energía.
Infraestructura Cloud – Ing. Eduardo Carlos Cetina	Servicios en la nube, conectividad remota, máquinas virtuales.
Infraestructura Redes – Ing. Ángela Vanessa Cárdenas	Enrutamiento, VPN, Firewalls, conectividad WAN.
Ingeniero de Sistemas – Ing. Luis Arturo Díaz	Diagnóstico inicial de incidentes funcionales en sistemas.
Oficial de Seguridad de la Información – Ing. Juan David Poveda	Incidentes de ciberseguridad o pérdida de confidencialidad/ disponibilidad.

- **Nivel 2 – Coordinación Técnica / Contingencia**

Responsables de activar el plan de continuidad o contingencias internas, asignar recursos y coordinar equipos del Nivel 1.

Rol / Persona	Función en el BCP
Dueño de Producto – Ing. Robinson Enrique Rincón	Prioriza incidentes críticos de aplicaciones, coordina con desarrolladores.
Oficial de Seguridad – Ing. Juan David Poveda	Activación de protocolos de seguridad (ISO 27001, MSPI).
Infraestructura Cloud / Redes / Local – Ingenieros especializados	Contención avanzada, activación de redundancias, restauraciones parciales.
Apoyo a la Gestión – Juliana Valentina Díaz	Apoyo documental, comunicaciones internas, seguimiento.

- **Nivel 3 – Dirección y Toma de Decisiones Estratégicas**

Aprueba activación oficial del BCP, comunica a la Alta Dirección y coordina con áreas externas.

Rol / Persona	Función en el BCP
Profesional Especializado – Ing. Laura Marcela Perdomo Fonseca	Responsable final del BCP en TIC. Declara incidentes mayores, activa planes de recuperación, gestiona comunicación con la Alta Gerencia del Distrito y entes de control.

6.1. Matriz de Escalamiento Operacional

Tipo de Incidente	Nivel 1 – Responsable Inicial	Tiempo para Escalar	Nivel 2 – Escalamiento	Nivel 3 – Escalamiento Final
Falla de usuario / equipos de oficina	Soporte 60 / Soporte 26	30 min	Infraestructura Local	Profesional Especializado TIC
Caída de red local	Infraestructura Local	20 min	Infraestructura Redes	Profesional Especializado TIC
Caída de Internet / VPN	Redes	15 min	Cloud / Seguridad	Profesional Especializado TIC
Fallas en servidores locales	Infraestructura Local	15 min	Cloud / Redes	Profesional Especializado TIC
Falla en servicios cloud	Infraestructura Cloud	15 min	Seguridad / Coordinación TIC	Profesional Especializado TIC
Fallas en aplicaciones	Desarrolladores	30 min	Dueño de Producto	Profesional Especializado TIC
Incidente de ciberseguridad	Seguridad	Inmediato	Coordinación Técnica / Cloud	Profesional Especializado TIC
Pérdida de información	Seguridad / Infraestructura	10 min	Dueño de Producto	Profesional Especializado TIC
Interrupción mayor de servicios (≥2 sedes)	Redes / Local	10 min	Seguridad / Coordinación	Profesional Especializado TIC
Interrupción total de servicios críticos	Seguridad / Cloud	Inmediato	Coordinación Integrada TIC	Profesional Especializado TIC (Activa BCP)

7. Normatividad asociada al Plan

ISO/IEC 22301:2019 (Sistema de Gestión de la Continuidad del Negocio)

- **Descripción:** Esta norma internacional establece los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de la continuidad del negocio. Abarca la gestión de crisis, la gestión de riesgos y la recuperación ante desastres.
- **Relevancia:** La norma ISO/IEC 22301 es fundamental para asegurar que el DRP esté alineado con las mejores prácticas internacionales en cuanto a la continuidad de los negocios y la recuperación ante desastres.
- **Objetivo:** Garantizar que una organización sea capaz de continuar operando durante una crisis o después de un desastre, restaurando sus servicios críticos en el menor tiempo posible.

ISO/IEC 27001:2013 (Sistema de Gestión de Seguridad de la Información)

- **Descripción:** Establece los requisitos para implementar un sistema de gestión de seguridad de la información (SGSI) dentro de una organización. La norma cubre la identificación de riesgos, el tratamiento y la mitigación de esos riesgos, y la protección de la confidencialidad, integridad y disponibilidad de la información.
- **Relevancia:** Un DRP eficaz debe estar alineado con la protección de la información sensible y la continuidad operativa, que es un aspecto clave en la seguridad de la información. Además, esta norma es utilizada por organizaciones que gestionan datos críticos y requieren protección ante desastres.
- **Objetivo:** Asegurar que la infraestructura crítica de TI y los sistemas de información estén protegidos durante un desastre, y que los datos puedan ser restaurados rápidamente.

NIST SP 800-34 (Planificación de la Continuidad del Negocio y Recuperación ante Desastres)

- **Descripción:** Publicado por el National Institute of Standards and Technology (NIST), este documento proporciona un enfoque detallado para la planificación de la continuidad del negocio y la recuperación ante desastres en organizaciones de todos los tamaños.
- **Relevancia:** NIST SP 800-34 es una de las guías más completas para la creación y ejecución de planes de recuperación ante desastres, cubriendo aspectos técnicos, operacionales y organizacionales.
- **Objetivo:** Ayudar a las organizaciones a mantener la continuidad de los servicios esenciales ante un desastre, detallando pasos claros para la recuperación y los recursos necesarios.

BS 25999 (British Standard for Business Continuity Management)

- **Descripción:** Es una norma británica que proporciona un marco para la gestión de la continuidad del negocio y la recuperación ante desastres, con un enfoque en la creación, implementación y mantenimiento de un sistema de gestión de continuidad empresarial.
- **Relevancia:** Aunque ha sido reemplazada parcialmente por la ISO 22301, BS 25999 sigue siendo relevante como un conjunto de directrices para gestionar la recuperación ante desastres, especialmente en el contexto de las organizaciones británicas.
- **Objetivo:** Ofrecer un conjunto claro de buenas prácticas para la continuidad del negocio y recuperación ante desastres, ayudando a las organizaciones a proteger sus operaciones críticas.

Normas Relacionadas con la Infraestructura y Tecnologías de la Información ITIL

(Information Technology Infrastructure Library)

- **Descripción:** ITIL es un conjunto de mejores prácticas para la gestión de servicios de TI, que incluye procesos para la continuidad del servicio, la gestión de incidentes y la recuperación ante desastres.
- **Relevancia:** ITIL ofrece una estructura para gestionar el ciclo de vida de los servicios de TI, y dentro de su marco, incluye procedimientos para la recuperación ante desastres que ayudan a restaurar los servicios tecnológicos críticos de manera eficiente.
- **Objetivo:** Asegurar la continuidad de los servicios de TI mediante la implementación de procedimientos efectivos de gestión de incidentes, gestión de cambios y planificación de la continuidad.