



Plan de Continuidad del Negocio (PCN) Alcaldía de Cartagena

**Componente de Tecnologías de la
Información**



Tabla de Contenido

1. Introducción	2
2. Objetivos	3
Objetivo General	3
Objetivos Específicos	3
3. Alcance	4
4. Marco Normativo para el Plan de Continuidad del Negocio (PCN)	6
5. Preparación de las TIC para la Continuidad del Negocio - IRBC	8
6. Planificación:	9
Análisis de Impacto al Negocio (BIA) con Enfoque en las TIC de la Alcaldía de Cartagena	16
Identificación de Procesos Críticos	18
Revisión del Marco Normativo y Estratégico	18
Análisis Modelo de Operación por Procesos de la Alcaldía de Cartagena de Indias.	19
Mapeo de dependencias TIC:	27
Análisis de Riesgos Potenciales	1
Planes de Respuesta a Incidentes y Gestión de Crisis	6
Componentes del Plan de Respuesta a Incidentes	6
Componentes del Plan de Gestión de Crisis	7
Pruebas y Ejercicios de Continuidad	9
Tipos de Prueba	9
Escenarios de Prueba	10
Planificación de Pruebas	10
Pasos Para Implementar Pruebas y Ejercicios	10
Mantenimiento y Mejora Continua	11
Roles y Responsabilidades	11
Indicadores Clave de Desempeño (KPIs) del Plan de Continuidad del Negocio	12
Cronograma de Mantenimiento del Plan de Continuidad del Negocio	12

1. Introducción

La Alcaldía de Cartagena, como ente gubernamental que lidera el desarrollo administrativo, social y económico del Distrito Turístico y Cultural, tiene la responsabilidad de garantizar la continuidad en la prestación de servicios esenciales a los ciudadanos. En un entorno donde la dependencia de las Tecnologías de la Información y las Comunicaciones (TIC) es cada vez más crítica, resulta indispensable contar con mecanismos que permitan mitigar los riesgos asociados a interrupciones inesperadas y asegurar la operatividad de los procesos clave.

El Plan de Contingencia del Negocio (PCN) tiene como objetivo principal establecer estrategias y acciones que permitan a la Alcaldía de Cartagena prevenir, responder y recuperarse de eventos que puedan afectar la continuidad de sus servicios TIC. Este plan está alineado con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y se fundamenta en las mejores prácticas internacionales en gestión de riesgos, continuidad del negocio y seguridad de la información. El PCN abarca todas las dependencias y procesos críticos que dependen de las TIC para su funcionamiento, identificando riesgos potenciales, analizando su impacto y definiendo los tiempos y recursos necesarios para su recuperación. Además, promueve una cultura organizacional orientada a la resiliencia, integrando medidas de planificación, implementación, monitoreo y mejora continua.

Este documento no solo busca salvaguardar la operatividad de la Alcaldía ante contingencias, sino también fortalecer la confianza de la ciudadanía en los servicios públicos, contribuyendo al desarrollo sostenible de Cartagena.

2. Objetivos

Objetivo General

Garantizar la continuidad operativa de los servicios y procesos críticos de la Alcaldía de Cartagena mediante la implementación de estrategias de recuperación, gestión de riesgos, y aseguramiento de las Tecnologías de la Información y las Comunicaciones (TIC), minimizando los impactos ante eventos disruptivos y fortaleciendo la confianza de la ciudadanía.

Objetivos Específicos

- Analizar las capacidades de infraestructura tecnológica con la que cuenta la Alcaldía de Cartagena, como preparación para desarrollar el Plan de Continuidad del negocio.
- Identificar los procesos misionales y estratégicos que dependen de las TIC, mapeando sus interdependencias y clasificando su criticidad para priorizar esfuerzos de continuidad.
- Establecer tiempos y puntos objetivos de recuperación (RTO y RPO) para procesos y sistemas críticos, definiendo procedimientos claros que garanticen una pronta restauración de los servicios ante incidentes.
- Implementar medidas preventivas y soluciones de respaldo para asegurar la disponibilidad de sistemas, minimizar los riesgos tecnológicos, y garantizar la resiliencia operativa.
- Desarrollar capacidades internas mediante capacitaciones y simulacros regulares, asegurando que el personal esté preparado para ejecutar el plan eficazmente y se fomente una cultura de prevención.

3. Alcance

El **Plan de Continuidad del Negocio de las TIC** de la Alcaldía de Cartagena abarca todos los procesos, servicios, infraestructuras y sistemas tecnológicos que son esenciales para garantizar la operatividad de las funciones misionales, estratégicas y de apoyo del nivel central de la Entidad. Este plan define las estrategias, procedimientos y recursos necesarios para prevenir, responder y recuperarse de incidentes disruptivos que puedan afectar la continuidad de los servicios tecnológicos.

4. Glosario:

Gestión Federada de Recursos (Multi-Site Federation)

Es un modelo de administración unificada entre dos o más centros de datos, permitiendo controlar todos los recursos tecnológicos (máquinas virtuales, redes, almacenamiento) desde una misma consola. Facilita la recuperación y movilidad de servicios entre sitios.

Túneles Seguros

Son conexiones cifradas que permiten enviar datos sensibles entre dos puntos a través de redes públicas o privadas de forma segura. Se usan para proteger la información y asegurar la continuidad del servicio entre data centers.

L2VPN (Layer 2 Virtual Private Network)

Tecnología que extiende una red local (LAN) entre sitios geográficos diferentes. Permite que máquinas virtuales en distintos centros de datos compartan el mismo espacio de red, facilitando la migración o recuperación de servicios sin reconfiguración.

vCloud Director (vCD)

Plataforma de gestión de entornos virtuales multicliente basada en VMware. Permite crear, administrar y controlar recursos en la nube de manera centralizada.

vCenter

Herramienta de administración de VMware que supervisa los servidores físicos (hosts) y las máquinas virtuales. Gestiona tareas como balanceo de carga, actualizaciones, backups y migración de servicios.

ESXi Host

Servidor físico que aloja y ejecuta máquinas virtuales mediante el hipervisor ESXi de VMware. Conformar la infraestructura base sobre la que se operan los servicios virtualizados.

Plan de Continuidad del Negocio (PCN)

Es una estrategia organizacional que tiene como objetivo garantizar que los procesos críticos de una entidad pública continúen operando ante situaciones adversas, tales como fallos tecnológicos, desastres naturales o ataques cibernéticos. Incluye análisis de impacto, gestión de riesgos, estrategias de recuperación y protocolos de respuesta a incidentes.

BIA (Business Impact Analysis):

Proceso que permite identificar y evaluar el impacto que tendría la interrupción de procesos, servicios o sistemas críticos en el cumplimiento de las funciones institucionales.

DRP (Disaster Recovery Plan)

Es un subconjunto del Plan de Continuidad del Negocio enfocado exclusivamente en la recuperación tecnológica. El DRP contiene procedimientos detallados para restaurar sistemas de TI, bases de datos, aplicaciones y redes tras un evento disruptivo, asegurando la restauración de servicios en el menor tiempo posible.

RPO (Recovery Point Objective)

Es el punto máximo de pérdida de datos tolerable, medido en tiempo. Indica cuánto tiempo atrás puede recuperarse la información sin afectar significativamente las operaciones. Por ejemplo, un RPO de 1 hora implica que se pueden perder hasta 60 minutos de datos.

RTO (Recovery Time Objective)

Es el tiempo máximo aceptable que un proceso, sistema o servicio puede estar inactivo tras una interrupción. Representa el límite para restaurar la funcionalidad antes de que se generen impactos críticos en la entidad.

5. Marco Normativo para el Plan de Continuidad del Negocio (PCN)

Normas y Políticas	Detalle y Aplicabilidad
Ley 1581 de 2012 - Protección de Datos Personales	Establece las directrices para la protección de la información personal en Colombia. En el contexto de TIC, el plan debe garantizar que los datos personales y la información sensible de los ciudadanos sean protegidos durante cualquier incidente o crisis. Esto implica: • Cifrado de datos. • Políticas de acceso restringido a información. • Procedimientos para asegurar la integridad de la información.
Ley 1341 de 2009 - Ley TIC	Esta ley establece el marco de las Tecnologías de la Información y las Comunicaciones en Colombia. El Plan de Continuidad de TIC debe cumplir con sus directrices, en particular: • La infraestructura tecnológica debe ser adecuada para garantizar la continuidad de los servicios públicos.
Resolución 5398 de 2016 - MinTIC (Política de Gestión de Riesgos en el Ámbito TIC)	El MinTIC establece en esta resolución políticas de gestión de riesgos asociados a las tecnologías de la información y las comunicaciones. El PCN debe alinearse con estas políticas, que incluyen: • Identificación y evaluación de riesgos. • Definición de planes de contingencia y recuperación. • Implementación de medidas para reducir los impactos de los riesgos identificados.
Resolución 1518 de 2010 - MinTIC (Planes de Continuidad del Negocio para el Sector Público)	Esta resolución obliga a las entidades públicas a contar con un plan de continuidad del negocio en el ámbito de las TIC. Esta normativa establece los requisitos para: • El diseño y ejecución de planes de continuidad. • La capacitación del personal encargado de la gestión de crisis. • La evaluación de la infraestructura tecnológica y su capacidad para operar de forma continua.
Ley 1712 de 2014 - Ley de Transparencia y Acceso a la Información Pública Nacional	El acceso a la información pública debe ser garantizado por la Alcaldía, incluso en situaciones de crisis. El plan debe prever mecanismos para asegurar la disponibilidad de la información pública en todo momento.
Decreto 4912 de 2011 - Política Nacional de Ciberseguridad	Este decreto establece lineamientos para la protección de la infraestructura tecnológica contra ciberataques y otras amenazas cibernéticas. El plan de continuidad debe:



ISO 22301:2019 - Sistema de Gestión de la Continuidad del Negocio	• Incorporar medidas de seguridad cibernética. • Prever protocolos ante incidentes de seguridad informática. Esta norma establece los requisitos para la implementación de un sistema de gestión de continuidad del negocio. En el contexto del PCN, se deben seguir las mejores prácticas en: • Gestión de riesgos. • Diseño de planes de continuidad. • Ejecución de simulacros de recuperación. • Mantenimiento del sistema de gestión.
ISO 27001:2013 - Sistema de Gestión de Seguridad de la Información	El PCN debe garantizar la integridad, confidencialidad y disponibilidad de la información, lo que incluye la implementación de controles de seguridad basados en la ISO 27001, que establece requisitos específicos para: • Gestión de accesos. • Protección ante ciberataques. • Gestión de incidentes de seguridad.
ISO 27031:2011 - Directrices para la Continuidad de las Tecnologías de la Información	Esta norma está enfocada en la continuidad de los servicios tecnológicos en situaciones de crisis. Asegura que los servicios TIC de la Alcaldía sigan operando en caso de interrupciones, a través de medidas como: • Respaldo de infraestructura. • Planificación de recuperación ante desastres.
Política de Gestión y Desempeño de Gobierno Digital	Tiene como objetivo la mejora de la administración pública mediante el uso de tecnologías digitales, garantizando la continuidad de los servicios gubernamentales.
Decreto 1081 de 2015 (Art. 2.2.2.1.1) - Política de Gestión de TIC para el Sector Público	Establece las condiciones para la gestión efectiva de las TIC en el sector público, incluyendo la obligatoriedad de tener planes de contingencia en los sistemas críticos del gobierno, como los servicios que dependen de la infraestructura tecnológica. Promueve la transparencia y el buen uso de los recursos públicos, lo cual incluye la correcta gestión de los sistemas de información en la Alcaldía.
Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC)	Reglas aplicables al uso y gestión de TIC en entidades públicas.
Circular 001 de 2022 del MinTIC	Directrices para implementar medidas de ciberseguridad y continuidad operativa
Ley 2052 de 2020 (Gobierno Digital)	Enfoque en la prestación de servicios digitales continuos y seguros.

6. Preparación de las TIC para la Continuidad del Negocio – IRBC

Para desarrollar el Plan de Continuidad del Negocio de la Alcaldía Mayor de Cartagena, se aplicarán los lineamientos establecidos por el Ministerio de la TIC en Colombia para la preparación de las TIC para la continuidad del negocio y el modelo de operación de seguridad y privacidad de la información, estableciendo acciones para desarrollar las cuatro (4) fases que comprenden dicho modelo, estas, contienen objetivos, metas y herramientas que permiten que la continuidad del negocio sea un sistema de sostenible dentro de las entidades.

La siguiente ilustración presenta el modelo de operación de seguridad y privacidad de la información MSPI, centrándonos únicamente en las fases de planificación, implementación, gestión y mejora continua, tal como lo indica el Mintic.



Ilustración 1. Modelo de operación seguridad y privacidad de la información. Fuente: Guía para la preparación de las TIC para la continuidad del negocio. MinTIC

De acuerdo con lo anterior, el Ministerio de las TIC, desarrolló el Marco Continuidad del Negocio para Seguridad y Privacidad de la Información, el cual comprende las siguientes actividades:

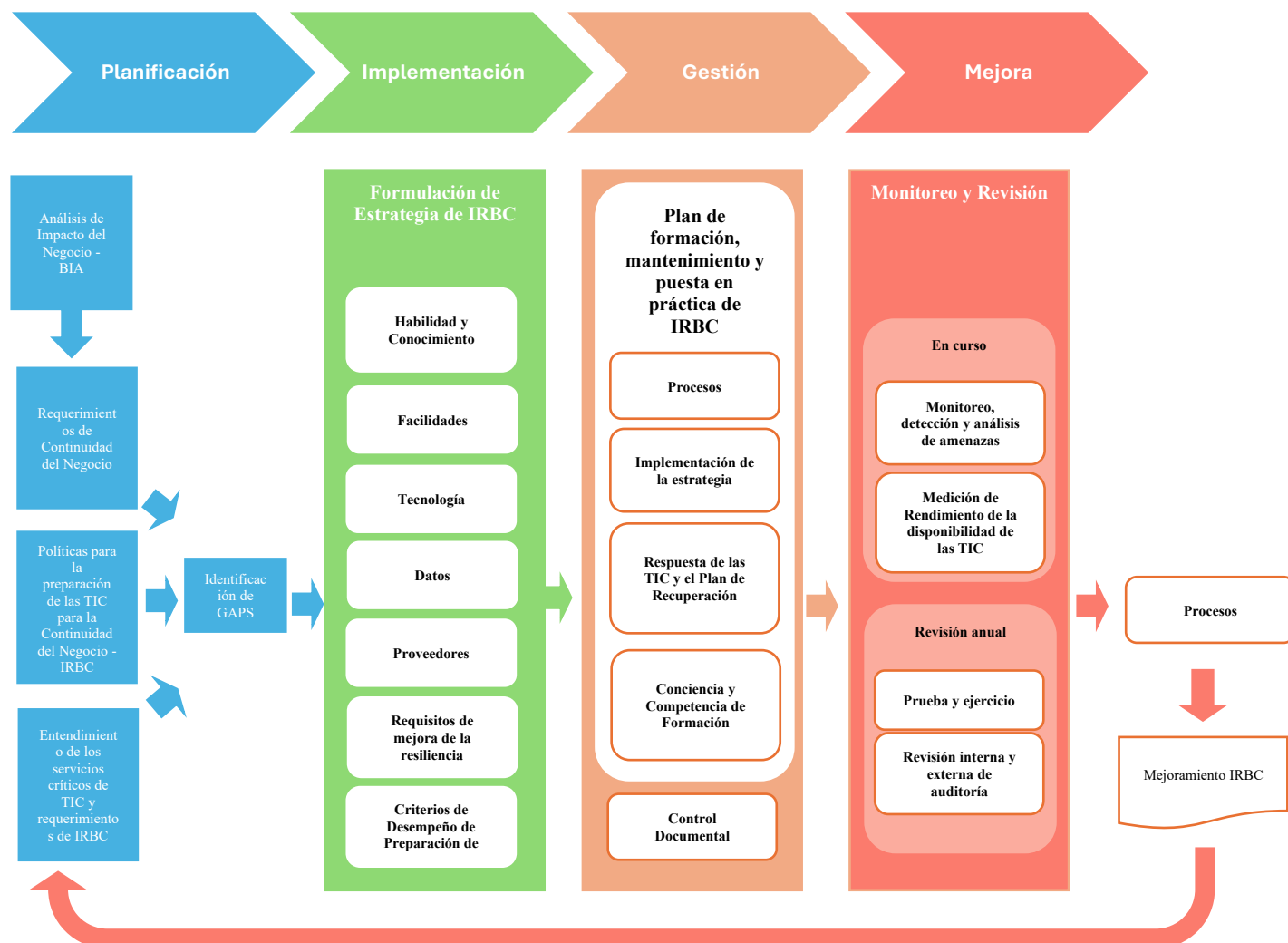


Ilustración 2. Marco Continuidad del Negocio para Seguridad y Privacidad de la Información. Fuente: Guía No. 10 - Guía para la preparación de las TIC para la continuidad del negocio. MINTIC. Diciembre de 2010.

7. Planificación:

Información Técnica y de Infraestructura: Insumos para el Plan de Continuidad del Negocio

Como parte fundamental de la preparación para el Análisis de Impacto al Negocio (BIA), se realiza la caracterización técnica de la infraestructura tecnológica que soporta los servicios y procesos de la Alcaldía de Cartagena. Este apartado ofrece una visión integral de los activos tecnológicos, aplicaciones, capacidades de recuperación y acuerdos de servicio, que permiten establecer la línea base para la continuidad del negocio.

Servidores y Dispositivos de Seguridad Perimetral

Los servidores y dispositivos de red constituyen el núcleo de la infraestructura tecnológica de la Alcaldía, ya que soportan la ejecución de aplicaciones institucionales, bases de datos, almacenamiento de información crítica y control de tráfico interno y externo.

Los servidores, en un entorno tradicional o virtualizado, permiten ejecutar múltiples procesos simultáneos que dan soporte a funciones misionales, estratégicas y administrativas. En contextos gubernamentales, estos equipos deben ser altamente disponibles, contar con mecanismos de respaldo automático y permitir la recuperación oportuna en caso de fallos.

En complemento, **los dispositivos de seguridad perimetral**, como los *firewalls*, aseguran el acceso autorizado a los sistemas, previenen ataques externos, filtran contenido malicioso y gestionan conexiones cifradas mediante VPN.

Análisis de Equipamiento Actual

La Alcaldía de Cartagena dispone de:

- ⇒ **64 servidores** orientados al soporte de almacenamiento, procesamiento masivo de datos, y ejecución de servicios de red institucional: 44 servidores en la sede del IASS (Infrastructure as a Service) y 20 servidores instalados en la sede Aduana.

Los servidores son el corazón de la infraestructura tecnológica de una entidad pública, ya que sobre ellos se soportan múltiples servicios críticos, como bases de datos, aplicaciones institucionales, almacenamiento de información y virtualización de entornos de trabajo. Su correcto funcionamiento es indispensable para asegurar la continuidad de los procesos administrativos, financieros, sociales y de salud que gestiona la Alcaldía de Cartagena.

Estos servidores operan como nodos principales del ecosistema TIC distrital, distribuyendo cargas de trabajo y alojando sistemas esenciales que no pueden interrumpirse sin afectar la operación institucional.

	Tipo de Elemento	Estado	Total
IASS	Base de datos	Encendido	4
	Directorio Activo	Encendido	2
	Servidor de Aplicaciones	Encendido	38
Aduana	Servidor de Aplicaciones	Encendido	20
Gran Total			64

- **Equipos Fortigate 100F, 200F, 60F, 400E y 600E**, distribuidos en sedes como Torices, Manga, Aduana, Dadis, Chiquinquirá, Santa Rita entre otros. Todos estos dispositivos cuentan con versiones recientes del firmware (7.2.x), lo cual garantiza actualizaciones de seguridad activas.

Cada dispositivo cuenta con un **nombre lógico de ubicación**, facilitando la gestión remota y el monitoreo centralizado.

Estos equipos cumplen funciones de *firewall*, segmentación de red, gestión de políticas de acceso, soporte para VPN y detección de amenazas en tiempo real. son fundamentales para garantizar la continuidad de los servicios críticos, como salud, hacienda pública, atención al ciudadano y sistemas institucionales transversales, se constituyen como una herramienta de seguridad muy completa, que ayuda a proteger la información y garantizar que los sistemas funcionen sin interrupciones.

La siguiente tabla detalla los dispositivos Fortigate implementados en las distintas sedes de la Alcaldía de Cartagena. Estos equipos están distribuidos estratégicamente para proteger la infraestructura tecnológica y garantizar la continuidad operativa de los servicios digitales.

Plataform	Firmware Version			Total
	7.2.10 build1706 (Mature)	7.2.8 build1639 (Mature)	7.2.9 build1688 (Mature)	
FortiGate-100F	3	2		5
FortiGate-200F	1	6		7
FortiGate-400E		1		1
FortiGate-600E		2		2
FortiGate-600F		1	1	2
FortiGate-60F		16		16
Total	4	28	1	33

Equipos de Conectividad y Red

La conectividad de red es uno de los pilares fundamentales para el funcionamiento continuo de los servicios digitales institucionales. La Alcaldía de Cartagena ha diseñado su infraestructura para garantizar estabilidad, velocidad y seguridad en la comunicación entre sedes, servidores y usuarios finales.

Switches FortiSwitch

Los switches gestionables FortiSwitch permiten una interconexión confiable entre los equipos de cómputo, servidores, impresoras, cámaras y demás dispositivos conectados en red. Su administración centralizada facilita el control de tráfico, la segmentación lógica mediante VLANs y la priorización de servicios críticos. Para ellos, se destacan las siguientes características técnicas:

- Modelos FortiSwitch 124 24XGE y 48XGE.
- Capacidad de integración con dispositivos Fortigate para gestión unificada.
- Instalación distribuida en más de 20 dependencias del Distrito.
- Relación directa con los sistemas de información institucionales ("impacta todos los sistemas").

Este conjunto de dispositivos constituye la **columna vertebral de la red interna** de la entidad, permitiendo un acceso eficiente a los sistemas de información y garantizando una base sólida para servicios como autenticación, correo, bases de datos, plataformas web y comunicaciones internas. Un switch gestionable permite:

- Conectar múltiples dispositivos (computadores, impresoras, servidores) dentro de la red institucional.
- Establecer políticas de calidad de servicio (QoS), priorizando el tráfico según la criticidad del servicio.
- Segmentar la red en VLANs (Redes Virtuales), lo cual mejora la seguridad y el rendimiento.
- Monitorear, gestionar y configurar remotamente el estado de la red, permitiendo detectar y resolver incidentes de forma proactiva.

Análisis de Equipamiento Actual

La Alcaldía ha implementado de forma masiva equipos **FortiSwitch modelo 124 24XGE**, un dispositivo de alta capacidad, diseñado para redes empresariales con alta demanda de conectividad y control de tráfico. Estas son sus características clave:

- 24 puertos Gigabit Ethernet para conexión de dispositivos.
- Integración nativa con firewalls FortiGate, permitiendo una gestión unificada de red y seguridad.
- Compatibilidad con redes de voz, datos y video.
- Configuración centralizada a través de FortiLink.

De acuerdo con el catálogo técnico, se registran **más de 220 switches FortiSwitch**, con ubicación en dependencias clave como:

- Secretaría de Hacienda
- DADIS (salud pública)
- ADUANA
- Centros administrativos descentralizados
- Infraestructuras educativas y sociales

Cada uno de estos dispositivos está identificado por su número de serie, placa de inventario, dependencia responsable y sistemas de información que impacta, siendo **"Todos los sistemas"** en la mayoría de los casos.

Esta cobertura garantiza la **interconexión eficiente y segura** entre las sedes, dependencias y sistemas digitales, lo cual es esencial para mantener la operación continua y estable de los servicios TIC.

Dependencias Más Críticas por Densidad de Conectividad

La densidad de conectividad puede medirse por la cantidad de switches instalados en cada sede o dependencia. Esta métrica refleja el volumen de usuarios, la complejidad de los servicios prestados y el nivel de interdependencia tecnológica, lo cual es clave para establecer prioridades dentro del Plan de Continuidad del Negocio.

A continuación, se presentan las principales dependencias con mayor número de switches registrados:

Dependencia	Cantidad de Switches
EN BODEGA - ALMACÉN	30
DADIS Fátima	22
T14	16
PORTUS	13
ADUANA	12
PISO 1 Secretaría de Hacienda	10
PISO 2 Secretaría de Hacienda	9
ALPES	8
Secretaría de Educación	8

Estas ubicaciones deben ser clasificadas como *zonas de alta prioridad*, ya que una interrupción en cualquiera de ellas podría afectar múltiples procesos misionales y servicios ciudadanos.

Equipos de Usuario Final

Los equipos de usuario final son los dispositivos a través de los cuales los funcionarios, contratistas y colaboradores acceden a los sistemas institucionales, ejecutan procesos administrativos y prestan servicios a la ciudadanía. Su disponibilidad, seguridad y capacidad técnica impactan directamente en la eficiencia operativa de la Entidad.

Computadores Institucionales

De acuerdo con el inventario, la Alcaldía de Cartagena dispone de un parque informático conformado por:

- Equipos **tipo desktop, low profile** y **mini tower**, utilizados en sedes técnicas y administrativas.

- Computadores **All-in-One** modernos, destinados principalmente a usuarios de atención directa.
- Equipos portátiles para personal operativo o con alta movilidad.

Especificaciones generales:

- Sistema operativo: Windows 10 Pro (64 bits).
- Procesadores: Intel Core i7 de tercera generación y AMD Ryzen 5.
- Memoria RAM: entre 4GB y 16GB.
- Asignación por dependencia: Aduana, Cascada, Secretaría de Educación, Archivo, entre otros.

Estos dispositivos son esenciales para el funcionamiento diario de trámites, seguimiento de programas sociales, gestión tributaria y otros procesos. Se requiere que estén contemplados en el Plan de Continuidad con mecanismos de respaldo de información local, perfiles móviles o sincronizados en la nube, además de estar integrados al dominio institucional para facilitar su administración remota.

Impresoras y Periféricos

Para la prestación de servicios y la ejecución de procesos, existen múltiples **impresoras de red**, distribuidas por sede y oficina. Se cuenta con:

- Modelos HP Enterprise como **E52645** y **E-62555**.
- Insumos compatibles como tóneres CF289X y CF237YC.
- Dependencias como **Aduana, Cascada, Archivo, Bazurto, Portus**, entre otras.

Estas impresoras están configuradas para uso compartido, con conectividad local o remota, y permiten la impresión de documentos oficiales, contratos, certificados y formularios.

Equipos en Sedes Desconcentradas

Además de la sede principal de la Alcaldía, se tienen múltiples sedes desconcentradas que cuentan con una infraestructura tecnológica significativa, especialmente en cuanto a equipos de usuario final. Estas sedes desempeñan funciones operativas, administrativas y de atención al ciudadano en distintas zonas del Distrito.

Distribución de Equipos de Cómputo por Sede

El inventario muestra las siguientes sedes con mayor concentración de equipos:

Sede o Ubicación	Cantidad de Equipos
Centro Administrativo EPM	409
Aduana	173
Alpes	158
Centro	131
Getsemaní	116

T14	116
T17	102
Espinal	89
Manga	73

Estas sedes representan nodos relevantes para la operación descentralizada de la entidad, y deben ser incluidas en las estrategias de respaldo, soporte y recuperación ante incidentes TIC.

Diagrama de Arquitectura de Cloud Data Center

El siguiente diagrama ilustra la arquitectura híbrida del Data Center de la Alcaldía de Cartagena, integrando componentes en sitio y en la nube. Esta arquitectura permite garantizar la continuidad de los servicios críticos mediante la distribución de cargas de trabajo, la replicación de datos y la implementación de mecanismos de seguridad y respaldo.

La infraestructura tecnológica se encuentra organizada en diferentes capas:

- **Capa de acceso:** conformada por ciudadanos, servidores públicos y contratistas, quienes acceden a los sistemas institucionales desde diferentes ubicaciones.
- **Capa de red:** incluye switches gestionables FortiSwitch, dispositivos de seguridad FortiGate y túneles VPN para conectar sedes remotas.
- **Infraestructura en sitio:** 44 servidores en la sede del IASS (Infrastructure as a Service) y 20 servidores instalados en la sede Aduana.
- **Infraestructura en la nube:** máquinas virtuales, almacenamiento y sistemas replicados, garantizando alta disponibilidad.
- **Módulos de respaldo y monitoreo:** sistemas de copias de seguridad).

La interconexión entre estas capas permite una gestión eficiente de los servicios TIC y la aplicación de medidas de recuperación ante desastres, asegurando la operación continua de los procesos institucionales de la Alcaldía.

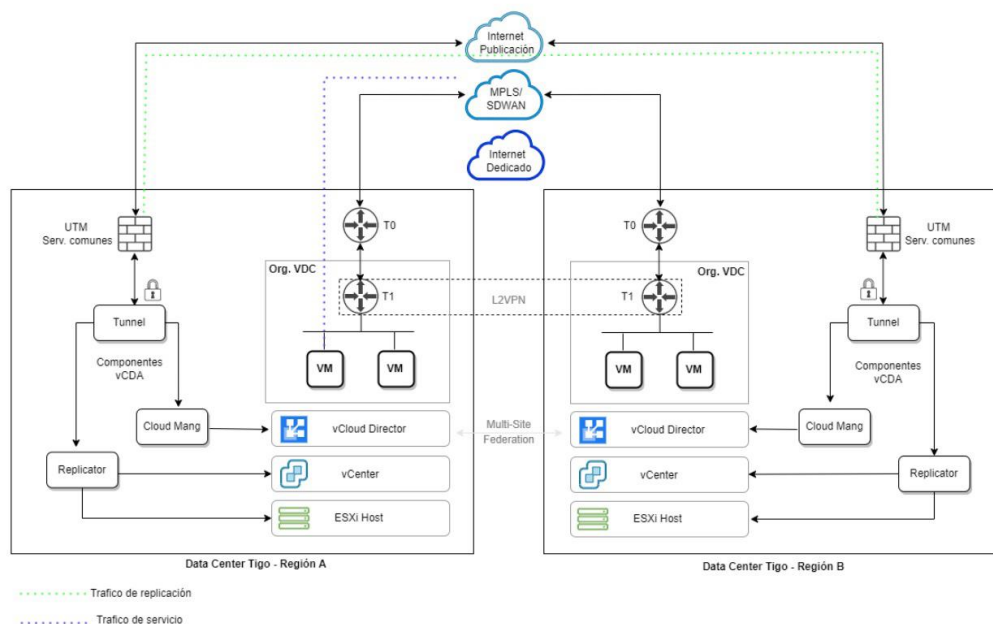


Figure 1. Diagrama de Arquitectura de Cloud Data Center_ Alcaldía de Cartagena

Esta arquitectura ofrece una solución robusta para garantizar la continuidad de los servicios tecnológicos críticos de la Alcaldía, permitiendo mantener la operación institucional en caso de fallos, incidentes de ciberseguridad o desastres físicos. Además, se alinea con las buenas prácticas de continuidad del negocio (ISO 22301) y recuperación ante desastres TIC (ISO 27031).

La arquitectura presentada representa un esquema de continuidad operativa y recuperación ante desastres, implementado en modalidad multisitio (Multi-Site Federation) entre dos regiones geográficas (Región A y Región B), ambas bajo la infraestructura de **Tigo Cloud**.

El modelo contempla dos Data Centers (Región A y Región B) conectados entre sí, con capacidades de replicación de máquinas virtuales (VMs), gestión federada de recursos y túneles seguros para garantizar la disponibilidad, redundancia y recuperación de servicios ante incidentes.

Componentes Principales

⇒ Región A – Data Center Primario:

- **vCloud Director y vCenter:** Plataforma de gestión de infraestructura virtualizada.
- **ESXi Hosts:** Servidores físicos que ejecutan las máquinas virtuales (VM).
- **VMs (máquinas virtuales):** Infraestructura crítica de servicios institucionales.
- **Redes T0 y T1 (NSX):** Encargadas del ruteo y seguridad interna.
- **UTM (Firewall unificado):** Filtra el tráfico de entrada y salida, asegurando comunicaciones cifradas.
- **vCDA Components + Tunnel:** Establecen túneles seguros para servicios internos.
- **Replicator:** Motor de replicación que sincroniza datos con la Región B.
- **Cloud Manager:** Orquestador que coordina la continuidad y gestión multisitio.

⇒ Región B – Data Center Secundario (Recuperación)

- Mismos componentes que la Región A (vCloud, vCenter, ESXi Hosts, VMs).
- Configurado en espera activa para garantizar una rápida recuperación ante fallos en la Región A.

Interconexión entre Regiones

- ⇒ **L2VPN:** Túnel privado de capa 2 que interconecta las redes virtuales de ambas regiones, preservando el direccionamiento IP.
- ⇒ **Multi-Site Federation:** Sincronización entre los vCloud Directors para gestión centralizada de recursos.

Flujos de Tráfico

- ⇒ **Tráfico de replicación** (línea verde punteada): Encargado de replicar los datos y configuraciones de las VMs desde la Región A a la Región B, asegurando la disponibilidad de una copia actualizada.
- ⇒ **Tráfico de servicio** (línea azul punteada): Flujo normal de operación entre usuarios finales, servicios publicados en internet y las cargas de trabajo virtualizadas.

Conectividad Externa

- ⇒ **Internet Público (Publicación):** Para exposición de servicios web u otras aplicaciones hacia usuarios externos.
- ⇒ **Internet Dedicado / MPLS / SD-WAN:** Para interconexión segura entre sedes institucionales y los data centers.
- ⇒ **UTM Firewall:** Puntos de control para inspección profunda del tráfico, políticas de acceso y protección contra amenazas.

Seguridad y Resiliencia

- ⇒ **Túneles cifrados:** para comunicaciones internas entre componentes y entre regiones.
- ⇒ **Redundancia de rutas y servicios:** gracias al esquema activo-pasivo entre los dos data centers.
- ⇒ **Replicación continua:** lo que permite cumplir con RPO bajos y garantizar una rápida restauración bajo esquemas RTO definidos.

Análisis de Impacto al Negocio (BIA) con Enfoque en las TIC de la Alcaldía de Cartagena

El Análisis de Impacto al Negocio (BIA, por sus siglas en inglés) constituye una herramienta crítica para identificar y priorizar los procesos y servicios que dependen de las TIC, así como para evaluar los impactos de su interrupción en las operaciones de la Alcaldía. Este análisis permite establecer bases sólidas para el diseño de estrategias de recuperación, alineadas con los objetivos del Plan de Continuidad del Negocio (PCN) de TIC.

El presente BIA tiene como objetivo principal evaluar cómo la interrupción de los servicios TIC impactaría las operaciones esenciales de la Alcaldía y sus dependencias, así como identificar los recursos y plazos críticos para la recuperación de estos servicios. Para ello, se adoptan las mejores prácticas internacionales y se considera el marco normativo aplicable en Colombia, incluyendo la Ley 2052 de 2020 sobre Gobierno Digital y el Decreto 1078 de 2015.

El alcance del análisis comprende:

- **Identificación de Procesos y Aplicaciones Críticas:** Aquellos procesos y aplicaciones cuya interrupción afectaría significativamente el cumplimiento de las funciones misionales de la Alcaldía.
- **Análisis de Riesgos Potenciales:** Analizar los **riesgos** que podrían interrumpir estos servicios (desastres naturales, ataques cibernéticos, fallas de infraestructura).
- **Evaluación de Impacto:** Determinar los efectos de la interrupción en términos operativos, financieros, legales y reputacionales.
- **Establecimiento de Tiempos de Recuperación:** Definir los objetivos de tiempo para la restauración de servicios TIC (RTO y RPO).
- **Identificación de Dependencias Críticas:** Reconocer los sistemas, infraestructura, personal y otros recursos esenciales para cada proceso identificado.

El desarrollo de este BIA está orientado a fortalecer la resiliencia de los servicios TIC de la Alcaldía de Cartagena, asegurando su continuidad y minimizando los riesgos asociados a eventos disruptivos. Este esfuerzo refuerza el compromiso de la Alcaldía con la excelencia administrativa, la protección de los datos ciudadanos y la garantía de servicios públicos de calidad.

Identificación de Procesos Críticos

La identificación de procesos críticos es una etapa fundamental para determinar aquellas actividades esenciales cuyo funcionamiento continuo es indispensable para el cumplimiento de las funciones misionales y la prestación de servicios clave de la Alcaldía. Para la Alcaldía de Cartagena, estos procesos están alineados con los objetivos estratégicos institucionales y responder a las necesidades de la ciudadanía.

Revisión del Marco Normativo y Estratégico

El Plan de Desarrollo Cartagena Ciudad de Derechos 2024-2027, establece aspectos claves y desafíos que apuntan a mejorar la calidad de vida de los habitantes de la ciudad, precisa que, es necesario garantizar ciertas condiciones institucionales y territoriales para atender estas demandas. De este modo, es necesario crear estructuras de innovación pública y participación ciudadana que garanticen instituciones inclusivas, estas instituciones deben proveer seguridad jurídica, ser transparentes, participativas, inclusivas y democráticas. Además, deben asegurar la igualdad ante la ley y generar las condiciones institucionales necesarias para que los mercados funcionen de manera competitiva¹.

¹ Plan de Desarrollo Cartagena Ciudad de Derechos 2024-2024

El programa *Cartagena Digital, Inclusiva y Conectada* del Plan de Desarrollo, se concentra en proporcionar plataformas tecnológicas institucionales que faciliten el intercambio seguro, controlado y transparente de información entre las entidades estatales y los ciudadanos, con el objetivo último de mejorar la eficiencia en los trámites y servicios ofrecidos hacia los usuarios y asegurando una gestión pública moderna, ágil y centrada en el ciudadano.

En este sentido, se desarrollará la estrategia de gobierno abierto, con el fin de aumentar la cantidad de conjuntos de datos publicados en datos.gov.co. Paralelamente, se diseñará, construirá e implementará una estrategia integral de gobernanza de datos, que establecerá un modelo óptimo de explotación de estos para el Distrito, permitiendo así el desarrollo de sistemas de información innovadores basados en el aprovechamiento de los datos.

Otro programa con el que cuenta la entidad es *Seguridad Digital*, este, garantizará la protección de los activos de información que manejan funcionarios, contratistas y terceros, contenida en los procesos, las tecnologías de información, hardware y el software. Es una de las grandes apuestas de desarrollo tecnológico que determinan en gran parte la calidad de los servicios y la forma como los entregamos a la ciudadanía.

Es por esto que se apunta a implementación de mecanismos en materia de Seguridad Digital, el Modelo de Gestión de Riesgos de Seguridad Digital permitirá a la entidad, articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política de Gobierno Digital, cuyo principal objetivo es conservar un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

Desde la Política de Seguridad Digital se apuesta en fortalecer la implementación del Plan de Seguridad y Privacidad de la información, propendiendo por la transparencia en la gestión pública a través del modelo de seguridad y privacidad de la información MSPI del Distrito y sus 18 dominios, así como identificar el nivel de confianza para la autenticación digital, identificar trámites y servicios ciudadanos digitales que deben contar con autenticación digital en la Alcaldía de Cartagena.

Estas apuestas se relacionan estrechamente con los objetivos estratégicos de la entidad, especialmente con el que busca fortalecer la relación del Estado con la ciudadanía cartagenera, incrementando los niveles de recaudo tributario y mejorando el índice de desempeño institucional, mediante la innovación pública, optimización y simplificación de procesos, la modernización administrativa y la eficiente participación ciudadana, garantizando una gobernanza eficiente, transparente y orientada al servicio de la ciudadanía, durante el periodo de gobierno 2024-2027.

Análisis Modelo de Operación por Procesos de la Alcaldía de Cartagena de Indias.

La Alcaldía de Cartagena de Indias, cuenta con el Sistema de Gestión regido por el Modelo Integrado de Planeación y Gestión - MIPG, el cual integra los sistemas de Gestión y el Modelo Estándar de Control Interno - MECI; a partir de este lineamiento, establece mecanismos, políticas

de operación y procesos, que le permitan gestionar eficientemente sus recursos y producir servicios y bienes con altas estándares de calidad, que resuelvan los problemas de la ciudadanía.

En la actualidad, de acuerdo con el Modelo de Operación por procesos, la entidad cuenta con: 4 *Macroprocesos Estratégicos*, 7 *Macroprocesos Misionales* y 5 *Macroprocesos de Apoyo*.



Ilustración 3. Mapa de Procesos Alcaldía de Cartagena. Fuente: www.mipgcartagena.gov.co

De acuerdo con este modelo y con respecto al uso de las TIC encontramos que los procesos hacen uso de sistemas de información y aplicativos para el desarrollo de sus actividades, en este orden de ideas tenemos la siguiente relación, en este orden de ideas, la entidad registra activos 45 sistemas de información, los cuales son utilizados para las diferentes operaciones de la entidad, en su mayoría son soportados por la Oficina Asesora de Informática a continuación, distribuidos de la siguiente forma:

Proceso	Aplicaciones en Uso
Gestión de Hacienda	10
Gestión en Salud	9
Gestión en Educación	8
Gestión Administrativa	6
Planeación Territorial y Desarrollo Estratégico	4
Gestión de Tecnologías de la información	4
Gestión Legal	2
Comunicación Pública	1
Gestión de Tránsito y Transporte	2
Total General	48

De lo anterior, se infiere que, por la naturaleza de algunos procesos, es necesario el uso de mayor cantidad de sistemas de información, como es el caso de la Gestión en Salud, proceso que se ejecuta en el DADIS, así como la Gestión de Hacienda, proceso que se ejecuta desde la Secretaría de Hacienda Distrital, seguidos por la Gestión de Tecnologías de la Información, y la Planeación Territorial.

Del mismo modo se identifican sistemas de información o aplicativos que tienen una connotación de transversalidad, y su uso se da en todos los procesos como el SIGOB (sistema de correspondencia), Treasury (gestión Financiera), el aplicativo Mi Cuenta (Gestión de Hacienda) y Certico.

A continuación, se detallan los sistemas de información/aplicativos que operan en la Alcaldía Mayor de Cartagena:

Software/Aplicativo	Descripción	Proveedor	Almacenado en	Proceso
Certificados Laborales	Aplicación web que apoya el proceso de talento humano del Departamento Administrativo y su Dirección Administrativa y Financiera, utilizada por los contratistas (personas naturales) para descargar certificados de contratos que han ejecutado con el DADIS.	Alcaldía	Nube	Gestión en Salud
Sede Electrónica DATT	Plataforma web para que los ciudadanos consulten sus trámites de tránsito y transporte, multas de tránsito, certificados de desembargo, solicitar permisos de pico y placa	Externo	Datatools	Gestión de Tránsito y Transporte
Circulemos	Software utilizado por el Departamento Administrativo de Tránsito y Transporte (DATT) de Cartagena para la gestión de trámites y procesos relacionados con el tránsito y transporte. Más específicamente, "Circulemos DATT" se refiere al sistema informático que administra la información y procedimientos del DATT en Cartagena, incluyendo registro de vehículos, licencias de conducción, comparendos, entre otros.	Datatools	Nube	Gestión de Tránsito y Transporte



Colombia evaluadora	Sistema para la gestión escolar, notas, seguimiento	Solinces	Externo	Gestión en Educación
Copsis	Portal para la gestión de los contratos por órdenes de prestación de servicios: Herramienta de apoyo al proceso de contratación de prestación de servicios, en las fases precontractual y contractual, permite generar los documentos soporte de forma normalizada, para facilitar el proceso el proceso en la Plataforma SECOP 2	Alcaldía	Nube	Gestión administrativa
DadisPQR	Permite el registro interno para seguimiento a peticiones	Alcaldía	Nube	Gestión en Salud
FortiEDR	FortiEDR es una solución de seguridad de endpoints (dispositivos como computadoras y servidores) desarrollada por Fortinet, enfocada en la detección y respuesta automatizada a amenazas. Combina tecnologías de protección, detección y respuesta a incidentes, funcionando antes, durante y después de una infección. En Cartagena, FortiEDR se utiliza para proteger los dispositivos finales de las amenazas cibernéticas, ofreciendo capacidades como la detección y detención de malware en tiempo real, la prevención de ataques de ransomware y la automatización de la respuesta a incidentes.	Alcaldía	Nube	Gestión de tecnologías de la información
Humano Web	Sistema de administración de gestión de personal, novedades de planta y nómina de la Secretaría de Educación Distrital	Ministerio de Educación	Externo	Gestión en Educación
INFORMACIÓN POR VÍA GENERAL(EXOGENA)	Portal para la recepción de la información exógena, la cual permite al Distrito fiscalizar tributos.	Alcaldía	Nube	Gestión de Hacienda
LIMAY	sistema de manejo para el registro de todas las transacciones económicas del Distrito, contiene información de libros contables utilizados para la emisión y presentación de estados financieros. Solo consulta en reemplazo de Treasury	Alcaldía	Datacenter Distrito	Gestión de Hacienda
MATEO	Sistema de manejo de Información tributaria, predial, industria y comercio y contribución por valorización	Alcaldía	Datacenter Distrito	Gestión de Hacienda
Microsoft 365 (aplicaciones)	es una plataforma basada en la nube que proporciona a los usuarios aplicaciones de productividad como Word, Excel, PowerPoint, Outlook y OneDrive, así como servicios inteligentes en la nube y seguridad avanzada	Microsoft	Nube	Gestión de tecnologías de la información
Micrositio Secretaría de Planeación	Plataforma informativa para las entidades y ciudadanía en general, entes de control y demás sobre inversión y ordenamiento territorial del Distrito.	Alcaldía	Nube	Planeación Territorial y Desarrollo Estratégico
Midas	Aplicación web que permite consulta, recopilación, procesamiento y consolidación de información geográfica de la ciudad de Cartagena	Alcaldía	Nube	Planeación Territorial y Desarrollo Estratégico



Next - Poc	Telecomunicaciones con ambulancias del distrito. Para Geoposicionamiento (CRUE): Permite conocer la posición de las ambulancias, para la atención de emergencias y monitorear los recorridos.	Porescom	Externo	Gestión en Salud
Pagina Web Alcaldía de Cartagena	Sede electrónica del Distrito que permite garantizar el acceso a la información pública como entidad obligada según la normatividad vigente	Alcaldía	Nube	Gestión de Tecnologías de la información
PREDIS	Sistema de manejo d información presupuestal y de pagaduría del Distrito, disponibilidad presupuestal, generación de orden de planilla. Solo consulta reemplazado por Treasury	Alcaldía	Datacenter Distrito	Gestión de Hacienda
QUERY	Sistema para la consulta de reporte de requerimientos de las dependencias del Distrito	Alcaldía	Nube	Gestión de Hacienda
Portal ReporteSP	Aplicativo web para el reporte de indicadores de salud pública, Seguimiento nominal PAI, Certificados de Discapacidad de Personas Naturales, Registro Nominal de Vacunación Electrónica	Alcaldía	Nube	Gestión en Salud
SAC V2	Sistema de correspondencia interna y externa y los tiempos de cumplimientos de las PROQS a toda la ciudadanía no se podría atender en los tiempos de cumplimiento.	Ministerio de Educación	Externo	Gestión en Educación
SAUS	Sistema de soporte y apoyo a usuarios de sistema: es una herramienta para el manejo y gestión del Departamento de Soporte Técnico de la Oficina Asesora de Informática al servicio de los empleados y contratistas de la Alcaldía Mayor de Cartagena.	Alcaldía	Nube	Gestión de tecnologías de la información
SECOP 1	Plataforma transaccional que permite a las entidades estatales y a los proveedores realizar el proceso de contratación de forma digital	Colombia Compra Eficiente	Nube	Gestión Legal
SECOP 2	Plataforma transaccional que permite a las entidades estatales y a los proveedores realizar el proceso de contratación de forma digital	Colombia Compra Eficiente	Nube	Gestión Legal
Sede Electrónica DADIS	Página Web del DADIS, permite publicar contenidos y consulta de información	Alcaldía	Data Center DADIS	Gestión en Salud
SIAF	Sistema que permite la gestión financiera y contable, incluyendo la ejecución del presupuesto, el registro de ingresos y gastos, el control de la ejecución presupuestal, la generación de reportes financieros, entre otras funciones relacionadas con la gestión de los recursos económicos FOSE	Alcaldía	Data center SED	Gestión en Educación
SIET	Sistema que permite brindar información confiable a la comunidad sobre la legalidad de las instituciones y programas de Educación para el Trabajo y el Desarrollo.	Ministerio de Educación	Externo	Gestión en Educación
Sigdadis	Sistema de información que apalanca el proceso de recepción, radicación, auditoría, conciliación y certificación de facturas reportadas por las IPS, a la población no asegurada	Alcaldía	Nube	Gestión en Salud



SIGEP Nómina	Sistema de gestión de la nómina de la Alcaldía de Cartagena	Heinsohn	Nube	Gestión administrativa
SIGOB	El SIGOB es el Sistema de Gestión de Gobierno, una plataforma tecnológica diseñada para apoyar la planificación, seguimiento, evaluación y rendición de cuentas de los compromisos y acciones de los gobiernos, especialmente en el ámbito de la administración pública. Sistema de correspondencia de la entidad	PENUD	Nube	Gestión administrativa
SIMAT	El SIMAT establece un servicio permanente de información que genera reportes, alertas y seguimiento respecto de apariciones de la organización y de los actores de interés en los medios de comunicación, permitiendo el análisis permanente de la favorabilidad con que son referidos en los medios de comunicación. Ello se logra mediante informes base, además de análisis que permiten la toma de decisiones político-comunicacionales para la detección y manejo de crisis y la construcción o adecuación de estrategias de comunicación e intervención.	PENUD	Nube	Comunicación Pública
SIMAT	Aplicativo para la gestión del proceso de matrícula de las instituciones educativas Alcaldía de Cartagena	Ministerio de Educación	Externo	Gestión en Educación
SOL	Aplicativo para realizar trámites en línea	PENUD	Nube	Gestión administrativa
TAXATION SMART	Sistema de manejo de Información de los tributos del Distrito (liquidación y facturación de impuesto predial, aplicación de declaraciones y pagos de industria y comercio, delineación urbana, sobretasa a la gasolina, alumbrado público y rentas varias)	Informática y Tributos	Informática y Tributos	Gestión de Hacienda
TRBONet	Se encarga de manejar la comunicación a través de radio, con IPS y Ambulancias	Comsatelite	Externo	Gestión en Salud
TREASURY	Sistema para manejo de información contable y presupuestal del Distrito. Disponibilidad presupuestal, generación de ordenes de planillas, modificaciones presupuestales, se registran transacciones económicas realizadas por el Distrito, libros contables, es utilizada para la emisión y presentación de estados contables.	Informática y Tributos	Informática y Tributos	Gestión de Hacienda
Validador Archivos Planos	Sistema de Información de apoyo que le permite alas IPS revisar, verificar la estructura de los archivos RPIS a reportar para su facturación.	Alcaldía	Nube	Gestión en Salud
XENCO	Software de apoyo para las operaciones contables del DADIS, en este momento sirve de consulta para apoyo al TREASURY	Alcaldía	Nube	Gestión en Salud
Zeus Nomina	Antiguo sistema de gestión de la nómina de funcionarios solo consulta	Zeus	Nube	Gestión administrativa



SIUCE	Sistema para acceder a la identificación, registro y seguimiento de los casos de acoso y violencia escolar, en los establecimientos educativos oficiales y no oficiales de Colombia	Ministerio de Educación	Externo	Gestión en Educación
OPERADOR	Apoyo a los directivos docentes y administrativos de las UNALDES, en el manejo de plataformas tecnológicas	Alcaldía	Nube	Gestión en Educación
CERTIFICADO DE RETENCIONES	Aplicativo para la consulta y generación de certificado de retenciones a terceros	Alcaldía	Nube	Gestión de Hacienda
SIPI	Sistema de información para el inversionista	Alcaldía	Nube	Gestión de Hacienda
CLÚSTER 2,0	Plataforma para facilitar el encadenamiento productivo entre las empresas locales, nacionales e internacionales.	Alcaldía	Nube	Gestión de Hacienda
SEGUIMIENTO POT	Permite hacer seguimiento al POT actual a través de los documentos que se generan de el. Licencias, uso de suelo, acuerdos, decretos, actas	Alcaldía	Nube	Planeación Territorial y Desarrollo Estratégico
SISBEN APP	Aplicativo programa informático diseñado por el DNP para recopilar la información concerniente a procesos de solicitudes, modificaciones e inclusiones en la base de datos de Sisbén 4	DNP	Nube	Planeación Territorial y Desarrollo Estratégico

Para micrositios que están disponibles 35, los cuales permiten garantizar el derecho a la información a los ciudadanos e interesados de la Alcaldía de Cartagena, en algunos casos realizar trámites ciudadanos, realizar operaciones internas, y en general, dar cumplimiento a la normatividad vigente, a continuación se detallan:

Nombre	URLSitio	Área o Dependencia
	http://ai.cartagena.gov.co	
Es una plataforma digital de la Alcaldía de Cartagena que permite reportar y activar alertas sobre niñas, niños, adolescentes y mujeres desaparecidas, recopilando datos clave a través de un formulario para agilizar la respuesta de las autoridades y la comunidad	http://alertarosa.cartagena.gov.co	Secretaría del interior
Sede electrónica de la Alcaldía de Cartagena	http://cartagena.gov.co	Oficina Asesora de Informatica
Catalina es una innovadora herramienta de inteligencia artificial creada por la Oficina Asesora de Informática de la Alcaldía de Cartagena. Su misión es optimizar los servicios públicos, facilitar el acceso a la información y fortalecer la relación entre la administración distrital y los ciudadanos	http://catalina.cartagena.gov.co	
Portal de Certificación de Prestación de Servicios. Es una plataforma en línea donde los contratistas del Distrito de Cartagena pueden generar el certificado de supervisión necesario para tramitar el pago de sus cuentas.	http://certico.cartagena.gov.co	Secretaría de Hacienda Distrital
Clúster Cartagena es una Plataforma que facilita el encadenamiento productivo entre las empresas Locales, Nacionales e Internacionales y los principales Clúster de la Ciudad.	http://cluster.cartagena.gov.co	Secretaría de Hacienda Distrital
El Portal de Gobierno Abierto promueve y garantiza el acceso a la información para fortalecer la transparencia y la participación ciudadana en la gestión y el control de lo público en el Distrito de Cartagena de Indias. Aquí encontrarás información gubernamental relevante, presentada de forma clara y accesible, así como conjuntos de datos en formatos abiertos y reutilizables que facilitan el acceso ciudadano a la información. Además, se fomenta la participación activa en la toma de decisiones y la colaboración entre el gobierno, la ciudadanía y otras partes interesadas.	http://gobiernoabierto.cartagena.gov.co	Oficina Asesora de Informatica



Micrositio que evidencia lo relacionado con la política de mejora normativa del Distrito de Cartagena de Indias	http://mejoranormativa.cartagena.gov.co	Oficina Asesora Jurídica
La Alcaldía de Cartagena, en su objetivo de transparentar la Administración Pública y establecer un puente de comunicación entre comunidad y gobierno, pone a su alcance la consulta virtual de pagos para agilizar los pagos a Contratistas	http://micuenta.cartagena.gov.co	Secretaría de Hacienda Distrital
MIDAS Cartagena, o Mapa Interactivo Digital de Asuntos del Suelo, es una herramienta digital del Distrito de Cartagena que permite visualizar y analizar información relacionada con el territorio y el Plan de Ordenamiento Territorial (POT) vigente.	http://midas.cartagena.gov.co	Secretaría de Planeación
Micrositio que evidencia lo relacionado con el Modelo Integrado de Planeación y Gestión y el Modelo de Operación por Procesos de la Entidad	http://mipg.cartagena.gov.co	Secretaría General - Calidad
Este portal web es una plataforma digital e interactiva de la Secretaría de Planeación, cuyo objeto es compilar y brindar información geoespacial y estadística que se procesa y analiza en relación con las condiciones y situaciones sociales, económicas, ambientales, demográficas, urbanas y territoriales del Distrito de Cartagena.	http://odus.cartagena.gov.co	Secretaría de Planeación
	http://operador.cartagena.gov.co	Secretaría de Educación
Portal web que almacena información relacionada con el Plan de Ordenamiento Territorial de Cartagena	http://pot.cartagena.gov.co	Secretaría de Planeación
Es un programa liderado por la Secretaría del Interior y Convivencia Ciudadana, el cual se encargará de la promoción de la convivencia y autorregulación de los establecimientos de comercio para promover que sus propietarios, administradores, empleados, así como quienes lo frecuentan, adopten buenas prácticas de legalidad, responsabilidad y respeto con el entorno social y ambiental en el que desarrollan su actividad económica.	http://rumbasegura.cartagena.gov.co	Secretaría de Interior
Aplicativo de soporte y apoyo a usuarios de sistemas.	http://saus.cartagena.gov.co	Oficina Asesora de Informática
herramienta versátil y eficiente, hecha para el monitoreo, control y entrega de información actualizada sobre la prestación de los servicios públicos. Uno de sus principales objetivos es el aseguramiento de la calidad en el suministro de estos mientras se mantiene una constante comunicación con la comunidad.	http://servinfo.cartagena.gov.co	Secretaría General
Sistema de Caracterización Ciudadana	http://sic2.cartagena.gov.co	Secretaría General
Sistema de Caracterización Ciudadana	http://sic.cartagena.gov.co	Secretaría General
SIGOB permite a las entidades públicas gestionar eficientemente la correspondencia, los archivos y los procesos internos, estandarizando la producción y manejo de la información.	http://sigob.cartagena.gov.co	Secretaría General
Sistema de Información de Matricula Contratada	http://simco3.cartagena.gov.co	Secretaría de Educación
Sistema de Información de Matricula Contratada	http://simco.cartagena.gov.co	Secretaría de Educación
Sistema de Información para Inversionistas: Es el espacio en donde encuentran la información de las entidades que permite el establecimiento de empresas en la ciudad de Cartagena y los pasos que deben cumplir en cada uno de ellos, para el cumplimiento de los requisitos en los procesos de inversión que realizan las partes interesadas.	http://sipi.cartagena.gov.co	Secretaría de Hacienda Distrital
Información SISBEN	http://sisben.cartagena.gov.co	Secretaría de Planeación
Micrositio con información sobre la gestión del talento humano	http://talentohumano.cartagena.gov.co	Dirección Administrativa Talento Humano
Información Sobre Trámites	http://tramites.cartagena.gov.co	Secretaría General



	http://vpn.cartagena.gov.co	Sin información
	http://vpn.dev.cartagena.gov.co	Sin información
	http://vuc.cartagena.gov.co	Sin información
	http://webhooks-ai.cartagena.gov.co	Sin información
	http://webxdigital.cartagena.gov.co	Sin información
Información sobre inmuebles propiedad del Distrito de Cartagena	https://sapi.cartagena.gov.co/	
Micrositio que contiene la información relacionada con el código de integridad-	https://soyintegridad.cartagena.gov.co/	dirección Administrativa Talento Humano
PEMP: Portal web del plan de ordenamiento territorial del CENTRO HISTORICO. Permite hacer seguimiento a la protección del centro histórico, conocer la fecha de las mesas de participación, noticias, convocatoria a participación, parte del proceso, historial de publicaciones	https://pemp.cartagena.gov.co/	Secretaría de Planeación

Mapecto de dependencias TIC:

Para desarrollar este componente, es necesario identificar cuáles procesos dependen directamente de plataformas, infraestructura o servicios tecnológicos, con el fin de asegurar su continuidad y recuperación en caso de interrupciones.

El análisis de criticidad de los procesos se establece atendiendo los siguientes criterios:

1. Impacto Operacional:

- ¿Qué tan crítico es el proceso para las funciones diarias?
- ¿Puede la Alcaldía operar sin este proceso por un tiempo prolongado?

2. Impacto Legal y Regulatorio:

- ¿Qué implicaciones legales tiene la interrupción del proceso?
- ¿Existe cumplimiento normativo obligatorio asociado al proceso?

3. Impacto Financiero:

- ¿Se generarían pérdidas económicas significativas?
- ¿Afecta el proceso la recaudación de ingresos (por ejemplo, impuestos)?

4. Impacto en la Reputación:

- ¿Cómo afectaría la imagen institucional ante la ciudadanía?
- ¿Se generaría desconfianza pública o pérdida de credibilidad?

5. Dependencia Tecnológica:

- ¿Qué grado de dependencia tiene el proceso de las TIC?
- ¿Qué tan rápido puede ser recuperado desde un respaldo?

Determinación de Tiempos de Recuperación

Los Tiempos de Recuperación Objetivo (RTO - Recovery Time Objective) y Puntos de Recuperación Objetivo (RPO - Recovery Point Objective) son dos conceptos fundamentales:

- **RTO (Tiempo de Recuperación Objetivo):** Es el tiempo máximo tolerable para la recuperación de un servicio o sistema crítico tras una interrupción. Esto define cuán rápido debe ser el proceso de restauración para evitar impactos graves.

Criterio RTO (Tiempo de Recuperación Objetivo)	Tiempo
Crítico- en tiempo real (pagos, recaudos, etc.)	RTO de 1-2 horas
Crítico – alta continuidad (tramites, términos perentorios, etc.)	RTO de 4-6 horas
Importante (registros, operaciones que pueden esperar al final del día)	RTO de 8 horas
No crítico (registros, información que puede ser procesada en diferentes tiempos)	RTO > 12 horas

- **RPO (Punto de Recuperación Objetivo):** Indica el punto en el tiempo al que se puede recuperar la información, es decir, cuánto tiempo de datos se puede perder sin afectar de manera inaceptable los servicios. A continuación, se detalla la escala utilizada para asignar los RPO:

Criterio RPO (Punto de Recuperación Objetivo)	Tiempo
Procesos críticos en tiempo real o con gran sensibilidad a la pérdida de datos (por ejemplo, emergencias en salud, transporte, seguridad pública).	15 minutos
Procesos que requieren información reciente para su continuidad pero no en tiempo real (por ejemplo, gestión financiera, educación).	1 hora
Procesos moderadamente críticos que pueden tolerar una pequeña pérdida de datos recientes (por ejemplo, desarrollo social, infraestructura).	2-4 horas
Procesos no críticos donde la pérdida de datos no afecta de forma inmediata las operaciones (por ejemplo, evaluaciones internas, espacio público).	12 horas

En atención a la tabla anterior tenemos que:

- **Impacto Operacional:** Evalúa si el proceso afecta directamente las operaciones diarias.
- **Impacto Legal:** Determina si hay obligaciones normativas que se verían comprometidas.
- **Impacto Financiero:** Considera pérdidas económicas derivadas de la interrupción.
- **Impacto en Reputación:** Analiza cómo podría afectar la confianza pública en la Alcaldía.
- **Dependencia TIC:** Valora qué tanto depende el proceso de las tecnologías.
- **Prioridad Final:** Clasifica el proceso como **Crítico** o **Importante**.



- **Tiempo Máximo de Recuperación (RTO):** Define cuánto tiempo puede estar inactivo antes de causar daños significativos, reflejan la urgencia para restablecer cada proceso en caso de interrupción.
- **Procesos Críticos:** Marcados como **Críticos** debido a su alta dependencia de TIC y su impacto legal, financiero o en reputación.
- **Procesos Importantes:** Necesarios para mantener la operatividad, pero pueden tolerar tiempos de recuperación más largos.
- **Procesos No Críticos:** No generan impactos inmediatos significativos y pueden ser recuperados en plazos más amplios.

Matriz de Priorización de Aplicativos/Software Críticos - Alcaldía de Cartagena

Software	tramites ciudadanos	Realiza pagos?	Proveedo r	Almacen ado en	Proceso	Área o Dependenci a	Impacto	Impacto Operaciona l	Impacto Legal	Impacto Financiero	Impacto en Reputación	Dependencia TIC	Prioridad Final	Tiempo Máximo de Recuperación (RTO)	Tiempo RTO	RPO (Pérdida Máxima Aceptable de Datos)
Certificados Laborales	No	No	Alcaldía	Nube	Gestión en Salud	DADIS	Operacional	Bajo	bajo	bajo	bajo	Alto	7	No crítico	>12 horas	12 horas
Sede Electrónica Datt	si	si	Externo	Datatools	Gestión de Tránsito y transporte	DATT	Operacional	alto	alto	alto	alto	medio	14	Crítico (en tiempo real)	1-2 horas	15 minutos
Circulemos	si	si	Datatools	Nube	Gestión de Tránsito y Transporte	DATT	Operacional	alto	alto	alto	alto	Bajo	14	Crítico (en tiempo real)	1-2 horas	15 minutos
Colombia evaluadora	Si	NO	Solinces	Externo	Gestión en Educación	Secretaría de Educación	Operacional	Alto	bajo	bajo	alto	bajo	9	No crítico	>12 horas	12 horas
Copsis	No	No	Alcaldía	Nube	Gestión administrati va	Dirección Administrati va Talento Humano	Operacional	Alto	bajo	bajo	Medio	Alto	10	Importante	8 horas	2-4 horas
DadisPQR	No	No	Alcaldía	Nube	Gestión en Salud	DADIS	Operacional	Bajo	bajo	bajo	bajo	Alto	7	No crítico	>12 horas	12 horas
FortiEDR			Alcaldía	Nube	Gestión de tecnologías de la información	Oficina asesora de Informatica	Operacional	alto	alto	alto	alto	alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
Humano Web	Si	Si	Ministerio de Educación	Externo	Gestión en Educación	Secretaría de Educación	Operacional	Alto	alto	alto	alto	bajo	13	Crítico (alta continuidad)	4-6 horas	1 hora
INFORMACIÓ N POR VÍA GENERAL(EXO GENA)	si	no	Alcaldía	Nube	Gestión de Hacienda	Secretaría de Hacienda Distrital	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
LIMAY	No	No	Alcaldía	Datacente r Distrito	Gestión de Hacienda	Secretaría de Hacienda Distrital	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
MATEO	si	Si	Alcaldía	Datacente r Distrito	Gestión de Hacienda	Secretaría de Hacienda Distrital	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos

Alcaldía Mayor de Cartagena de Indias



Microsoft 365 (aplicaciones)	no	no	Microsoft	Nube	Gestión de tecnologías de la información	Oficina Asesora de Informática	Operacional	alto	alto	bajo	alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
Micrositio Secretaría de Planeación	Si	No	Alcaldía	Nube	Planeación Territorial y Desarrollo Estratégico	Secretaría de Planeación	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
Midas	Si	No	Alcaldía	Nube	Planeación Territorial y Desarrollo Estratégico	Secretaría de Planeación	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
Next - Poc	Si	No	Porescom	Externo	Gestión en Salud	DADIS	Operacional	Alto	alto	alto	alto	bajo	13	Crítico (alta continuidad)	4-6 horas	1 hora
Pagina Web Alcaldía de Cartagena	si	no	Alcaldía	Nube	Gestión de tecnologías de la información	Oficina Asesora de Informática	Operacional	alto	alto	alto	alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
PREDIS	No	No	Alcaldía	Datacenter Distrito	Gestión de Hacienda	Secretaría de Hacienda Distrital	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
QUERY	No	No	Alcaldía	Nube	Gestión de Hacienda	Secretaría de Hacienda Distrital	Operacional	Medio	Bajo	Bajo	Bajo	Alto	8	No crítico	>12 horas	12 horas
Portal ReporteSP	Si	No	Alcaldía	Nube	Gestión en Salud	DADIS	Operacional	Alto	alto	alto	alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
SAC V2	Si	No	Ministerio de Educación	Externo	Gestión en Educación	Secretaría de Educación	Operacional	Alto	alto	bajo	alto	bajo	11	Importante	8 horas	2-4 horas
SAUS	no	no	Alcaldía	Nube	Gestión de tecnologías de la información	Oficina Asesora de Informática	Operacional	Medio	bajo	bajo	bajo	alto	8	No crítico	>12 horas	12 horas
SECOP 1	Si	No	Colombia Compra Eficiente	Nube	Gestión Legal	Oficina Asesora Jurídica	operacional	alto	alto	alto	alto	bajo	13	Crítico (alta continuidad)	4-6 horas	1 hora
SECOP 2	si	no	Colombia Compra Eficiente	Nube	Gestión Legal	Oficina Asesora Jurídica	Operacional	alto	alto	alto	alto	bajo	13	Crítico (alta continuidad)	4-6 horas	1 hora
Sede Electrónica DADIS	No	No	Alcaldía	Data Center DADIS	Gestión en Salud	DADIS	Operacional	Bajo	alto	bajo	alto	Alto	11	Importante	8 horas	2-4 horas
SIAF	no	si	Alcaldía	Data center SED	Gestión en Educación	Secretaría de Educación	Operacional	Alto	alto	alto	alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
SIET	si	no	Ministerio de Educación	Externo	Gestión en Educación	Secretaría de Educación	Operacional	Bajo	bajo	bajo	alto	bajo	7	No crítico	>12 horas	12 horas
Sigdadis	No	Si	Alcaldía	Nube	Gestión en Salud	DADIS	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
SIGEP	No	si	Heinsohn	Nube	Gestión administrativa	Dirección Administrativa Talento Humano	Operacional	Alto	Alto	Alto	Alto	Bajo	13	Crítico (alta continuidad)	4-6 horas	1 hora
SIGOB	Si	no	PENUD	Nube	Gestión administrativa	Secretaría General - Atención al ciudadano	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos



SIMAT	no	no	PENUD	Nube	Comunicación Pública	Prensa y Comunicación	Operacional	Alto	Bajo	Bajo	Alto	Alto	11	Importante	8 horas	2-4 horas
SIMAT	si	no	Ministerio de Educación	Externo	Gestión en Educación	Secretaría de Educación	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
SOL	si	si	PENUD	Nube	Gestión administrativa	Secretaría General - Servicio al Ciudadano	Operacional	Alto	Alto	Alto	Medio	Alto	14	Crítico (en tiempo real)	1-2 horas	15 minutos
TAXATION SMART	Si	Si	Informática y Tributos	Informática y Tributos	Gestión de Hacienda	Secretaría de Hacienda Distrital	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
TRBONet	Si	No	Comsatelite	Externo	Gestión en Salud	DADIS	Operacional	Alto	Alto	Alto	Alto	Bajo	13	Crítico (alta continuidad)	4-6 horas	1 hora
TREASURY	No	No	Informática y Tributos	Informática y Tributos	Gestión de Hacienda	Secretaría de Hacienda Distrital	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
Validador Archivos Planos	Si	Si	Alcaldía	Nube	Gestión en Salud	DADIS	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
XENCO	No	No	Alcaldía	Nube	Gestión en Salud	DADIS	Operacional	Bajo	Bajo	Alto	Alto	Alto	11	Importante	8 horas	2-4 horas
Zeus Nomina	no	No	Zeus	Nube	Gestión administrativa	Fondo Territorial de pensiones	Operacional	Bajo	Bajo	Bajo	Bajo	Bajo	5	No crítico	>12 horas	12 horas
SIUCE	si	no	Ministerio de Educación	Externo	Gestión en Educación	Secretaría de Educación	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
OPERADOR	si	no	Alcaldía	Nube	Gestión en Educación	Secretaría de Educación	Operacional	Bajo	Bajo	Bajo	Bajo	Bajo	5	No crítico	>12 horas	12 horas
CERTIFICADO DE RETENCIONES	Si	No	Alcaldía	Nube	Gestión de Hacienda	Secretaría de Hacienda Distrital	Operacional	Medio	Bajo	Bajo	Medio	Alto	9	No crítico	>12 horas	12 horas
SIPI	No	No	Alcaldía	Nube	Gestión de Hacienda	Secretaría de Hacienda Distrital	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
CLUSTER 2,0	Si	No	Alcaldía	Nube	Gestión de Hacienda	Secretaría de Hacienda Distrital	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
SISBEN APP	No	No	DNP	Nube	Planeación Territorial y Desarrollo Estratégico	Secretaría de Planeación	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora

Tabla 1. Matriz de Priorización de Aplicativos - Alcaldía de Cartagena. Elaboración Propia



Matriz de Priorización de Sitios WEB - Alcaldía de Cartagena

Información General					Valoración de Impacto							Recuperación	
Nombre	URLSitio	URL	Área o Dependencia	Tipo de Impacto	Operacional	Legal	Financiero	Reputación	Dependencia TIC	Prioridad Final	Tiempo Máximo de Recuperación (RTO)	Tiempo RTO	RPO (Pérdida Máxima Aceptable de Datos)
	http://ai.cartagena.gov.co	http://ai.cartagena.gov.co		Operacional	Bajo	Bajo	Bajo	Bajo	Bajo	5	No crítico	>12 horas	12 horas
Es una plataforma digital de la Alcaldía de Cartagena que permite reportar y activar alertas sobre niñas, niños, adolescentes y mujeres desaparecidas, recopilando datos clave a través de un formulario para agilizar la respuesta de las autoridades y la comunidad	http://alertarosa.cartagena.gov.co	http://alertarosa.cartagena.gov.co	Secretaría del interior	Operacional	Bajo	Bajo	Bajo	Alto	Alto	9	No crítico	>12 horas	12 horas
Sede electrónica de la Alcaldía de Cartagena	http://cartagena.gov.co	http://cartagena.gov.co	Oficina Asesora de Informática	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
Catalina es una innovadora herramienta de inteligencia artificial creada por la Oficina Asesora de Informática de la Alcaldía de Cartagena. Su misión es optimizar los servicios públicos, facilitar el acceso a la información y fortalecer la relación entre la administración distrital y los ciudadanos	http://catalina.cartagena.gov.co	http://catalina.cartagena.gov.co		Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
Es una plataforma digital donde los contratistas del distrito pueden generar el certificado de supervisión necesario para tramitar el pago de sus cuentas. Este portal facilita la gestión de contratos, incluyendo la certificación de supervisión, contratos electrónicos, registros presupuestales, entre otros aspectos relevantes para el pago.	http://certico.cartagena.gov.co		Secretaría de Hacienda Distrital	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
Clúster Cartagena es una Plataforma que facilita el encadenamiento productivo entre las empresas Locales, Nacionales e Internacionales y los principales Clúster de la Ciudad.	http://cluster.cartagena.gov.co	http://cluster.cartagena.gov.co	Secretaría de Hacienda Distrital	Operacional	Bajo	Bajo	Bajo	Alto	Alto	9	No crítico	>12 horas	12 horas
El Portal de Gobierno Abierto promueve y garantiza el acceso a la información para fortalecer la transparencia y la participación ciudadana en la gestión y el control de lo público en el Distrito de Cartagena de Indias. Aquí encontrarás información gubernamental relevante, presentada de forma clara y accesible, así como conjuntos de datos en formatos abiertos y reutilizables que facilitan el acceso ciudadano a la información. Además, se fomenta la participación activa en la toma de decisiones y la colaboración entre el gobierno, la ciudadanía y otras partes interesadas.	http://gobiernoabierto.cartagena.gov.co	http://gobiernoabierto.cartagena.gov.co	Oficina Asesora de Informática	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
Micrositio que evidencia lo relacionado con la política de mejora normativa del Distrito de Cartagena de Indias	http://mejoranormativa.cartagena.gov.co	http://mejoranormativa.cartagena.gov.co	Oficina Asesora Jurídica	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas

Alcaldía Mayor de Cartagena de Indias



La Alcaldía de Cartagena, en su objetivo de transparentar la Administración Pública y establecer un puente de comunicación entre comunidad y gobierno, pone a su alcance la consulta virtual de pagos para agilizar los pagos a Contratistas	http://micuenta.cartagena.gov.co	http://micuenta.cartagena.gov.co	Secretaría de Hacienda Distrital	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos
MIDAS Cartagena, o Mapa Interactivo Digital de Asuntos del Suelo, es una herramienta digital del Distrito de Cartagena que permite visualizar y analizar información relacionada con el territorio y el Plan de Ordenamiento Territorial (POT) vigente.	http://midas.cartagena.gov.co	http://midas.cartagena.gov.co	Secretaría de Planeación	Operacional	Alto	Alto	Bajo	Alto	Bajo	11	Importante	8 horas	2-4 horas
Micrositio que evidencia lo relacionado con el Modelo Integrado de Planeación y Gestión y el Modelo de Operación por Procesos de la Entidad	http://mipg.cartagena.gov.co	http://mipg.cartagena.gov.co	Secretaría General - Calidad	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
Este portal web es una plataforma digital e interactiva de la Secretaría de Planeación, cuyo objeto es compilar y brindar información geoespacial y estadística que se procesa y analiza en relación con las condiciones y situaciones sociales, económicas, ambientales, demográficas, urbanas y territoriales del Distrito de Cartagena.	http://odus.cartagena.gov.co	http://odus.cartagena.gov.co	Secretaría de Planeación	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
	http://operador.cartagena.gov.co	http://operador.cartagena.gov.co	Secretaría de Educación	Operacional	Alto	Alto	Bajo	Alto	Bajo	11	Importante	8 horas	2-4 horas
Portal web que almacena información relacionada con el Plan de Ordenamiento Territorial de Cartagena	http://pot.cartagena.gov.co	http://pot.cartagena.gov.co	Secretaría de Planeación	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
Es un programa liderado por la Secretaría del Interior y Convivencia Ciudadana, el cual se encargará de la promoción de la convivencia y autorregulación de los establecimientos de comercio para promover que sus propietarios, administradores, empleados, así como quienes lo frecuentan, adopten buenas prácticas de legalidad, responsabilidad y respeto con el entorno social y ambiental en el que desarrollan su actividad económica.	http://rumbasegura.cartagena.gov.co	http://rumbasegura.cartagena.gov.co	Secretaría de Interior	Operacional	Alto	Bajo	Bajo	Bajo	Alto	9	No crítico	>12 horas	12 horas
Aplicativo de soporte y apoyo a usuarios de sistemas.	http://saus.cartagena.gov.co	http://saus.cartagena.gov.co	Oficina Asesora de informática	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
herramienta versátil y eficiente, hecha para el monitoreo, control y entrega de información actualizada sobre la prestación de los servicios públicos. Uno de sus principales objetivos es el aseguramiento de la calidad en el suministro de estos mientras se mantiene una constante comunicación con la comunidad.	http://servinfo.cartagena.gov.co	http://servinfo.cartagena.gov.co	Secretaría General	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
Sistema de Caracterización Ciudadana	http://sic2.cartagena.gov.co	http://sic2.cartagena.gov.co	Secretaría General	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
Sistema de Caracterización Ciudadana	http://sic.cartagena.gov.co	http://sic.cartagena.gov.co	Secretaría General	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
SIGOB permite a las entidades públicas gestionar eficientemente la correspondencia, los archivos y los procesos internos, estandarizando la producción y manejo de la información.	http://sigob.cartagena.gov.co	http://sigob.cartagena.gov.co	Secretaría General	Operacional	Alto	Alto	Alto	Alto	Alto	15	Crítico (en tiempo real)	1-2 horas	15 minutos

Alcaldía Mayor de Cartagena de Indias



Sistema de Información de Matricula Contratada	http://simco3.cartagena.gov.co	http://simco3.cartagena.gov.co	Secretaría de Educación	Operacional	Alto	Medio	Bajo	Alto	Bajo	10	Importante	8 horas	2-4 horas
Sistema de Información de Matricula Contratada	http://simco.cartagena.gov.co	http://simco.cartagena.gov.co	Secretaría de Educación	Operacional	Alto	Medio	Bajo	Alto	Bajo	10	Importante	8 horas	2-4 horas
Sistema de Información para Inversionistas: Es el espacio en donde encuentran la información de las entidades que permite el establecimiento de empresas en la ciudad de Cartagena y los pasos que deben cumplir en cada uno de ellos, para el cumplimiento de los requisitos en los procesos de inversión que realizan las partes interesadas.	http://sipi.cartagena.gov.co	http://sipi.cartagena.gov.co	Secretaría de Hacienda Distrital	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
Información SISBEN	http://sisben.cartagena.gov.co		Secretaría de Planeación	Operacional	Alto	Alto	Bajo	Alto	Bajo	11	Importante	8 horas	2-4 horas
Micrositio con información sobre la gestión del talento humano	http://talentohumano.cartagena.gov.co	http://talentohumano.cartagena.gov.co	Dirección Administrativa Talento Humano	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
Información Sobre Trámites	http://tramites.cartagena.gov.co		Secretaría General	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
	http://vpn.cartagena.gov.co		Sin información	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
	http://vpn.dev.cartagena.gov.co	http://vpn.dev.cartagena.gov.co	Sin información	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
	http://vuc.cartagena.gov.co	http://vuc.cartagena.gov.co	Sin información	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
	http://webhooks-ai.cartagena.gov.co	http://webhooks-ai.cartagena.gov.co	Sin información	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
	http://webxdigital.cartagena.gov.co	http://webxdigital.cartagena.gov.co	Sin información	Operacional	Bajo	Bajo	Bajo	Bajo	Alto	7	No crítico	>12 horas	12 horas
información sobre inmuebles	https://sapi.cartagena.gov.co/			Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
Micrositio que contiene la información relacionada con el código de integridad-	https://soyintegridad.cartagena.gov.co/		dirección Administrativa Talento Humano	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora
PEMP: Portal web del plan de ordenamiento territorial del CENTRO HISTORICO. Permite hacer seguimiento a la protección del centro histórico, conocer la fecha de las mesas de participación, noticias, convocatoria a participación, parte del proceso, historial de publicaciones	https://pemp.cartagena.gov.co/		Secretaría de Planeación	Operacional	Alto	Alto	Bajo	Alto	Alto	13	Crítico (alta continuidad)	4-6 horas	1 hora



Interrelaciones Procesos Críticos:

Visualización de cómo los procesos críticos dependen entre sí.

Procesos Relacionados (Interdependencias):

Proceso Origen	Procesos Dependientes
Gestión Administrativa	Gestión Hacienda, Gestión Legal, Control Disciplinario, Comunicación Pública.
Gestión Hacienda	Gestión de Infraestructura, Gestión en Salud, Gestión en Educación, Gestión Legal.
Gestión en Salud	Planeación Territorial, Gestión de Desarrollo Social, Seguridad y Convivencia Ciudadana.
Gestión en Educación	Planeación Territorial, Gestión de Desarrollo Social, Comunicación Pública.
Gestión de Tecnologías de la Información	Todos los procesos dependen directamente de las TIC para soporte y operación continua.
Planeación Territorial y Direccionamiento Estratégico	Gestión en Infraestructura, Gestión del Pensamiento Estratégico y de la Comunidad, Gestión de Desarrollo Social.
Gestión en Infraestructura	Gestión de Tránsito y Transporte, Planeación Territorial, Seguridad y Convivencia Ciudadana.
Gestión de Desarrollo Social	Seguridad y Convivencia Ciudadana, Gestión de Participación Ciudadana, Gestión en Salud, Gestión en Educación.
Control Disciplinario	Gestión Administrativa, Gestión Legal.
Gestión del Pensamiento Estratégico y de la Comunidad	Gestión de Participación Ciudadana, Planeación Territorial.
Comunicación Pública	Todos los procesos requieren comunicación pública para difusión de información y manejo de crisis.
Gestión de Participación Ciudadana	Gestión del Pensamiento Estratégico, Gestión de Desarrollo Social.
Gestión Legal	Gestión Hacienda, Control Disciplinario, Gestión Administrativa, Seguridad y Convivencia Ciudadana.
Gestión de Tránsito y Transporte	Gestión en Infraestructura, Planeación Territorial, Seguridad y Convivencia Ciudadana.
Evaluación Independiente	Todos los procesos, especialmente Gestión Administrativa y Control Disciplinario.
Seguridad y Convivencia Ciudadana	Gestión en Salud, Gestión de Desarrollo Social, Gestión de Infraestructura, Gestión de Tránsito y Transporte.

Interconectividad: El proceso de **Gestión de Tecnologías de la Información** es el eje central que soporta todos los procesos

Comunicación Pública: Sirve como apoyo transversal para mantener informados a los ciudadanos y gestionar situaciones críticas.

Análisis de Riesgos Potenciales

El análisis de riesgos tiene como objetivo identificar, clasificar y evaluar los riesgos que podrían interrumpir los servicios TIC de la Alcaldía de Cartagena.

Identificación de Amenazas:

las amenazas que pueden identificarse pueden ser de tipo:

- **Naturales:** Huracanes, inundaciones, terremotos, deslizamientos.
- **Tecnológicas:** Fallos en hardware o software, interrupciones de energía, pérdida de conectividad.
- **Humanas:** Errores operativos, sabotaje interno, ataques cibernéticos.
- **Legales y Regulatorias:** Cambios normativos que afecten la disponibilidad de servicios.

Amenazas	Tipo
Huracanes y tormentas tropicales (alta probabilidad en el Caribe).	Natural
Inundaciones en zonas vulnerables de la ciudad.	Natural
Sismos o movimientos telúricos.	Natural
Deslizamientos en áreas periférica	Natural
Fallos de infraestructura TIC (servidores, redes, almacenamiento).	Tecnológica
Interrupciones de energía eléctrica	Tecnológica
Ataques cibernéticos como ransomware, phishing o DDoS	Tecnológica
Errores operativos en la gestión de sistemas TIC.	Humana
Sabotajes internos o accesos no autorizados.	Humana
Falta de capacitación del personal ante incidentes tecnológicos.	Humana
Cambios normativos que impacten la operación de los sistemas.	Legales y Regulatorias
Incumplimiento en la protección de datos sensibles.	Legales y Regulatorias

Clasificación de Riesgos

Utilizamos una **Matriz de Riesgos** para evaluar las amenazas con base en dos factores principales: la **probabilidad de ocurrencia** y el **impacto del riesgo**. Estos criterios se definen en función de datos históricos, experiencia, y evaluaciones específicas del contexto. Criterios establecidos para la Alcaldía de Cartagena:

○ Probabilidad de Ocurrencia

La **probabilidad** mide la frecuencia o la posibilidad de que un evento ocurra en un periodo de tiempo dado. Los niveles se definen de la siguiente manera:

Nivel de Probabilidad	Descripción	Ejemplo Aplicado a la Alcaldía
Alta	Es muy probable que el evento ocurra al menos una vez al año.	Huracanes, fallos eléctricos recurrentes, ciberataques frecuentes en sistemas gubernamentales.
Media	Existe una posibilidad moderada de que ocurra (una vez cada pocos años).	Inundaciones localizadas, errores operativos, ataques cibernéticos ocasionales.
Baja	Es poco probable que ocurra, pero no imposible (una vez en varios años o menos).	Sabotaje interno, sismos de baja magnitud, cambios normativos repentinos.

○ Impacto del Riesgo

El **impacto** mide las consecuencias de un evento si este llegara a ocurrir. Se evalúa en términos de cuatro dimensiones clave:

Nivel de Impacto	Descripción	Ejemplo Aplicado a la Alcaldía
Alto	Afecta significativamente las operaciones, causa pérdidas financieras importantes o daños legales/reputacionales graves.	Interrupción del recaudo de impuestos, caída de servicios de salud pública, pérdida masiva de datos.
Medio	Afecta parcialmente las operaciones, con consecuencias manejables y pérdidas moderadas.	Fallos en el sistema de atención al ciudadano o interrupciones temporales en sistemas educativos.
Bajo	Impacto menor o local, con efectos que no alteran significativamente la operatividad general.	Caídas temporales de sistemas no críticos o pérdida de datos respaldados.

○ Combinación en la Matriz de Riesgos

La **Matriz de Riesgos** cruza estos dos criterios para obtener un **nivel de riesgo** que permita priorizar las amenazas más críticas:

Probabilidad / Impacto	Bajo	Medio	Alto
Alta	Moderado	Alto	Crítico
Media	Bajo	Moderado	Alto
Baja	Bajo	Bajo	Moderado

○ **Criterios:**

1. **Crítico:** Requiere atención inmediata. Necesita estrategias preventivas y de mitigación efectivas.
2. **Alto:** Necesita medidas de control y respuesta activa para reducir su probabilidad o impacto.
3. **Moderado:** Monitoreo constante y medidas preventivas menores.
4. **Bajo:** Riesgo aceptable con impactos limitados y bajo costo de manejo.

Matriz de Riesgos de la Alcaldía de Cartagena

Riesgo	Probabilidad	Impacto	Nivel de Riesgo
Huracanes	Alta	Alto	Crítico
Inundaciones	Alta	Medio	Alto
Fallos de Energía Eléctrica	Alta	Medio	Alto
Ataques Cibernéticos	Media	Alto	Alto
Errores Operativos	Media	Medio	Moderado
Sabotaje Interno	Baja	Medio	Moderado
Cambios Normativos	Baja	Alto	Moderado
Deslizamiento	Baja	Medio	Moderado
Sismos	Baja	Medio	Moderado

Tabla 2. Matriz de Riesgos Alcaldía de Cartagena. Elaboración Propia

Evaluación de Riesgos

La evaluación de riesgos permite priorizar las amenazas con base en la probabilidad de ocurrencia y su impacto, utilizando la matriz previamente establecida. Esta metodología clasifica los riesgos en críticos, altos y moderados, definiendo las acciones necesarias para cada nivel.

Este enfoque garantiza que los recursos se asignen de manera eficiente, priorizando las amenazas que representan mayores peligros para la continuidad del negocio de las TIC.

Definición de Estrategias de Recuperación

Este componente establece las acciones y recursos necesarios para garantizar la pronta recuperación de los servicios TIC tras una interrupción, priorizando los procesos críticos y reduciendo los impactos operativos, financieros, legales y reputacionales.

○ Riesgos Críticos

Son los riesgos con alta probabilidad de ocurrencia y un impacto significativo en las operaciones y servicios esenciales. Su gestión requiere **planes de respuesta inmediata** y estrategias de recuperación bien definidas. Se espera mitigación rápida y directa mediante estrategias probadas y con recursos disponibles.

Riesgo	Impacto	Medidas de Gestión	Recuperación Inmediata
Huracanes	Interrupción total de los servicios TIC debido a daños en infraestructura y cortes de energía. Afectación masiva en la prestación de servicios críticos como salud, educación y atención ciudadana.	Implementar protocolos de migración de datos a centros de datos seguros o en la nube. Mantener equipos de respaldo en ubicaciones geográficamente alejadas de las zonas de impacto.	Contar con generadores de energía de alta capacidad y sistemas de redundancia tecnológica.

○ Riesgos Altos

Riesgos con alta o media probabilidad y un impacto significativo, pero que no necesariamente implican una interrupción total. Requieren **medidas preventivas específicas** y planes de contingencia diseñados para minimizar sus efectos.

Riesgo	Impacto	Medidas de Gestión
Inundaciones	Fallas en la continuidad y prestación de servicio. Daños de equipos	Reubicar los servidores críticos a zonas elevadas Diseñar sistemas de drenaje eficientes en instalaciones clave.
Fallos de Energía Eléctrica	Interrupción en la prestación de Servicios.	Implementar sistemas de energía ininterrumpida (UPS).

		Establecer acuerdos de servicio con proveedores eléctricos para respuesta prioritaria.
Ataques Cibernéticos	Perdida de información	Instalación de firewalls avanzados y sistemas de detección de intrusos. Realización de simulacros de ciberseguridad para preparar al personal ante posibles incidentes.

○ **Riesgos Moderados**

Riesgos con probabilidad media o baja y un impacto manejable. Se gestionan **mediante acciones de mitigación**, como controles internos, capacitación y actualización de políticas. Se espera implementación de medidas preventivas que reduzcan la probabilidad o el impacto. Se espera reforzar la resiliencia operativa mediante capacitación, controles internos y monitoreo continuo.

Riesgo	Impacto	Medidas de Gestión
Errores Operativos	Retrasos en procesos administrativos y operativos debido a configuraciones incorrectas o errores humanos en sistemas TIC. Posible necesidad de soporte técnico adicional para resolver fallos. Costos derivados de la reparación de errores o la contratación de servicios externos para su corrección. En casos extremos, errores en el manejo de datos sensibles pueden derivar en incumplimientos normativos (protección de datos).	Documentar procedimientos claros y capacitar regularmente al personal en el uso de sistemas TIC. Implementar controles de auditoría para minimizar errores.
Sabotaje Interno	Interrupciones parciales o temporales en servicios críticos si el sabotaje afecta sistemas clave. Posibilidad de pérdida de datos importantes o accesos indebidos. Costos de reparación de daños y potencial pérdida económica por la inhabilitación de servicios. Gastos asociados a investigaciones internas y reforzamiento de controles. Posibles sanciones legales si el sabotaje afecta datos personales o procesos regulados	Reforzar la seguridad en el control de accesos a las infraestructuras TIC. Realizar revisiones periódicas de permisos de usuarios en los sistemas.

Cambios Normativos	Necesidad de ajustes internos que pueden retrasar otros procesos clave. Posible incompatibilidad temporal de sistemas TIC con nuevas regulaciones. Riesgo de incumplimiento de normativas nuevas si no se adaptan los sistemas o políticas a tiempo. Percepción negativa por parte de los ciudadanos o autoridades si la institución no cumple con los nuevos estándares.	Participar en programas de formación y actualización legal. Designar un equipo responsable de evaluar y adaptar las políticas internas ante cambios regulatorios
---------------------------	---	--

Recursos Necesarios

Recursos	Detalles
Infraestructura Tecnológica	- Centros de datos alternativos y redundantes. - Sistemas de respaldo automatizados en servidores locales y en la nube. - Generadores eléctricos de alta capacidad.
Personal Clave	- Equipo de TI especializado en recuperación de sistemas. - Líderes de procesos críticos para coordinar acciones.
Presupuesto	Asignación para mantenimiento de infraestructura redundante y contratación de servicios externos de recuperación.

Planes de Respuesta a Incidentes y Gestión de Crisis

Un **Plan de Respuesta a Incidentes** establece los pasos necesarios para identificar, contener, erradicar y recuperar los servicios TIC tras un incidente disruptivo. El objetivo del **Plan de Gestión de Crisis** es coordinar los recursos y la comunicación interna y externa para minimizar el impacto del incidente en la operación de la Alcaldía.

Componentes del Plan de Respuesta a Incidentes

Etapa	Detalle
Detección	Implementar sistemas de monitoreo continuo que alerten sobre posibles fallos, ciberataques o interrupciones. Ejemplo: Firewalls, sistemas IDS/IPS (detección y prevención de intrusos).



Clasificación	Clasificar el incidente según su criticidad: ○ Crítico: Interrupción de servicios esenciales (recaudo de impuestos, salud pública). ○ Moderado: Impacto parcial o localizado. ○ Menor: Fallos menores sin impacto significativo en la operación.
Respuesta Inicial	Activación del Equipo de Respuesta: ○ Notificar al equipo de TI, líderes de procesos críticos y personal clave. ○ Usar canales de comunicación predefinidos (teléfono, correo, sistemas de mensajería)
Aislamiento del Incidente	○ Contener la propagación del impacto. Ejemplo: Desconectar un sistema afectado por malware para evitar que infecte otros sistemas
Investigación y Mitigación	Investigación: ○ Identificar la causa raíz del incidente. ○ Documentar los sistemas y procesos afectados. Mitigación: ○ Aplicar soluciones rápidas para detener el impacto. ○ Ejemplo: Parches de seguridad para vulnerabilidades detectadas.
Recuperación y Validación	Restauración de Servicios: ○ Recuperar los sistemas desde respaldos o redundancias. ○ Priorizar los servicios críticos según el RTO/RPO definido. Validación: ○ Asegurar que los servicios recuperados funcionan correctamente. Cierre del Incidente: ○ Documentar las acciones realizadas y las lecciones aprendidas.

Componentes del Plan de Gestión de Crisis

Etapas	Detalle
Activación del Plan	Criterios de Activación: ○ Incidentes que impacten significativamente las operaciones misionales o la reputación de la Alcaldía.

	Equipo de Gestión de Crisis: ○ Compuesto por representantes de TIC, comunicación pública, y líderes de dependencias clave.
Comunicación en Crisis	Protocolos de Comunicación Interna: ○ Notificar a todo el personal afectado sobre el estado del incidente. ○ Usar herramientas de comunicación rápidas como aplicaciones de mensajería o correos grupales. Protocolos de Comunicación Externa: ○ Informar a la ciudadanía y partes interesadas sobre el estado del servicio. ○ Designar voceros oficiales para evitar desinformación. Mensajes Predefinidos: ○ Crear plantillas para comunicar interrupciones de servicios y tiempos estimados de recuperación.
Coordinación de Recursos	Asignación de Responsabilidades: ○ Delegar tareas específicas a los miembros del equipo de crisis. Acceso a Recursos Clave: ○ Asegurar acceso a equipos de respaldo, contratos con proveedores, y presupuestos para la recuperación.
Evaluación Post-Crisis	Análisis Post-Mortem: ○ Evaluar las causas y las acciones realizadas. ○ Documentar áreas de mejora para futuras crisis. Actualización del Plan: ○ Incorporar las lecciones aprendidas en la próxima iteración del plan.

A continuación se presenta un **ejemplo del plan de acción a seguir en caso de la materialización de un riesgo**, de acuerdo con los componentes anteriormente descritos, con el fin de generar una ruta clara a seguir por el equipo designado:

Incidente: Ataque Cibernético

Etapas	Acción	Responsable	Plazo
Detección	Monitorear alertas del IDS/IPS.	Equipo de Seguridad TIC	Inmediato
Respuesta Inicial	Desconectar servidores infectados.	Administrador de Redes	15 minutos
Investigación	Identificar el origen del ataque y sistemas afectados.	Analista de Seguridad	1 hora

Mitigación	Aplicar parches de seguridad y restaurar desde respaldo.	Equipo de TI	2 horas
Comunicación	Informar a los líderes y la ciudadanía sobre el estado del incidente.	Comunicación Pública	Inmediato
Recuperación	Validar que los sistemas estén operativos y sin vulnerabilidades.	Administrador de TI	3 horas
Evaluación Post-Crisis	Documentar el incidente y actualizar procedimientos de seguridad.	Equipo de Continuidad	1 semana

Pruebas y Ejercicios de Continuidad

Con las pruebas se busca garantizar la efectividad y viabilidad del Plan de Continuidad del Negocio TIC mediante simulaciones y pruebas regulares que permitan evaluar, mejorar y fortalecer las estrategias definidas para responder a incidentes y crisis.

Los resultados esperados son resultados esperados son la validación de la efectividad del Plan de Continuidad TIC, la identificación de áreas de mejora y ajustes necesarios, un personal preparado para responder eficientemente a incidentes una mayor confianza en la resiliencia operativa de la Alcaldía.

Tipos de Prueba

Tipo de Prueba	Descripción	Objetivo	Frecuencia
Pruebas Teóricas	Ejercicios para revisar escenarios hipotéticos y discutir acciones necesarias.	Identificar brechas en la planificación y aclarar roles y responsabilidades.	Al menos dos veces al año.
Pruebas Simuladas	Simulación de incidentes específicos en entornos controlados.	Evaluar capacidad de respuesta y validar estrategias de recuperación.	Anual.
Pruebas Funcionales	Ejecución parcial o total de las estrategias del plan.	Verificar funcionalidad de sistemas de respaldo y tiempos de recuperación.	Anual para sistemas críticos, bianual para otros.
Simulacros Complejos	Ejercicio integral que involucra todas las	Evaluar la coordinación general	Cada dos años.

	áreas, simulando un incidente a gran escala.	y la interacción entre dependencias.	
--	--	--------------------------------------	--

Escenarios de Prueba

Escenario	Descripción	Objetivo
Ciberataque Simulado	Simular un ataque ransomware en los sistemas TIC.	Evaluar tiempos de respuesta y capacidad de recuperación de datos.
Fallos de Energía	Interrupción prolongada del suministro eléctrico en una dependencia clave.	Probar el uso de sistemas de respaldo energético.
Desastres Naturales	Huracán que afecta infraestructura física y conectividad.	Simular la activación de centros de datos
Errores Operativos	Configuración incorrecta de un sistema clave.	Probar la capacidad de detección y corrección en tiempo real.

Planificación de Pruebas

Pasos Para Implementar Pruebas y Ejercicios	Detalle
Definición de Objetivos	Establecer qué aspectos del plan se desean evaluar (e.g., tiempos de recuperación, comunicación, uso de recursos).
Creación del Escenario	Diseñar un caso basado en riesgos identificados y procesos críticos.
Selección de Participantes	Incluir a personal clave de TIC, líderes de procesos críticos, y representantes de comunicación pública.
Ejecución de la Prueba	Simular el escenario siguiendo un cronograma y documentar todas las acciones realizadas.
Evaluación de Resultados	Identificar brechas en el plan y áreas que requieren ajustes.
Reporte y Revisión	Elaborar un informe detallado de los resultados y actualizar el plan según sea necesario.

Indicadores de Desempeño de Planes de Incidentes y Gestión de Crisis

Indicador	Descripción	Frecuencia
Cumplimiento de RTO/RPO	Porcentaje de procesos que cumplen los tiempos definidos.	90% de cumplimiento.
Tiempos de Respuesta	Tiempo promedio en detectar y responder al incidente.	Reducir a menos de 1 hora.
Participación del Personal	Porcentaje de participantes en las pruebas	100% en pruebas planificadas

Mantenimiento y Mejora Continua

El objetivo de este componente es garantizar que el Plan de Continuidad del Negocio (PCN) de TIC se la Alcaldía, se mantenga actualizado, relevante y efectivo mediante revisiones periódicas, análisis de incidentes y adaptación a cambios tecnológicos, organizativos y normativos. A continuación se detalla el proceso de mantenimiento del Plan de Continuidad del Negocio de la Alcaldía de Cartagena.

Actividad	Frecuencia	Descripción
Revisión general del Plan	Anual	Evaluar el estado general del plan y su aplicabilidad.
Revisión parcial (componentes críticos)	Semestral	Actualizar componentes críticos del plan de forma más frecuente.
Cambios en infraestructura tecnológica	Durante cada revisión	Revisar nuevas aplicaciones, sistemas o hardware implementados.
Actualización de riesgos identificados	Durante cada revisión	Actualizar amenazas o riesgos con cambios en probabilidad/impacto.
Evaluación de tiempos de recuperación (RTO/RPO)	Durante cada revisión	Verificar si los tiempos de recuperación siguen siendo válidos.
Documentación de cambios	Tras pruebas o simulacros	Integrar aprendizajes de ejercicios y simulacros.
Ajustar procedimientos según resultados	Tras pruebas o simulacros	Modificar tiempos y estrategias de recuperación según resultados.
Validación post-incidente	Tras cada incidente	Analizar el impacto y acciones realizadas durante incidentes.
Documentación post-incidente	Tras cada incidente	Documentar lo que funcionó y áreas a mejorar tras incidentes.

Roles y Responsabilidades

Rol	Detalle
Equipo de Continuidad TIC	Coordinar revisiones y pruebas, implementar cambios, y documentar actualizaciones.
Líderes de Procesos Críticos	Proporcionar retroalimentación sobre cambios en los procesos y necesidades específicas.
Responsable de Seguridad	Garantizar que los cambios cumplan con las normativas de ciberseguridad y protección de datos.

Indicadores Clave de Desempeño (KPIs) del Plan de Continuidad del Negocio

Indicador	Detalle/Meta
Frecuencia de Actualización	Actualización anual o tras un incidente significativo.
Cumplimiento de Pruebas	100% de pruebas programadas realizadas
Cumplimiento de RTO/RPO	Al menos el 90% de los procesos cumplen con los tiempos establecidos.
Incidentes Analizados	100% de los incidentes relevantes evaluados post-evento.

Cronograma de Mantenimiento del Plan de Continuidad del Negocio

Actividad	Frecuencia	Responsable
Revisión General del PCN	Anual	Equipo de Continuidad TIC
Pruebas y Simulacros	Semestral	Equipo de Continuidad TIC
Análisis Post-Incidente	Tras cada incidente	Líderes de Procesos Críticos
Revisión de Riesgos	Anual	Responsable de Seguridad

Con el desarrollo de las actividades antes descritas, se pretende contar en la Alcaldía de Cartagena con un plan siempre actualizado y alineado con los cambios en el entorno operativo y tecnológico, mejora continua en la efectividad del plan para responder a incidentes y mayor resiliencia operativa y confianza en la gestión de riesgos TIC.