



**RESOLUCIÓN No. 699**  
**(Del 31 de diciembre de 2025)**

“Por medio de la cual se adopta la Política de Respaldo Institucional, el Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres Tecnológicos (DRP) del Municipio de Turbaco – Bolívar.”

**LA ALCALDESA DEL MUNICIPIO DE TURBACO – BOLÍVAR** en ejercicio de sus facultades constitucionales y legales, en especial las conferidas por el artículo 315 de la Constitución Política de Colombia, la Ley 489 de 1998, la Ley 1712 de 2014, el Decreto 1078 de 2015 y el Decreto 767 de 2022, y

**CONSIDERANDO**

Que la Constitución Política de Colombia establece que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de eficiencia, eficacia, economía, celeridad, imparcialidad y publicidad.

Que el Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, establece los lineamientos para la implementación de la Política de Gobierno Digital en las entidades públicas del país.

Que el Decreto 767 de 2022 actualiza la Política de Gobierno Digital y establece la necesidad de que las entidades públicas implementen mecanismos de seguridad digital, continuidad del servicio y protección de la información institucional.

Que, en desarrollo de las políticas digitales, el municipio de Turbaco, tiene la necesidad de adoptar diferentes planes y modelos para su funcionamiento, protección y seguridad informática y de este tipo de información, entre los cuales, se encuentra, el Plan de Continuidad del Negocio (BCP), el Plan de Recuperación ante Desastres Tecnológicos (DRP) y la política de respaldo institucional.

Que el Modelo Integrado de Planeación y Gestión – MIPG establece la necesidad de implementar estrategias orientadas a la gestión del riesgo, la seguridad de la información, la continuidad del negocio y la recuperación ante desastres tecnológicos.

Que, por su parte, el Plan de Continuidad del Negocio (BCP) establece los lineamientos, procedimientos y estrategias que permiten garantizar la continuidad de los procesos institucionales ante eventos que puedan interrumpir la prestación de los servicios de la administración municipal.

Que, además de lo anterior, el Plan de Recuperación ante Desastres Tecnológicos (DRP) establece los procedimientos técnicos para la restauración de la infraestructura tecnológica, los sistemas de información y los servicios digitales ante incidentes críticos, fallas tecnológicas o desastres que afecten la operación institucional.



Que la Política de Respaldo Institucional define los lineamientos para la gestión, protección y respaldo de la información institucional mediante la implementación de mecanismos de copia de seguridad que garanticen su disponibilidad, integridad y recuperación.

Que, en sesión del Comité Institucional de Gestión y Desempeño, realizada el 19 de diciembre de 2025, fueron presentados, revisados y aprobados los documentos correspondientes a la Política de Respaldo Institucional, el Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres Tecnológicos (DRP).

Que, en mérito de lo expuesto,

**RESUELVE**



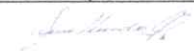
**ARTÍCULO PRIMERO: ADÓPTESE** la Política de Respaldo Institucional, el Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres Tecnológicos (DRP) del Municipio de Turbaco – Bolívar, como instrumentos de gestión institucional orientados a garantizar la protección de la información, la continuidad de los procesos institucionales y la recuperación de los servicios tecnológicos ante incidentes o desastres que afecten la operación de la administración municipal, los cuales, fueron aprobados mediante acta N° 004 de 2025, del comité de gestión y desempeño de Turbaco llevado a cabo el 23 de diciembre de 2025 y que harán parte integrante del presente acto administrativo.

La presente resolución rige a partir de la fecha de su expedición.

**PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE**

Dada en el Municipio de Turbaco – Bolívar, a los 31 días del mes de diciembre de 2025.

  
**CLAUDIA ELENA ESPINOSA PUELLO.**  
ALCALDESA MUNICIPAL  
Municipio de Turbaco – Bolívar

	Nombres y Apellidos	Cargo	Firma
<b>Aprobó</b>	GUSTAVO RAFAEL CARDONA HERRERA	secretario tic's	
<b>Revisó</b>	IVER MAURICIO DÍAZ PÉREZ	jefe de la oficina asesora jurídica	
<b>Proyectó</b>	ROSSET TIRADO GUERRA	Profesional Universitario	

Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las disposiciones legales, técnicas y Administrativas vigentes y por tanto bajo nuestra responsabilidad lo presentamos para la firma del remitente



Alcaldía Municipal de  
**Turbaco**  
Nit. 890.481.149-0

---

Versión	Fecha Versión	Observación
1	10 de octubre 2025	Borrador para validación

## **Alcaldía de Turbaco Bolívar Secretaría TIC**

### **POLÍTICA DE RESPALDO INSTITUCIONAL Proceso Tecnologías de la Información**





1. Introducción .....	3
2. Objetivo.....	3
3. Alcance .....	3
4. Marco Normativo.....	3
5. Principios Rectores .....	3
6. Roles y Responsabilidades .....	3
7. Estrategia de Respaldo .....	4
8. Pruebas de Restauración.....	4
9. Seguridad y Custodia.....	5
10. Revisión y Mejora Continua.....	5
11. Vigencia .....	5
FIRMAS DE VALIDACIÓN.....	5
CONTROL DE ELABORACIÓN DEL DOCUMENTO.....	5
Anexo Bitácora 1 .....	6
Anexo 2 Formato de Prueba de Restauración.....	6





## 1. Introducción

La Secretaría TIC, de la Alcaldía de Turbaco reconoce la importancia de garantizar la protección, disponibilidad e integridad de la información institucional. Esta política se deriva del diagnóstico realizado en septiembre de 2025, en cumplimiento del FURAG 2025, componente de Seguridad Digital. Se articula con el Plan de Continuidad Institucional, la Política de Seguridad Digital y las directrices del Comité TIC, en el marco del cumplimiento de los lineamientos del MinTIC y del Modelo Integrado de Planeación y Gestión (MIPG).

## 2. Objetivo

Definir los lineamientos para la generación, almacenamiento, custodia y restauración de copias de seguridad de la información institucional, garantizando su disponibilidad, integridad y recuperación ante fallas o incidentes tecnológicos.

## 3. Alcance

Aplica a todos los equipos, servidores, bases de datos, sistemas de información y archivos digitales administrados por la Secretaría TIC, así como a las dependencias que generen, almacenen o gestionen información institucional en formato digital.

## 4. Marco Normativo

- Ley 1581 de 2012 – Protección de Datos Personales.
- Ley 594 de 2000 – Ley General de Archivos.
- Decreto 620 de 2020 – Política de Seguridad Digital del Estado.
- Decreto 767 de 2022 – Lineamientos de Gobierno Digital.
- ISO/IEC 27001 y ISO/IEC 27002 – Seguridad de la información, Ciberseguridad y protección de la privacidad
- ISO 22301 – Continuidad del Negocio.
- Guía MinTIC de Seguridad Digital 4.0.
- Política de Seguridad Digital de la Alcaldía de Turbaco.

## 5. Principios Rectores

La política se fundamenta en los principios de confidencialidad, integridad, disponibilidad, trazabilidad y mejora continua, buscando que la información institucional sea protegida y gestionada de manera segura.

## 6. Roles y Responsabilidades

- Secretario TIC / Oficial de Seguridad Digital: aprueba la política, supervisa su implementación y gestiona los recursos necesarios.





- Apoyos Técnicos TIC: ejecutan los respaldos, pruebas de restauración y registros técnicos.
- Apoyo a la Gestión TIC: coordina la documentación, seguimiento FURAG y consolidación de evidencias.
- Líder GESCO: valida la articulación con el MIPG y el seguimiento de los compromisos de mejora.

## 7. Estrategia de Respaldo

Los respaldos institucionales se realizarán según la criticidad de la información y la capacidad técnica disponible. Se establecen los siguientes lineamientos:

- Bases de datos misionales: respaldo semanal completo.
- Documentos administrativos: respaldo quincenal.
- Configuraciones de red y sistemas: respaldo previo a cambios significativos.

Retención: los respaldos completos se conservarán por tres (3) meses y los incrementales por un (1) mes. Una copia se almacenará en ubicación secundaria (offsite) o nube institucional con cifrado y control de acceso. Todos los respaldos deberán registrarse en la Bitácora Institucional (Anexo 1).

## 8. Pruebas de Restauración

La Secretaría TIC realizará pruebas de restauración de información como mínimo una vez por trimestre, o cada vez que se realicen actualizaciones o cambios en sistemas críticos.

Estas pruebas tienen como propósito verificar la efectividad y trazabilidad de los respaldos institucionales, evaluando los indicadores RTO (Tiempo Objetivo de Recuperación) y RPO (Punto Objetivo de Recuperación) definidos para cada sistema o aplicación.

Los resultados deberán registrarse en el Formato de Prueba de Restauración (Anexo 2) y conservarse junto con la Bitácora Institucional de Respaldo (Anexo 1), como soporte de control y mejora continua del proceso.

En caso de presentarse fallas durante una prueba o una restauración real, se abrirá un incidente técnico y se activará el Plan de Contingencia correspondiente. Toda desviación o excepción en la frecuencia, medios o procedimientos deberá justificarse formalmente y contar con la autorización del Oficial de Seguridad Digital.

De manera transitoria, mientras la política se encuentra en proceso de aprobación, se implementará un plan piloto conforme al Oficio de Notificación del 30 de octubre





de 2025, mediante el cual se formaliza la aplicación de los formatos anexos y la generación de las evidencias técnicas respectivas.

## 9. Seguridad y Custodia

Las copias de respaldo se almacenarán en un espacio seguro, bajo llave y con acceso restringido. Los medios extraíbles deberán cifrarse y rotularse con código de control. El traslado de medios físicos deberá realizarse mediante acta de entrega y recepción.

## 10. Revisión y Mejora Continua

La política será revisada anualmente o cuando se presenten cambios tecnológicos, incidentes o recomendaciones del Comité TIC. Las actualizaciones serán registradas en el control de versiones del documento.

## 11. Vigencia

La presente política entrará en vigor una vez sea validada por el Comité TIC y aprobada por la Secretaría TIC. Su cumplimiento será obligatorio para todo el personal de la dependencia.

## FIRMAS DE VALIDACIÓN

Gustavo Rafael Cardona Herrera  
Secretario TIC / Oficial de Seguridad Digital

Rosset Paulina Tirado Guerra  
Líder GESCO – Funcionaria de Planta

## CONTROL DE ELABORACIÓN DEL DOCUMENTO

Revisó: Gustavo Rafael Cardona Herrera

Secretario TIC / Oficial de Seguridad Digital


Validó: Rosset Paulina Tirado Guerra – Líder GESCO

Elaboró: Luz Katherine Ibáñez Castro – Apoyo a la Gestión TIC






Anexo Bitácora 1

 <b>FORMATO DE BITÁCORA DE RESPALDO INSTITUCIONAL</b>						
Fecha	Sistema o Carpeta	Tipo de Respaldo (Completo / Incremental)	Medio Utilizado	Responsable	Resultado / Observación	Firma

Anexo 2 Formato de Prueba de Restauración

 <b>FORMATO DE PRUEBA DE RESTAURACIÓN</b>								
Fecha	Sistema Evaluado	Tipo de Prueba (Total / Parcial)	Resultado	RTO (min)	RPO (min)	Observaciones / Acciones Correctivas	Responsable	Firma





**Versión**

1

**Fecha Versión**

17 agosto del 2025

**Observación**

Primera versión del BCP

## **PLAN DE CONTINUIDAD DEL NEGOCIO (BCP)**





## Contenido

1. Marco Normativo y de Referencia .....	3
2. Introducción .....	3
3. Objetivo y Alcance .....	3
4. Contexto Institucional .....	3
5. Procesos Críticos Identificados .....	3
6. Análisis de Impacto en el Negocio (BIA) .....	4
7. Estrategias de Continuidad .....	4
8. Procedimiento de Activación .....	4
9. Plan de Comunicación .....	5
10. Pruebas y Mejora Continua .....	5
11. Riesgos y Escenarios .....	5
12. Conclusiones.....	5
13. Firmas y Aprobación .....	5





## 1. Marco Normativo y de Referencia

- Ley 527 de 1999 – Comercio Electrónico.
- Ley 1581 de 2012 – Protección de Datos Personales.
- Decreto 620 de 2020 – Política de Gobierno Digital.
- Decreto 767 de 2022 – Lineamientos de Seguridad Digital.
- Norma Técnica ISO 22301:2019 – Gestión de la Continuidad del Negocio.
- Política de Seguridad Digital de la Secretaría TIC.
- Plan de Recuperación de Desastres Tecnológicos (DRP v1.1, 2025).
- Manual de Seguridad de la Información y PESI 2024–2027.

## 2. Introducción

El presente Plan de Continuidad del Negocio (BCP) busca garantizar la continuidad operativa de los servicios digitales y misionales de la Secretaría TIC, asegurando la prestación de los servicios institucionales aun en escenarios de interrupción. Este documento consolida el cumplimiento del indicador FURAG de Seguridad Digital y se integra con el DRP v1.1 y el BIA institucional.

## 3. Objetivo y Alcance

Objetivo: Garantizar la continuidad operativa de los procesos y servicios críticos de la Secretaría TIC.

Alcance: Aplica a todos los servicios digitales, misionales y de apoyo que dependan de los sistemas tecnológicos de la Secretaría TIC.

## 4. Contexto Institucional

La Secretaría TIC, tiene como propósito liderar la transformación digital del municipio. Su rol incluye la administración de la infraestructura tecnológica, los servicios digitales y los programas de inclusión digital. Este BCP se aplica a todos los servicios y procesos que dependen de estos sistemas para garantizar la prestación continua.

## 5. Procesos Críticos Identificados





Proceso / Servicio	Descripción	Prioridad	Responsable
Correo institucional	Comunicación interna y externa oficial	Alta	Secretario TIC
Portal web y sede electrónica	Trámites y servicios en línea	Alta	Coordinador Web
Conectividad institucional-costatel	Internet y enlaces dedicados	Alta	Técnico de soporte
Plataformas externas (1Cero1, PQRSD.)	Soporte a trámites ciudadanos	Media	Apoyo TIC
Programas de capacitación (1Cero1, PQRSD.)	Base de datos de beneficiarios	Baja	Enlace de Inclusión Digital

## 6. Análisis de Impacto en el Negocio (BIA)

Proceso	Impacto	RTO (objetivo de Tiempo de Recuperación)	RPO (objetivo de Punto de Recuperación)	Recursos críticos	Dependencias
Correo institucional	Alto	8h	2h	Google Workspace, Internet	Todas las dependencias
Portal web	Alto	24h	12h	Hosting, dominio, soporte 1Cero1	Planeación
Conectividad	Alto	8h	1h	Proveedores Costatel / Claro	Todas las dependencias
Trámites digitales	Medio	24h	8h	Plataforma 1Cero1	Atención al Ciudadano
Capacitación digital	Bajo	48h	24h	Bases de datos locales	Programas

## 7. Estrategias de Continuidad

- Acceso remoto seguro a los sistemas institucionales.
- Internet alternativo mediante módem de respaldo.
- RespalDOS automáticos en la nube y en disco externo.
- Coordinación con proveedores TIC externos. Costatel, 1Cero1, SAFE
- Uso de canales alternos (teléfono).

## 8. Procedimiento de Activación

1. Identificar la interrupción o incidente.
2. Evaluar impacto según la matriz BIA.
3. Activar el BCP mediante comunicación de la Alcaldía municipal.
4. Implementar estrategias de recuperación y comunicación.
5. Registrar acciones en bitácora y elaborar informe de cierre.





## 9. Plan de Comunicación

Público	Medio	Responsable	Frecuencia
Servidores públicos	Correo y PQRSD	todas las dependencias	Inmediata
Proveedores TIC	Llamada y correo	Apoyo de Gestión	Según evento
Comunidad	Portal web y redes sociales	Oficina de Prensa	Según necesidad

## 10. Pruebas y Mejora Continua

Se realizarán simulacros anuales de continuidad. Los resultados serán documentados en actas internas y servirán para actualizar el plan. Indicadores: cumplimiento de RTO/RPO, efectividad de comunicación y cierre de incidentes.

## 11. Riesgos y Escenarios

- Falla de conectividad principal o energía.
- Daño en servidores locales o en la nube.
- Ataques cibernéticos o ransomware.
- Desastres naturales o fallas humanas.

## 12. Conclusiones

El BCP versión 1.1 consolida la metodología ISO 22301 y se integra al DRP v1.1, garantizando una respuesta coordinada ante interrupciones tecnológicas. La Secretaría TIC lidera la gestión de continuidad operativa y la mejora continua del servicio.

## 13. Firmas y Aprobación

Gustavo Rafael Cardona Herrera  
Secretario TIC – Responsable de Seguridad Digital





Versión	Fecha Versión	Observación
1	17 agosto del 2025	Primera versión del DRP

## **PLAN DE RECUPERACIÓN ANTE DESASTRES TECNOLÓGICOS (DRP)**





Contenido

1. INTRODUCCIÓN .....	3
2. OBJETIVO Y ALCANCE .....	3
3. CRITERIOS DE ACTIVACIÓN .....	3
4. CONTEXTO Y DIAGNÓSTICO TECNOLÓGICO .....	3
5. PROCESOS CRÍTICOS Y ACTIVOS IDENTIFICADOS .....	3
6. ESTRATEGIA DE RECUPERACIÓN (RTO / RPO).....	3
7. INTEGRACIÓN CON EL BIA INSTITUCIONAL .....	3
8. PROCEDIMIENTOS DE RESPALDO Y RESTAURACIÓN .....	4
9. OPERACIÓN DEGRADADA / SITIO ALTERNO .....	4
10. ROLES Y RESPONSABILIDADES .....	4
11. MATRIZ DE PROVEEDORES Y SLA.....	4
12. PLAN DE COMUNICACIÓN.....	4
13. PRUEBAS, INDICADORES Y CICLO PDCA.....	4
14. ARTICULACIÓN INSTITUCIONAL (MIPG, MECI, POLÍTICAS TIC).....	5
15. MARCO NORMATIVO ACTUALIZADO 2025.....	5
16. ANÁLISIS DE RIESGOS Y ESCENARIOS .....	6
17. CONCLUSIONES .....	6
18. ELABORACIÓN Y APROBACIÓN .....	6
NOTA TÉCNICA INTERNA – TRAZABILIDAD FURAG .....	6





## 1. INTRODUCCIÓN

El presente Plan de Recuperación de Desastres Tecnológicos (DRP) de la Secretaría TIC, de la Alcaldía de Turbaco corresponde a la versión 1.1 Final Actualizada. Este documento actualiza el marco normativo e incorpora el ciclo de mejora continua (PDCA), conforme a las guías MinTIC y al modelo de continuidad del negocio.

## 2. OBJETIVO Y ALCANCE

Garantizar la continuidad operativa y la recuperación oportuna de los sistemas, procesos y activos tecnológicos críticos de la Alcaldía de Turbaco, minimizando el impacto en la gestión institucional. El plan aplica a todos los servicios tecnológicos institucionales, internos o provistos por terceros (Costatel, 1Cero1, nube institucional, entre otros).

## 3. CRITERIOS DE ACTIVACIÓN

El DRP se activa cuando ocurre:

- Interrupción superior a 60 minutos en un servicio crítico.
- Pérdida de datos superior al RPO definido.
- Incidente de seguridad digital de nivel Alto o Crítico.

La activación es ordenada por el Coordinador del DRP y formalizada mediante acta de Comité TIC.

## 4. CONTEXTO Y DIAGNÓSTICO TECNOLÓGICO

La Secretaría TIC administra la infraestructura tecnológica de la Alcaldía, incluyendo conectividad institucional, correo, portal web, sistemas de trámites digitales y servicios en la nube, fundamentales para la gestión administrativa y atención ciudadana.

## 5. PROCESOS CRÍTICOS Y ACTIVOS IDENTIFICADOS

Proceso / Servicio	Tipo de Activo	Impacto	Prioridad
Correo institucional	Google Workspace	Alto	Alta
Portal web / Sede electrónica	Servidor web / Hosting	Alto	Alta
Trámites digitales	Plataforma 1Cero1	Medio	Media
Conectividad institucional	Red / Firewall / Enlaces	Alto	Alta

## 6. ESTRATEGIA DE RECUPERACIÓN (RTO / RPO)

Servicio	RTO (máximo tiempo de recuperación)	RPO (pérdida máxima aceptable de datos)
Correo institucional	8 horas	2 horas
Portal web	24 horas	12 horas
Conectividad institucional	8 horas	1 hora
Trámites digitales	24 horas	8 horas

## 7. INTEGRACIÓN CON EL BIA INSTITUCIONAL





El DRP se articula con el Análisis de Impacto al Negocio (BIA) institucional elaborado conforme a la Guía 11 del MinTIC. Cada actualización del BIA conlleva revisión del presente plan.

## 8. PROCEDIMIENTOS DE RESPALDO Y RESTAURACIÓN

Los respaldos se ejecutan semanalmente en medios cifrados y en la nube institucional. Toda restauración será verificada mediante controles de integridad y registrada en bitácora técnica. La primera prueba de restauración se realizará en el cuarto trimestre de 2025 y se documentará en el Anexo B.

## 9. OPERACIÓN DEGRADADA / SITIO ALTERNO

Ante incidentes mayores, la Secretaría TIC habilitará la operación degradada mediante:

- Uso de plataformas en la nube (correo y portal alternos).
- Procedimientos manuales temporales.
- Reubicación a sitio alternativo definido por la Alcaldía.

## 10. ROLES Y RESPONSABILIDADES

El Comité DRP está conformado por: Coordinador (Secretario TIC), Oficial de Seguridad Digital, Apoyo Técnico TIC, Jurídica y Comunicaciones.

## 11. MATRIZ DE PROVEEDORES Y SLA

Proveedores clave: Costatel (conectividad y firewall, SLA 99.5%), 1Cero1 (plataformas de trámites, servicio de nube SLA 98%).

## 12. PLAN DE COMUNICACIÓN

Los canales alternos incluyen correo institucional alternativo, teléfono institucional y PQRSD del portal web.

## 13. PRUEBAS, INDICADORES Y CICLO PDCA

El DRP se evaluará semestralmente mediante simulacros controlados, con los siguientes indicadores:

Elemento	Descripción / Indicador	Frecuencia	Responsable
Pruebas de restauración	Simulacros controlados de recuperación de sistemas críticos.	Semestral	Secretario TIC / Oficial de Seguridad Digital
Indicador MTTR	Tiempo promedio de recuperación frente a incidentes.	Semestral	Apoyo Técnico
% RTO cumplido	Porcentaje de sistemas recuperados dentro del tiempo objetivo (RTO).	Semestral	Comité TIC





% Restauraciones validadas	Porcentaje de respaldos verificados correctamente tras cada prueba.	Trimestral	Técnico de Soporte
% Hallazgos cerrados ≤ 60 días	Cumplimiento del plan de mejora derivado de simulacros.	Trimestral	Comité de Gestión

Fase	Descripción
Planificar (Plan)	Identificación de procesos críticos y definición de tiempos de recuperación (RTO/RPO).
Hacer (Do)	Ejecución de respaldos, restauraciones y simulacros planificados.
Verificar (Check)	Evaluación de resultados, cumplimiento de indicadores y hallazgos.
Actuar (Act)	Ajuste de procedimientos, actualización del plan y comunicación a los comités.

#### 14. ARTICULACIÓN INSTITUCIONAL (MIPG, MECI, POLÍTICAS TIC)

Este DRP se articula con la Política de Seguridad Digital 2025, la Política de Respaldo Institucional y el Plan de Continuidad del Negocio (BCP). Además, se integra con la gestión del riesgo del MIPG y el MECI, garantizando coherencia en la gestión de la continuidad institucional.

#### 15. MARCO NORMATIVO ACTUALIZADO 2025

El presente plan se fundamenta en las siguientes normas y guías:

Norma / Guía	Descripción o Enfoque Aplicable al BCP
<b>Decreto 767 de 2022</b>	Adopta la Política de Gobierno Digital, estableciendo lineamientos para la gestión de servicios digitales y continuidad operativa.
<b>Decreto 620 de 2020</b>	Define la Política de Seguridad Digital del Estado colombiano, orientando la gestión de riesgos, recuperación y resiliencia tecnológica.
<b>Resolución 1519 de 2020</b>	Reglamenta la implementación de los lineamientos de Gobierno Digital, incluyendo los componentes de seguridad y continuidad.
<b>Ley 1712 de 2014</b>	Regula el derecho de acceso a la información pública y la obligación de garantizar la disponibilidad continua de los servicios informativos.
<b>Ley 1581 de 2012</b>	Establece principios y disposiciones para la protección de datos personales durante incidentes o restauraciones de sistemas.
<b>Ley 527 de 1999</b>	Reconoce la validez jurídica de los mensajes de datos y las firmas digitales, esenciales en la gestión electrónica de información.
<b>Guía 10 MinTIC (2023)</b>	Establece los lineamientos para la elaboración del Plan de Continuidad del Negocio TIC en entidades públicas.
<b>Guía 11 MinTIC (2023)</b>	Define la metodología para desarrollar el Análisis de Impacto al Negocio (BIA) y determinar los tiempos de recuperación (RTO/RPO).





---

<b>Guía DAFP (2024)</b>	Proporciona orientaciones para el diseño del Plan de Recuperación Institucional y su articulación con el MIPG.
<b>ISO 22301:2019 e ISO/IEC 27031</b>	Normas internacionales para la gestión de continuidad del negocio y la preparación ante incidentes de Tecnologías de la Información.

---

## 16. ANÁLISIS DE RIESGOS Y ESCENARIOS

Riesgos críticos: ciberataques, fallas eléctricas, inundaciones, sabotaje o robo de equipos. Controles existentes: antivirus, firewall, UPS, CCTV y protocolos de contingencia. Escenarios contemplados: interrupciones prolongadas, ataques cibernéticos, pérdida de información y desastres naturales.

## 17. CONCLUSIONES

El DRP versión 1.1 Final Actualizada consolida la capacidad institucional para responder ante incidentes TIC, fortalece la continuidad del negocio digital y garantiza el cumplimiento de los lineamientos MinTIC, DAFP y FURAG.

## 18. ELABORACIÓN Y APROBACIÓN

---

Gustavo Rafael Cardoria Herrera  
Secretario TIC – Coordinador DRP

### NOTA TÉCNICA INTERNA – TRAZABILIDAD FURAG

Este documento corresponde a la versión 1.1 en revisión técnica inicial del Plan de Recuperación ante Desastres Tecnológicos (DRP). Cumple con la estructura definida por las guías MinTIC 10 y 11, la Guía DAFP 2024 y los criterios de Seguridad Digital del FURAG 2025. Actualmente se encuentra en proceso de revisión técnica y jurídica, pendiente de ejecución de prueba piloto y aprobación en comité.

