POLÍTICA DE GENERACIÓN Y RESTAURACIÓN DE COPIAS DE RESPALDO

Alcaldía de Yarumal

2025

Control de versiones

Año	Versión
2025	Versión 1

Tabla de contenido

Introducción

La Alcaldía Municipal de Yarumal, en su compromiso con la gestión eficiente, transparente y segura de la información, establece la presente Política de Generación y Restauración de Copias de Respaldo como un pilar fundamental para garantizar la continuidad operativa, la protección de datos críticos y el cumplimiento de las normativas nacionales e internacionales aplicables. Esta política responde a la necesidad de salvaguardar la integridad, confidencialidad y disponibilidad de la información generada y gestionada por las dependencias de la Alcaldía, en un contexto donde los riesgos tecnológicos, como fallos de hardware, ciberataques o errores humanos, representan una amenaza constante.

Propósito

El propósito de esta política es definir los lineamientos, procedimientos y responsabilidades para la generación, almacenamiento y restauración de copias de respaldo de la información crítica y misional de la Alcaldía. Se busca minimizar la pérdida de datos, garantizar la recuperación oportuna frente a incidentes y cumplir con los requisitos legales y normativos que rigen la gestión de la información en el sector público colombiano.

Alcance

Esta política aplica a todos los sistemas de información, bases de datos, aplicaciones y procesos de la Alcaldía Municipal de Yarumal, abarcando la información generada por todas las dependencias, con especial énfasis en datos personales, financieros, de almacén y otros datos considerados críticos para la operación de la entidad. La política involucra a todo el personal, contratistas y terceros que interactúen con los sistemas de información de la Alcaldía.

Marco normativo

Norma	Descripción
constitución política	artículo 15 que reconoce el derecho a la intimidad personal y familiar y al buen nombre. Artículo 20 en donde se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de

Norma	Descripción
	informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Artículo 76 que establece que el espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del estado. Artículo 101 que incluye al espectro electromagnético como parte del territorio colombiano.
Ley 527 de 1999 (Comercio Electrónico)	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2 y 5), el principio de equivalencia funcional (artículos 6, 7, 8, 12, 13 y 28), la autenticación electrónica (artículo 17), la firma electrónica simple (artículo 7), la firma digital (artículo 28), y la firma electrónica certificada (artículo 30, modificado por el artículo 161 del Decreto Ley 019 de 2012)
Ley 594 de 2000 (Ley General de Archivos).	Habilita el uso de nuevas tecnologías de manera general, lo cual viabiliza el uso de firmas electrónicas simples, certificadas y firmas digitales.
Ley 599 de 2000 (Código Penal)	En particular las materias atinentes a: i) violación a los derechos patrimoniales de autor y derechos conexos (modificación

Norma	Descripción
	introducida por la Ley 1032 de 2006); ii) protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las TIC (modificación introducida por la Ley 1273 de 2009).
Ley 1266 de 2008.	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1437 de 2011 (Utilización de medios electrónicos en el procedimiento administrativo).	Consagra la utilización de medios electrónicos en el procedimiento administrativo, permitiendo adelantar trámites electrónicos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes electrónicos y sedes electrónicas. Lo anterior, con el fin de que los ciudadanos interactúen con validez jurídica y probatoria

Norma	Descripción
	(Capítulo IV, artículos 53 al 64)
Ley 1581 de 2012.	Por la cual se dictan disposiciones generales para la protección de datos. Esta Ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1928 de 2018	Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.
Ley 2080 de 2021	Por medio de la cual se reforma el Código de Procedimiento Administrativo y de lo Contencioso Administrativo -Ley 1437 de 2011- y se dictan otras disposiciones en materia de descongestión en los procesos que se tramitan ante la jurisdicción.
Decreto 2609 de 2012.	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental

Norma	Descripción
	para todas las Entidades del Estado.
Decreto 2758 de 2012 (Modifica la Estructura del ministerio De Defensa Nacional).	Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente, le encarga a la Dirección de Seguridad Pública y de Infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales
Decreto 103 De 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1081 de 2015	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República. Libro 2 Parte 1 Título 1 Disposiciones generales en materia de trasparencia y del derecho de acceso a la información pública nacional.

Norma	Descripción
Decreto 1413 de 2017.	Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto338 de 2022.	Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
Decreto 767 de 2022.	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del

Norma	Descripción
	Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1263 de 2022	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información Y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.
Decreto Municipal 477 de 2021	Por medio del cual se establece y regula la estrategia territorial de ciberseguridad en el municipio de Itagüí para la vigencia 2020-2023.
Acuerdo 003 de 2015	Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y ciberdefensa.
CONPES 3854 de 2016.	Política Nacional de Seguridad Digital.

Definiciones y Conceptos Clave

Para garantizar una comprensión clara y unificada de los términos utilizados en esta política, se presentan las siguientes definiciones, basadas en estándares internacionales (ISO/IEC 27001:2022, ISO/IEC 38500:2015), el marco normativo colombiano y las buenas prácticas en gestión de la información:

- **Copia de Respaldo (Backup)**: Réplica de datos, sistemas o aplicaciones, creada y almacenada con el propósito de restaurar la información en caso de pérdida, corrupción o interrupción del servicio. Puede ser completa, incremental o diferencial, según el método empleado.
- **Restauración**: Proceso de recuperación de datos, sistemas o aplicaciones a partir de una copia de respaldo, con el objetivo de restablecer la operatividad tras un incidente.
- **Datos Críticos**: Información esencial para la operación de la Alcaldía, incluyendo datos personales, financieros, de almacén y aquellos necesarios para cumplir con obligaciones legales o misionales.
- **RPO (Recovery Point Objective)**: Cantidad máxima de datos que la Alcaldía puede permitirse perder, medida en tiempo entre la última copia de respaldo y el momento del incidente. Representa la pérdida de datos aceptable.
- **RTO (Recovery Time Objective)**: Tiempo máximo aceptable que un sistema, aplicación o proceso puede estar inactivo antes de causar un impacto significativo en las operaciones de la Alcaldía.
- **Integridad**: Propiedad de la información que asegura que no ha sido alterada o modificada de manera no autorizada.
- **Confidencialidad**: Propiedad que garantiza que la información solo es accesible para las personas o sistemas autorizados.
- **Disponibilidad**: Propiedad que asegura que la información y los sistemas están accesibles y operativos para los usuarios autorizados cuando se requieran.
- **Gestión de Riesgos Tecnológicos**: Proceso sistemático de identificación, evaluación y mitigación de riesgos que puedan afectar la seguridad, continuidad o integridad de los sistemas de información.

- **Almacenamiento Seguro**: Ubicación física o lógica (on-site, off-site o en la nube) donde se guardan las copias de respaldo, protegidas mediante medidas de seguridad como cifrado y controles de acceso.
- **Incidente de Seguridad**: Evento que compromete la confidencialidad, integridad o disponibilidad de la información, como ciberataques, fallos de hardware o errores humanos.
- **Sistema Misional**: Plataforma tecnológica que soporta procesos críticos de la Alcaldía, como la gestión financiera, documental o de servicios públicos.
- **Auditoría de TIC**: Revisión sistemática de los procesos, sistemas y controles tecnológicos para verificar el cumplimiento de esta política y normativas aplicables.
- **Gestión Documental**: Conjunto de procesos y actividades orientados a la producción, organización, conservación, uso y disposición final de los documentos generados o recibidos por la Alcaldía, conforme a los lineamientos del Archivo General de la Nación.
- **Documento Electrónico de Archivo**: Registro de información generado o recibido en el ejercicio de las funciones de la Alcaldía, almacenado en formato digital, que debe ser respaldado y conservado según las normas de gestión documental.

Objetivos de la Política

La Política de Generación y Restauración de Copias de Respaldo de la Alcaldía Municipal de Yarumal establece los siguientes objetivos para garantizar la seguridad, continuidad y cumplimiento normativo en la gestión de la información:

1. **Garantizar la Continuidad Operativa**: Asegurar que los sistemas misionales, procesos y servicios críticos de la Alcaldía permanezcan operativos ante incidentes tecnológicos, mediante la generación y restauración oportuna de copias de respaldo, minimizando interrupciones en la atención a la ciudadanía y la ejecución de funciones públicas.
2. **Proteger la Integridad, Confidencialidad y Disponibilidad de la Información**: Salvaguardar los datos críticos, incluyendo datos personales, financieros y de almacén, mediante la implementación de copias de respaldo seguras y procedimientos de restauración confiables, alineados con los

principios de seguridad de la información establecidos en la norma ISO/IEC 27001:2022.

3. **Cumplir con Requisitos Legales y Normativos**: Asegurar que la gestión de copias de respaldo cumpla con las disposiciones de la Ley 1581 de 2012 (protección de datos personales), la Ley 1712 de 2014 (transparencia y acceso a la información), los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y las normas del Archivo General de la Nación para la conservación de documentos electrónicos.
4. **Minimizar la Pérdida de Datos**: Establecer procedimientos que reduzcan al mínimo la pérdida de información crítica, definiendo puntos objetivos de recuperación (RPO) adecuados para los procesos misionales de la Alcaldía, considerando las limitaciones actuales de infraestructura.
5. **Optimizar los Tiempos de Recuperación**: Implementar procesos de restauración que permitan recuperar sistemas y datos en el menor tiempo posible, definiendo tiempos objetivos de recuperación (RTO) que garanticen la continuidad de los servicios esenciales de la Alcaldía.
6. **Fomentar una Cultura de Seguridad de la Información**: Promover la sensibilización y capacitación del personal y contratistas en buenas prácticas de generación y restauración de copias de respaldo, fortaleciendo la resiliencia tecnológica de la entidad.
7. **Facilitar la Gobernanza de TIC**: Alinear la gestión de copias de respaldo con los principios de gobernanza de tecnologías de la información establecidos en la norma ISO/IEC 38500:2015, asegurando una administración eficiente, transparente y responsable de los recursos tecnológicos.
8. **Mitigar Riesgos Tecnológicos**: Identificar y gestionar riesgos asociados a la pérdida de datos, fallos de hardware o ciberataques, implementando medidas preventivas como el almacenamiento seguro y la verificación periódica de las copias de respaldo.

Principios Rectores

La Política de Generación y Restauración de Copias de Respaldo de la Alcaldía Municipal de Yarumal se fundamenta en los siguientes principios rectores, que orientan la gestión de la información y aseguran la alineación con los objetivos

estratégicos de la entidad, los estándares internacionales (ISO/IEC 27001:2022, ISO/IEC 38500:2015) y el marco normativo colombiano:

1. **Seguridad de la Información**: Garantizar la confidencialidad, integridad y disponibilidad de los datos críticos de la Alcaldía, implementando medidas técnicas y organizativas que protejan la información contra accesos no autorizados, alteraciones o pérdidas, en cumplimiento de la Ley 1581 de 2012 y la norma ISO/IEC 27001:2022.
2. **Continuidad Operativa**: Priorizar la disponibilidad de los sistemas misionales y servicios esenciales, mediante la generación y restauración oportuna de copias de respaldo, para minimizar interrupciones en la atención a la ciudadanía y el cumplimiento de las funciones públicas.
3. **Gobernanza de TIC**: Asegurar una gestión responsable, transparente y eficiente de los recursos tecnológicos, alineada con los principios de la norma ISO/IEC 38500:2015, promoviendo la toma de decisiones informadas y el uso óptimo de la infraestructura existente.
4. **Cumplimiento Normativo**: Adherirse a las disposiciones legales y regulatorias aplicables, incluyendo la Ley 1712 de 2014 (transparencia y acceso a la información), los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y las normas del Archivo General de la Nación, asegurando que las copias de respaldo soporten los requisitos de conservación documental.
5. **Gestión de Riesgos**: Adoptar un enfoque proactivo para identificar, evaluar y mitigar riesgos tecnológicos que puedan comprometer la información, como fallos de hardware, ciberataques o errores humanos, integrando medidas preventivas en los procesos de respaldo y restauración.
6. **Eficiencia y Austeridad**: Optimizar el uso de los recursos tecnológicos disponibles, como servidores físicos y dispositivos de almacenamiento, para implementar soluciones de respaldo efectivas y sostenibles, considerando las limitaciones presupuestales de la Alcaldía.
7. **Transparencia y Rendición de Cuentas**: Documentar y auditar los procesos de generación y restauración de copias de respaldo, garantizando trazabilidad y facilitando la supervisión por parte de entidades de control y la ciudadanía, en línea con los principios de la Ley 1712 de 2014.

8. **Capacitación y Concienciación**: Fomentar la formación continua del personal y contratistas en buenas prácticas de gestión de copias de respaldo, promoviendo una cultura de seguridad de la información y responsabilidad compartida.
9. **Mejora Continua**: Revisar y actualizar periódicamente los procesos de respaldo y restauración, incorporando lecciones aprendidas, avances tecnológicos y retroalimentación de auditorías, para fortalecer la resiliencia tecnológica de la Alcaldía.

Alcance y Aplicación

Alcance

La **Política de Generación y Restauración de Copias de Respaldo** abarca todos los sistemas de información, bases de datos, aplicaciones y procesos tecnológicos que soportan las funciones misionales y administrativas de la Alcaldía Municipal de Yarumal. Incluye, de manera no limitativa, la información generada, almacenada o procesada en:

- Sistemas misionales que gestionan datos financieros, personales, de almacén, documental y otros procesos críticos para la operación de la Alcaldía.
- Infraestructura tecnológica, como servidores físicos, dispositivos de almacenamiento y plataformas web institucionales.
- Documentos electrónicos de archivo, conforme a los requisitos del Archivo General de la Nación.
- Cualquier otro medio digital que contenga información necesaria para el cumplimiento de las obligaciones legales, normativas o misionales de la entidad.

La política cubre todos los datos críticos identificados por la Alcaldía, con especial énfasis en:

- Datos personales, protegidos bajo la Ley 1581 de 2012.
- Datos financieros, esenciales para la gestión presupuestal y la rendición de cuentas.
- Información de almacén, clave para la administración de recursos.

- Información generada por las dependencias, que soporta la planeación, ejecución y control de las actividades institucionales.

Aplicación

Esta política es de obligatorio cumplimiento para:

- **Personal interno**: Todos los funcionarios y empleados de la Alcaldía, independientemente de su nivel jerárquico o área de trabajo, que interactúen con sistemas de información o datos críticos.
- **Contratistas**: Los contratistas de TI y cualquier otro contratista que acceda, gestione o procese información de la Alcaldía.
- **Terceros**: Proveedores, aliados o entidades externas que, en el marco de contratos, convenios o acuerdos, tengan acceso a los sistemas o datos de la Alcaldía, debiendo cumplir con los lineamientos establecidos en esta política.
- **Dependencias**: Todas las áreas administrativas y misionales de la Alcaldía, incluyendo, pero no limitándose a, las responsables de finanzas, planeación, gestión documental, almacén y atención ciudadana.

La política se aplica a todos los procesos relacionados con la gestión de copias de respaldo, desde la planificación y ejecución hasta el monitoreo y auditoría, y debe integrarse en las actividades diarias de las dependencias y los contratistas de TI. Los responsables de su implementación deberán garantizar que los procedimientos sean consistentes con los principios de seguridad, continuidad y cumplimiento normativo establecidos en esta política.

Cualquier excepción al alcance o aplicación de esta política debe ser justificada, documentada y aprobada por el responsable de tecnologías de la información o la autoridad competente designada por la Alcaldía, previa evaluación de los riesgos asociados.

Políticas Específicas

Las siguientes políticas específicas establecen los lineamientos operativos y técnicos para la generación, almacenamiento, restauración y gestión de riesgos asociados a las copias de respaldo en la Alcaldía Municipal de Yarumal. Estas políticas aseguran la protección de datos críticos, la continuidad operativa y el cumplimiento de las normativas aplicables, considerando las limitaciones tecnológicas actuales de la entidad.

1. Frecuencia y Tipos de Copias de Respaldo

1.1. **Copia Completa**: Se realizará una copia de respaldo completa de todos los datos críticos al menos una vez al mes, utilizando los dispositivos de almacenamiento disponibles.
1.2. **Copia Incremental**: Se generarán copias incrementales diarias de los datos críticos modificados desde la última copia, programadas fuera del horario laboral para minimizar el impacto en los sistemas misionales.
1.3. **Priorización de Datos**: Los datos personales y financieros tendrán prioridad para copias incrementales diarias, mientras que otros datos podrán respaldarse semanalmente, según la criticidad y frecuencia de actualización.
1.4. **Automatización**: Cuando sea posible, se utilizarán las funciones de respaldo integradas en los sistemas misionales, gestionadas por los proveedores, para garantizar consistencia y reducir errores humanos.

2. Almacenamiento Seguro de Copias de Respaldo

2.1. **Ubicación Física (On-Site)**: Las copias de respaldo se almacenarán en el dispositivo NAS ubicado en una de las sedes de la Alcaldía, en un entorno físico seguro con controles de acceso restringido.
2.2. **Ubicación Secundaria (Off-Site)**: Se mantendrá una copia completa mensual en discos duros externos, almacenados en una ubicación física diferente a la sede principal, para mitigar riesgos de desastres naturales o incidentes locales.
2.3. **Cifrado**: Todas las copias de respaldo deberán cifrarse utilizando algoritmos estándar para proteger la confidencialidad de los datos, especialmente los datos personales, en cumplimiento de la Ley 1581 de 2012.
2.4. **Inventario**: Se llevará un registro actualizado de todas las copias de respaldo, incluyendo fecha, tipo, ubicación y responsable, para facilitar la trazabilidad y auditoría.

3. Procedimientos de Restauración

3.1. **Plan de Restauración**: Se establecerá un procedimiento documentado para la restauración de datos, que incluirá pasos claros, responsables asignados y tiempos estimados de recuperación.
3.2. **Pruebas de Restauración**: Se realizarán pruebas de restauración al menos una vez al semestre, utilizando copias de respaldo seleccionadas, para verificar la

integridad y funcionalidad de los datos recuperados. Los resultados se documentarán y se utilizarán para mejorar los procedimientos.
3.3. **Prioridad en la Restauración**: En caso de incidente, se priorizará la restauración de datos personales y financieros, seguida de otros datos críticos, según las necesidades operativas de la Alcaldía.
3.4. **Soporte Externo**: Se coordinará con los proveedores de los sistemas misionales para agilizar la restauración, aprovechando su soporte técnico cuando sea necesario.

4. Gestión de Riesgos Asociados

4.1. **Identificación de Riesgos**: Se mantendrá un registro de riesgos tecnológicos que puedan afectar las copias de respaldo, como fallos de hardware, accesos no autorizados o pérdida de dispositivos de almacenamiento.
4.2. **Controles de Acceso**: Solo el personal autorizado tendrá acceso a las copias de respaldo, mediante credenciales seguras y autenticación de dos factores, cuando sea factible.
4.3. **Protección Física**: Los dispositivos de almacenamiento (NAS, discos duros) estarán protegidos contra robos, incendios o daños ambientales, mediante medidas como gabinetes ignífugos o ubicaciones seguras.
4.4. **Revisión Periódica**: Se revisarán los riesgos al menos una vez al año, actualizando las medidas de mitigación según las necesidades y los resultados de auditorías internas.

Estas políticas específicas se implementarán de manera progresiva, optimizando los recursos tecnológicos disponibles y promoviendo la seguridad y continuidad de las operaciones de la Alcaldía. Cualquier desviación de estas políticas deberá ser justificada y aprobada por el responsable de tecnologías de la información, con registro de las razones y medidas correctivas aplicadas.

Roles y Responsabilidades

La implementación efectiva de la Política de Generación y Restauración de Copias de Respaldo en la Alcaldía Municipal de Yarumal requiere la asignación clara de roles y responsabilidades para garantizar la seguridad, continuidad y cumplimiento normativo en la gestión de la información. A continuación, se detallan las responsabilidades de los actores clave involucrados:

1. Responsables de Tecnologías de la Información (TI)

El responsable de TI, en ausencia de una figura formal de jefe de TI, liderará la gestión de copias de respaldo y tendrá las siguientes responsabilidades:

- Coordinar la implementación de esta política, asegurando su alineación con los lineamientos de MINTIC y los estándares ISO/IEC 27001:2022 e ISO/IEC 38500:2015.
- Supervisar la generación, almacenamiento y restauración de copias de respaldo, verificando el cumplimiento de las frecuencias y procedimientos establecidos.
- Gestionar el acceso seguro al NAS y discos duros, asegurando que solo el personal autorizado manipule las copias de respaldo.
- Coordinar con los proveedores de sistemas misionales para garantizar el soporte técnico en procesos de respaldo y restauración.
- Documentar incidentes relacionados con la pérdida o restauración de datos, proponiendo medidas correctivas.
- Reportar anualmente el estado de la gestión de copias de respaldo a la alta dirección de la Alcaldía.

2. Redes y seguridad

La persona especializada en redes y seguridad tendrá las siguientes responsabilidades:

- Configurar y mantener los controles de acceso al NAS y otros dispositivos de almacenamiento, implementando autenticación segura.
- Asegurar que las copias de respaldo estén cifradas para proteger la confidencialidad de los datos, en cumplimiento de la Ley 1581 de 2012.
- Monitorear posibles riesgos de seguridad que puedan comprometer las copias de respaldo.
- Colaborar en la identificación y mitigación de riesgos tecnológicos, actualizando el registro de riesgos al menos una vez al año.

3. Soporte e Infraestructura

El personal especializado en soporte e infraestructura tendrá las siguientes responsabilidades:

- Ejecutar las copias de respaldo completas e incrementales según las frecuencias establecidas, utilizando las herramientas disponibles en los sistemas misionales o dispositivos de almacenamiento.
- Verificar la integridad de las copias de respaldo generadas, asegurando que sean accesibles y completas.
- Gestionar el almacenamiento físico de copias off-site, garantizando su protección contra robos o daños.
- Realizar pruebas de restauración semestrales, documentando los resultados y reportando cualquier anomalía al responsable de TI.
- Mantener el inventario actualizado de copias de respaldo, incluyendo fecha, tipo y ubicación.

4. Portal web

El personal encargado del portal web, tendrá las siguientes responsabilidades:

- Asegurar que las copias de respaldo del portal web institucional se realicen conforme a las frecuencias establecidas, coordinando con el proveedor del servidor compartido.
- Verificar que los datos del portal web cumplan con la Ley 1712 de 2014 y estén respaldados adecuadamente.
- Apoyar en la documentación de procedimientos y registros relacionados con la gestión de copias de respaldo, facilitando auditorías internas y externas.
- Proponer mejoras a los procesos de respaldo basadas en normativas de MINTIC o avances tecnológicos, dentro de las limitaciones presupuestales.

5. Dependencias

Cada dependencia de la Alcaldía tendrá las siguientes responsabilidades:

- Identificar y reportar al responsable de TI los datos críticos generados o gestionados, especificando su nivel de criticidad.

- Notificar al equipo de TI cualquier incidente que pueda requerir la restauración de datos.
- Colaborar en las pruebas de restauración, validando que los datos recuperados sean funcionales y completos para sus procesos.

6. Auditoría Interna

El área o persona designada para auditoría interna, o en su defecto el responsable de TI, tendrá las siguientes responsabilidades:

- Revisar semestralmente el cumplimiento de esta política, incluyendo la generación, almacenamiento y pruebas de restauración de copias de respaldo.
- Verificar que los registros de copias y los reportes de incidentes estén actualizados y sean trazables.
- Reportar hallazgos y recomendaciones a la alta dirección para la mejora continua de los procesos.

7. Proveedores de Sistemas Misionales

Los proveedores de los sistemas misionales tendrán las siguientes responsabilidades:

- Proporcionar soporte técnico para la generación y restauración de copias de respaldo, utilizando las funcionalidades integradas en sus sistemas.
- Garantizar que las copias generadas cumplan con los requisitos de integridad y disponibilidad establecidos en esta política.
- Informar al responsable de TI sobre cualquier limitación o incidente relacionado con las funciones de respaldo de sus sistemas.

8. Alta Dirección

La alta dirección de la Alcaldía tendrá las siguientes responsabilidades:

- Aprobar y promover la implementación de esta política como parte de la estrategia de gobernanza de TIC.
- Asignar los recursos necesarios, dentro de las posibilidades presupuestales, para fortalecer la infraestructura de copias de respaldo.

- Revisar los reportes anuales del responsable de TI y los hallazgos de auditorías, tomando decisiones para la mejora continua.

Todos los roles mencionados deberán cumplir con esta política y colaborar en su implementación, asegurando la protección de los datos críticos y la continuidad operativa de la Alcaldía. El incumplimiento de estas responsabilidades será sujeto a las sanciones establecidas en las disposiciones finales de esta política.

Procedimientos Operativos

Los siguientes procedimientos operativos detallan los pasos específicos para la generación, almacenamiento, restauración y monitoreo de copias de respaldo en la Alcaldía Municipal de Yarumal. Estos procedimientos están diseñados para ser prácticos, considerando la infraestructura tecnológica y el soporte de los proveedores de los sistemas misionales. Se prioriza la simplicidad para facilitar su ejecución por los contratistas de TI y el cumplimiento de las normativas aplicables, incluyendo la Ley 1581 de 2012, la Ley 1712 de 2014 y los lineamientos del Archivo General de la Nación.

1. Generación de Copias de Respaldo

1.1. **Planificación y Programación**

- Las copias completas se realizarán el primer lunes de cada mes, entre las 19:00 y las 21:00, para minimizar el impacto en las operaciones diarias.
- Las copias incrementales se realizarán diariamente, de lunes a viernes, entre las 18:00 y las 20:00.
- El encargado de soporte e infraestructura coordinará con los proveedores de los sistemas misionales para utilizar las funcionalidades de respaldo integradas, cuando estén disponibles.

1.2. **Ejecución de Copias Completas**

- Iniciar sesión en el sistema de administración del NAS con credenciales seguras.
- Seleccionar los directorios o bases de datos que contienen datos críticos.
- Ejecutar la copia completa al NAS, asegurando que el destino tenga suficiente espacio de almacenamiento.

- Verificar que la copia se haya completado sin errores, revisando los registros generados por el NAS o el sistema misional.
- Registrar la copia en el inventario de respaldos.

1.3. **Ejecución de Copias Incrementales**

- Iniciar sesión en el sistema de administración del NAS.
- Configurar la copia incremental para respaldar solo los datos modificados desde la última copia.
- Ejecutar la copia al NAS y verificar su finalización sin errores.
- Actualizar el inventario de respaldos con los detalles de la copia incremental.

1.4. **Priorización**

- Priorizar los datos personales y financieros para copias incrementales diarias.
- Incluir datos de almacén y documentos electrónicos de archivo en copias completas mensuales, con copias incrementales semanales si se detectan cambios significativos.

2. Almacenamiento Seguro

2.1. **Almacenamiento en el NAS (On-Site)**

- Guardar todas las copias en el NAS, ubicado en una sala de servidores con acceso restringido.
- Asegurar que el NAS esté protegido contra fallos eléctricos mediante un sistema de respaldo de energía.
- Cifrar las copias utilizando herramientas disponibles en el NAS para proteger la confidencialidad, en cumplimiento de la Ley 1581 de 2012.

2.2. **Almacenamiento Off-Site**

- Copiar la copia completa mensual a un disco duro externo el primer lunes de cada mes.
- Almacenar el disco duro en una ubicación secundaria (ej. otra dependencia de la Alcaldía), en un gabinete ignífugo con acceso restringido.
- Verificar que el disco duro esté cifrado antes de su traslado.

- Actualizar el inventario de respaldos con la ubicación del disco duro off-site.

2.3. **Gestión de Espacio**

- Monitorear mensualmente la capacidad del NAS para evitar la falta de espacio, eliminando copias obsoletas (anteriores a 6 meses) tras verificar que no sean necesarias para auditorías.
- Mantener al menos dos copias completas recientes en el NAS y una en el disco duro off-site.

3. Pruebas de Restauración

3.1. **Frecuencia y Planificación**

- Realizar pruebas de restauración cada seis meses, programadas para un fin de semana fuera del horario laboral.
- Seleccionar una copia completa y una incremental reciente para la prueba.

3.2. **Procedimiento de Prueba**

- Iniciar sesión en el sistema de administración del NAS con credenciales seguras.
- Restaurar la copia seleccionada a un entorno de prueba para evitar interferencias con los sistemas en producción.
- Verificar la integridad de los datos restaurados, asegurando que sean accesibles y completos.
- Coordinar con las dependencias relevantes para validar la funcionalidad de los datos restaurados.
- Documentar los resultados en un informe de prueba, firmado por el encargado de soporte e infraestructura y el responsable de TI.

3.3. **Acciones Correctivas**

- Si se detectan errores en la restauración, investigar la causa (ej. corrupción de datos, configuración incorrecta) y coordinar con el proveedor del sistema misional, si es necesario.
- Actualizar los procedimientos operativos según los hallazgos para prevenir problemas futuros.

4. Monitoreo y Auditoría

4.1. **Monitoreo Continuo**

- El encargado del proceso de redes y seguridad revisará semanalmente los registros del NAS para detectar errores o intentos de acceso no autorizados.
- El encargado del proceso de soporte e infraestructura verificará mensualmente la capacidad del NAS y la integridad de las copias recientes.

4.2. **Auditoría Interna**

- La persona designada para auditoría interna, revisará semestralmente el inventario de respaldos, los informes de pruebas de restauración y los registros de incidentes.
- Verificar el cumplimiento de las frecuencias de respaldo, el cifrado de copias y la protección física de los dispositivos de almacenamiento.
- Generar un informe de auditoría para la alta dirección, incluyendo recomendaciones de mejora.

4.3. **Respuesta a Incidentes**

- En caso de un incidente que requiera restauración, el encargado de soporte e infraestructura iniciará la restauración siguiendo el procedimiento documentado, priorizando datos personales y financieros.
- Notificar al responsable de TI y registrar el incidente (causa, impacto, tiempo de recuperación).
- Coordinar con los proveedores de los sistemas misionales para soporte técnico, si es necesario.

5. Documentación

5.1. **Inventario de Respaldos**

- Mantener un registro digital con los detalles de cada copia: fecha, tipo (completa/incremental), tamaño, ubicación (NAS/disco duro), responsable.
- Almacenar el inventario en el NAS, con una copia en el disco duro off-site.

5.2. **Informes y Registros**

- Documentar todas las copias, pruebas de restauración e incidentes en formatos estandarizados.
- Archivar los informes en el sistema de gestión documental de la Alcaldía, conforme a las normas del Archivo General de la Nación.
- Asegurar que los registros sean accesibles para auditorías internas y externas.

Estos procedimientos operativos deberán revisarse anualmente o tras cambios significativos en la infraestructura tecnológica, para garantizar su efectividad y alineación con las necesidades de la Alcaldía. Cualquier desviación de estos procedimientos debe ser aprobada por el responsable de TI, con registro de las razones y acciones correctivas.

Gestión de Riesgos y Seguridad

La gestión de riesgos y la seguridad son componentes esenciales para garantizar la integridad, confidencialidad y disponibilidad de las copias de respaldo en la Alcaldía Municipal de Yarumal. Esta sección establece los lineamientos para identificar, evaluar y mitigar riesgos tecnológicos asociados a la generación, almacenamiento y restauración de copias de respaldo, alineándose con la norma ISO/IEC 27001:2022, los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y las normativas colombianas, incluyendo la Ley 1581 de 2012 y las disposiciones del Archivo General de la Nación.

1. Identificación de Riesgos

1.1. **Riesgos Tecnológicos**

- **Fallos de Hardware**: Pérdida de datos debido a fallos en servidores físicos, NAS o discos duros externos.
- **Ciberataques**: Accesos no autorizados, malware o ransomware que comprometan las copias de respaldo o los sistemas misionales.
- **Errores Humanos**: Eliminación accidental de copias, configuración incorrecta de respaldos o mal manejo de dispositivos de almacenamiento.

1.2. **Riesgos Físicos**

- **Desastres Naturales**: Inundaciones, terremotos o incendios que dañen los servidores o dispositivos de almacenamiento on-site u off-site.

- **Robo o Vandalismo**: Pérdida de discos duros externos o acceso físico no autorizado a la sala de servidores.
- **Interrupciones Eléctricas**: Fallos en el suministro eléctrico que interrumpan la generación de copias o dañen el NAS.

1.3. **Riesgos Operativos**

- **Falta de Pruebas**: Copias de respaldo corruptas o no funcionales que no se detecten por la ausencia de pruebas de restauración.
- **Limitaciones de Infraestructura**: Insuficiente capacidad de almacenamiento en el NAS o discos duros, lo que impida generar nuevas copias.
- **Dependencia de Proveedores**: Retrasos o fallos en el soporte técnico de los proveedores de sistemas misionales para respaldos o restauraciones.

1.4. **Registro de Riesgos**

- El encargado de redes y seguridad mantendrá un registro de riesgos actualizado, documentando cada riesgo identificado, su probabilidad, impacto y medidas de mitigación propuestas.
- El registro se revisará anualmente o tras incidentes significativos, incorporando nuevos riesgos detectados.

2. Evaluación de Riesgos

2.1. **Metodología**

- Clasificar los riesgos según su probabilidad (baja, media, alta) y su impacto (bajo, moderado, crítico) en la continuidad operativa y la seguridad de los datos.
- Priorizar los riesgos con alta probabilidad y alto impacto, como fallos de hardware o ciberataques, para la implementación inmediata de medidas de mitigación.

2.2. **Criterios de Impacto**

- **Confidencialidad**: Pérdida de datos personales que viole la Ley 1581 de 2012.
- **Integridad**: Corrupción de datos financieros o documentos electrónicos de archivo, afectando la rendición de cuentas o la gestión documental.

- **Disponibilidad**: Interrupción de sistemas misionales por más de 48 horas (RTO objetivo), impactando los servicios ciudadanos.

2.3. **Responsabilidad**

- El encargado de redes y seguridad liderará la evaluación de riesgos, con apoyo del responsable de TI y el encargado de soporte e infraestructura.
- Los resultados de la evaluación se documentarán en el registro de riesgos y se presentarán al responsable de TI para su aprobación.

3. Medidas de Mitigación

3.1. **Mitigación de Riesgos Tecnológicos**

- **Fallos de Hardware**: Mantener un sistema de respaldo de energía (UPS) para el NAS y los servidores, y verificar mensualmente el estado físico de los dispositivos de almacenamiento.
- **Ciberataques**: Implementar controles de acceso estrictos al NAS (contraseñas seguras, autenticación de dos factores cuando sea posible) y cifrar todas las copias de respaldo con AES-256.
- **Errores Humanos**: Capacitar anualmente a los encargados de TI en procedimientos de respaldo, y establecer listas de verificación para la generación y verificación de copias.

3.2. **Mitigación de Riesgos Físicos**

- **Desastres Naturales**: Almacenar copias off-site en discos duros externos, en una ubicación secundaria protegida (ej. gabinete ignífugo en otra dependencia).
- **Robo o Vandalismo**: Restringir el acceso físico a la sala de servidores mediante cerraduras y asignar un responsable para el control de llaves.
- **Interrupciones Eléctricas**: Asegurar que el NAS y los servidores estén conectados a un UPS con capacidad para al menos 30 minutos de operación, permitiendo el apagado seguro de los equipos.

3.3. **Mitigación de Riesgos Operativos**

- **Falta de Pruebas**: Realizar pruebas de restauración semestrales, documentando los resultados para garantizar la funcionalidad de las copias.

- **Limitaciones de Infraestructura**: Monitorear mensualmente la capacidad del NAS, eliminando copias obsoletas (anteriores a 6 meses) tras verificar su irrelevancia para auditorías.
- **Dependencia de Proveedores**: Establecer acuerdos claros con los proveedores de sistemas misionales, definiendo tiempos de respuesta para soporte en respaldos y restauraciones.

4. Seguridad de las Copias de Respaldo

4.1. **Controles de Acceso**

- Limitar el acceso al NAS y discos duros externos a los encargados de TI autorizados (redes/seguridad, soporte/infraestructura).
- Utilizar contraseñas robustas (mínimo 12 caracteres, combinando letras, números y símbolos) y cambiarlas cada 6 meses.
- Registrar todos los accesos al NAS en un log, revisado semanalmente por el encargado de redes y seguridad.

4.2. **Cifrado**

- Cifrar todas las copias de respaldo (on-site y off-site) utilizando herramientas disponibles en el NAS o software de cifrado estándar (ej. AES-256).
- Gestionar las claves de cifrado de manera segura, almacenándolas en un medio físico separado (ej. USB en un gabinete ignífugo), accesible solo para el responsable de TI.

4.3. **Protección Física**

- Ubicar el NAS en una sala de servidores con cerradura física y acceso restringido.
- Almacenar los discos duros off-site en un gabinete ignífugo en una ubicación secundaria, con control de acceso documentado.
- Verificar trimestralmente las condiciones físicas de los dispositivos de almacenamiento (ej. temperatura, humedad, integridad).

5. Respuesta a Incidentes de Seguridad

5.1. **Detección y Notificación**

- El encargado de redes y seguridad monitoreará semanalmente los logs del NAS para detectar accesos no autorizados o anomalías.
- Cualquier incidente debe notificarse al responsable de TI dentro de las 2 horas posteriores a su detección.

5.2. **Respuesta**

- Iniciar la restauración de datos según el procedimiento operativo, priorizando datos personales y financieros.
- Coordinar con los proveedores de sistemas misionales para soporte técnico, si el incidente afecta sus plataformas.
- Documentar el incidente (causa, impacto, acciones tomadas) en un informe, archivado en el sistema de gestión documental.

5.3. **Lecciones Aprendidas**

- Analizar cada incidente para identificar causas raíz y actualizar el registro de riesgos.
- Revisar los procedimientos operativos y las medidas de mitigación según los hallazgos, con aprobación del responsable de TI.

6. Monitoreo y Mejora Continua

6.1. **Revisión Periódica**

- El responsable de TI coordinará una revisión anual de los riesgos y medidas de seguridad, con participación de los contratistas de TI.
- Incorporar avances tecnológicos o cambios normativos dentro de las limitaciones presupuestales.

6.2. **Auditoría**

- Incluir la gestión de riesgos y seguridad en las auditorías internas semestrales, verificando el cumplimiento de esta sección.
- Facilitar el acceso a registros de riesgos, logs de acceso y informes de incidentes para auditorías externas por entidades de control.

Monitoreo, Evaluación y Mejora Continua

La Alcaldía Municipal de Yarumal reconoce que el monitoreo, la evaluación y la mejora continua son fundamentales para garantizar la efectividad, seguridad y cumplimiento normativo de los procesos de generación, almacenamiento y restauración de copias de respaldo. Esta sección establece los lineamientos para supervisar el desempeño de la política, evaluar su implementación mediante indicadores clave y promover mejoras basadas en retroalimentación, auditorías y avances tecnológicos. Los procedimientos se alinean con la norma ISO/IEC 27001:2022 (gestión de la seguridad de la información), ISO/IEC 38500:2015 (gobernanza de TIC), los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y las normativas colombianas, incluyendo la Ley 1581 de 2012 y la Ley 1712 de 2014.

1. Monitoreo Continuo

1.1. **Objetivo**

- Supervisar regularmente los procesos de generación, almacenamiento y restauración de copias de respaldo para detectar desviaciones, errores o riesgos potenciales, asegurando la continuidad operativa y la seguridad de los datos críticos.

1.2. **Actividades de Monitoreo**

- **Verificación de Copias**: Los encargados de soporte e infraestructura revisará semanalmente los registros del NAS para confirmar que las copias completas e incrementales se generen según las frecuencias establecidas.
- **Control de Seguridad**: El contratista de redes y seguridad monitoreará semanalmente los logs de acceso al NAS, identificando intentos de acceso no autorizados o anomalías.
- **Capacidad de Almacenamiento**: El encargado de soporte e infraestructura verificará mensualmente la capacidad del NAS, asegurando suficiente espacio para nuevas copias y gestionando copias.
- **Incidentes**: El responsable de TI revisará mensualmente los reportes de incidentes relacionados con copias de respaldo, evaluando su impacto y las acciones correctivas implementadas.

1.3. **Documentación**

- Los resultados del monitoreo se registrarán en un formato, incluyendo fecha, actividad, hallazgos y responsable.
- Los registros se archivarán en el sistema de gestión documental, conforme a las normas del Archivo General de la Nación, y estarán disponibles para auditorías internas y externas.

2. Evaluación del Desempeño

2.1. **Indicadores Clave de Desempeño (KPIs)**

- **Tasa de Éxito de Copias**: Porcentaje de copias completas e incrementales generadas sin errores, con un objetivo del 95% mensual.
- **Tiempo de Restauración (RTO)**: Tiempo promedio para restaurar datos críticos durante pruebas semestrales, con un objetivo de 48 horas o menos.
- **Cumplimiento de Frecuencia**: Porcentaje de copias realizadas según el cronograma, con un objetivo del 100%.
- **Tasa de Detección de Incidentes**: Porcentaje de incidentes de seguridad identificados y reportados dentro de las 2 horas, con un objetivo del 90%.
- **Cumplimiento Normativo**: Porcentaje de auditorías internas que no identifican no conformidades graves, con un objetivo del 80%.

2.2. **Frecuencia de Evaluación**

- El responsable de TI coordinará evaluaciones semestrales del desempeño, recopilando datos de los registros de monitoreo, informes de pruebas de restauración y reportes de incidentes.
- Los resultados se consolidarán en un informe semestral, presentado a la alta dirección, que detalle el cumplimiento de los KPIs y las áreas de mejora identificadas.

3. Mejora Continua

3.1. **Fuentes de Retroalimentación**

- **Auditorías Internas y Externas**: Incorporar los hallazgos y recomendaciones de las auditorías semestrales internas y de las revisiones de entidades de control.

- **Pruebas de Restauración**: Analizar los resultados de las pruebas semestrales para identificar fallos en los procedimientos o copias corruptas.
- **Incidentes de Seguridad**: Revisar los reportes de incidentes para actualizar los procedimientos operativos y las medidas de mitigación de riesgos.
- **Retroalimentación de Dependencias**: Recopilar comentarios de las dependencias sobre la funcionalidad de los datos restaurados durante pruebas o incidentes.
- **Avances Tecnológicos**: Evaluar soluciones de respaldo viables cuando se disponga de presupuesto, alineadas con los lineamientos de MINTIC.

3.2. **Revisión de la Política**

- La política será revisada anualmente por el responsable de TI, con participación de los contratistas de TI, para incorporar:
    - Cambios normativos.
    - Lecciones aprendidas de auditorías, pruebas e incidentes.
    - Mejoras en la infraestructura tecnológica, si se asignan recursos.
- Las actualizaciones propuestas se presentarán a la alta dirección para su aprobación, y la versión revisada se comunicará a todo el personal y contratistas involucrados.

3.3. **Acciones de Mejora**

- Implementar acciones correctivas dentro de los 30 días posteriores a la identificación de un problema, ajustando procedimientos o capacitando al personal.
- Priorizar mejoras que no requieran inversión significativa, como optimizar el uso del NAS, mejorar la documentación o reforzar los controles de acceso.
- Documentar todas las acciones de mejora, incluyendo su impacto en los KPIs, y archivarlas en el sistema de gestión documental.

3.4. **Capacitación para la Mejora**

- Realizar sesiones de sensibilización anuales para los contratistas de TI, enfocadas en los resultados de las evaluaciones y las actualizaciones de la política.

- Incluir a las dependencias en sesiones bianuales para reforzar la importancia de reportar datos críticos y participar en pruebas de restauración.

4. Trazabilidad y Transparencia

4.1. **Registros**

- Mantener un archivo digital de todos los informes de monitoreo, evaluaciones semestrales y acciones de mejora, protegido contra modificaciones no autorizadas.
- Asegurar que los registros cumplan con los requisitos de conservación del Archivo General de la Nación y sean accesibles para auditorías.

4.2. **Reportes**

- El responsable de TI presentará un reporte anual a la alta dirección, resumiendo los resultados de las evaluaciones, el cumplimiento de los KPIs y las mejoras implementadas.
- El reporte estará disponible para solicitudes ciudadanas o revisiones de entidades de control, en cumplimiento de la Ley 1712 de 2014.

4.3. **Comunicación**

- Informar a las dependencias y contratistas sobre los resultados de las evaluaciones y las actualizaciones de la política mediante comunicados internos.
- Publicar un resumen de los avances en el portal web institucional, si es requerido por los lineamientos de transparencia.

Disposiciones Finales

Mecanismos de Actualización

- Las actualizaciones de la política serán propuestas por el responsable de TI, con base en:
    - Resultados de auditorías internas y externas.
    - Retroalimentación de las dependencias y contratistas de TI.

  - Cambios en las normativas aplicables (ej. Ley 1581 de 2012, Ley 1712 de 2014, lineamientos de MINTIC, normas del Archivo General de la Nación).
  - Mejoras en la infraestructura tecnológica o asignación de nuevos recursos.
- Las propuestas de actualización deberán ser aprobadas por la alta dirección mediante acto administrativo, y la versión actualizada se comunicará a todos los involucrados.

Cumplimiento Obligatorio

- Esta política es de obligatorio cumplimiento para todo el personal, contratistas y terceros que interactúen con los sistemas de información y datos críticos de la Alcaldía, conforme a lo establecido en la sección de Alcance y Aplicación.
- El responsable de TI supervisará el cumplimiento, reportando cualquier desviación a la alta dirección para la aplicación de medidas correctivas o sanciones, según corresponda.

Sanciones por Incumplimiento

- El incumplimiento de esta política, incluyendo la omisión de procedimientos, el manejo indebido de copias de respaldo o la violación de controles de seguridad, será considerado una falta disciplinaria, sujeta a las disposiciones del Código Disciplinario Único (Ley 734 de 2002) para funcionarios públicos, o a las sanciones contractuales aplicables para contratistas y terceros.
- Las sanciones serán evaluadas por la alta dirección o la oficina de control interno disciplinario, según el procedimiento interno de la Alcaldía, garantizando el debido proceso.

Derogación o Reemplazo

- Esta política podrá ser derogada o reemplazada mediante acto administrativo de la alta dirección, en caso de:
  - Adopción de una nueva política de gestión de copias de respaldo que incorpore avances tecnológicos o normativos significativos.
  - Cambios estructurales en la infraestructura tecnológica de la Alcaldía.

- Directrices de entidades de control o normativas superiores que requieran una reformulación.

- La derogación o reemplazo será comunicado a todo el personal, contratistas y terceros, y el responsable de TI asegurará la transición a los nuevos lineamientos, manteniendo la continuidad de los procesos de respaldo.

Divulgación y Capacitación

- El responsable de TI coordinará la divulgación inicial de la política, asegurando que todas las dependencias, contratistas y terceros relevantes reciban una copia y comprendan sus responsabilidades.

Resolución de Conflictos

- En caso de ambigüedades, conflictos o interpretaciones divergentes de esta política, el responsable de TI, en consulta con la alta dirección, resolverá las discrepancias, documentando la decisión y comunicándola a las partes involucradas.
- Las decisiones estarán alineadas con los principios rectores de la política y las normativas aplicables, priorizando la seguridad de la información y la continuidad operativa.

Anexos

Formato de Registro de Pruebas de Restablecimiento

Fecha	Hora	Copia Restaurada	Entorno de Prueba	Resultados	Validación de Dependencias	Referencia de Evidencia	Observaciones	Firma Responsable de la Prueba	Firma Responsable de TI

Formato de Registro de Incidentes de Seguridad

Fecha	Hora	Tipo de Incidente	Descripción	Impacto	Acciones Tomadas	Referencia de Evidencia	Observaciones	Firma Responsable del Registro	Firma Responsable de TI

Formato de Inventario de Copias de Respaldo

Fecha	Tipo de Copia	Datos Respaldados	Ubicación	Tamaño	Estado	Referencia de Evidencia	Observaciones	Firma Responsable del Registro	Firma Responsable de TI