CONVENIO INTERADMINISTRATIVO PARA CUSTODIA EXTERNA Y RESGUARDO DE COPIAS DE SEGURIDAD

PROPUESTA INTEGRAL

ENTRE LA EMPRESA DE OBRAS SANITARIAS DE SANTA ROSA DE CABAL EMPOCABAL ESP–EICE Y LA ALCALDÍA MUNICIPAL DE SANTA ROSA DE CABAL

1. OBJETIVO GENERAL

Establecer un esquema de cooperación interadministrativa entre EMPOCABAL ESP–EICE y la Alcaldía Municipal de Santa Rosa de Cabal para la custodia externa, intercambio, validación, almacenamiento seguro y controlado de copias de seguridad institucionales, garantizando la disponibilidad, integridad, confidencialidad y recuperación de la información crítica de ambas entidades ante eventos de pérdida, daño, desastre tecnológico, incidentes de ciberseguridad o contingencias operativas.

2. JUSTIFICACIÓN TÉCNICA Y ADMINISTRATIVA

Las entidades públicas y empresas de servicios públicos requieren implementar mecanismos de continuidad operativa y recuperación ante desastres que permitan garantizar la protección de la información institucional, la continuidad de los servicios tecnológicos y el cumplimiento de las obligaciones legales relacionadas con seguridad de la información, archivo, protección de datos y gestión documental.

Actualmente, tanto EMPOCABAL ESP–EICE como la Alcaldía Municipal de Santa Rosa de Cabal dependen de plataformas tecnológicas, sistemas de información, correo electrónico institucional, servicios digitales, archivos electrónicos y documentación crítica para el desarrollo de sus funciones administrativas y operativas.

En virtud de lo anterior, se hace necesario implementar un mecanismo de respaldo externo bajo custodia segura, mediante el cual ambas entidades almacenen recíprocamente copias de seguridad institucionales en instalaciones independientes, bajo condiciones de control, validación, trazabilidad y custodia física.

El presente esquema permitirá:

- Mitigar riesgos de pérdida total de información.
- Fortalecer los planes de continuidad del negocio y recuperación ante desastres.

- Garantizar almacenamiento externo fuera del sitio principal (Offsite Backup).
- Generar trazabilidad documental de entrega y recepción.
- Validar técnicamente la integridad de las copias de seguridad.
- Mejorar las prácticas de seguridad informática institucional.
- Cumplir lineamientos de Gobierno Digital y seguridad de la información.

3. FUNDAMENTOS JURÍDICOS

El presente convenio interadministrativo se fundamenta principalmente en:

Constitución Política de Colombia

- Artículo 2: Finalidad del Estado y garantía de la prestación eficiente de servicios.
- Artículo 209: Principios de la función administrativa.
- Artículo 269: Obligación de diseñar y aplicar métodos y procedimientos de control interno.

Ley 489 de 1998

- Artículos 95 y 96 relacionados con la cooperación entre entidades públicas mediante convenios interadministrativos.

Ley 80 de 1993

- Principios de la contratación estatal.
- Cooperación entre entidades estatales.

Ley 1150 de 2007

- Modalidades de contratación entre entidades públicas.

Ley 1712 de 2014

- Transparencia y acceso a la información pública.

Ley 1581 de 2012

- Protección de datos personales.

Decreto 1078 de 2015

- Decreto Único Reglamentario del sector TIC.
- Lineamientos de seguridad digital y Gobierno Digital.

Modelo de Seguridad y Privacidad de la Información – MinTIC

- Implementación de controles de seguridad.
- Gestión de continuidad.
- Protección de activos de información.

Ley 594 de 2000

- Ley General de Archivos.

Norma ISO 27001 (referencia técnica)

- Gestión de seguridad de la información.
- Control de respaldos y continuidad.

4. ALCANCE DEL CONVENIO

El convenio comprende:

1. Custodia física externa de copias de seguridad institucionales.
2. Intercambio recíproco de medios de almacenamiento.
3. Validación técnica de integridad de respaldos.
4. Control documental de entregas y devoluciones.
5. Custodia en caja fuerte o espacio seguro definido.
6. Registro de trazabilidad de los medios almacenados.
7. Procedimientos de recuperación y devolución.
8. Protocolos de confidencialidad y acceso restringido.
9. Aplicación de controles de seguridad física y lógica.
10. Definición de responsables institucionales.

5. ESQUEMA OPERATIVO PROPUESTO

5.1 Tipos de información respaldada

EMPOCABAL ESP–EICE

Copias cuatrimestrales

- Hosting institucional.
- Correo electrónico institucional.
- Configuraciones críticas.
- Bases de datos asociadas.

Copias bimestrales

- Documentos institucionales.
- Archivos compartidos.
- Ficheros operativos.
- Información administrativa.
- Repositorios internos.
- Archivos históricos.

Alcaldía Municipal

Se aplicará el mismo esquema o el definido por la entidad conforme a sus necesidades institucionales.

6. PROCEDIMIENTO DE ENTREGA Y VALIDACIÓN

ETAPA 1 – GENERACIÓN DEL RESPALDO

La entidad origen:

1. Generará la copia de seguridad.
2. Verificará integridad previa.
3. Etiquetará el medio.
4. Registrará:
    - Fecha.
    - Hora.
    - Responsable.
    - Tipo de respaldo.
    - Tamaño.
    - Número de archivos.
    - Hash de verificación.

ETAPA 2 – ENTREGA FÍSICA

El funcionario autorizado:

1. Transportará el medio de almacenamiento.
2. Presentará formato de entrega.
3. Hará entrega oficial bajo firma.
4. Se verificará estado físico del dispositivo.

ETAPA 3 – VALIDACIÓN TÉCNICA

La entidad receptora:

1. Conectará el medio en estación segura.
2. Ejecutará el software de validación.
3. Validará:
    - Peso total.
    - Cantidad de archivos.
    - Estructura.

- Hash o firma digital.
- Integridad de lectura.

4. Generará comprobante de validación.
5. Imprimirá acta de recibido.
6. Firmará conjuntamente con quien entrega.

ETAPA 4 – CUSTODIA

El medio será:

- Guardado en caja fuerte.
- Almacenado en gabinete seguro.
- Registrado en inventario.
- Custodiado bajo acceso restringido.

ETAPA 5 – RETIRO O DEVOLUCIÓN

Cuando el disco sea retirado:

1. Se validará nuevamente la información.
2. Se comparará con el registro inicial.
3. Se imprimirá acta de devolución.
4. Ambas partes firmarán conformidad.

7. CONTROLES DE SEGURIDAD RECOMENDADOS

Seguridad Física

- Caja fuerte.
- Área restringida.
- Cámaras de vigilancia.
- Registro de acceso.
- Protección contra humedad y calor.
- Protección eléctrica.

Seguridad Lógica

- Cifrado de discos.
- Contraseñas robustas.
- Hash SHA-256.

- Software antivirus.
- Equipos exclusivos de validación.
- Control de usuarios autorizados.

Seguridad Administrativa

- Registro de cadena de custodia.
- Formatos firmados.
- Inventario actualizado.
- Trazabilidad documental.
- Responsables designados.

8. RESPONSABILIDADES DE LAS PARTES

EMPOCABAL ESP–EICE

- Generar adecuadamente las copias.
- Validar integridad previa.
- Entregar medios correctamente identificados.
- Mantener actualizado inventario.
- Garantizar confidencialidad.

ALCALDÍA MUNICIPAL

- Custodiar físicamente la información.
- Validar integridad al recibir.
- Restringir acceso.
- Garantizar condiciones de almacenamiento.
- Llevar trazabilidad documental.

RESPONSABILIDAD RECÍPROCA

Ambas entidades deberán:

- Proteger la confidencialidad.
- No acceder al contenido salvo autorización.
- Garantizar integridad.
- Reportar incidentes.
- Mantener reserva institucional.

9. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

Toda la información almacenada tendrá carácter reservado y confidencial.

Las partes se comprometen a:

- No divulgar información.
- No copiar ni modificar archivos.
- Limitar acceso exclusivamente a personal autorizado.
- Cumplir la Ley 1581 de 2012.
- Aplicar controles de seguridad de la información.

10. PLAN DE CONTINGENCIA

En caso de:

- Incendio.
- Inundación.
- Ataque cibernético.
- Pérdida de información.
- Falla tecnológica.
- Ransomware.
- Daño físico.

La entidad afectada podrá solicitar recuperación inmediata del respaldo custodiado.
La entrega deberá realizarse prioritariamente dentro de las primeras 24 horas posteriores a la solicitud oficial.

11. PROPUESTA DE VIGENCIA

Se recomienda:

- Vigencia inicial: 3 años.
- Renovación automática previo acuerdo.
- Revisión anual técnica y jurídica.

12. FORMATOS PROPUESTOS

FORMATO 1

INFORMACIÓN SUGERIDA PARA ACTA DE ENTREGA DE COPIAS DE SEGURIDAD

DATOS GENERALES

- Entidad que entrega:
- Entidad que recibe:
- Fecha:
- Hora:
- Responsable entrega:
- Responsable recibe:
- Tipo de respaldo:
- Periodo:
- Medio de almacenamiento:
- Serial del disco:
- Capacidad:

INFORMACIÓN VALIDADA

- Peso total:
- Cantidad de archivos:
- Hash SHA-256:
- Estado físico:
- Observaciones:

DECLARACIÓN

Las partes dejan constancia que el medio fue recibido correctamente y validado conforme a los procedimientos establecidos.

Firma entrega: _____

Firma recibe: _____

FORMATO 2

ACTA DE DEVOLUCIÓN DE MEDIO DE ALMACENAMIENTO

- Fecha:
- Hora:
- Entidad que devuelve:
- Entidad que recibe:
- Medio:
- Serial:
- Estado físico:
- Resultado validación:
- Observaciones:

Firma entrega: _____
Firma recibe: _____

FORMATO 3

REGISTRO DE CUSTODIA

Fecha	Medio	Serial	Responsable ingreso	Resp retiro	Ubicación	Observaciones

FORMATO 4

CADENA DE CUSTODIA

Fecha	Hora	Responsable	Acción realizada	Firma

FORMATO 5

INVENTARIO DE RESPALDOS

Código	Tipo respaldo	Fecha generación	Tamaño	Hash	Ubicación	Estado

14. RECOMENDACIONES TÉCNICAS ADICIONALES

MEDIOS DE ALMACENAMIENTO

Se recomienda utilizar:

- Discos cifrados.
- Discos SSD empresariales.
- Etiquetado QR.
- Estuches antiestáticos.

SOFTWARE DE VALIDACIÓN

El software desarrollado debería validar:

- Hash SHA-256.
- Peso total.
- Número de archivos.
- Integridad.
- Registro automático.

- Historial de entregas.
- Generación PDF.
- Firma digital.

BUENAS PRÁCTICAS

- Mantener mínimo tres copias.
- Aplicar regla 3-2-1.
- Probar restauraciones periódicamente.
- Realizar auditorías semestrales.

15. PROPUESTA DE SUPERVISIÓN

Se recomienda que la supervisión esté a cargo de:

EMPOCABAL ESP–EICE

- Coordinador de Sistemas.

ALCALDÍA MUNICIPAL

- Dirección TIC o dependencia equivalente.

16. CONCLUSIÓN

La implementación del presente convenio permitirá fortalecer la estrategia de continuidad tecnológica y seguridad de la información de ambas entidades, estableciendo mecanismos formales de respaldo externo, control documental, trazabilidad y recuperación ante contingencias, contribuyendo así a la protección de los activos digitales institucionales y a la continuidad de los servicios públicos y administrativos prestados a la comunidad.

CONVENIO INTERADMINISTRATIVO PARA LA CUSTODIA EXTERNA Y MANEJO DE COPIAS DE SEGURIDAD No. 001 DE 2026

ENTRE

La EMPRESA DE OBRAS SANITARIAS DE SANTA ROSA DE CABAL EMPOCABAL ESP–EICE, identificada con NIT 800050603-7, representada legalmente por OSCAR JAVIER VASCO GIL, quien para efectos del presente convenio se denominará EMPOCABAL ESP–EICE, de una parte; y de la otra, el MUNICIPIO DE SANTA ROSA DE CABAL – ALCALDÍA MUNICIPAL, identificado con NIT _____, representado legalmente por _____, quien para efectos del presente convenio se denominará LA ALCALDÍA; hemos acordado celebrar el presente CONVENIO INTERADMINISTRATIVO PARA LA CUSTODIA EXTERNA Y MANEJO DE COPIAS DE SEGURIDAD, el cual se regirá por las siguientes consideraciones y cláusulas:

CONSIDERACIONES

1. Que las entidades públicas deben implementar mecanismos de protección, respaldo, recuperación y continuidad de la información institucional, garantizando la disponibilidad, integridad y confidencialidad de los activos digitales.
2. Que tanto EMPOCABAL ESP–EICE como LA ALCALDÍA administran información crítica y estratégica necesaria para el cumplimiento de sus funciones institucionales y la prestación de servicios a la comunidad.
3. Que las buenas prácticas de seguridad de la información y continuidad operativa recomiendan mantener copias de seguridad externas bajo esquemas de custodia fuera del sitio principal de operación.
4. Que las partes consideran pertinente establecer un esquema de cooperación recíproca para el almacenamiento, validación, custodia y control de medios de respaldo institucional.
5. Que el presente convenio se celebra al amparo de los artículos 95 y 96 de la Ley 489 de 1998 y demás normas concordantes sobre cooperación interadministrativa entre entidades públicas.

CLÁUSULAS

PRIMERA – OBJETO

Aunar esfuerzos técnicos, administrativos y operativos entre EMPOCABAL ESP–EICE y LA ALCALDÍA para la custodia externa, almacenamiento seguro, validación, control y protección de copias de seguridad institucionales, mediante un esquema recíproco de respaldo y contingencia tecnológica.

SEGUNDA – ALCANCE

El presente convenio comprende:

1. La entrega y recepción recíproca de medios de almacenamiento que contengan copias de seguridad institucionales.
2. La validación técnica de integridad de la información almacenada.
3. La custodia física segura de los medios de almacenamiento.
4. La administración de registros de trazabilidad y cadena de custodia.
5. La devolución controlada de los medios entregados.
6. La implementación de controles de seguridad física y lógica.
7. La protección de la confidencialidad de la información institucional.
8. La aplicación de procedimientos de contingencia y recuperación ante incidentes tecnológicos.

TERCERA – OBLIGACIONES DE EMPOCABAL ESP–EICE Y CUARTA – OBLIGACIONES DE LA ALCALDÍA

EN LA ENTREGA:

1. Generar las copias de seguridad institucionales conforme a los procedimientos internos establecidos.
2. Validar previamente la integridad de la información antes de su entrega.
3. Entregar los medios de almacenamiento debidamente identificados y rotulados.
4. Mantener actualizado el inventario de medios entregados.

5. Garantizar que la información entregada se encuentre protegida mediante mecanismos de seguridad y cifrado cuando aplique.
6. Designar los funcionarios autorizados para la entrega y retiro de los medios.
7. Suscribir las respectivas actas de entrega y devolución.
8. Cumplir los protocolos de cadena de custodia establecidos en el presente convenio.

EN CUSTODIA

1. Recibir los medios de almacenamiento entregados.
2. Validar técnicamente la integridad de la información recibida.
3. Custodiar los medios de almacenamiento en condiciones adecuadas de seguridad física.
4. Mantener restringido el acceso a los medios únicamente al personal autorizado.
5. Llevar registro documental de ingreso, custodia y devolución.
6. Garantizar condiciones ambientales y de seguridad apropiadas para el almacenamiento.
7. Informar oportunamente cualquier incidente relacionado con los medios custodiados.
8. Suscribir las respectivas actas de recibido y devolución.

QUINTA – CONFIDENCIALIDAD

Las partes se obligan a mantener absoluta reserva y confidencialidad sobre toda la información contenida en los medios de almacenamiento objeto del presente convenio.

En consecuencia:

1. Ninguna de las partes podrá acceder, divulgar, copiar, modificar o utilizar la información almacenada sin autorización expresa de la entidad propietaria.
2. La información tendrá carácter reservado y será utilizada exclusivamente para fines de custodia y contingencia.
3. Las partes deberán adoptar medidas administrativas, técnicas y operativas para proteger la información custodiada.
4. Esta obligación subsistirá aún después de la terminación del convenio.

SEXTA – SEGURIDAD DE LA INFORMACIÓN

Las partes implementarán controles mínimos de seguridad orientados a garantizar la integridad, disponibilidad y confidencialidad de la información, incluyendo:

1. Custodia en caja fuerte o espacio seguro.
2. Control de acceso físico.
3. Registro de trazabilidad.
4. Validación técnica de integridad.
5. Protección contra acceso no autorizado.
6. Uso de mecanismos de cifrado cuando aplique.
7. Procedimientos de recuperación ante incidentes.

SÉPTIMA – CADENA DE CUSTODIA

Toda entrega, recepción, almacenamiento y devolución de medios deberá quedar soportada mediante formatos físicos o digitales que permitan garantizar la trazabilidad completa del proceso.
Las partes deberán registrar como mínimo:

- Fecha y hora.
- Responsable de entrega.
- Responsable de recepción.
- Identificación del medio.
- Estado físico.
- Resultado de validación técnica.
- Observaciones.

OCTAVA – RESPONSABILIDAD SOBRE LOS MEDIOS

Cada entidad será responsable por:

1. La adecuada generación de sus copias de seguridad.
2. La integridad de la información entregada.
3. El transporte seguro de los medios.
4. La custodia de los medios recibidos mientras permanezca bajo su responsabilidad.

Las partes no serán responsables por fallas derivadas de daños preexistentes en los medios entregados o por información corrupta generada previamente por la entidad propietaria.

NOVENA – VIGENCIA

El presente convenio tendrá una vigencia inicial de tres (3) años contados a partir de la suscripción del acta de inicio, pudiendo ser prorrogado previo acuerdo escrito entre las partes.

DÉCIMA – SUPERVISIÓN

La supervisión del presente convenio estará a cargo de:

Por EMPOCABAL ESP–EICE

El Coordinador de Sistemas o quien se designe expresamente por el representante legal

Por LA ALCALDÍA

El director TIC, jefe de Sistemas o quien sea designado formalmente.

Los supervisores deberán velar por el correcto cumplimiento de las obligaciones establecidas.

DÉCIMA PRIMERA – TERMINACIÓN

El presente convenio podrá darse por terminado por:

1. Mutuo acuerdo entre las partes.
2. Incumplimiento de las obligaciones pactadas.
3. Vencimiento del plazo de vigencia.
4. Fuerza mayor o caso fortuito que imposibilite su ejecución.
5. Decisión unilateral debidamente motivada.

DÉCIMA SEGUNDA – SOLUCIÓN DE CONTROVERSIAS

Las diferencias que surjan con ocasión de la ejecución del presente convenio serán resueltas inicialmente mediante mecanismos de arreglo directo entre las partes. En caso

de no lograrse acuerdo, se acudirá a los mecanismos legales y jurisdiccionales correspondientes.

DÉCIMA TERCERA – PERFECCIONAMIENTO Y EJECUCIÓN

El presente convenio se perfecciona con la firma de las partes y requerirá para su ejecución la suscripción del acta de inicio correspondiente.

FIRMAN

EMPOCABAL ESP–EICE

Nombre:
Cargo:
Fecha:

LA ALCALDÍA MUNICIPAL DE SANTA ROSA DE CABAL

Nombre:
Cargo:
Fecha: