1. INTRODUCCIÓN 3

2. MARCO LEGAL 5

3. REQUISITOS TÉCNICOS 6

4. OBJETIVO 6

5. ALCANCE 6

6. PRINCIPIOS DE LA PRESERVACIÓN DIGITAL 7

7. OPORTUNIDADES DE MEJORA: 8

8. DEFINICIONES 8

9. METODOLOGÍA 19

9.1 CONCEPTOS FUNDAMENTALES DE LA SEGURIDAD INFORMÁTICA:(SCIELO.ORG, 2010) 19
9.2 ¿QUÉ ES UN PLAN DE PRESERVACIÓN? 23
9.3 DIFERENCIAS Y SIMILITUDES EN LA CONSERVACIÓN 24
9.4 AMENAZAS INFORMÁTICAS 25
9.5 VULNERABILIDADES INFORMÁTICAS 26
9.6 RIESGOS INFORMÁTICOS 28
9.7 IMPACTOS 28

10. CRITERIOS ISO PARA LA CONSERVACIÓN DE DOCUMENTOS ELECTRÓNICOS 29

11. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES. 35

11.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 35
11.2 POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN 36
11.3 POLÍTICAS ESPECÍFICAS PARA USUARIOS DEL ALCALDÍA MUNICIPAL DE BELLO 37
POLÍTICAS ESPECÍFICAS PARA FUNCIONARIOS Y CONTRATISTAS DEL ÁREA DE SISTEMAS DE INFORMACIÓN. 39
11.5 POLÍTICAS ESPECÍFICAS PARA WEB MASTER 41
11.6 POLÍTICA DE RETENCIÓN Y ARCHIVO DE DATOS. 42
11.7 POLÍTICA DE DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS. 42
11.8 POLÍTICA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN. 42
11.9 POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN 43
11.10 POLÍTICA DE USO DE LOS ACTIVOS. 44
11.11 POLÍTICA DE USO DE ESTACIONES CLIENTE. 46
11.12 POLÍTICA DE USO DE INTERNET. 47
11.13 POLÍTICA DE USO DE MENSAJERÍA INSTANTÁNEA Y REDES SOCIALES 47
11.14 POLÍTICA DE USO DE DISCOS DE RED O CARPETAS VIRTUALES 48
11.15 POLÍTICA DE USO DE IMPRESORAS Y DEL SERVICIO DE IMPRESIÓN 48
11.16 POLÍTICA DE USO DE PUNTOS DE RED DE DATOS (RED DE ÁREA LOCAL – LAN). 49

11.17 POLÍTICAS DE SEGURIDAD DEL CENTRO DE DATOS Y CENTROS DE CABLEADO 49
11.18 POLÍTICAS DE SEGURIDAD DE LOS EQUIPOS 51
11.19 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA 52
11.20 POLÍTICA DE USO DE CORREO ELECTRÓNICO. 53

12. POLÍTICA DE PRESERVACIÓN DIGITAL. 55

12.1 OAIS. OPEN ARCHIVAL INFORMATION SYSTEM 55
12.2 ACCIONES DE PRESERVACIÓN DIGITAL. 57
12.3 DESARROLLO DE PROCEDIMIENTOS DE PRESERVACIÓN DIGITAL 59
12.4 RESPONSABLES DEL PLAN DE PRESERVACIÓN DIGITAL 65
12.5 MAPA DE RUTA 66
12.6 ARTICULACIÓN CON LOS INSTRUMENTOS DE LA GESTIÓN DOCUMENTAL 67
12.7 ARTICULACIÓN CON LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. 67
12.8 ARTICULACIÓN CON LA GESTIÓN DEL RIESGO DE LA ENTIDAD 67

13. RECOMENDACIONES EN LA PRESERVACIÓN DIGITAL 68

14. MEJORA CONTINUA 69

15. HERRAMIENTA DE SEGUIMIENTO Y CONTROL 70

16. CONTROL DE CAMBIOS 71

17. ANEXOS 71

18. BIBLIOGRAFÍA 72

1. INTRODUCCIÓN

La informática penetró en los archivos como una herramienta para la gestión, especialmente con el uso de bases de datos para controlar inventarios y con la conexión de ordenadores en red, a fin de asegurar la comunicación telemática de cierta información en bases de datos. En su momento, en la década de los setenta, este uso de la informática se conocía como *automatización de archivos*, y entre las revistas destacadas para plantear estos retos profesionales estaba la publicada por el Consejo Internacional de Archivos: Automatic Data Processing and Archives (APDA).

La creación de documentos electrónicos por los equipos informáticos no era una finalidad en sí misma, sino un medio para poder imprimir el documento en papel, que sería el auténtico tras el sellado y la firma de los responsables.

Cuando Steven Sasson inventó la cámara digital en 1975, patentada luego en 1978 por la United States Patent and Trademark Office (USPTO), propició otro aspecto que irrumpiría en la década siguiente: la digitalización de documentos y, por tanto, la aparición de una copia digital de un documento original, generalmente en soporte papel.

En los años ochenta, este recurso empezó a implantarse en los archivos con la digitalización de los documentos históricos, para preservar el original en papel, como en el caso del Archivo General de Indias (González García, 1988, 1999). En su forma visual, la imagen de un documento empieza a generalizarse frente al documento nacido digitalmente (que no tenía la apariencia de documento como tal), elaborado con los procesadores de texto en sistemas MS-DOS, como WordStar o Wordperfect.

Cuando a finales de los años ochenta salió la primera versión de Word para Windows, se podía visualizar en la pantalla el documento tal cual iba a ser impreso, y aunque todavía el interés del *software* correspondía simplemente al de una funcionalidad de una máquina de escribir avanzada, se plantea ya en los años noventa aprovechar ese documento digital que era eliminado tras su impresión.

En este contexto, a principios de la década de los noventa empiezan a aparecer tímidamente proyectos y artículos científicos que se preocupan por la producción, gestión y conservación de los documentos digitales. Aunque una gran parte de los proyectos son de bibliotecas digitales y de sus repositorios, ya aparecen artículos científicos en los cuales se plantea la problemática que gira alrededor de los documentos electrónicos de las administraciones (los *records*).

Se empezó a vislumbrar, entonces, que, en el futuro, gran parte de los documentos serían creados electrónicamente, que ocuparían menos sitio que los documentos en

papel y que habría problemas de obsolescencia tecnológica y vulnerabilidad en los sistemas informáticos.

Además, para prevenir los desastres en los documentos electrónicos, estos deberían ser gestionados mejor que los documentos en papel (Catherine Hare, 1995). El avance tecnológico y el bajo costo de la infraestructura para la creación y difusión de los documentos digitales (*hardware*, *software* y redes de telecomunicaciones) han favorecido que en la primera década del presente siglo se difunda la implantación, en diferentes organizaciones públicas y privadas, de lo que conocemos como *administración electrónica*, por la cual los usuarios y las organizaciones se comunican o establecen relaciones administrativas y contractuales enteramente electrónicas.

En la actualidad, disponemos de dos tipos de documentos electrónicos de archivo: los que han nacido electrónicamente y los que surgen de un proceso de digitalización (que son copias y pueden ser autenticados). Cuando una organización desea implantar una administración-gestión basada en tramitaciones electrónicas, seguramente tendrá que incorporar al sistema de gestión de documentos electrónicos los documentos en papel, mediante la digitalización. Por ello, un reto presente es poder gestionar una administración mixta de documentos nacidos digitalmente y de documentos digitalizados, hasta que en un futuro finalice la brecha digital.

Por esta razón, el problema actual de la preservación digital abarca tanto a los documentos nacidos digitalmente como a los documentos digitalizados. Es importante que una organización defina un plan de preservación de los documentos electrónicos integrados en su sistema de gestión documental. El plan de preservación está diseñado para ayudar a garantizar que los documentos conserven sus características de autenticidad, fiabilidad, integridad, y disponibilidad a lo largo del tiempo.

2. MARCO LEGAL

- Constitución Política de Colombia 1991.
- Código Penal Colombiano - Decreto 599 de 2000
- Ley 906 de 2004, Código de Procedimiento Penal.
- Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
- Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- Ley 527 de 1999, por 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.
- Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012
- Ley 1712 de 2014, "De transparencia y del derecho de acceso a la información pública nacional"

3. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTCIISO 27001 Sistemas de gestión de la seguridad de la información
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.
- ISO/IEC 27005 Information technology Systems- Security techniques- information security risk management.
- Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema: Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información".
- Norma Técnica Colombiana NTC - ISO 19011 "Directrices para la Auditoria de los Sistemas de Gestión de la Calidad y/o Ambiental"

4. OBJETIVO

Implementar el plan de preservación a largo plazo que garanticen la preservación y conservación de los documentos electrónicos de archivo durante sus períodos de vigencia de gestión e intermedios, finalizando con la aplicación técnica de medidas de preservación a largo plazo acordes con las características de los mismos.

5. ALCANCE

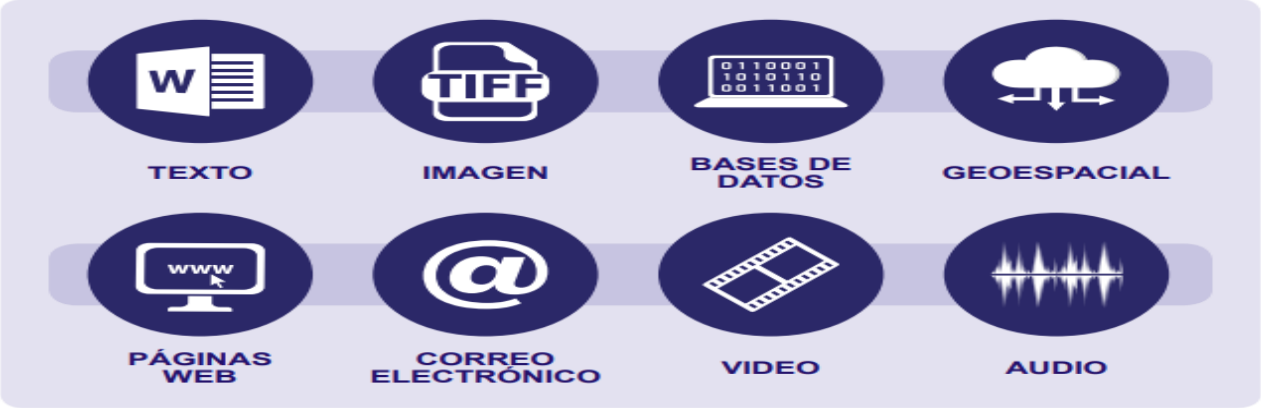
El plan de preservación digital a largo plazo aplica para los archivos de gestión, central y centro de documentación técnica de la entidad teniendo en cuenta los procesos archivísticos aplicados a los mismos (producción hasta disposición final) y será implementado en todas las áreas de la entidad incluidos todos los servidores que manejen y/o produzcan información y documentos de y para la entidad, en aras de mantener la integridad de los documentos.

Según lo establecido por la UNESCO, el alcance de la preservación digital a largo plazo incluye los “recursos de carácter cultural, educativo, científico o administrativo e información técnica, jurídica, médica y de otras clases, que se generan en formato digital o se convierten a este a partir del material analógico ya existente. Puede ser cualquier tipo de objeto digital”.

La selección de los documentos o información que será objeto de preservación a largo plazo se soporta en el proceso de valoración documental y la evaluación de los riesgos que pudieran afectar la permanencia y accesibilidad de la información o documentos digitales durante el tiempo que se considere necesario.

De acuerdo con el contenido, se presentan a continuación los tipos de información

más comunes:



Tipos de información. Fuente: Rangel y otros, 2017

Las Políticas de Seguridad de la Información, surgen como una herramienta institucional para sensibilizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Alcaldía Municipal De Bello sobre la importancia y sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

6. PRINCIPIOS DE LA PRESERVACIÓN DIGITAL [1]

Principio de Integridad
Asegurar que el contenido informativo, la estructura lógica y el contexto no se han modificado ni se ha afectado el grado de fiabilidad ni la autenticidad del documento original.

Principio de Equivalencia
Modificar, cuando sea necesario, la forma tecnológica sin alterar el valor evidencia de los documentos, como una medida para enfrentar la obsolescencia tecnológica y para garantizar el acceso a la información.

Principio de Economía
Aplicar procesos, procedimientos, métodos y técnicas de preservación viables, prácticos y apropiados para el contexto de los documentos, de tal modo que se asegure la sostenibilidad técnica y económica de la preservación digital.

Principio de Actualidad

[1] Tomado de Fundamentos de preservación digital a largo plazo AGN (Archivo General de la Nación, 2018)

Evolucionar al ritmo de la tecnología y utilizar los medios disponibles en el momento actual para garantizar la preservación de los documentos en el futuro. Esto significa que un sistema de preservación digital debería mantener la capacidad de evolucionar, de ajustarse a los cambios dimensionales y añadir nuevas prestaciones y servicios.

Principio de Cooperación
Reutilizar y compartir soluciones ya existentes y desarrolladas de forma conjunta con otros archivos digitales, especialmente las relacionadas con los procesos que pueden ser gestionados de forma centralizada.

Principio de normalización
Generar lineamientos y herramientas basadas en normas, estándares y buenas prácticas, como apoyo a la gestión y preservación de los documentos digitales.

7. OPORTUNIDADES DE MEJORA:

- Conservación preventiva de la información digital
- Interoperabilidad de los sistemas de la Entidad
- Migración y back up (copia de seguridad) de la información
- Capacidad de Almacenamiento de la información

8. DEFINICIONES

Acción correctiva: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva: Medida de tipo pro-activo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.

Aceptación del Riesgo: Decisión de aceptar un riesgo.

Activo: Según [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.
Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos del ALCALDÍA MUNICIPAL DE BELLO. Se pueden clasificar de la siguiente manera:

Datos: Son todos aquellos elementos básicos de la información (en cualquier

formato) que se generan, recogen, gestionan, transmiten y destruyen en el ALCALDÍA MUNICIPAL DE BELLO. Ejemplo: archivo de Word “listado de personal.docx”

Aplicaciones: Es todo el software que se utiliza para la gestión de la información. Ejemplo: SIGEPRE.

Personal: Es todo el personal del ALCALDÍA MUNICIPAL DE BELLO, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del ALCALDÍA MUNICIPAL DE BELLO. Ejemplo: Pedro Pérez.

Servicios: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.

Ejemplo: Publicación de hojas de vida, solicitud de vacaciones.

Tecnología: Son todos los equipos utilizados para gestionar la información y las comunicaciones

Ejemplo: equipo de cómputo, teléfonos, impresoras.

Instalaciones: Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Oficina Pagaduría.

Equipamiento auxiliar: Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado, destructora de papel.

Administración de riesgos: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Administración de incidentes de seguridad: Un sistema de seguimiento de incidentes (denominado en inglés como issue tracking system, trouble ticket system o incident ticket system) es un paquete de software que administra y mantiene listas de incidentes, conforme son requeridos por una institución. Los sistemas de este tipo son comúnmente usados en la central de llamadas de servicio al cliente de una

organización para crear, actualizar y resolver incidentes reportados por usuarios, o inclusive incidentes reportados por otros funcionarios, contratistas, colaboradores de la entidad o de terceras partes. Un sistema de seguimiento de incidencias también contiene una base de conocimiento que contiene información de cada cliente, soluciones a problemas comunes y otros datos relacionados. Un sistema de reportes de incidencias es similar a un Sistema de seguimiento de errores (bugtracker) y, en algunas ocasiones, una entidad de software puede tener ambos, y algunos bugtrackers pueden ser usados como un sistema de seguimiento de incidentes, y viceversa.

Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditabilidad: Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara, Se aplica a entidades tales como usuarios, procesos, sistemas de información.

Base de datos de gestión de configuraciones (CMDB, Configuration Management Database): Es una base de datos que contiene toda la información

pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.

B57799: Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información –no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información -es certificable-o La parte primera es el origen de ISO 17799 e ISO 27002 Y la parte segunda de ISO 27001. Como tal el estándar, ha sido derogado ya, por la aparición de estos últimos.

Características de la Información: las principales características son la confidencialidad, la disponibilidad y la integridad.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

CobiT - Control Objectives for Information and related Technology: Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Cómputo forense: El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o exanimación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Denegación de servicios: Acción iniciada por una persona u otra causa que incapacite el hardware o el software, o ambos y después niegue el servicio.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva: Según [ISO/IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las

políticas.

Disponibilidad: Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Gusanos: Es un programa de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Siempre dañan la red (aunque sea simplemente consumiendo ancho de banda).

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección

adecuada. La información puede existir de muchas maneras. Puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Ingeniería Social: En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IPS: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 20005.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información

(transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de Julio de 2007.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

ISO/IEC TR 13335-3: "Information technology. Guidelines for the management of IT Security .Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

ISO/IEC TR 18044: "Information technology. Security techniques. Information security incident management". Guía de utilidad para la gestión de incidentes de seguridad de la información.

ITIL IT Infrastructure Library: Un marco de gestión de los servicios de tecnologías de la información.

Keyloggers: Aplicaciones que registran el teclado efectuado por un usuario.

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.
No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete

mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

Política dé escritorio despejado: La política de la empresa que indica a los funcionarios, contratista y demás colaboradores del ALCALDÍA MUNICIPAL DE BELLO, que deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día.

Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual: Según [ISOIIEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

Salvaguarda: Véase: Control.

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 20005]: la parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Servicios de tratamiento de información: Según [ISO/IEC 27002:20005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Usuario: en el presente documento se emplea para referirse a directivos,

funcionarios, contratistas, terceros y otros colaboradores del ALCALDÍA MUNICIPAL DE BELLO, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red del ALCALDÍA MUNICIPAL DE BELLO y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Virus: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Documento electrónico: Es la información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares.

Documento electrónico de archivo: Registro de información generada, recibida, almacenada y comunicada por medios electrónicos, que permanece almacenada electrónicamente durante todo su ciclo de vida, producida por una persona o entidad en razón de sus actividades o funciones, que tiene valor administrativo, fiscal, legal o valor científico, histórico, técnico o cultural y que debe ser tratada conforme a los principios y procesos archivísticos.

Documento digital: Información representada por medio de valores numéricos diferenciados – discretos o discontinuos -, por lo general valores numéricos binarios (bits), de acuerdo con un código o convención preestablecidos.

Preservación digital: Es el conjunto de principios, políticas, estrategias y acciones específicas que tienen como fin asegurar la estabilidad física y tecnológica de los datos, la permanencia y el acceso a la información de los documentos digitales y proteger el contenido intelectual de los mismos por el tiempo que se considere necesario.

Prevención a largo plazo: Conjunto de acciones y estándares aplicados a los documentos durante su gestión para garantizar su preservación en el tiempo, independientemente de su medio y forma de registro o almacenamiento. La preservación a largo plazo aplica al documento electrónico de archivo con su medio correspondiente en cualquier etapa de su ciclo vital.

Sistema Integrado de Conservación: Es el conjunto de planes, programas,

estrategias, procesos y procedimientos de conservación documental y preservación digital, bajo el concepto de archivo total, acorde a la política de gestión documental y demás sistemas organizacionales, tendiente a asegurar el adecuado mantenimiento de cualquier tipo de información, independiente del medio o tecnología con la cual se haya elaborado, conservando atributos tales como unidad, integridad, autenticidad, inalterabilidad, originalidad, fiabilidad y accesibilidad, desde el momento de su producción y/o recepción, durante su gestión, hasta su disposición final, es decir, en cualquier etapa de su ciclo vital.

Seguridad De La Información De acuerdo con lo expuesto por DOYLE, Murielle y FRÉNIÉRE, André. **La preparación de manuales de gestión de documentos para las administraciones públicas: un estudio Ramp**. UNESCO, 1991. Vol. 0, P. 40-41. Se deberá observar en relación con la seguridad de los documentos lo siguiente:
La protección de documentos esenciales va más allá de las medidas habituales de protección de los documentos contra incendios, robos, inundaciones, actos de vandalismo y sustancias peligrosas, existe una serie de recursos preventivos para proteger contra catástrofes naturales y guerras.

Copias de seguridad: Se refiere al proceso de hacer duplicados exactos del objeto digital. Aunque es un componente esencial de todas las estrategias de preservación, las copias de seguridad en sí mismas no son una técnica de mantenimiento a largo plazo, ya que se ocupa exclusivamente con la cuestión de pérdida de datos debido a un fallo de hardware, bien debido a causas normales, bien a desastres naturales bien a destrucción malintencionada. En ocasiones, se combina con almacenamiento remoto de tal forma que el original y las copias no estén sujetas a los mismos eventos de desastre. Las copias de seguridad deberían ser consideradas la estrategia de mantenimiento mínima para incluso los materiales más efímeros y con menos valor que dispongamos.

9. METODOLOGÍA

9.1 CONCEPTOS FUNDAMENTALES DE LA SEGURIDAD INFORMÁTICA:(SCIELO.ORG, 2010)

Para poder comprender el concepto integral de la seguridad informática, es indispensable entender los diversos conceptos básicos que la rigen, ya que de otra forma no es posible establecer una base de estudio.

***Recursos Informáticos*:** el equipo de cómputo y telecomunicaciones; los sistemas, programas y aplicaciones, así como los datos e información de una organización. También se les conoce como "activos informáticos"

***Amenaza*:** fuente o causa potencial de eventos o incidentes no deseados que

pueden resultar en daño a los recursos informáticos de la organización.

***Impacto*:** la medida del efecto nocivo de un evento.

***Vulnerabilidad*:** característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza.

***Riesgo*:** la probabilidad de que un evento nocivo ocurra combinado con su impacto en la organización.

Principio básico de la seguridad informática: la seguridad informática no es un producto, es un proceso.

El objetivo primario de la *seguridad informática* es el de mantener al mínimo los riesgos sobre los recursos informáticos, –todos los recursos– y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable. Para ello utilizaremos estructuras organizacionales técnicas, administrativas, gerenciales o legales.

El objetivo secundario de la *seguridad informática* –y subrayo que es de nuestro especial interés desde el punto de vista de la preservación documental– consiste en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad total.

Este concepto varía de acuerdo a distintos autores, a los contextos documentales y al tipo de organización a la que la información esté asociada. En un contexto archivístico y en donde tratamos de interoperar un enfoque de seguridad informática con uno de preservación digital, podemos establecer esa confiabilidad como la unión de seis características esenciales:

- permanencia
- accesibilidad
- disponibilidad
- confidencialidad (privacidad)
- autenticidad (integridad)
- aceptabilidad (no repudio)

La característica de ***permanencia*** estará asociada a la medida en la que podemos asegurar que el documento existirá y estará disponible por un lapso considerable, si es necesario, eternamente. la permanencia depende del *almacenamiento permanente seguro*. en este caso documentos de archivo– se requiere de

estrategias, procedimientos y técnicas adecuadas para crear, operar y mantener archivos documentales a largo plazo. Tales estrategias deben permitir preservar la *cadena de bits*3 y sus formatos. Por lo mismo se deben diseñar y llevar a cabo meticulosamente esas técnicas y procedimientos para la conservación tanto de los soportes documentales como de sus contenidos digitales: la información del documento en sí misma y los metadatos asociados a él. La preservación del soporte, la cadena de bits, su estructura y su formato nos da la permanencia.

Es común confundir esta característica con la de ***accesibilidad***, la cual tiene que ver con que el documento, existiendo, pueda ser accedido por nosotros y sea visible.

Como podemos concluir, una cosa es que un documento exista, permanezca en buen estado, y otra cosa es que se pueda acceder y se pueda ver y analizar su contenido. Dependiendo de nuestra capacidad de disponer de esos artefactos, programas, sistemas operativos, formatos, etcétera, tendremos acceso a esos documentos. Habrá o no "accesibilidad", independientemente de su "permanencia".

Hoy en día ya se maneja el concepto de "archivo permanente", el cual consiste en una serie de estrategias y técnicas tendientes a lograr la interoperabilidad máxima, es decir, que la arquitectura de los sistemas de archivos de información digital para preservación sea independiente de la tecnología usada para crearlos, precisamente para reducir el problema de la accesibilidad.

La técnica archivística conocida como: "preservación de objeto persistente" *persistent object preservation* o "POP"– tiene como propósito asegurar que los documentos de archivo digitales permanezcan accesibles por medio de la autodescripción hecha de ellos, incluyendo formatos, características estructurales y tecnológicas, etcétera, hecha de manera independiente del equipo o programas en donde operen.

La característica de ***disponibilidad*** *tiene* que ver con la facilidad de poder acceder al documento cuando, como sea y por quien sea necesario. *Disponibilidad* no significa obligatoriamente que todos los documentos deban estar disponibles todo el tiempo en-línea para todo el mundo. De acuerdo a ciertas reglas establecidas por cada organización es necesario que el documento esté disponible en los tiempos, bajo las condiciones y para las personas preestablecidas.

La característica de la ***confidencialidad*** o privacidad tiene que ver con el hecho de que los registros documentales deben estar disponibles siempre, pero sólo para las personas autorizadas, durante las circunstancias y bajo condiciones válidas y preestablecidas. No deberá ser posible obtener ninguna información de los archivos fuera de esas condiciones.

La característica de ***autenticidad* o *integridad*** es sumamente importante. Algunos autores lo consideran uno de los elementos más importantes de la preservación. Tiene que ver con la confianza de un documento de archivo como tal; esto es, la cualidad de un documento de archivo de ser lo que pretende ser sin alteraciones o corrupciones. Los documentos auténticos son los que han mantenido su identidad e integridad al paso del tiempo.

Este concepto es directamente proporcional al grado en que el documento digital refleja al original, no en su apariencia física, sino en su esencia, su espíritu, su intención. Un documento *íntegro* es el que refleja totalmente la esencia del original; es decir, no ha sido corrompido en su contexto: alterado, mutilado, interpretado, aumentado, recortado, deformado, censurado, etcétera: es confiable y por tanto aceptable. Su mensaje, autoría, fechas asociadas, lugares, etcétera, son en realidad las consignadas en el documento desde siempre; en suma: es auténtico. Aunque hubiese cambiado físicamente, en su esencia refleja de manera completa lo que se estableció en el documento original.

El original de un documento electrónico –llamado la primera instanciación (representación de una abstracción a través de una instancia concreta)– desaparece en el ambiente digital la primera vez que es salvado. Lo que se recupera *siempre* es una copia. En realidad, no se puede preservar documentos
digitales: sólo se puede preservar la capacidad de reproducirlos una y otra vez. Lo importante al poder acceder y reproducir una y otra vez un documento, es la condición de que sea íntegro, auténtico.

Es necesario subrayar que un cierto documento no tiene que ser idéntico al documento que le dio origen para ser íntegro; de hecho, es perfectamente natural que los documentos electrónicos sean modificados de tiempo en tiempo, para actualizar su formato, versión, sistema operativo, código de caracteres, etcétera. Pero si no se puede preservar en realidad a largo plazo un documento digital y lo que se preserva es nuestra capacidad de reproducirlo correctamente es necesario por tanto garantizar de alguna forma que, aunque su estructura física cambie, su contenido sea el mismo, y sus "contextos" sean documentados; esto es, todavía sea íntegro, auténtico.

La característica final de la información segura implica la ***aceptabilidad* o "no repudio".** En lo relativo a documentos sobre soportes *tradicionales,* la autenticidad fue establecida siempre a través del objeto mismo, del documento, así que el custodio sólo necesitó preocuparse de que el usuario analizase el objeto y sacara sus propias conclusiones acerca de su autenticidad. Con los medios digitales, lo que el usuario necesita para analizar y concluir la aceptabilidad es conocer la calidad del proceso de creación de un documento, la autoridad y capacidad –competencia– del

custodio, así como la calidad de la documentación del proceso de conservación y su seguridad.

La consecuencia final de la unión de las seis características antes descritas en un documento y/o archivo que los contenga es la de la **fiabilidad**, entendida esta como la confianza en un documento de archivo como establecimiento de un acto o declaración de un hecho. Implica que un documento de archivo puede sostener al hecho del que es relativo y es establecida examinando las características que dan forma al documento de archivo, así como el nivel de control ejercido durante su proceso de creación y preservación.

9.2 ¿QUÉ ES UN PLAN DE PRESERVACIÓN?

Un plan de preservación es un plan para preservar una colección específica o una parte de la colección de objetos digitales, teniendo en cuenta:

- la política de preservación;
- las obligaciones legales;
- las limitaciones de la organización;
- las limitaciones técnicas;
- las necesidades del usuario; y
- los fines de la preservación.

Describe el contexto de la preservación, las estrategias de preservación evaluadas (como la migración, la conversión y la emulación) y la decisión resultante a favor de una estrategia, incluyendo la justificación de dicha decisión.

Además, un plan de preservación define una serie de acciones de preservación para ser adoptadas por la institución responsable en respuesta a los riesgos identificados para un conjunto dado de objetos digitales o documentos (denominado colección).

El plan de preservación debería garantizar que todos los documentos, cualquiera que sea su formato y medio de almacenamiento, sean conservados con vistas a que sean accesibles en alguna fecha posterior.

Los planes de preservación deberían garantizar que los documentos digitales al menos sean:

- localizables y disponibles para el acceso en manera oportuna.
- interpretables (disponibilidad, presentación, representación, vista, cifrado);
- recuperables, incluyendo los metadatos apropiados;

- protegidos contra pérdidas de derechos tales como propiedad intelectual, y confidencialidad;
- disponibles para el acceso todo el tiempo que se requiera por aquellas personas autorizadas para acceder al documento.
- supervisados para la calidad del suministro del acceso (disponibilidad, oportunidad, entrega, historial de uso).

9.3 DIFERENCIAS Y SIMILITUDES EN LA CONSERVACIÓN

Una comparación entre la conservación tradicional de los documentos en soporte papel y los nuevos retos de la preservación digital puede ayudar a comprender el entorno y los requisitos que demandan estos documentos para que sean usables a lo largo del tiempo.

Documento en papel	Documento electrónico
El soporte puede durar muchos años	El soporte tiene una vida corta
Aun defectuoso o no restaurado se puede interpretar (leer)	Si está defectuoso, impide la interpretación (lectura)
La entidad debe establecer un plan de conservación y restauración	La entidad debe establecer un plan de preservación
La entidad debe establecer un plan contra el robo o sustracción ilegal	La entidad debe establecer un plan contra el robo o sustracción ilegal
Si está dañado, se puede restaurar mediante injertos, limpiezas y otras técnicas de carácter químico; tiene gran dependencia del soporte	Si está dañado, es casi imposible de recuperar; excepcionalmente, algunos programas pueden extraer parte de la información; tiene gran dependencia del formato (se prefieran formatos que incluyan la compatibilidad retrospectiva)
Se puede conservar durante muchos años sin intervención o uso, en condiciones ambientales adecuadas (poco exigentes)	Se necesita de la intervención humana periódica para realizar una política de migraciones y asegurar la conservación de la información por la obsolescencia tecnológica (hardware y software)
Su autenticidad está asegurada por la política de custodia, el sello de La entidad o la firma de los autores	Su autenticidad está asegurada por la política de custodia, la firma electrónica u otro sistema de encriptación con clave asimétrica
Su identificación en la organización se realiza mediante técnicas de descripción (analógica o electrónica) y localización (estanterías, cajas, tejuelos descriptivos, etc.)	Su identificación en la organización se realiza mediante metadatos en el entorno digital

Documento en papel	Documento electrónico
No suele cambiar de sitio físico, y su traslado supone un elevado costo humano y económico	Suele trasladarse con frecuencia a otros sitios físicos, mediante el transporte de sus soportes o mediante la transferencia telemática
Conocimientos o perfil profesional del conservador: química, biología, historia, paleografía, etc.	Conocimientos o perfil profesional del conservador: informática (software y hardware), gestión de documentos electrónicos
Los archivos conservan documentación de productores propios y de productores desaparecidos	Los archivos, a corto término, empezarán a conservar documentos digitales de productores propios, y a largo término deberán contemplar la conservación de los organismos desaparecidos
Los archivos conservan documentación de productores propios y de productores desaparecidos	El acceso es en línea (intranet, internet, etc.); la red debe cumplir requisitos de seguridad, usabilidad y accesibilidad, para evitar la sustracción o infección por virus informático

9.4 AMENAZAS INFORMÁTICAS

Las amenazas, como ya hemos mencionado, consisten en la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los insumos informáticos de la organización y ulteriormente a ella misma.

Entre ellas, identificamos como las principales:

- ✓ El advenimiento y proliferación de "malware" o "malicious software", programas cuyo objetivo es el de infiltrase en los sistemas sin conocimiento de su dueño, con objeto de causar daño o perjuicio al comportamiento del sistema y por tanto de la organización.

- ✓ La pérdida, destrucción, alteración, o sustracción de información por parte de personal de la organización debido a negligencia, dolo, mala capacitación, falta de responsabilidad laboral, mal uso, ignorancia, apagado o elusión de dispositivos de seguridad y/o buenas prácticas.

- ✓ La pérdida, destrucción, alteración, sustracción, consulta y divulgación de información por parte de personas o grupos externos malintencionados.

- ✓ El acceso no autorizado a conjuntos de información.
- ✓ La pérdida, destrucción o sustracción de información debida a vandalismo.
- ✓ Los ataques de negación de servicio o de intrusión a los sistemas de la organización por parte de ciber-criminales: personas o grupos malintencionados quienes apoyan o realizan actividades criminales y que usan estos ataques o amenazan con usarlos, como medios de presión o extorsión.
- ✓ Los "phishers", especializados en robo de identidades personales y otros ataques del tipo de "ingeniería social".
- ✓ Los "spammers" y otros mercadotecnistas irresponsables y egoístas quienes saturan y desperdician el ancho de banda de las organizaciones.
- ✓ La pérdida o destrucción de información debida a accidentes y fallas del equipo: fallas de energía, fallas debidas a calentamiento, aterriza miento, des magnetización, ralladura o descompostura de dispositivos de almacenamiento, etcétera.
- ✓ La pérdida o destrucción de información debida a catástrofes naturales: inundaciones, tormentas, incendios, sismos, etcétera.
- ✓ El advenimiento de tecnologías avanzadas tales como el cómputo quantum, mismas que pueden ser utilizadas para des encriptar documentos, llaves, etcétera al combinar complejos principios físicos, matemáticos y computacionales.

9.5 VULNERABILIDADES INFORMÁTICAS

Una vulnerabilidad es alguna característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza, intencional o accidentalmente. Las vulnerabilidades pueden provenir de muchas fuentes, desde el diseño o implementación de los sistemas, los procedimientos de seguridad, los controles internos, etcétera; se trata en general de protecciones inadecuadas o insuficientes, tanto físicas como lógicas, procedimentales o legales de alguno de los recursos informáticos. Las vulnerabilidades al ser explotadas resultan en fisuras en la seguridad con potenciales impactos nocivos para la organización. Más detalladamente, provienen de:

- ✓ Fallas en el diseño o construcción de programas, sobre todo en aquellos que provienen de un mercado masivo; por ejemplo, sistemas operativos, programas de aplicación, el protocolo de comunicaciones TCP/IP, etcétera.

- ✓ Uso de computadoras, programas y equipos de red de tipo genérico en aplicaciones críticas.
- ✓ Atención insuficiente al potencial error humano durante el diseño, implementación o explotación de sistemas, particularmente debidas a desviaciones u omisiones de buenas prácticas en estas etapas.
- ✓ Confianza excesiva en algún único dispositivo u oficina de seguridad.
- ✓ Relajamiento de las políticas y procedimientos de seguridad, debidos a falta de seguimiento de los mismos, producidas por un desempeño de seguridad adecuado durante cierto lapso.
- ✓ Fallas de seguimiento en el monitoreo o indicadores de seguridad.
- ✓ Pobre o nula gobernanza de los activos informáticos, debida principalmente a un mal seguimiento de esos activos y sus contextos de seguridad asociados de forma integral.
- ✓ Cambio frecuente de elementos de la plataforma informática.
- ✓ Falla en la adjudicación o seguimiento de responsabilidades.
- ✓ Planes de contingencia nulos o pobres, tanto para situaciones cotidianas como extremas.
- ✓ Ignorancia, negligencia o curiosidad por parte de usuarios en general de los sistemas.
- ✓ Equipos, programas y redes “heredados” de generaciones tecnológicas anteriores.
- ✓ Errores inherentes al diseño de microprocesadores y micro códigos que se encuentran en rutinas básicas o “núcleo” de los sistemas, o en el encriptado o virtualización.
- ✓ Falta de concientización del personal en general acerca de la importancia de la seguridad y responsabilidades compartidas e integrales.

9.6 RIESGOS INFORMÁTICOS

Como se mencionó también, riesgo se define como la probabilidad de que un evento nocivo ocurra combinado con su impacto o efecto nocivo en la organización. Se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto. Los principales riesgos se agrupan como:

- ✓ Sustracción de datos personales para usos malintencionados.
- ✓ Fugas de información, extracción o pérdida de información valiosa y/o privada.
- ✓ Introducción de programas maliciosos a los sistemas de la organización, que pueden ser utilizados para destruirlos u obstaculizarlos, usurpar recursos informáticos, extraer o alterar información sin autorización, ejecutar acciones ocultas, borrar actividades, robo y detentación de identidades, etcétera.
- ✓ Acciones de "ingeniería social" malintencionada: "phishing", "spam", espionaje, etcétera.
- ✓ Uso indebido de materiales sujetos a derechos de propiedad intelectual.
- ✓ Daño físico a instalaciones, equipos, programas, etcétera.

9.7 IMPACTOS

Los impactos son los efectos nocivos contra la información de la organización al materializarse una amenaza informática. Al suceder incidentes contra la seguridad informática pueden devenir en:

- ✓ Alteración en las rutinas y procesos de la organización con posibles consecuencias a su capacidad operativa.
- ✓ Pérdida de la credibilidad y reputación de la organización por parte del consejo directivo de la organización, público en general, medios de información, etcétera.
- ✓ Costo político y social derivado de la divulgación de incidentes en la seguridad informática.
- ✓ Violación por parte de la organización a la normatividad acerca de confidencialidad y privacidad de datos de las personas.

- ✓ Multas, sanciones o fincado de responsabilidades por violaciones a normatividad de confidencialidad.

- ✓ Pérdida de la privacidad en registros y documentos de personas.

- ✓ Pérdida de confianza en las tecnologías de información por parte del personal de la organización y del público en general.

- ✓ Incremento sensible y no programado en gastos emergentes de seguridad.

- ✓ Costos de reemplazo de equipos, programas, y otros activos informáticos dañados, robados, perdidos o corrompidos en incidentes de seguridad.

Cada uno de estos efectos nocivos puede cuantificarse de tal forma de ir estableciendo el impacto de ellos en la información y consecuentemente en la organización.

En resumen, la seguridad informática pretende identificar las amenazas y reducir los riesgos al detectar las vulnerabilidades nulificando o minimizando así el impacto o efecto nocivo sobre la organización.

10. CRITERIOS ISO PARA LA CONSERVACIÓN DE DOCUMENTOS ELECTRÓNICOS

Políticas de seguridad. Es indispensable en toda organización que posea activos informáticos contar con políticas de seguridad documentadas y procedimientos internos de la organización acerca de las estrategias y disposiciones que guíen los principales rubros y áreas relacionados con la seguridad de los bienes informáticos y que permitan su actualización y revisión por parte de un comité de seguridad interno. Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- ✓ Políticas y procedimientos internos generales de seguridad informática.
- ✓ Políticas de acceso a instalaciones sensibles.
- ✓ Políticas y procedimientos de inventarios de bienes informáticos
- ✓ Políticas y procedimientos de respaldo de datos.
- ✓ Políticas y procedimientos de resguardo de información.
- ✓ Políticas y procedimientos para asignación de usuarios y lineamientos normativos de acceso
- ✓ Políticas y procedimientos para la creación y mantenimiento de software.

Aspectos formales para la seguridad organizacional. La existencia de un marco formal de seguridad que debe integrar la organización, formados por una oficina o comité de administración de la seguridad de la información, un oficial de seguridad —*Information System Security Officer*— ISSO, un equipo de recuperación contra desastres, auditorías y revisiones externas a la infraestructura de seguridad, así como controles a los servicios de tercerización –*outsourcing*–, entre otros aspectos. Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- ✓ Elaboración de diagnósticos de seguridad
- ✓ Establecimiento de personas, áreas o comités específicamente creados para la seguridad informática.

Clasificación y control de activos. El análisis de riesgos utiliza un inventario de activos de información —instalaciones, equipos, programas, datos, personas—, que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado respecto de la información; es decir, los activos deben ser etiquetados de acuerdo con su nivel de confidencialidad y sensibilidad. Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- ✓ Definición de políticas y procedimientos claramente establecidos y distribuidos para la realización de inventarios de equipos, programas y procesos, así como para cambios, modificaciones y baja de los mismos.

- ✓ Realización de inventarios y clasificación de activos informáticos en cuanto a infraestructura de equipo de cómputo de alto rendimiento, equipo de comunicaciones, equipo donde se procesa o genera información sensible, equipo cotidiano.

- ✓ Realización de un inventario completo de bases de datos y sistemas y aplicaciones informáticos. Establecer y dar seguimiento a la periodicidad de estos inventarios.

Seguridad de las acciones del personal. En este aspecto, la seguridad se orienta a diseñar, implementar y proporcionar controles a las acciones del personal que opera con los activos de información. El objetivo de esta área es contar con los elementos necesarios para mitigar el riesgo de dolo, negligencia o accidente inherentes a la acción humana; es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información. Debe tomarse en cuenta que, según los expertos, las personas son en general el eslabón más débil en la cadena de seguridad informática y son responsables de la mayoría de las fallas [Schneier, 2000]. Algunos de los principales objetivos de control y acciones dentro de este

dominio son:

- ✓ Elaboración de los "perfiles de usuario" con acceso a cada una de las diversas bases de datos y recursos de información de la organización, tanto para el personal como para otros usuarios externos.

- ✓ Establecimiento de normas y políticas de uso correcto de las instalaciones, de los recursos y de la información por parte del personal y usuarios externos, así como correcta difusión de las mismas.

- ✓ Establecimiento de normas y políticas para el uso correcto de las redes y la Internet.

- ✓ Establecimiento de normas, políticas y procedimientos para asignación, uso e inhabilitación de cuentas del personal de la organización, así como de otros usuarios.

- ✓ En su caso, diseño y uso de cartas compromiso de confidencialidad –non disclosure agreement– con el personal que maneja información confidencial o sensible.

- ✓ Establecimiento de políticas, procedimientos y bitácoras de acceso a las instalaciones y uso de equipo de cómputo para usuarios externos (personal de mantenimiento enviado por proveedores, visitantes, etcétera).

- ✓ Seguridad física y de entorno. Identificar las instalaciones y los perímetros de seguridad, de forma que se puedan establecer controles del acceso físico a las distintas áreas con equipo, infraestructura y sistemas sensibles, de acuerdo con el tipo de seguridad preestablecida. Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- ✓ Establecimiento de normas, políticas y procedimientos para regular el acceso restringido a instalaciones, equipos e infraestructura sensibles.

- ✓ Establecimiento de normas, políticas y procedimientos para adquirir, instalar y supervisar los elementos recomendados universalmente para seguridad física: energía ininterrumpida, baterías, planta de energía de respaldo, pararrayos, tierras, físicas, cortafuegos, climatización, ductos adecuados, restringidos y señalizados, separando los de potencia de los de red; redes redundantes, pisos falsos, circuitos cerrados de televisión, detectores de humo y sistemas profesionales de extinción de incendios, etcétera.

Administración de operaciones, comunicaciones y equipo. Integrar los

procedimientos bajo los que opera la infraestructura tecnológica, así como los controles de seguridad inherentes documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, control de código malicioso, etcétera. Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- ✓ Establecimiento de normas, políticas y procedimientos para regular el acceso a los sistemas y redes: listas de acceso en ruteadores, equipos cortafuegos con programación interna de las políticas que facilitan o deniegan acceso a los usuarios, etcétera.

- ✓ Establecimiento de normas, políticas y procedimientos para regular el acceso a redes estándares, así como a las inalámbricas, las cuales se recomienda que estén todas bajo la modalidad de acceso protegido WPA –Wi-fi Protected Access– o semejante.

- ✓ Monitoreo frecuente del acceso a sistemas, aplicaciones y bases de datos.

- ✓ Monitoreo de enlaces a la red y logs o bitácoras de memoria de usos y accesos a sistemas operativos y bases de datos, tanto de sus administradores –DBA– como de personal y usuarios en general.

- ✓ Establecimiento de normas, políticas y procedimientos para verificar de la integridad de la información que se crea y almacena.

- ✓ Establecimiento de normas, políticas y procedimientos para depurar y auditar periódicamente la calidad de los datos contenidos en las bases de datos y archivos digitales de la organización.

- ✓ Establecimiento de normas, políticas y procedimientos para llevar registros de control de acceso a aplicaciones informáticas a través de identificación y autenticación y registros de auditoría.

- ✓ Establecimiento de normas, políticas y procedimientos para llevar bitácoras y controles de fallas de equipos y sistemas.

Control de acceso a los sistemas. Habilitar los mecanismos que permitan monitorear el acceso a los activos lógicos de información, que incluyen los procedimientos de administración de usuarios y sus privilegios, definición de responsabilidades o perfiles de seguridad y el control de acceso y cambios a las aplicaciones y bases de datos. Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- ✓ Establecimiento de normas, políticas y procedimientos para regular el acceso a todas las bases de datos y sistemas de información.

- ✓ Establecimiento de normas, políticas y procedimientos para creación de cuentas de usuarios de las bases de datos.

- ✓ Establecimiento de normas, políticas y procedimientos para asignación, modificación y baja de contraseñas o passwords.

- ✓ Establecimiento de normas, políticas y procedimientos para validación e integridad de datos, así como para depuraciones, descartes / disposiciones periódicas.

- ✓ Establecimiento de normas, políticas y procedimientos para llevar bitácoras de memoria de usos y accesos a las bases de datos.

- ✓ Establecimiento de normas, políticas y procedimientos para acceso a los sistemas y aplicaciones informáticos a través de identificación y autenticación.

- ✓ Establecimiento de normas, políticas y procedimientos para establecer y llevar registros de auditorías informáticas, en especial de la seguridad.

Desarrollo de sistemas y su mantenimiento. La organización debe disponer de procedimientos que garanticen la calidad y seguridad de origen de los sistemas desarrollados para tareas específicas de la organización, así como su mantenimiento periódico. Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- ✓ Establecer y seguir una metodología estándar para el desarrollo de sistemas de información, como por ejemplo RUP —*Rational Unified Process*— o Proceso Racional Unificado.

- ✓ Establecer y llevar procedimientos normados para la etapa de pruebas y liberación de nuevas versiones de sistemas de información.

- ✓ Diseñar y establecer un laboratorio de pruebas para el monitoreo y evaluación de desarrollos informáticos. Cabe subrayar que estos laboratorios no son instalaciones físicas propiamente, sino ambientes especializados, mayormente procedimentales y estandarizados para las pruebas.

- ✓ Establecimiento de procedimientos estandarizados para la creación de manuales de usuario y manuales técnicos de todos los sistemas de información y mantenerlos actualizados.

- ✓ Establecimiento de procedimientos estandarizados para el mantenimiento de programas y aplicaciones, control de versiones, gestión del cambio, etcétera.

- ✓ Establecimiento de procedimientos estandarizados de permiso a modificaciones y mantenimiento de los sistemas y aplicaciones informáticos a través de identificación y autenticación, así como registros de auditorías informáticas.

Control de incidentes de seguridad de la información y continuidad de las operaciones de la organización. La organización debe disponer de procedimientos que garanticen la detección oportuna de incidentes dentro de la seguridad de la información, así como los procedimientos para contender con estas contingencias; el sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias graves, garantizando la operación de la organización desde el punto de vista de la información. Estos planes deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar los alcances y eficacia de los mismos. Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- ✓ Diseñar y establecer uno o varios "centros maestros" de procesamiento de datos acordes al tamaño de la organización los cuales integren todo tipo de seguridades lógicas, físicas y organizativas construidos o adaptados con la intención para manejo adecuado y seguro de bases de datos y archivos de la organización.

- ✓ Diseñar y establecer "centros espejo" o "bases de datos espejo" o "archivos espejo", supervisando su actualización rigurosa de acuerdo a lo estipulado por la organización del RFE.

- ✓ Establecimiento de procedimientos estandarizados en todas las áreas para que lleven reportes de eventos relacionados con la seguridad.

- ✓ Establecimiento de procedimientos estandarizados en todas las áreas respecto a la solución de incidentes o escalamiento de los mismos a instancias superiores.

- ✓ Recordar periódicamente a todas las áreas que el programa de seguridad es permanente.

- ✓ Establecimiento de planes de contingencia, salvaguarda y recuperación de datos

Aspectos legales y normativos de la seguridad informática. La organización acatará las leyes, normas y reglamentos establecidos, y/o establecerá los pertinentes, con que debe cumplir internamente en materia de seguridad, así como los requerimientos de seguridad derivados de estos con los que deben cumplir todos

sus proveedores, socios, contratistas y usuarios. Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- ✓ Conocer y difundir las leyes, reglamentaciones, normas, etcétera dentro del marco jurídico que rigen y/o afectan a la organización.
- ✓ Revisar y difundir periódicamente las normas y procedimientos específicos relacionados con la seguridad, así como sus actualizaciones, tanto al interior de la misma como con proveedores y usuarios externos.
- ✓ Establecer y aplicar procedimientos normativos que rijan la adquisición y/o contratación de bienes y servicios informáticos, especialmente los dedicados a la seguridad informática.
- ✓ Diseñar, establecer y supervisar los mecanismos para verificar el correcto seguimiento de normas, políticas y procedimientos de seguridad informática en todas las áreas de la organización.

11. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES. [2]

11.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.
- Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información, los cuales estarán a cargo de la Oficina de Control Interno.
- Todo aplicativo informático o software debe ser comprado o aprobado por Dirección Técnica de TIC y Soporte Tecnológico en concordancia con la política de adquisición de bienes de la entidad de acuerdo con lo definido en el proceso

La Alcaldía Municipal De Bello debe contar con un *firewall* o dispositivo de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en *outsourcing* o de terceros.

[2] Tomado del Manual de políticas de Seguridad de la Información, presidencia de la república. (Presidencia de la republica, 2018)

La conexión remota a la red de área local de la Alcaldía Municipal De Bello debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, a excepción de los casos que autorice el Área de Sistemas de Información.

Los jefes de área o dependencia deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la Alcaldía Municipal De Bello

La Alcaldía Municipal De Bello en caso de tener un servicio de transferencia de archivos deberá realizarlo empleando protocolos seguros. Cuando el origen sea de la Alcaldía hacia entidades externas, se establecerán los controles necesarios para preservar la seguridad de la información; cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con esa entidad; en todo caso se deben revisar y proponer controles en concordancia con las políticas de seguridad de la información de la Alcaldía; los resultados de la revisión de requerimientos de seguridad se documentarán y preservarán para futuras referencias o para demostrar el cumplimiento con las políticas y con los controles de seguridad de la entidad.

El comité de seguridad informática y de sistemas de la Alcaldía Municipal De Bello definirá de acuerdo a la clasificación de la información (TRD), que datos deben ser cifrados y dará las directrices necesarias para la implementación de los respectivos controles (dispositivos a emplear, mecanismos de administración de claves, políticas de uso de sistemas de cifrado de datos).

11.2 POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la Alcaldía Municipal De Bello como, por ejemplo:

- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información transmitida vía oral o por cualquier otro medio de comunicación.

Los usuarios responsables de la información de la Alcaldía, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o

digitalmente por personal interno o externo.

Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como "Valiosa" para la entidad; Independiente del tipo de activo, se deben considerar las siguientes características.

- El activo de información es reconocido como valioso para la entidad.
- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
- Forma parte de la identidad de la organización y sin el cual la Alcaldía puede estar en algún nivel de riesgo.
- Los niveles de clasificación de la información que se ha establecido son: Información Pública Reservada, Información Pública Clasificada (Privada Y Semi-Privada) E Información Pública.

Los aspectos detallados de la política de clasificación de la información se deben identificar en los instrumentos "**REGISTRO DE ACTIVOS DE INFORMACIÓN" y TCA (Tabla de Control de accesos)**

11.3 POLÍTICAS ESPECÍFICAS PARA USUARIOS DEL ALCALDÍA MUNICIPAL DE BELLO

- La Alcaldía Municipal de Bello, suministra una cuota de almacenamiento de la información en un servidor de archivos con los permisos necesarios para que cada usuario guarde la información que crea importante y sobre ella se garantizará la disponibilidad en caso de un daño en el equipo asignado, esta información será guardada el tiempo establecido en la TRD.

- La Alcaldía Municipal de Bello instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización de la Alcaldía Municipal de Bello (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la entidad, por lo que ésta práctica no está autorizada.

- Todo el software usado en la plataforma tecnológica de la Alcaldía Municipal de Bello debe tener su respectiva licencia y acorde con los derechos de autor.

- La Alcaldía Municipal de Bello no se hace responsable por las copias no

autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas.

- El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) pueden ocasionalmente generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal e individual de Dirección Técnica de TIC y Soporte Tecnológico de la Alcaldía Municipal de Bello, previa solicitud escrita por parte del jefe inmediato.

- Los programas instalados en los equipos son de propiedad de la Alcaldía Municipal de Bello, la copia no autorizada de programas o de su documentación, implica una violación a la política general de la Alcaldía Municipal de Bello. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por la Alcaldía Municipal de Bello o las sanciones que especifique la ley.

- La Alcaldía Municipal de Bello se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad de la entidad. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.

- Los recursos tecnológicos y de software asignados a los funcionarios de la Alcaldía Municipal de Bello son responsabilidad de cada funcionario.

- Los usuarios son los responsables de la información que administran en sus equipos personales y deben abstenerse de almacenar en ellos información no institucional.

- Los usuarios solo tendrán acceso a los datos y recursos autorizados por la Alcaldía Municipal de Bello, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.

- Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.

- Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.

- Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente a la mesa de ayuda (PUC – Punto Único de Contacto) de Dirección Técnica de TIC y Soporte Tecnológico de la Alcaldía Municipal de Bello o al CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad).

- Los jefes de las diferentes áreas de la Alcaldía Municipal de Bello, en conjunto con el Comité de Seguridad Informática y de Sistemas propiciarán actividades para concienciar al personal sobre las precauciones necesarias que deben realizar los usuarios finales, para evitar revelar información confidencial cuando se hace una llamada telefónica, que pueda ser interceptada mediante acceso físico a la línea o al auricular o ser escuchada por personas que se encuentren cerca. Lo anterior debe aplicar también cuando el funcionario, contratista o colaborador se encuentre en sitios públicos como restaurantes, transporte público, ascensores, etc.

- Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizando archivos compartidos en los computadores, discos virtuales, CD, DVD, medios removibles; deben usarse los mismos servicios del sistema de información, los cuales están controlados y auditados.

11.4 POLÍTICAS ESPECÍFICAS PARA FUNCIONARIOS Y CONTRATISTAS DEL ÁREA DE SISTEMAS DE INFORMACIÓN.

- El personal de Dirección Técnica de TIC y Soporte Tecnológico no debe dar a conocer su clave de usuario a terceros sin previa autorización del Jefe del Área de Sistemas de Información.

- Los usuarios y claves de los administradores de sistemas y del personal del Área de Sistemas de Información son de uso personal e intransferible.

- El personal de Dirección Técnica de TIC y Soporte Tecnológico debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado.

- Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Jefe de

Dirección Técnica de TIC y Soporte Tecnológico o el Asesor de Seguridad Informática.

- Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.

- Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo con el software disponible en la entidad. Ej.: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.

- Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.

- Los funcionarios de Dirección Técnica de TIC y Soporte Tecnológico no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Jefe de Dirección Técnica de TIC y Soporte Tecnológico y el registro en el sistema de la mesa de ayuda (PUC).

- Los funcionarios de Dirección Técnica de TIC y Soporte Tecnológico se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.

- Los funcionarios de Dirección Técnica de TIC y Soporte Tecnológico no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.

- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.

- Las copias licenciadas y registradas del software adquirido deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.

- La copia de programas o documentación requiere tener la aprobación escrita de la Alcaldía Municipal de Bello y del proveedor si éste lo exige.

- El personal de Dirección Técnica de TIC y Soporte Tecnológico debe velar por que se cumpla con el registro en la bitácora de acceso al datacenter, de las personas que ingresen y que hayan sido autorizadas previamente por la jefatura

del área o por quien esta delegue.

- Por defecto deben ser bloqueados, todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por la entidad a través del Comité de Seguridad Informática y de Sistemas.

- Aquellos servicios y actividades que no son esenciales para el normal funcionamiento de los sistemas de información deben ser aprobados oficialmente por la entidad, a través del Comité de Seguridad Informática y de Sistemas, y deben ser asegurados mediante controles que permitan la preservación de la seguridad de la información.

- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.

- Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.

- Las pruebas de laboratorio o piloto deben ser autorizadas por el Comité de Seguridad Informática y de Sistemas, para sistemas de información, de software tipo freeware o shareware o de sistemas que necesiten conexión a internet; estas deben ser realizadas sin conexión a la red LAN de la entidad y con una conexión separada de internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción.

11.5 POLÍTICAS ESPECÍFICAS PARA WEB MASTER

Los responsables de los contenidos de las páginas Web (*web masters*), deben preparar y depurar la información de su Área o dependencia y reportar a la mesa de ayuda (PUC) los requerimientos de actualización de la versión del software; deben disponer de un archivo actualizado con la información de la página inicial del sitio; y deben registrar la autorización de publicación por parte del funcionario autorizado y coordinar con el administrador web del Área de Sistemas de Información los lineamientos del sitio.

Se deberá seguir la Política Editorial y Actualización de Contenidos Web, que permita auditar la publicación o modificación de información oficial en las páginas web.

Las claves de acceso de los responsables de los contenidos de las páginas Web (*web masters*), son estrictamente confidenciales, personales e intransferibles.

11.6 POLÍTICA DE RETENCIÓN Y ARCHIVO DE DATOS.

La política de retención de archivos debe establecer cuánto tiempo se deben mantener almacenados los archivos en la Alcaldía Municipal de Bello de acuerdo a las tablas de retención documental – TRD. Las reglas y los principios generales que regulan la función archivística del Estado se encuentran definidos por la Ley, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.

La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

11.7 POLÍTICA DE DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS.

Los medios y equipos donde se almacena procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento; para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

11.8 POLÍTICA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN.

- La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como cinta, cartucho, CD, DVD, etc.

- Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.

- Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.

- Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

- Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.

- Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones de la Alcaldía Municipal de Bello.

- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.

- Semanalmente los administradores de infraestructura de la Alcaldía Municipal de Bello verificarán la correcta ejecución de los procesos de backup, suministrarán las cintas requeridas para cada trabajo y controlarán la vida útil de cada cinta o medio empleado.

- Dirección Técnica de TIC y Soporte Tecnológico debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de la Alcaldía Municipal de Bello.

- Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

- Es responsabilidad de cada dependencia mantener depurada y clasificada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento que entrega de la Alcaldía Municipal de Bello a los usuarios.

11.9 POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

Inventario de activos de información

La Alcaldía Municipal de Bello mantendrá un inventario o registro actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el Área de Sistemas de Información. El Registro de Activos de Información deberá ser publicado en la página web de la Entidad, acorde con lo establecido en el literal j del Artículo 11 de la Ley 1712 de 2014.

Una parte de los activos de información se mantendrá en una base de datos bajo la responsabilidad del Área de Sistemas de Información. (Base de datos de gestión de configuraciones - *Configuration Management Database* CMDB).

Propietarios de los activos de información

La Alcaldía Municipal de Bello es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la entidad (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de

información o aplicaciones informáticas, hardware o infraestructura de tecnología de información y comunicaciones (TIC).

11.10 POLÍTICA DE USO DE LOS ACTIVOS.

- Los activos de información pertenecen a la Alcaldía Municipal de Bello y el uso de estos debe emplearse exclusivamente con propósitos laborales.

- La Alcaldía Municipal de Bello proporcionará a los usuario los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la Alcaldía Municipal de Bello, los funcionarios solo podrán realizar backup de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por la Alcaldía Municipal de Bello. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.

- Periódicamente, Dirección Técnica de TIC y Soporte Tecnológico efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considera como una violación a las Políticas de Seguridad de la Información de la Alcaldía Municipal de Bello.

- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados a través de la mesa de ayuda de Dirección Técnica de TIC y Soporte Tecnológico con su correspondiente justificación para su respectiva viabilidad.

- Estarán bajo custodia de Dirección Técnica de TIC y Soporte Tecnológico los medios magnéticos/electrónicos (disquetes, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.

- En caso de ser necesario y previa autorización del Comité de Seguridad Informática y de Sistemas de la Alcaldía Municipal de Bello, los funcionarios podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su cargo.

- Los recursos informáticos de la entidad no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos. Estos actos incluyen, pero no se limitan a: envió de correo electrónico masivo con fines no institucionales y práctica de juegos en línea.

- Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Área de Sistemas de Información:

- Instalar software en cualquier equipo de la Alcaldía Municipal de Bello.

- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la entidad.

- Modificar, revisar, transformar o adaptar cualquier software propiedad de la Alcaldía Municipal de Bello.
- Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la Alcaldía Municipal de Bello.

- Copiar o distribuir cualquier software de propiedad de la Alcaldía Municipal de Bello

- El usuario deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad o uso indebido que tenga conocimiento.

- El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.

- Ningún usuario deberá acceder a la red o a los servicios TIC de la Alcaldía Municipal de Bello, utilizando una cuenta de usuario o clave de otro usuario.

- Cada usuario es responsable de asegurar que el uso de redes externas, tal como Internet, no comprometa la seguridad de los recursos informáticos de la Alcaldía Municipal de Bello. Dirección Técnica de TIC y Soporte Tecnológico de la entidad, es el área responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad; esta responsabilidad

incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.

- Todo archivo o material recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas destructivos antes de ser instalados en la infraestructura TIC de la Alcaldía Municipal de Bello

- Todo cambio a la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios de Dirección Técnica de TIC y Soporte Tecnológico de la Alcaldía Municipal de Bello.

- La información de la Alcaldía Municipal de Bello debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información este seguro y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.

11.11 POLÍTICA DE USO DE ESTACIONES CLIENTE.

- La instalación de software en los computadores suministrados por la Alcaldía Municipal de Bello, es una función exclusiva del Área de Sistemas de Información. Se mantendrá una lista actualizada del software autorizado para instalar en los computadores.

- Los usuarios no deben mantener almacenados en los discos duros, de las estaciones cliente o discos virtuales de red, archivos de vídeo, música y fotos que no sean de carácter institucional.

- En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a estos archivos.

- Los usuarios podrán trabajar sus documentos institucionales en borrador en la estación cliente asignada por la Alcaldía Municipal de Bello y deberán ubicar copias y documentos finales en las carpetas virtuales centralizadas que se establezca para cumplir con las tablas de retención documental TRD de la Entidad.

- El préstamo de equipos de cómputo, computadores portátiles y vídeo proyectores se debe tramitar a través de la mesa de ayuda con anticipación y se proveerá de acuerdo con la disponibilidad.

- Los equipos que ingresan temporalmente a la Alcaldía Municipal de Bello que son de propiedad de terceros: deben ser registrados en las porterías de la entidad para poder realizar su retiro sin autorización, la Alcaldía Municipal de Bello no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.

- Dirección Técnica de TIC y Soporte Tecnológico no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de la Alcaldía Municipal de Bello.

11.12 POLÍTICA DE USO DE INTERNET.

- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales

- No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de la Alcaldía Municipal De Bello o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la entidad.

- El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del Comité de Seguridad Informática y de Sistemas de la Alcaldía Municipal De Bello.

- La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

11.13 POLÍTICA DE USO DE MENSAJERÍA INSTANTÁNEA Y REDES SOCIALES

- No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.

- La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la Alcaldía Municipal De Bello, que sea creado a nombre personal, como redes sociales, twitter®, facebook®, youtube® LinkedIn® o blogs, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

11.14 POLÍTICA DE USO DE DISCOS DE RED O CARPETAS VIRTUALES

- Para que los usuarios tengan acceso a la información ubicada en los discos de red, se debe registrar la solicitud a través de servicios compartidos especificando el acceso y permisos, correspondientes al rol y funciones a desempeñar, a la mesa de ayuda de Dirección Técnica de TIC y Soporte Tecnológico de la Alcaldía Municipal De Bello. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.

  - La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.

  - La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.

  - Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en los discos de red.
  - Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.

  - Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

  - La responsabilidad de generar las copias de respaldo de la información de los discos de red está a cargo del Área de Sistemas de Información.

  - La responsabilidad de custodiar la información en copias de respaldo controladas, fuera de las instalaciones de la Alcaldía Municipal de Bello, estará a cargo del Área de Dirección Técnica de TIC y Soporte Tecnológico.

11.15 POLÍTICA DE USO DE IMPRESORAS Y DEL SERVICIO DE IMPRESIÓN

- Los documentos que se impriman en las impresoras de la Alcaldía Municipal De Bello deben ser de carácter institucional.

- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto

funcionamiento.

- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la mesa de ayuda del Área de Sistemas de Información.

11.16 POLÍTICA DE USO DE PUNTOS DE RED DE DATOS (RED DE ÁREA LOCAL – LAN).

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos estándar. Los equipos de uso personal, que no son de propiedad de la Alcaldía Municipal De Bello, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por Dirección Técnica de TIC y Soporte Tecnológico de la Alcaldía Municipal De Bello.

- La instalación, activación y gestión de los puntos de red es responsabilidad del Área de Dirección Técnica de TIC y Soporte Tecnológico.

11.17 POLÍTICAS DE SEGURIDAD DEL CENTRO DE DATOS Y CENTROS DE CABLEADO

- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.

- Dirección Técnica de TIC y Soporte Tecnológico debe garantizar que el control de acceso al centro de datos de la Alcaldía Municipal de Bello cuenta con dispositivos electrónicos de autenticación o sistema de control biométrico.

- Dirección Técnica de TIC y Soporte Tecnológico deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía

- La limpieza y aseo del centro de datos debe efectuarse en presencia de un funcionario o contratista de Dirección Técnica de TIC y Soporte Tecnológico de la Alcaldía Municipal De Bello. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que

no sean estrictamente necesarios para su labor de limpieza y aseo.

- En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

- El centro de datos debe estar provisto de:

- Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.

- Pisos elaborados con materiales no combustibles.

- Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.

- Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.

- Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.

- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.

- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

- La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por el Comité de Seguridad Informática y de Sistemas y exclusivamente con fines institucionales.

- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista autorizado de la Alcaldía Municipal De Bello

- Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.

- Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.

- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

- Los equipos del centro de datos que lo requieran deben estar monitoreados para poder detectar las fallas que se puedan presentar.

11.18 POLÍTICAS DE SEGURIDAD DE LOS EQUIPOS

Seguridad del cableado

Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
Deben existir planos que describan las conexiones del cableado.
El acceso a los centros de cableado (Racks), debe estar protegido.

Mantenimiento de los Equipos

La Alcaldía Municipal De Bello *debe mantener contratos de soporte y mantenimiento de los equipos críticos.* Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.

Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.

Los equipos que requieran salir de las instalaciones de la Alcaldía Municipal De Bello para reparación o mantenimiento deben estar debidamente autorizados y se debe garantizar que en dichos elementos no se encuentra información establecida como crítica en la clasificación de la información de acuerdo con los niveles de clasificación

de la información.

Para que los equipos puedan salir de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos, teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de la Alcaldía Municipal De Bello.

Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar sobreescrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.

Ingreso y retiro de activos de información de terceros.

El retiro e ingreso de todo activo de información de propiedad de los usuarios de la Alcaldía Municipal De Bello, utilizados para fines personales, se realizará mediante los procedimientos establecidos por la Administración del Edificio. La Alcaldía Municipal De Bello no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica.

El retiro e ingreso de todo activo de información de los visitantes que presten servicios de la Alcaldía Municipal De Bello (consultores, pasantes, visitantes, etc.) será registrado y controlado en las porterías del edificio. El personal de vigilancia de recepción verificará y registrará las características de identificación del activo de información.

11.19 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

- El personal de la Alcaldía Municipal De Bello debe conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

- El personal de la Alcaldía Municipal De Bello debe bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

- Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

- No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos

11.20 POLÍTICA DE USO DE CORREO ELECTRÓNICO.

Esta política define y distingue el uso de correo electrónico aceptable/apropiado e inaceptable/inapropiado y establece las directrices para el uso seguro del servicio.

Servicio de correo electrónico:

Se permite a los usuarios de la Alcaldía Municipal De Bello, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones.

Principios guía

- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

- Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la entidad. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de la Alcaldía Municipal De Bello se consideran bajo el control de la entidad.

- Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada de la Alcaldía Municipal De Bello y no debe utilizarse para ningún otro fin.

- El envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red, no está autorizado.

- No está autorizado, el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.

Condiciones de uso del servicio:

Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de la Alcaldía Municipal De Bello, su cuenta de correo será desactivada. Los correos electrónicos deben contener la siguiente nota respecto al manejo del contenido:

El contenido de este mensaje y sus anexos son propiedad de la Alcaldía Municipal de Bello, es únicamente para el uso del destinatario ya que puede contener información pública reservada o información pública clasificada (privada o semiprivada), las cuales no son de carácter público. Si usted no es el destinatario, se informa que cualquier uso, difusión, distribución o copiado de esta comunicación está prohibido. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto a la información contenida, por personas o entidades diferentes al propósito original de la misma, es ilegal. Si usted es el destinatario, le solicitamos dar un manejo adecuado a la información; de presentarse cualquier suceso anómalo, por favor informarlo al correo notificaciones@bello.gov.co

El tamaño del buzón de correo electrónico estará determinado por el rol desempeñado por el usuario en la Alcaldía Municipal De Bello.

Cada área deberá solicitar la creación de las cuentas electrónicas, sin embargo, las áreas de Recursos Humanos y de Contratación son las responsables de solicitar la modificación o cancelación de las cuentas electrónicas a la Oficina de información y sistemas de la Alcaldía Municipal De Bello

Las cuentas de correo electrónico son propiedad de la Alcaldía Municipal De Bello, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la entidad, ya sea como personal de planta, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Entidad y no debe utilizarse para ningún otro fin.

Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo a la clasificación de la información establecida por la Alcaldía Municipal De Bello.

Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Entidad.

Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar al correo del Área de Dirección Técnica de TIC y Soporte Tecnológico con la frase "correo sospechoso" en el asunto.

El único servicio de correo electrónico autorizado en la entidad es el asignado por el

Área de Dirección Técnica de TIC y Soporte Tecnológico.

Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios, contratistas y otros colaboradores de la Alcaldía Municipal De Bello. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la Alcaldía Municipal de Bello tomará las acciones disciplinarias y legales correspondientes.

12. POLÍTICA DE PRESERVACIÓN DIGITAL. [3]

A continuación, se identifican y describen las razones que han motivado a la Alcaldía Municipal de Bello, a crear el archivo digital y a desarrollar la política de preservación digital, los beneficios de contar con dicha política, las áreas definidas que se incluyen, las problemáticas más importantes discutidas, las estrategias y limitaciones de la institución y demás aspectos específicos y relevantes relacionados con la preservación digital.

Los principales referentes de la política de preservación digital a largo plazo son: el Modelo de referencia OAIS y el marco legal colombiano.

12.1 OAIS. OPEN ARCHIVAL INFORMATION SYSTEM

Es un modelo conceptual destinado a la gestión, al archivo y a la preservación longeva de documentos. OAIS se ha registrado como norma ISO 14721:2003. El Modelo OAIS constituye un referente internacional en responsabilidad del Consulative Committee for Space Data System (CCSDS), que describe de forma genérica las funciones, las responsabilidades y la organización de un conjunto de componentes (sistema) para preservar información (documentos) a largo plazo. El largo plazo está definido como el cálculo de tiempo para que los documentos electrónicos resistan el impacto de la evolución tecnológica y se garantice, en ese período, un acceso al contenido informativo archivado.

El Modelo OAIS se desarrolla en un entorno de interacción con tres entidades:

- Productores de documentos, que generan evidencias a partir de las funciones asignadas;
- Usuarios, que explotan el contenido intelectual de los documentos; y
- Administración, controla la gestión, uso y respaldo de la información

Y está conformado seis entidades funcionales:

[3] Tomado de Fundamentos de preservación digital Agn. (Archivo General de la Nación, 2018)

Módulo de ingreso: Ofrece el servicio y funciones para aceptar Paquetes de Información de Transferencia-PIT, desde los productores y preparar los contenidos para el almacenamiento y gestión en el Archivo Digital.

Módulo de almacenamiento: Provee los servicios y funciones para el almacenamiento, mantenimiento y recuperación de los Paquetes de Información de Archivo - PIA.

Módulo de gestión de datos: Proporciona servicios y funciones para ingresar datos, mantener y acceder a la información descriptiva y a los datos administrativos para la gestión del archivo. Incluye la administración y actualización de la base de datos.

Módulo de administración: Suministra los servicios y funciones para gestión de los usuarios, de las políticas del archivo, de plantillas y esquemas de metadatos que describen los PIT, de la jerarquía documental y de la auditoría y trazabilidad de los eventos realizados en el archivo.

Módulo de planeación de la preservación: Proporciona los servicios y funciones de control del entorno del archivo, para proveer recomendaciones y planes de preservación digital a largo plazo.

Módulo de acceso: Ofrece servicios y funciones de apoyo a los usuarios para determinar la existencia, localización y disponibilidad de la información; esto incluye distintas interfaces para el acceso a los contenidos, visualización de los objetos digitales y acceso a los documentos y metadatos aplicando controles que limitan el acceso a dichos contenidos; permite el descargue de copias de PIA.

El Sistema Abierto de Información de Archivo - OAIS es el marco para la normalización de la preservación digital y es la principal referencia conceptual para establecer la política, requisitos y acciones.

Fuente: Agn.

12.2 ACCIONES DE PRESERVACIÓN DIGITAL. [4]

Cómo estrategias para el manejo de los documentos electrónicos, a continuación, se listan alguna de las estrategias de preservación digital más utilizadas, que se pueden encontrar en el medio, sin embargo, al momento de implementarlas la alcaldía municipal de Bello, deberá investigar las más actualizadas y que ajusten a sus presupuestos.

a. Renovación de medios.

También conocida como refresco es la transferencia de los datos de un soporte a otro nuevo para reducir el riesgo de la perdida. Se efectúa sin producir cambio alguno en el software o el formato. Esto se hace para mitigar los niveles de obsolescencia tecnológica, controlar el riesgo frente a la durabilidad de los soportes, la vulnerabilidad del deterioro, la perdida por intrusiones humanas, fallas catastróficas o desastres naturales.

b. Integración de documentos.

Basado en la realización de duplicado de los datos almacenados. Se debe contar con una aplicación que permita integrar todos los documentos y los datos de los demás aplicativos a un gestor documental que cumpla con el SGDEA; de esta manera la alcaldía municipal de Bello mantendrá una copia local de dichos documentos.

c. Normalización de los formatos

Por medio de políticas claras identificadas en este plan de preservación digital a largo plazo, y estrategias establecidas, en Modelo de requisito de documento electrónico de archivo (MR), instrumento archivístico que deberá ser construido por la

[4] Tomado de Plan de preservación digital Ministerio de Educación Nacional. (Ministerio de Educación Nacional, 2020)

alcaldía municipal de Bello; se establecerán los formatos reglamentarios para la producción de los documentos electrónicos, de tal manera que facilitarán lo siguiente:

Nivel de transparencia: grado en que los formatos son accesibles pues provienen de código abierto.

Apertura: grado de independencia frente respecto de una patente de derechos de autor

Independencia: grado de independencia con respecto a hardware o software

Interoperabilidad: Capacidad de intercambio con otros entornos tecnológicos

Estabilidad: Grado en que el formato mantiene su funcionalidad con respecto a versiones anteriores.

Estandarización: grado de cumplimiento con un estándar establecido por un organismo de normalización.

Mecanismos de protección técnica: Grado en que estos mecanismos no establecen restricciones o interfieren en la recuperación de datos o interfieren en los procesos de evolución tecnológica.

En archivo adjunto se proponen algunos formatos, dependiendo de los tipos de documentos electrónicos que existen al momento, y que se podrán tener en cuenta para el proceso de implementación.

d. Utilización de metadatos de preservación.

Los aplicativos y el software de gestión documental, deberán cumplir con las guías y protocolos establecidos por el ente rector, Archivo General de la nación; por lo tanto, los aplicativos que se adquieran deben cumplir con los metadatos de preservación digital a largo plazo qué se proponen en archivo anexo a este documento, y la guía de estructuración de metadatos establecida en la política nacional.

e. Migración.

Esta es una de las técnicas o estrategias más utilizadas hoy en día, este método consiste en convertir los documentos almacenados a nuevos formatos, con el fin de no perder la información que contienen. Mediante este proceso se mantienen las características esenciales de los datos; aunque se pueden producir pequeños cambios que con el paso del tiempo y la acumulación de migraciones pueden verse amplificados, tales como una pérdida de información en un dos por ciento; de tal

manera que estos procesos se deben hacer por expertos y con control de los documentos.

Sin embargo, esta estrategia de migración es necesaria para todos los documentos cuyos soportes son considerados obsoletos, y que los equipos que tenemos hoy día no los leen; tales cómo disquetes, microfichas entre otros

Dicha técnica debe garantizar la autenticidad la integridad la fiabilidad y la disponibilidad de los documentos.

f. Emulación

Está técnica permite simular el comportamiento del software original con el que se crearon los documentos digitales, de forma que puedan ejecutarse y utilizarse pudiendo prescindir del programa de origen. Es muy útil para abrir archivos que por su versiona miento ya no abren. Se recomienda utilizarlo para aquellos archivos necesarios e históricos de la institución. También debe ser de cuidado su implementación.

g. Mantenimiento de firmas electrónicas

La ley y 527 de 1999 permite la utilización de firmas electrónicas y otras, con el fin de disminuir los volúmenes de documentos físicos, a documentos electrónicos y permitir el comercio electrónico. De tal manera que la alcaldía municipal de Bello deberá garantizar la emisión, renovación y revocación de firmas electrónicas. Las áreas de sistemas deberán implementar las medidas necesarias para preservar los documentos electrónicos Y garantizar su originalidad y accesibilidad.

12.3 DESARROLLO DE PROCEDIMIENTOS DE PRESERVACIÓN DIGITAL

A continuación, se mencionan los procedimientos de preservación digital qué deben implementar en la alcaldía municipal de Bello, con el fin de cumplir la política de preservación digital de documento electrónico, y garantizar la estrategia propuesta de Gobierno digital.

a. Procedimiento de identificación y análisis de series documentales a preservar a largo plazo:

Este procedimiento consiste en identificar las tipologías documentales agrupadas en sus diferentes series documentales y mencionadas en la tabla de retención documental de la alcaldía de Bello.

Dichos documentos deberán ser normalizados y estandarizados con los formatos reglamentados por el archivo general de la nación.

También es importante definir las cantidades y capacidad de almacenamiento requerido en los servidores de la entidad, elaborar el inventario de documentos electrónicos de archivo con los campos específicos, reglamentados en el decreto 29 del 2015.

También verificar los formatos en que se producen, y validar que garanticen la preservación digital a largo plazo.

b. Procedimiento de transferencias documentales electrónicas. [5]

Para la entrega y/o transferencia y recibo de información, documentos y archivos electrónicos o almacenados en medios magnéticos, dispositivos electrónicos, unidades en estado sólido o cualquier otro dispositivo similar, se deberán seguir las siguientes instrucciones:

a) Determinar el estado de conservación de las unidades de almacenamiento;
b) Determinar el volumen de los documentos en información (en GB o TB);
c) Organizar la información electrónica siguiendo una estructura de archivos que facilite su transferencia, consulta y administración;
d) Identificar exteriormente las unidades con el nombre de la información, las fechas extremas y las características del formato, para facilitar su lectura o interpretación.

c. Descripción técnica de los medios electrónicos. [6]

Se acompañará al medio electrónico de almacenamiento, un documento técnico en el cual se describan las características de la información electrónica entregada, así:
a) El sistema operativo requerido para leer la información;
b) El formato en el cual se está entregando la información;
c) La estructura de los directorios;
d) Las tablas utilizadas para interpretar la información;
e) Las características de las firmas digitales empleadas en la gestión de los documentos electrónicos.

A los documentos o información que se encuentre encriptada o cifrada, se les deberá retirar la protección antes de su entrega y/o transferencia a la entidad responsable de

[5] Tomado textualmente del Decreto 29 de 2015 (Ministerio de Cultura, 2015)
[6] Tomado textualmente del Decreto 29 de 2015 (Ministerio de Cultura, 2015)

recibirlos. De ser documentos sujetos a reserva legal o clasificados, se mantendrá la misma conforme lo establecido en la Ley 1712 de 2014 y las normas especiales que regulen este aspecto.

Medios electrónicos con documentos digitalizados.

Los medios electrónicos que contienen documentos digitalizados se entregarán mediante inventario, debidamente identificados exteriormente.

d. Procedimiento de administración del sistema de preservación digital:

Cómo parte del procedimiento, para la administración del sistema de preservación digital a largo plazo, es importante establecer, inicialmente las características del software y aplicativos que se utilizan en la entidad; con el fin de garantizar sus funcionalidades y los estándares técnicos establecidos, por las normas nacionales e internacionales.

Posteriormente por medio de capacitaciones se debe difundir las políticas mencionadas en el presente plan, así como los formatos recomendados para la producción documental.

Adicionalmente se deben realizar visitas de verificación a los funcionarios para hacerle seguimiento a lo siguiente:

- Obsolescencia de los formatos estandarizados
- Estado de los medios de almacenamiento
- Niveles de cumplimiento de las políticas
- Identificación de amenazas de perdida de información y las probabilidades de que ocurran.
- Identificación de ejecución periódica de copias de respaldo.
- Identificación de los repositorios para los documentos electrónicos
- Identificación de condiciones ambientales para los repositorios electrónicos.
- Análisis de diagnóstico y revisión de las estrategias
- Aprobación y ejecución de estrategias y acciones
- Implementación de las estrategias que se requieran
- Ajuste del plan de preservación

e. Procedimiento de selección de medios de almacenamiento digital. [7]

Todos los medios o sistemas de grabación se encuentran en riesgo de pérdida repentina de acceso a la información digital sin importa la tecnología, por lo tanto, un

[7] NTC-ISO-TR 17797:2016 (Icontec, 2016)

sistema de gestión de la información debería diseñarse de modo que mitigue el riesgo de pérdida dicha información.

La elección de sistemas de almacenamiento o medios es compleja debido al comportamiento impredecible durante su vida útil, la confiabilidad de los medios de almacenamiento la proporcionan con frecuencia los fabricantes, con relación al tipo de medio en particular la cual puede variar de 10 años a varios siglos; sin embargo, en el mercado se pueden encontrar vidas útiles de meses hasta 20 años.

Por lo tanto, se deben seleccionar soluciones de almacenamiento teniendo en cuenta lo siguiente:

- Resultados de pruebas de aceptación
- Trazabilidad de los procesos de manufactura
- Calidad mediante proceso de muestreo
- Monitoreo longitudinal de medios y controladores
- Condiciones ambientales de almacenamiento
- Seguimiento continuo en la evolución del suministro hardware y software en relación con el riesgo de retiro de productos comerciales

A continuación, se listan algunos medios de almacenamiento digitales más utilizados:

Unidades de discos duros: Estas unidades son dispositivos electromecánicos que por lo general contienen discos de aluminio que se encuentran en capas con material de registro magnético. Los datos se escriben desde y hacia sus cabezas móviles de lectura escritura que flotan sobre la superficie del disco, tienen una vida útil corta y se deberían reemplazar cada cinco años; Son susceptibles de perdida de datos derivado del uso extendido del disco, daños físicos de la unidad misma y falla repentina del disco entre otros.

Cómo estrategia De protección archivística se recomienda: Múltiple replica de autos archivados entre más replicas mayor será la protección, migrar periódicamente los datos en medio o sistemas actuales a fin de evitar el deterioro de los bits y la obsolescencia del sistema, almacenar los medios archivísticos en entornos de temperatura y humedad controlada para minimizar el deterioro y la corrosión del disco.

Cintas magnéticas: es un tipo de medio o soporte de almacenamiento de datos que se graba en pistas sobre una banda plástica con un material magnetizado, generalmente óxido de hierro o algún cromato. El tipo de información que se puede almacenar en las cintas magnéticas es variado, como vídeo, audio y datos.

Cada generación de unidad de cinta puede ser viable durante 4-6 años después de lo cual es muy importante migrar la información.

Para garantizar la calidad de las cintas es importante hacerle seguimiento a lo siguiente:

Propiedades mecánicas cómo cabezas de lectura de sonido, desgaste de las cintas, señal ruido y forma de onda, forma de grabación y reproducción.

Cómo recomendación para garantizar su preservación a largo plazo:

No se puede retirar la cinta del almacenamiento y reproducirse de inmediato, se debe dar un tiempo para que las cintas equilibren al entorno de temperatura y humedad, antes del procesamiento de la reproducción;

También se deben renovar de 3 a 5 años para medio de cintas magnéticas y el reemplazo de cada unidad de uno a cinco años.

Con relación a la limpieza es importante ya que el material particulado puede causar perdida de la señal.

Unidad de estado sólido o memoria flash: La memoria flash es una memoria no volátil qué se puede borrar y reprogramar en unidades de memoria llamadas bloques.

Los chips de memoria flash almacenan los datos en grandes arreglos, la memoria flash es susceptible al desgaste debido a los ciclos repetidos de programación y borrado, con el tiempo la constante programación y borrado de la misma la desgasta y la inválida. Para evitarlo se hace uso de algoritmos especiales Dentro de la SSD denominados nivelación desgaste. La vida útil de la SSD Es de 10 a 20 años.

Discos ópticos gravables y re- escribibles: Tales cómo CD DVD BD. Los gravables permiten escritura y lectura solo una vez, y es crítico para garantizar la autenticidad la información, y es una solución fundamental para archivar.

Son dispositivos que se degradan físicamente y así mismo se vuelven obsoletos ya que no cuentan con equipo de reproducción. Existen variaciones de longevidad significativa entre diferentes fabricantes, y pueden existir lotes de producción con vida útil de 70 a 300 años; sin embargo, se pueden encontrar problemas de relectura en periodos más cortos.

Dentro de las fallas más comunes que se identifican para estos dispositivos se

encuentran: la humedad y la temperatura durante el almacenamiento a largo plazo, daños mecánicos o físicos, rayas o mugre en el disco.

Cómo recomendaciones para garantizar su longevidad se debe realizar el almacenamiento bajo condiciones de temperatura y humedad controladas, se deben hacer limpiezas, retirar la mugre y el polvo, se deben ensayar antes de utilizar estos dispositivos para garantizar su preservación a largo plazo y que sean compatibles con las normas ISO 10995 e ISO 16963 control de error en lo posible.

12.4 RESPONSABLES DEL PLAN DE PRESERVACIÓN DIGITAL

Rol	Responsabilidades
Responsable institucional: Deberá velar por el cumplimiento del plan de preservación digital.	Unidad de Atención al Ciudadano
	Encargado de publicar y presentar formalmente el plan y la política de Preservación Digital a Largo Plazo en la Alcaldía.
Responsable de preservación digital: Garantizará la implementación y puesta en marcha de las políticas y estándares mencionados en este documento.	Responsable tecnológico de las funcionalidades requeridas para garantizar el cumplimiento de las directrices informáticas del Plan de Preservación Digital a Largo Plazo.
Asesor de tecnología: Velará por orientar a los responsables y al comité interadministrativo de gestión y desempeño en las mejores prácticas y el cumplimiento normativo.	Director conceptual del Plan de Preservación Digital a Largo Plazo
Profesional ciencias de información y documentación: Garantizará la preservación digital a largo plazo de los documentos electrónicos**.**	Responsable operacional del Plan de Preservación Digital a Largo Plazo.
Profesional en infraestructura tecnológica: Garantizará la funcionalidad de los aplicativos y software de acuerdo a protocolos y estándares normativos.	Responsable del almacenamiento longevo de los materiales documentales y aplicación de las políticas de mantenimiento para el aseguramiento auténtico e íntegro de los documentos electrónicos de archivo
Asesor jurídico: Velará por la aplicación normativa y la garantía de soportes electrónicos a largo plazo	Acompañamiento especializado para la determinación del carácter probatorio y evidencia jurídica de los documentos electrónicos de archivo, objeto de Preservación Digital a Largo Plazo

Fuente: Ministerio de Educación

12.5 MAPA DE RUTA

Actividades	2021				2022				2023			
	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
Definir responsables de la preservación digital												
Ver cuadro de responsables												
Identificación y análisis de series documentales a preservar a largo plazo:												
Según TRD y Diagnostico de soportes electrónicos												
Normalización de los formatos												
Utilizar Formatos longevos												
Transferencias documentales electrónicas												
Utilizar metadatos de preservación												
Aplicar protocolos sugeridos												
Realizar los ajustes en los aplicativos para capturar o inferir metadatos												
Integrar documentos												
Implementar características de interoperabilidad en las aplicaciones para el envío de documentos al SGDEA												
Integrar los documentos en el SGDEA												
Descripción técnica de los medios electrónicos												
Aplicar protocolos sugeridos												
Implementar los procedimientos de preservación documental												
Procedimiento de identificación y análisis de grupos documentales a preservar												
Procedimiento de administración del sistema de preservación digital (identificación de diferentes aspectos ya mencionados)												

Procedimiento de selección de medios de almacenamiento												
Características técnicas de unidades de almacenamiento.												
Mejora continua												
Implementar la ejecución periódica del proceso de revisión de las estrategias y acciones de preservación												

12.6 ARTICULACIÓN CON LOS INSTRUMENTOS DE LA GESTIÓN DOCUMENTAL

Este plan de presentación digital a largo plazo se articula con el Modelo de Requisito para el documento electrónico de archivo (MR), con las tablas de retención documental de la alcaldía de Bello en el componente de documento electrónico, con el programa gestión documental, y con el sistema integral de conservación.

12.7 ARTICULACIÓN CON LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La alcaldía municipal de Bello deberá formular la política de seguridad de la información enmarcar en el Modelo de requisitos para documento electrónico de archivo. Dicha política contará con los siguientes principios:

Todo el personal será informado y será responsable de la seguridad de la información según su cargo.

Se dispondrá de presupuesto para los controles relacionados con la seguridad de la información y los procesos para su implementación y mantenimiento.

Se presentarán informes regulares del seguimiento a los riesgos de seguridad de la información

Se adoptaras las medidas relevantes cuándo estos riesgos no sean aceptables

No serán tolerables situaciones que expongan a la Alcaldía a la violación de leyes y normas legales

12.8 ARTICULACIÓN CON LA GESTIÓN DEL RIESGO DE LA ENTIDAD

El análisis del riesgo relacionado con los procesos y sistemas de gestión documental deberá seguir las directrices de la ISO 18128 del 2016 y la NTC 31000; qué contempla las siguientes fases:

- Identificación del riesgo

- Análisis del riesgo
- Evaluación del riesgo

Debe permitir la identificación de los aspectos críticos en materia de preservación y las amenazas concretas del archivo digital, junto con las medidas preventivas qué pueden adaptasen.

Principales amenazas

- Errores en medio de almacenamiento cómo hardware y software.
- Comunicaciones y operaciones deficientes.
- Caídas de los servicios de red
- Desastres naturales
- Ataques externos e internos
- Obsolescencia de hardware y software, formatos y medios.
- Quiebra económica
- Perdida del contexto de los documentos (metadatos)

Medidas preventivas

- Migración y/o renovación de medios
- Migración a nuevos formatos
- Uso de formatos abiertos
- Actualización de versiones de software
- Emulación del software
- Técnicas de back up
- Almacenamiento de soportes en cintas magnéticas
- Uso de metadatos de preservación para asegurar la contextualización de los documentos.

13. RECOMENDACIONES EN LA PRESERVACIÓN DIGITAL [8]

La Unesco a través de la carta para la preservación del patrimonio digital 2003, llama la atención a los estados miembros, entre ellos Colombia, a salvaguardar la memoria digital, y mitigar el peligro inminente de la desaparición de los soportes digitales; e invita a todos los pueblos a conservar y a difundir el saber, velando por la protección del patrimonio universal e histórico.

Nos recuerda que el patrimonio digital es un recurso único, qué es el fruto del saber y de la expresión de los seres humanos, recuerda que los objetos digitales pueden ser: Textos, bases de datos, imágenes fijas en movimiento, grabaciones sonoras,

[8] Carta de la Unesco noviembre de 2015. (Unesco, 2015)

materiales gráficos, programas informáticos, páginas web entre otros, a menudo son efímeros y su conservación requiere un trabajo específico para garantizar su reproducción, mantenimiento y gestión.

De cualquier forma, se debe garantizar el acceso al patrimonio digital y se debe velar por mitigar el peligro de perdida, de esta manera se deben establecer estrategias y políticas, seleccionar los elementos para garantizar su conservación, proteger el patrimonio digital, preservar el patrimonio cultural y establecer alianzas de cooperación para lograr todo esto.

14. MEJORA CONTINUA

La Alcaldía Municipal de Bello debe mejorar continuamente en los procesos, y herramientas necesarias para la preservación digital a largo plazo. La entidad debe considerar el resultado del análisis y la evaluación, así como las políticas propuestas en el presente documento

Debe determinar y seleccionar las oportunidades de mejora e implementar cualquier acción necesaria para cumplir con los requisitos técnicos de este plan de preservación digital a largo plazo, y debe incluir en sus procesos:

- Mejorar los softwares y aplicativos
- Corregir, prevenir o reducir los efectos no deseados
- Mejorar el desempeño y la eficacia del software de gestión documental
- Tomar acciones para controlar y corregir las no conformidades
- Evaluar las necesidades de acciones para eliminar las causas de los hallazgos
- Actualizar permanentemente los riesgos inherentes a la administración del documento electrónico
- Hacer los cambios necesarios a los sistemas de la gestión de calidad
- Conservar Todos los soportes y las evidencias de esta mejora continua

15. HERRAMIENTA DE SEGUIMIENTO Y CONTROL

PLAN	ACTIVIDADES	INDICADORES	META
IMPLEMENTACIÓN DEL PLAN DE PRESERVACIÓN DIGITAL A LARGO PLAZO	**Definición de responsables de la preservación digital**	Responsables definidos x 100 responsables a definir	100%
	Identificación y análisis de series documentales a preservar a largo plazo:	Series identificadas x 100 Series a identificar	100%
	Normalización de los formatos	Formatos normalizados x 100 Formatos a normalizar	100%
	Transferencias documentales electrónicas	Transferencias documentales realizadas x 100 Transferencias documentales programadas	100%
	Integración documentos	Integración de documentos realizadas x 100 Integración de documentos programadas	100%
	Descripción técnica de los medios electrónicos	Descripción técnica de medios realizadas x 100 Descripción técnica de medios programadas	100%
	Implementación de los procedimientos de preservación documental	Implementación de procedimientos realizadas x 100 Implementación de procedimientos programadas	100%
	Selección de medios de almacenamiento	Selección de medios de almacenamiento realizadas x 100 Selección de medios de almacenamiento programadas	100%
	Mejora continua	Auditorías realizadas x 100 m Auditorias programadas	100%

16. CONTROL DE CAMBIOS

BREVE DESCRIPCIÓN DEL CAMBIO	VERSIÓN	FECHA aaaa-mm-dd
No aplica para la primera versión.	01	2020-08-100
Se reviso el "PLAN DE PRESERVACIÓN DIGITAL A LARGO PLAZO - SIC", se verifico que estuviera acorde con la normatividad vigente. se actualizo en el formato F- 53 Plantilla para elaboración de documentos, se realizaron algunas correcciones gramaticales, se actualizo la tabla de contenido. Se elimino el cuadro introductorio ya que la información de dicho cuadro esta contenida en el presente control de cambio	02	2022-09-22

Elaboró:	Viviana Andrea Arias Muñoz, Contratista Dirección de Gestión Documental y Atención al Ciudadano. Erasmo Arturo Herrera Lopera, Contratista Dirección de Gestión Documental y Atención al Ciudadano.	Fecha:	2022-09-15
Revisó:	Néstor Alberto García Sánchez Profesional Universitario Dirección de Gestión Documental y Atención al Ciudadano.	Fecha:	2022-09-20
Aprobó:	Juan David Naranjo Director de Gestión Documental y Atención al Ciudadano.	Fecha:	2022-09-22

17. ANEXOS

ANEXO 1: 3. Control de Mando del Sistema Integrado de conservación

ANEXO 2: 4. Informe de Seguimiento del Plan de Conservación Documental

ANEXO 3: 5. Mapa de riesgos Alcaldía de Bello

ANEXO 4: 6. Diagnóstico de depósitos de archivos

ANEXO 5: 8. Herramienta de estructura SIC

18. BIBLIOGRAFÍA

Archivo General de la Nación. (2018). *Fundamentos de preservación digital a largo plazo*. Obtenido de Agn: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/FundamentosPreservacionLargoPlazo.pdf

Icontec. (18 de Mayo de 2016). NTC-ISO-TR 17797:2016. Obtenido de https://tienda.icontec.org/gp-archivo-electronico-seleccion-de-medios-de-almacenamiento-digital-para-preservacion-a-largo-plazo-ntc-iso-tr17797-2016.html

La biblioteca británica. (2017). Construcción de una politica de preservación de documentos. Obtenido de https://www.bl.uk/conservation

Ministerio de Cultura. (14 de Enero de 2015). Decreto 29 de 2015. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60465

Ministerio de Educación Nacional. (2020). Plan de preservación digital. Obtenido de https://www.mineducacion.gov.co/1759/articles-362792_recurso_89.pdf

Presidencia de la republica. (2018). Manual de politica de seguridad de la Información . Obtenido de http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf

Scielo.org. (6 de Abril de 2010). Investigación bibliotecologica. Obtenido de Preservación documental digital y seguridad informática: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

Unesco. (15 de Noviembre de 2015). Carta de preservación digital . Obtenido de http://portal.unesco.org/es/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html

ALCALDIA MUNICIPAL DE BELLO

PROCESO DE GESTIÓN DOCUMENTAL

CONTROL DE MANDO DEL SISTEMA INTEGRADO DE CONSERVACIÓN

Nº	Instrumento archivístico	Actividad		Producto Entregable	Presupuesto	Ejecución/tiempo			Roles - Responsabilidadades											
		Titulo	Descripción Actividad			2020	2021	2022	Despacho del Alcalde	Secretaría General	Oficina Asesora Jurídica	Dirección Técnica de Formulación de Proyectos	Secretaría de Hacienda	Secretaría de Planeación	Dirección Técnica de TIC y Soporte Tecnológico	Dirección Administrativa de Gestión Documental y Atención al Ciudadano	Secretaría de Control Interno	Dirección Administrativa de Talento Humano	Oficina Asesora de Gestión del Riesgo
1	Programa de gestión documental	2.2.1 Planeación estratégica de la gestión documental	Elaborar, revisar, publicar implementar, controlar y actualizar el Programa de Gestión Documental	Programa de gestión documental publicado, implementado, controlado y actualizado	$ -	X	X	X	X	X					X	X	X		X
2			Elaborar, revisar, publicar implementar, controlar y actualizar el Plan Institucional de Archivos - PINAR	Plan de institucional de archivos publicado, implementado, controlado y actualizado	$ -	X	X	X	X	X					X	X	X		X
3			Elaborar, revisar, publicar implementar, controlar y actualizar el Sistema integrado de conservación - SIC	Sistema integrado de conservación publicado, implementado, controlado y actualizado	$ -	X	X	X		X					X	X	X		X
4			Elaborar, revisar, publicar implementar, la Política de Gestión Documental de la Entidad.	Política de Gestión Documental publicado, implementado, controlado y actualizado	$ -	X	X	X	X	X					X	X	X		X
5			Crear, revisar, implementar, controlar y actualizar los procedimientos del proceso de gestión documental.	Procedimientos de gestión documental documentados	$ -	X	X			X						X			
6			Desarrollar los programas específicos establecidos en el Programa de Gestión Documental	Programas específicos implementados	$ -	X	X	X		X					X	X	X		X
7			Establecer indicadores los indicadores de eficacia, eficiencia y efectividad de los procesos de gestión documental.	Indicadores de gestión procesos de gestión documental	$ -	X	X	X		X						X			
8		2.2.2 Planeación documental	Identificar y elaborar los registros de Activos de Información, así como elaborar el índice de Información clasificada y reservada, y diseñar y adoptar el esquema de publicación, acorde a la Ley 1712 de 2014.	Registros de activos de información	$ -	X	X			X					X	X			
9			Elaborar, diseñar, implementar y actualizar las formas, formatos y formularios para los documentos internos de la entidad.	Actualización de formas, formatos y formularios	$ -	X	X			X					X	X			
10			Automatizar las formas, formatos y formularios en un sistema de gestión de documentos electrónicos, acorde a la normatividad archivística vigente y las necesidades institucionales.	Automatización de formas, formatos y formularios	$ -	X	X			X					X	X			
11			Elaborar políticas, directrices y criterios claros para el diseño, la producción e ingreso de los documentos, a través de metadatos, mecanismos de autenticación y control de acceso	Políticas para la producción e ingreso de documentos	$ -	X	X			X					X	X			
12		2.2.3 Producción Documental	Actualizar las políticas de producción documental, que incluya las actividades relacionadas con preservación a largo plazo, documentos en soporte análogo, digital y electrónico, digitales y generación de copias idénticas	Actualización de políticas de producción documental	$ -	X	X			X					X	X			
13			Actualizar el procedimiento para la administración de los documentos, en relación con la responsabilidad compartida que tiene el área de gestión documental	Actualización de procedimientos en realación al sistema de gestión documental	$ -	X	X			X						X			X
14			Actualizar el manual de correspondencia en relación con determinar las áreas competentes de los trámites	Actualización de manual de correspondencia	$ -	X	X			X						X			
15		2.2.4 Gestión y trámite	Actualizar los procedimientos para atender, direccionar y hacer seguimiento a las PQRS de los ciudadanos; en cumplimiento con la normatividad vigente en términos de respuesta a las peticiones que reciben en la Entidad	Actualización de procedimientos PQRS	$ -	X	X			X						X			
16			Realizar Seguimiento, control y ampliación de canales de atención, difusión, acceso e información para facilitar la consulta de los documentos de archivos de los diferentes usuarios de la Entidad.	Seguimiento y control a los canales de atención, difusión y acceso	$ -	X	X	X		X					X	X	X		
17		2.2.5 Organización documental	Elaborar un procedimiento claro y preciso que permita la aplicación de las actividades relacionadas con la organización de los documentos (clasificación, ordenación y descripción),	Procedimiento organización documental	$ -	X	X			X						X			

Nº	Instrumento archivístico	Actividad		Producto Entregable	Presupuesto	Ejecución/tiempo			Roles - Resposabilidadades											
		Titulo	Descripción Actividad			2020	2021	2022	Despacho del Alcalde	Secretaría General	Oficina Asesora Jurídica	Dirección Técnica de Formulación de Proyectos	Secretaría de Hacienda	Secretaría de Planeación	Dirección Técnica de TIc y Soporte Tecnológico	Dirección Administrativa de Gestión Documental y Atención al Ciudadano	Secretaría de Control Interno	Dirección Administrativa de Talento Humano	Oficina Asesora de Gestión del Riesgo
18			Aplicar las tablas de retención documental de la Entidad y los cuadros de clasificación documental, permitiendo el vinculo archivístico	Tablas de retención aplicadas	$ -	X	X	X		X					X	X			
19			Publicar de los instrumentos archivísticos del Cuadro de Clasificación Documental - CCD y Tablas de Retención Documental -TRD en la respectiva pagina web de la Entidad.	Instrumentos archvísticos publicados	$ -	X				X					X	X			
20			Realizar seguimientos a los diferentes archivos de gestión de la entidad en relación con la correcta organización de los expedientes y unidades documentales simples	Seguimiento a los procesos de organización de la entidad	$ -	X	X	X		X						X	X		
21			Aplicar las tablas de valoración para la organización de los documentos resultantes de los fondos documentales acumulados de la Entidad.	Aplicación tablas de valoración documental	$ -	X	X			X						X			
22			Implementar procedimientos y actividades claras en relación con la descripción documental de la Entidad	Procedimientos descripción documental	$ -	X	X	X		X						X			
23		2.2.6.Transferencias	Elaborar el plan de transferencias documental institucional	Plan de transferencias	$ -	X				X						X			
24			Elaborar el procedimiento de transferencias documentales	Procedimientos transferencias documentales	$ -	X				X						X			
25			Establecer controles que permitan la verificación técnica de la aplicación de los procedimientos de organización documental	Controles transferencias documentales	$ -	X				X						X			
26			Diseñar políticas claras para la aplicación de migración, refreshing, emulación, conversación de los documentos en soportes distintos al papel	Políticas migración, efreshing, emulación, conversación de documentos	$ -	X				X					X	X			
27			Elaborar e implementar el procedimiento para la aplicación de la disposición final	Procedimiento disposición final	$ -	X	X			X						X			
28			Elaborar e implementar el instructivo de digitalización de documentos	Instructivo digitalización de documentos	$ -	X	X			X						X			
29			Aplicar las actvidades relacionadas con la eliminación de documentos	Eliminación de documentos	$ -	X	X	X		X						X			
30		2.2.8.Preservación a largo plazo.	Elaborar e Implementar el plan de conservación de documentos (documentos análogos) y el plan de preservación digital a largo plazo (documentos electrónicos)	Implementación documentos análogos y digitales	$ -	X	X	X		X					X	X			
31			Estandarizar los criterios para garantizar la preservación de la información electrónica	Estandarez preservación electrónica	$ -	X	X			X					X	X			
32		2.2.9.Valoración	Implementar políticas y procedimientos que permitan determinar criterios claros de valoración documental	Políticas y procedimientos criterios de valoración	$ -	X	X	X		X						X			
33			Actualización de las tablas de retención de la Entidad	Actualización tablas de retención documental	$ -	X	X	X		X						X			
34			Crear y actualizar actos administrativos necesarios desde la politica archivistica y detallados en el PINAR	Actualizar actos administrativos relacionados con la función archivistica	$ -	X			X	X	X					X	X		X
35			Aprobar e implementar el PGD ; garantizando así el cumplimiento en la política archivística del país y mitigando el riesgo de la perdida de la información en los tramites ciudadanos	Implementar Programa de Gestión Documental (PGD) Fase 1 Plan de capacitación para inducción y reinducción en gestión documental	$ 77,423,062.00	X	X			X		X	X	X	X	X	X	X	
36			Asignar presupuesto para el 2020-2023 de acuerdo a la formulación del PINAR, mitigando utilización de recursos sin tener en cuenta prioridades y aspectos críticos de la gestión documental.	Implementar el Plan Institucional de archivos (PINAR)	**$ 89,430,829,492.20**	X	X	X		X		X	X	X	X	X	X	X	
37			Poner en funcionamiento la política nacional el archivo histórico, para salvaguardar el patrimonio histórico del Municipio y de la Nación y prestar los servicios culturales, científicos e históricos a la comunidad.	Implementar el Archivo Histórico Municipal			X			X		X	X	X	X	X	X	X	
38	de archivos (PINAR)	2.6. Formulación De Planes Y Proyectos	Aplicar las TRD y TVD despues de convalidadas, para garantizar la conservación de documentos históricos, y liberación de depositos de archivo que se encuentran con altos niveles de acumulación, dificultando así la consulta, ubicación y recuperación de la información. Tambien unos tramites ordenados y seguros.	Implementar las Tablas de Retención Documental (TRD) y Tablas de Valoración documental (TVD) y Fase 2 PGD	$ 85,272,262,230.20		X	X		X		X	X	X	X	X	X	X	

Nº	Instrumento archivístico	Actividad		Producto Entregable	Presupuesto	Ejecución/tiempo			Roles - Resposabilidadades											
		Titulo	Descripción Actividad			2020	2021	2022	Despacho del Alcalde	Secretaría General	Oficina Asesora Jurídica	Dirección Técnica de Formulación de Proyectos	Secretaría de Hacienda	Secretaría de Planeación	Dirección Técnica de TIC y Soporte Tecnológico	Dirección Administrativa de Gestión Documental y Atención al Ciudadano	Secretaría de Control Interno	Dirección Administrativa de Talento Humano	Oficina Asesora de Gestión del Riesgo
39	Plan Institucional	Planes Y Proyectos	Elaborar, aprobar e implementar el programa de descripción documental, para evitar perdida de información, registros y datos por registros que no cumplen con los estándares establecidos en la descripción de documentos y cumplimiendo con la interoperabilidad exigida para las entidades públicas	Elaborar e Implementar el Programa de descripción documental para el Archivo Total	$ 50,000,000.00		X	X		X		X	X	X	X	X	X	X	
40			Elaborar, aprobar e implementar el MR (Modelo de requisitos para la gestión de documentos electrónicos), para mitigar el riesgo de perdida de la documentción en formato electrónico en servidores y estaciones de trabajo; y darle cumplimiento así al proceso de preservación a largo plazo exigido por el AGN.	Elaborar e implementar el Modelo de Requisitos para la gestión de documento electrónico (MR)	$ 100,000,000.00		X	X		X		X	X	X	X	X	X	X	
41			Elaborar, aprobar e implementar los mapas de procesos y flujos documentales que se requieren para estructurar correctamente los aplicativos y otras herramientas electrónicas, como también garantizar los tramites a los ciudadanos.	Elaborar e Implementar Mapas de procesos y flujos documentales para los tramites externos e internos.	$ 40,000,000.00		X	X		X		X	X	X	X	X	X	X	
42			Elaborar, aprobar e implementar las TCA (Tablas de Control de accesos) para el restablecimiento de categorías adecuadas de derechos y restricciones de acceso y seguridad de los documentos análogos (físicos como electrónicos).	Elaborar Tablas de Control de acceso TCA	$ 50,000,000.00		X	X		X		X	X	X	X	X	X	X	
43			Aprobar e implementar el SIC (Sistema Integrado de conservación), para garantizar la durabilidad e integridad de la información, y mitigar el riesgo de vulnerar los derechos de los ciudadanos en sus trámites.	Implementar Sistema Integrado de Conservación (SIC)		X	X	X	X	X		X	X	X	X	X	X	X	X
44	Sistema Integrado de Conservación (SIC)	8. Componentes - SIC.	como fin implementar los programas, procesos y procedimientos, tendientes a mantener las características físicas y funcionales de los	PLAN DE CONSERVACION DOCUMENTAL.		X	X	X	X	X		X	X	X	X	X	X	X	X
45			prácticas para la conservación de los documentos y el manejo de la información. Así mismo, se pueden utilizar plegables publicitarios,	Programa de Capacitación y sensibilización	$ 77,423,062.00	X	X	X	X	X		X	X	X	X	X	X	X	X
46			sistemas de almacenamiento (presencia de humedad, hongos, grietas, fisuras e inclinaciones en	Programa de Inspección y mantenimiento de sistemas de	$ 3,841,144,200.00	X	X	X	X	X		X	X	X	X	X	X	X	X
47			almacenamiento. 2. Jornadas de fumigación de áreas de archivo.	Programa de Saneamiento ambiental desinfección,		X	X	X	X	X		X	X	X	X	X	X	X	X
48			1. Medición y registro permanente de humedad y temperatura. 2. Medición de iluminancia (Infraroja, ultravioleta).	Programa de Monitoreo y control de condiciones		X	X	X	X	X		X	X	X	X	X	X	X	X
49			documentos de archivo de la entidad. 2. Establecer parámetros para la compra de unidades de	Programa de Almacenamiento y re-almacenamiento.		X	X	X	X	X		X	X	X	X	X	X	X	X
50			identificación de las acciones encaminadas a prevenir emergencias y mitigar daños enmarcadas en el Acuerdo	Plan de Prevención y atención de desastres para material		X	X	X	X	X		X	X	X	X	X	X	X	X
51			entidad. Articulación de la preservación digital con la política de seguridad de	PLAN DE PRESERVACIÓN DIGITAL A LARGO PLAZO	$ 57,983,062.00	X	X	X	X	X		X	X	X	X	X	X	X	X

NOTA: Estos valores no incluyen Adecuaciones en piso, muros, ni techos; tampoco equipos de seguridad, ni de monitoreo ambiental; tampoco infraestru

REFERENCIA	VALOR
Total en metros lineales	14,853.0
Total de folios presentes en la volumetría referenciada (Valor Aproximado).	140,360,850.0
Total de unidades presentes en la volumetría referenciada (Valor Aproximado).	2,005,155.0
Peso Estimado en toneladas (Valor Aproximado).	499.1
Espacio en metros cuadrados que ocupa la volumetría referenciada apilada, sin contar espacios de mobiliario ó área. (Valor Aproximado).	2,560.9

2475.5 estanterias

401031 cajas

Proyeccion de costos teniendo como base la Resolución 088 de 19 de febrero del 2020 Por medio de la cual se establecen tarifas del AGN por venta de bienes y servicios.

SERVICIO	TARIFAS IVA INCLUIDO	PROYECTADO PARA VOLUMENES Y VIGENCIA 1 AÑO
Imagen digitalizada tamaño inferior A3	250.0	35,090,212,500.0
Servicios de Custodia medios magneticos u opticos en boveda de seguridad minimo 10 unidadea anuales	8,400.0	842,165,100.0
Monitoreo ambiental, condiciones ambientales de los depositos de archivo (medicion puntual, temperatura, HR, luminosidad y radiación ultravioleta) por medicion.	212,300.0	11,464,200.0
Monitoreo ambiental condiciones ambientales (medición curva 24 horas temperatura y HR)	197,000.0	3,829,680,000.0
Asistencia Tecnica archivistica presencial minimo (3 horas) virtual gratuita hasta 8	160,000.0	24,160,000.0
Capacitaciones archivisticas (estos valores mas viaticos y gastos de desplazamiento) se dicta a través de cursos, talleres o seminarios, 32 horas por persona	626,353.0	33,823,062.0
Cursos del agn 40 horas por participante	360,000.0	19,440,000.0
Organización documental valor por metro lineal incluye clasificación, ordenación y descripción, aplicación de trd y tvd, foliación, FUID y 4 cajas x200 por metro lineal. No incluye hoja de control y otras actividades tales como atención de consultas, primeros auxilios a los documentos, desinfecciones de documentos, reprografia, entre otros.	2,375,000.0	35,275,875,000.0
Servicio de deposito según la sede, no incluye gastos de transporte, valor por metro lineal	5,200.0	77,235,600.0
Estanteria rodante mecanica, espacio por 1.000.000	1,000,000.0	2,475,500,000.0
Valor metro cuadrado en Bello Compra - Venta	1,800,000.0	4,609,530,520.20
caja x200	2,540.0	1,018,618,740.00
https://ecore cartulina legajadora desacificada de carton con revestimiento	2,934.0	5,883,124,770.0
Elaborar e Implementar el Programa de descripción documental para el Archivo Total	50,000,000.0	50,000,000.0
Elaborar e implementar el Modelo de Requisitos para la gestión de documento electrónico (MR)	100,000,000.0	100,000,000.0
Elaborar e Implementar Mapas de procesos y flujos documentales para los tramites externos e internos.	40,000,000.0	40,000,000.0
Elaborar Tablas de Control de acceso TCA	50,000,000.0	50,000,000.0

89,430,829,492.2

NOTA: Estos valores no incluyen Adecuaciones en piso, muros, ni techos; tampoco equipos de seguridad, ni de monitoreo ambiental; tampoco infraestructura tecnologica necesaria para el SGDEA ni softwre con los requerimientos tecnicos para soportar los documentos electronicos de archivo.

ANEXO 2

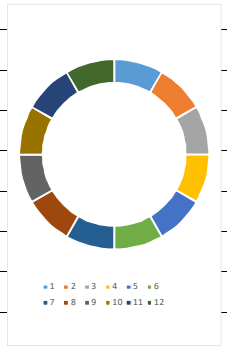
4 Informe de Seguimiento del Plan de Conservación Documental

	OBJETIVOS	

Una vez se han cumplido las fases de diseño e implementación del Plan de Conservación Documental, se debe proceder a su
actualización, la cual debe darse como mínimo finalizada una vigencia.
En esta fase, se debe verificar que los programas y las condiciones establecidas, se hayan cumplido de acuerdo a lo planeado y en concordancia con el Plan Estrategico Institucional, Plan de Acción, Plan Anual de Compras y en especial el Programa de Gestión Documental, de lo contrario, se debe actualizar de acuerdo a las necesidades detectadas.
Se sugiere, para la actualización y seguimiento del Plan de Conservación, desarrollar conjuntamente con el cuadro de mando establecido en la fase de implementación, un formato de informe que resuma las actividades, objetivos logrados
y resultados a nivel cualitativo y cuantitativo frente a la
programación planteada.

REPORTE DEL SEGUIMIENTO DEL SISTEMA INTEGRADO DE CONSERVACION Y PLAN DE PRESERVACIÓN DIGITAL A LARGO PLAZO

OBJETIVO	Garantizar la conservacion y presevacion de cualquier tipo de infromacion, independientemente del medio o tecologia con la cual se haya elaborado
RESUMEN	Consolidado de avance de la implementación del Sistema y sus planes
FECHA	

PROGRAMA	**MEDICION TRIMESTRAL**												**GRAFICO (Comportamiento ideal)**	**DEFICIENTE**	**SATISFACTORIO**	**SOBRESALIENTE**
	2021				**2022**				**2023**							
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**				
1. Plan De Conservación Documental.	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**				X
1.1. Programa de Capacitación y sensibilización	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**				X
1.2. Programa de Inspección y mantenimiento de sistemas de almacenamiento e instalaciones físicas	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**				X
1.3. Programa de Saneamiento ambiental: desinfección, desratización y desinsectación	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**				X
1.4. Programa de Monitoreo y control de condiciones ambientales.	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**				X
1.5. Programa de Almacenamiento y re-almacenamiento	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**				X
1.6. Plan de Prevención y atención de desastres para material documental	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**				X
1.7. Instructivo De Limpieza Y Desinfección De Áreas Y De Documentos De Archivo	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**				X
2. Plan De Preservación Digital A Largo Plazo	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**	**8.33**				X

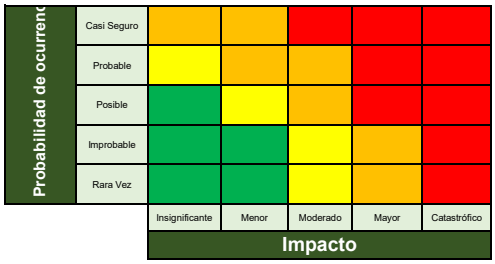
INTERPETACION Y ANALISIS

RESPONSABLE DE LA INTERPRESTACION
RESPONSABLE DE LA MEDICION
APROBADO

	FORMA	MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	
	ACTIVIDAD	SISTEMA INTEGRADO DE CONSERVACIÓN	VERSIÓN	
	PROCESO	Plan de Prevención y atención de desastres para material documental		

MAPA DE CALOR Y RIESGO INHERENTE

"Para los riesgos de Seguridd de la Información, el análisis de impacto se realizará teniendo en cuenta los niveles "Insignificante, Menor, moderado, mayor y catastrófico", dado que estos riesgos siempre serán significativos.



IMPACTO	PROBABILIDAD	NIVEL
Catastrófico	Casi seguro	EXTREMO
Catastrófico	Probable	EXTREMO
Catastrófico	Posible	EXTREMO
Catastrófico	Improbable	EXTREMO
Catastrófico	Rara Vez	EXTREMO
Mayor	Casi seguro	EXTREMO
Mayor	Probable	EXTREMO
Mayor	Posible	EXTREMO
Mayor	Improbable	ALTO
Mayor	Rara Vez	ALTO
Moderado	Casi seguro	EXTREMO
Moderado	Probable	ALTO
Moderado	Posible	ALTO
Moderado	Improbable	MODERADO
Moderado	Rara Vez	MODERADO
Menor	Casi seguro	ALTO
Menor	Probable	ALTO
Menor	Posible	MODERADO
Menor	Improbable	BAJO
Menor	Rara Vez	BAJO
Insignificante	Casi seguro	ALTO
Insignificante	Probable	MODERADO
Insignificante	Posible	BAJO
Insignificante	Improbable	BAJO
Insignificante	Rara Vez	BAJO

MATRICES PARA VALORACIÓN DEL IMPACTO Y PROBABILIDAD DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Valoración de probabilidad de ocurrencia del riesgo

Nivel	Descriptor	Descripción	Frecuencia
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara Vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Valoración del impacto del riesgo

Nivel	Descriptor	(CONSECUENCIAS) CUANTITATIVO	(CONSECUENCIAS) CUALITATIVO
5	**Catastrófico**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
4	**Mayor**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
3	**Moderado**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
2	**Menor**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
1	**Insignificante**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.

MATRICES PARA VALORACIÓN DEL DISEÑO Y EJECUCIÓN DE LOS CONTROLES

Valoración de la EJECUCION del control

Rango de calificación de la ejecución	Peso de la ejecución del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Valoración del DISEÑO del control

Criterio de evaluación	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
1.1 Asignación del responsable	Asignado	15
	No Asignado	0
1.2 Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5.Qué pasa con las observaciones o desviaciones	Se investigan oportunamente	15
	No se investigan oportunamente	0
Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0
Fuerte	Si su calificación es entre 96 y 100	
Moderado	Si su calificación es entre 86 y 95	
Débil	si su calificación es entre 0 y 85	

MATRICES PARA VALORACIÓN DE SOLIDEZ INDIVIDUAL Y DEL CONJUNTO DE LOS CONTROLES

VALORACIÓN SOLIDEZ INDIVIDUAL DEL CONTROL		
DISEÑO	EJECUCIÓN	SOLIDEZ INDIVIDUAL
Fuerte	Fuerte	**Fuerte**
Fuerte	Moderado	**Moderado**
Fuerte	Débil	**Débil**
Moderado	Fuerte	**Moderado**
Moderado	Moderado	**Moderado**
Moderado	Débil	**Débil**
Débil	Fuerte	**Débil**
Débil	Moderado	**Débil**
Débil	Débil	**Débil**

VALORACIÓN SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50

MATRIZ PARA CALCULO DE RIESGO RESIDUAL

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR EL IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No disminuye	1	0
Moderado	No disminuye	Directamente	0	1
Débil	Directamente	Directamente	0	0
Débil	Directamente	Indirectamente	0	0
Débil	Directamente	No disminuye	0	0
Débil	No disminuye	Directamente	0	

Directamente
No disminuye

Directamente
Indirectamente
No disminuye

ANEXO 3
5. Mapa de riesgos Alcaldia de Bello

	FORMA	MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
	ACTIVIDAD	SISTEMA INTEGRADO DE CONSERVACIÓN	SISTEMA INTEGRADO DE CONSERVACIÓN
	PROCESO	Plan de Prevención y atención de desastres para material documental	Plan de Prevención y atención de desastres para material documental

MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

IDENTIFICACION DEL RIESGO							Valoración del Riesgo				Diseño de controles C: Corrective					Valoración del Control				Valoración del Riesgo Residual				Plan de contingencia		Acciones Preventivas P: Preventivo					Cuadro de mando (Ver instrucciones)			
Proceso	No.	Riesgo	Clasificación		Causas	Consecuencias	Probabilidad	Impacto	Riesgo Inherente	Opción de manejo	N°	Actividad de Control	Soporte	Responsable	Tiempo	Indicador del control	Diseño del control	Ejecución del Control	Solidez del control	Solidez del conjunto	Probabilidad	Impacto	Riesgo Residual	Opción de manejo	Acciones de contingencia ante posible materialización	Evidencia-Registro de implementación de contingencia ante posible materialización	N°	Acción Preventiva	Responsable de la acción preventiva	Indicador de Acción Preventiva	Cantidad	COSTO	MEDIANO	LARGO
Gestión de la información	1	Poca formación y capacitación en temas archivísticos al personal encagado de los archivos de gestión, centrales e historicos; en ciclos de induccion y reinducción.	Aspectos Administrativos	De Formación Y Capacitación	Aun no se implementa el PGD (Programa de Gestión Documental)	Dificultad y resistencia al cambio por parte de los empleados Desconocimiento de la Normatividad Aplicación de procedimientos equivocados y errados Poco reconocimiento a la Gestión Documental Desconocimiento en la Organización de archivos. Desconocimiento para la reacción frente a una emergencia. Incumplimiento en la normatividad nacional. Fallas en los tramites de los ciudadanos. Fallas en el nivel de responsabilidad y dirección estratégica de dichos asuntos.	POSIBLE	Mayor	Extremo	Reducir	C-1	Implementar el PGD	De Integral de archivos	Secretario General	1 vez al año	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Fuerte	Moderado	IMPROBABLE	Menor	Moderado	Prevenir	Incluir plan de capacitación archivos en el plan institucional	Informe de hallazgo con plan de mejora	P.1	Aplicar los planes y programas de capacitación vinculados a los instrumentos archivísticos y cumplir con la ley 1409 de 2010.	Secretario General	Planes y programas de capacitación - PGD y SIC	2			
Gestión de la información	2	Falta definir funciones en asuntos de gestión documental en la mesa técnica de información y comunicaciones, ocasionando fallas en el nivel de responsabilidad y dirección estratégica de dichos asuntos.	Aspectos Administrativos	Instancias Asesoras	Falta de asesoramiento por parte del SNA	Fallas en el nivel de responsabilidad y dirección estratégica de dichos asuntos.	IMPROBABLE	Mayor	Alto	Reducir	C-1	Actualizar actos administrativos	De Integral de archivos	Secretario General	1 vez al año	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Fuerte	Fuerte	Fuerte	CASI SEGURO	Mayor	Alto	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	3	No se ha coordinado la gestion documental con el Consejo Departamental de archivo, y los instrumentos no han sido convalidados por esta instancia.	Aspectos Administrativos	Instancias Asesoras	Falta de asesoramiento por parte del SNA	No han sido convalidados los instrumentos archivísticos por esta instancia. Aun no se pueden implementar	PROBABLE	Mayor	Extremo	Reducir	C-1	Establecer contacto permanente con el SNA y convalidar los instrumentos archivísticos	De Integral de archivos	Secretario General	Cada que se requiera	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	POSIBLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	4	No se encuentra operando con política nacional el archivo histórico, ocasionando perdida del patrimonio historico del Municipio y de la Nación.	Aspectos Administrativos	Organizacionales	Falta de asesoramiento por parte del SNA	Perdida del patrimonio histórico del Municipio y de la Nación.	POSIBLE	Catastrófico	Extremo	Reducir	C-1	Ejecutar proyecto de mejorar el archivo historico	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	PROBABLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	5	No se cuenta con detalle de funciones archivísticas en el manual de funciones, ocasionando la posibilidad de eludir las responsabilidades archivísticas establecidas por el AGN en su normatividad.	Aspectos Administrativos	Organizacionales	Falta de asesoramiento por parte del SNA	Eludir las responsabilidades archivísticas establecidas por el AGN en su normatividad.	PROBABLE	Mayor	Extremo	Reducir	C-1	Actualizar actos administrativos	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Fuerte	Fuerte	Fuerte	IMPROBABLE	Mayor	Alto	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	6	Se evidencia falta de claridad en las funciones del área encargada de la gestión documental, ocasionando la posibilidad de eludir legalmente las responsabilidades asignadas a estas áreas por el AGN en su normativa.	Aspectos Administrativos	Organizacionales	Falta de asesoramiento por parte del SNA	Eludir legalmente las responsabilidades asignadas a estas áreas por el AGN en su normativa.	PROBABLE	Mayor	Extremo	Reducir	C-1	Actualizar actos administrativos	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Fuerte	Fuerte	Fuerte	IMPROBABLE	Mayor	Alto	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	7	Se evidencia que se derogó el acto administrativo de creacion del Archivo Central, ocasionando posicionamiento del archivo y violentando el principio de independencia y dignidad para quienes trabajan allí, poniendo en riesgo la conservacion de la información	Aspectos Administrativos	Organizacionales	Desconocimiento normativo	Ocasionando posicionamiento del archivo y violentando el principio de independencia y dignidad para quienes trabajan allí, poniendo en riesgo la administración de la información	PROBABLE	Catastrófico	Extremo	Reducir	C-1	Actualizar actos administrativos	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	PROBABLE	Catastrófico	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	8	Se evidencia asignación de presupuesto para el 2019 sin previa formulación del PINAR y no se soporto asignacion presupuestal del 2020, ocasionando utilizacion de recursos sin tener en cuenta prioridades y aspectos criticos de la gestion documental.	Aspectos Administrativos	Aspectos De Financiación	Falta de asesoramiento por parte del SNA	Ocasionando utilización de recursos sin tener en cuenta prioridades y aspectos críticos de la gestión documental.	PROBABLE	Catastrófico	Extremo	Reducir	C-1	Proyección presupuestal alineado con PINAR	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	POSIBLE	Catastrófico	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	9	Se identifica que no se ha aplicado la TVD por no encontrarse aun convalidada, esto ocasiona riesgo en la conservación de documentos históricos, y acumulación de otros que dificultan la consulta, ubicación y recuperación de la información.	Instrumentos Archivísticos	Instrumentos Archivísticos	Aun no se convalida	Ocasiona riesgo en la conservación de documentos históricos, y acumulación de otros que dificultan la consulta, ubicación y recuperación de la información.	PROBABLE	Mayor	Extremo	Reducir	C-1	Gestionar la convalidación para implementar de manera inmediata	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	PROBABLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	10	Se identifica que no se ha aplicado la TRD por no encontrarse aun convalidada, esto ocasiona riesgo en la conservación de documentos históricos, y acumulación de otros que dificultan la consulta, ubicación y recuperación de la información.	Aspectos De La Función Archivística	Instrumentos Archivísticos	Aun no se ha convalidado	Ocasiona riesgo en la conservación de documentos históricos, y acumulación de otros que dificultan la consulta, ubicación y recuperación de la información.	PROBABLE	Mayor	Extremo	Reducir	C-1	Gestionar la convalidación para implementar de manera inmediata	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	PROBABLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	11	Se identifica que los instrumentos archivísticos no se encuentran publicados en la página web, ocasionando incumplimiento en la ley de transparencia y acceso a la información, y alto riesgo de corrupción.	Aspectos De La Función Archivística	Instrumentos Archivísticos	Desconocimiento normativo	Ocasionando incumplimiento en la ley de transparencia y acceso a la información, y alto riesgo de corrupción.	PROBABLE	Mayor	Extremo	Reducir	C-1	Publicar los instrumentos en pagina web.	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Fuerte	Fuerte	Fuerte	IMPROBABLE	Mayor	Alto	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	12	El PGD no se aplica en la entidad, esto porque aun no se elabora y aplica; ocasionando incumplimiento en la política archivística del país y poniendo en riesgo la información de los tramites ciudadanos.	Aspectos De La Función Archivística	Instrumentos Archivísticos	Aun no se ha aprobado	Ocasionando incumplimiento en la política archivística del país y poniendo en riesgo la información de los tramites ciudadanos.	PROBABLE	Mayor	Extremo	Reducir	C-1	Implementar el PGD	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	POSIBLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	13	El PINAR no se utiliza en la entidad, esto porque aún no se elabora y aplica; ocasionando falta de planeación archivística y avances en el cumplimiento de la política archivística y marco normativo impuesto por el AGN.	Aspectos De La Función Archivística	Instrumentos Archivísticos	Aun no se aprueba	Ocasionando falta de planeación archivística y avances en el cumplimiento de la política archivística y marco normativo impuesto por el AGN.	PROBABLE	Mayor	Extremo	Reducir	C-1	Implementar el PINAR	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	PROBABLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	14	Los archivos de gestión, no cuentan con FUID al día, ocasionando falta de control de creación de expedientes, ubicación de la información, y perdida de la misma en los archivos de gestión, riesgo importante para la transparencia y acceso a la información.	Aspectos De La Función Archivística	Instrumentos Archivísticos	Falta de capacitación y actualizacion internas, control de transferencias primarias	Ocasionando falta de control de creación de expedientes, ubicación de la información, y perdida de la misma en los archivos de gestión, riesgo importante para la transparencia y acceso a la información.	PROBABLE	Mayor	Extremo	Reducir	C-1	Implementar instrumentos archivísticos	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	POSIBLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	15	No se ha elaborado ni implementado el MR (Modelo de requisitos para la gestión de documentos electrónicos), esto pone en riesgo la administración de los documentos en formato electrónico en servidores y estaciones de trabajo; incumpliendo así con el proceso de preservación a largo plazo exigido por el AGN.	Aspectos De La Función Archivística	Instrumentos Archivísticos	Desconocimiento normativo	Esto pone en riesgo la administración de los documentos en formato electrónico en servidores y estaciones de trabajo; incumpliendo así con el proceso de preservación a largo plazo exigido por el AGN.	CASI SEGURO	Catastrófico	Extremo	Reducir	C-1	Elaborar, aprobar e implementar MRDIEA	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Catastrófico	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	16	Los mapas de procesos y flujos documentales no se evidencian en el SGI, y se requieren para estructurar correctamente los aplicativos y otras herramientas electrónicas, como también garantizar los tramites a los ciudadanos.	Aspectos De La Función Archivística	Instrumentos Archivísticos	Desconocimiento normativo	Fallas en estructurar correctamente los aplicativos y otras herramientas electrónicas, como también garantizar los tramites a los ciudadanos.	CASI SEGURO	Catastrófico	Extremo	Reducir	C-1	Elaborar, aprobar e implementar Flujos documentales	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Catastrófico	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	17	Se evidencia que no se han elaborado, ni implementado las TCA (Tablas de control de acceso) para el restablecimiento de categorías adecuadas de derechos y restricciones de acceso y seguridad de los documentos análogos (físicos como electrónicos).	Aspectos De La Función Archivística	Instrumentos Archivísticos	Desconocimiento normativo	Fallas en las categorías adecuadas de derechos y restricciones de acceso y seguridad de los documentos análogos (físicos como electrónicos).	CASI SEGURO	Catastrófico	Extremo	Reducir	C-1	Elaborar, aprobar e implementar TCA	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Catastrófico	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	18	No se ha implementado el SIC (Sistema Integral de Archivos, esto porque apenas se encuentra en construcción, la no implementación de este pone en riesgo la integridad de la información y vulnera los derechos de los ciudadanos en sus trámites.	Aspectos De La Función Archivística	Instrumentos Archivísticos	Desconocimiento normativo	Pone en riesgo la integridad de la información y vulnera los derechos de los ciudadanos en sus trámites.	CASI SEGURO	Catastrófico	Extremo	Reducir	C-1	Aprobar e implementar SIC	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Catastrófico	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	19	Se evidencia que los expedientes y las unidades simples no están rotuladas con los datos del CCD (Cuadro de Clasificación documental); esto porque la TRD aún se encuentra en proceso de convalidación; ocasionando así perdida de información y duplicidad de la misma.	Aspectos De La Función Archivística	Organización Y Descripción	Falta de instrumentos archivísticos convalidados, capacitacion y auditorias internas de archivo.	Ocasionando así perdida de información y duplicidad de la misma.	CASI SEGURO	Catastrófico	Extremo	Reducir	C-1	Rotular unidades de conservación con CCD	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	PROBABLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	20	Los expedientes no cuentan con hoja de control requisito por transparencia y acceso a la información publica; tampoco las unidades simples tienen indices para acceder y evitar la manipulación de las piezas documentales en su interior.	Aspectos De La Función Archivística	Organización Y Descripción	Desconocimiento normativo	Perdida de información, dificultades para acceder a la misma, riesgo de corrupción.	IMPROBABLE	Mayor	Extremo	Reducir	C-1	Elaborar hoja de control para todas las unidades complejas e indices para las simples.	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	IMPROBABLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	21	No se evidencia el programa de descripción documental, ocasionando perdida de información, registros y datos por registros que no cumplen con los estándares establecidos en la descripción de documentos y evitando la interoperabilidad exigida para las entidades públicas.	Aspectos De La Función Archivística	Organización Y Descripción	Desconocimiento normativo	Ocasionando perdida de información, registros y datos por registros que no cumplen con los estándares establecidos en la descripción de documentos y evitando la interoperabilidad exigida para las entidades públicas.	CASI SEGURO	Mayor	Extremo	Reducir	C-1	Elaborar, aprobar e implementar el programa de descripción documental	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	22	No se han elaborado Instrumentos de descripción documentales tales como guías, catálogos, índices y censos documentales; ocasionando riesgos para el acceso a la información e interoperabilidad tecnológica.	Aspectos De La Función Archivística	Organización Y Descripción	Desconocimiento normativo	Ocasionando riesgos para el acceso a la información e interoperabilidad tecnológica.	PROBABLE	Mayor	Extremo	Reducir	C-1	Elaborar todos los instrumentos de descripción para el archivo de gestion, central e historico	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	23	No se realiza foliación a expedientes y unidades simples en los archivos de gestion durante el trámite de documentos; esta riesgo ocasiona vulneración a la transparencia y acceso a la información de trámites y falta de control sobre los volúmenes documentales.	Aspectos De La Función Archivística	Organización Y Descripción	Desconocimiento normativo	Ocasiona vulneración a la transparencia y acceso a la información de trámites y falta de control sobre los volúmenes documentales.	CASI SEGURO	Mayor	Extremo	Reducir	C-1	Foliar todas las unidades simples y complejas desde el archivo de gestión y todos los tramites abiertos	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	POSIBLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	24	Los inventarios FUID no se mantienen actualizados en el archivo de gestión, ocasionando falta de control en el archivo y riesgo de pérdida de la información.	Aspectos De La Función Archivística	Organización Y Descripción	Falta de auditorias internas en temas de archivo	Ocasionando falta de control en el archivo y riesgo de pérdida de la información.	CASI SEGURO	Mayor	Extremo	Reducir	C-1	Mantener actualizados los inventarios FUID en el archivo total y controlar por medio de auditorias internas	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	POSIBLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	25	El material gráfico (dibujos, croquis, mapas, planos, fotografías, ilustraciones, prensa, entre otros) no se extrae, ni se deja en su lugar un testigo; ocasionando riesgo de deterioro y perdida de información e incumplimiento en el proceso de preservación a largo plazo establecido por el AGN.	Aspectos De La Función Archivística	Organización Y Descripción	Desconocimiento normativo	Ocasionando riesgo de deterioro y perdida de información e incumplimiento en el proceso de preservación a largo plazo establecido por el AGN.	CASI SEGURO	Mayor	Extremo	Reducir	C-1	Implementar de forma correcta el programa de almacenamiento y reinmacenamiento del SIC	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	26	Se evidencia que las dependencias (AG) no realizan registro de los préstamos y menos solicitan su devolución; ocasionando riesgo en la perdida de información.	Aspectos De La Función Archivística	Organización Y Descripción	Falta de auditorias internas en temas de archivo	Ocasionando riesgo en la perdida de información.	CASI SEGURO	Mayor	Extremo	Reducir	C-1	Validar en las auditorias el diligenciamiento de la planilla de control de consultas y prestamos, hacer seguimientos a los inventarios.	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	POSIBLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	27	Se identifican procesos de digitalización de expedientes sin cumplir los protocolos del AGN y la recomendación de las TRD, esto ocasiona mal uso de recursos físicos y pone en riesgo la integridad de los expedientes.	Aspectos De La Función Archivística	Organización Y Descripción	Desconocimiento normativo	Ocasiona mal uso de recursos físicos y pone en riesgo la integridad de los expedientes.	CASI SEGURO	Mayor	Extremo	Reducir	C-1	Utilizar para la digitalización los protocolos del AGN, validar en auditorias internas, hacer muestreos para garantizar la calidad.	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	POSIBLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	28	No se cuentan con plan de transferencias primarias y seguimiento al mismo; ocasionando acumulación de documentos en los archivos de gestión, riesgo de pérdida y deterioro de los mismos.	Aspectos De La Función Archivística	Organización Y Descripción	Falta de auditorias internas en temas de archivo	Ocasionando acumulación de documentos en los archivos de gestión, riesgo de pérdida y deterioro de los mismos.	CASI SEGURO	Mayor	Extremo	Reducir	C-1	Elaborar, aprobar e implementar plan de transferencias, primarias y secundarias y realizarle auditoria.	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	PROBABLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	29	Se identifican las cajas para la transferencia primaria, cuando se realiza; pero estás no corresponden a las especificaciones técnicas necesarias y la rotulación utilizada para las mismas no contempla datos de TRD, ni de TVD; ocasionando duplicidad de información, dificultad para su recuperación y consulta y riesgo de pérdida.	Aspectos De La Función Archivística	Organización Y Descripción	No se aplica programa de almacenamiento y realmacenamiento	Ocasionando duplicidad de información, dificultad para su recuperación y consulta y riesgo de pérdida.	CASI SEGURO	Mayor	Extremo	Reducir	C-1	Rotular unidades de conservación con CCD, y hacer auditorias	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	PROBABLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			

ANEXO 3
5. Mapa de riesgos Alcaldia de Bello

Proceso	No.	Riesgo	Clasificación		Causas	Consecuencias	Probabilidad	Impacto	Riesgo Inherente	Opción de manejo	Nº	Actividad de Control	Soporte	Responsable	Tiempo	Indicador del control	Diseño del control	Ejecución del Control	Solidez del control	Solidez del conjunto	Probabilidad	Impacto	Riesgo Residual	Opción de manejo	Acciones de contingencia ante posible materialización	Evidencia-Registro de implementación de contingencia ante posible materialización	Nº	Acción Preventiva	Responsable de la acción preventiva	Indicador de Acción Preventiva	Cantidad	COSTO	MEDIANO	LARGO
Gestión de la información	35	Se identifican que muchas áreas utilizan AZ o fólderes de argollas incumpliendo así con la política archivística a nivel nacional; ocasionando riesgos de seguridad y conservación a la información.	Aspectos De La Función Archivística	Organización Y Descripción	Desconocimiento normativo	Ocasionando riesgos de seguridad y conservación a la información; como tambien incumplimiento normativo	CASI SEGURO	Mayor	Extremo	Reducir	C.1	No comprar AZ ni folders, reemplazar todos los documentos archivados en esta unidad por carpetas según programa de almacenamiento y realmacenamiento. Hacer auditorias internas	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	PROBABLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	37	No se ha creado con acto administrativo la unidad de correspondencia, incumpliendo así en la política archivística y poniendo en riesgo tramites y	Aspectos De La Función Archivística	Comunicaciones Oficiales	Desconocimiento normativo	Incumpliendo así en la política archivística y poniendo en riesgo tramites y derechos de los ciudadanos.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Elaborar, aprobar e implementar acto administrativo de creación ventanilla unica y aplicación proceso de gestión y tramite. Hacer auditorias internas	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	32	No se evidencia política de firmas responsables; esto ocasiona evasión de responsabilidad y seriedad frente a los tramites de los ciudadanos, también es un riesgo de corrupción.	Aspectos De La Función Archivística	Comunicaciones Oficiales	Desconocimiento normativo	Ocasiona evasión de responsabilidad y seriedad frente a los tramites de los ciudadanos, también es un riesgo de corrupción.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Elaborar, aprobar e implementar acto administrativo de creación ventanilla unica y aplicación proceso de gestión y tramite. Hacer auditorias internas	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	33	No se evidencia manual para la administracion de comunicaciones oficiales en cuanto a: procedimiento de radicación de documentos, numeración de actos administrativos, certificado de paz y salvo para la entrega de documentos a nivel interno, alertar de seguimiento a tiempos de respuestas; todo esto ocasiona riegos en atención de trámites y puede ocasionar vulneración a los derechos de los ciudadanos, así como genera riesgos de transparencia y corrupción	Aspectos De La Función Archivística	Comunicaciones Oficiales	Desconocimiento normativo	Ocasiona riegos en atención de trámites y puede ocasionar vulneración a los derechos de los ciudadanos, así como genera riesgos de transparencia y corrupción	PROBABLE	Mayor	Extremo	Reducir	C.1	Elaborar, aprobar e implementar acto administrativo de creación ventanilla unica y aplicación proceso de gestión y tramite. Hacer auditorias internas	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	PROBABLE	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	34	Se evidencia poco espacio para almacenar la documentación existente, posible causa que no se ha implementado TRD y TVD, tampoco se han hecho las proyecciones necesarias, para determinar el espacio en metros cuadrados necesario según el volumen documental generado anualmente; esto ocasiona deterioro de la documentación y perdida de la información.	Aspectos De Preservación	Condiciones De Edificios Y Locales Destinados A Archivos	No se ha implementado TRD y TVD, tampoco se han hecho las proyecciones necesarias, para determinar el espacio en metros cuadrados necesario según el volumen documental generado anualmente	Ocasiona deterioro de la documentación y perdida de la información, como tambien riesgo para la salud.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Implementar instrumentos archivisticos y realizar auditorias internas	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Moderado	Moderado	Moderado	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	35	Los depósitos no están adecuados climáticamente; ocasionando deterioro de los documentos análogos y perdida de información.	Aspectos De Preservación	Condiciones De Edificios Y Locales Destinados A Archivos	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro de los documentos análogos y perdida de información.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	36	Los depósitos no se han diseñado teniendo en cuenta sus diferentes zonas de distribución (custodia, trabajo archivístico, consulta, limpieza, reprografía entre otras); ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	Aspectos De Preservación	Condiciones De Edificios Y Locales Destinados A Archivos	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	37	Las estanterías que se utilizan no están diseñadas para los documentos dependiendo de sus formatos, tamaños y soportes; ocasionando deterioro de los mismos y perdida de información.	Aspectos De Preservación	Condiciones De Edificios Y Locales Destinados A Archivos	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	38	Muchas estanterías metálicas identificadas no cuentan con requisitos técnicos de resistencia, ensamble y anclaje; así como de distribución y distancias mínimas entre ellas, pisos y paredes; ocasionando deterioro de los documentos y riesgos ocupacionales para los funcionarios.	Aspectos De Preservación	Condiciones De Edificios Y Locales Destinados A Archivos	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	39	Se evidencia que no se tienen planes de mantenimiento para unidades de instalación como archivadores de gavetas, rodantes, fijos, plano tecas entre otros; ocasionando un riesgo para la conservación de los documentos y para la salud de los funcionarios.	Aspectos De Preservación	Condiciones De Edificios Y Locales Destinados A Archivos	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	40	Se evidencia riesgo de humedad en los depósitos de archivo, provocado por baños y cocinetas en algunos de ellos; ocasionando riesgo para la documentación y la información.	Aspectos De Preservación	Condiciones De Edificios Y Locales Destinados A Archivos	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	41	Los muros, techos y puertas de los depósitos de archivo no fueron construidos teniendo en cuenta los aspectos técnicos mínimos para ellos, es posible que sea a causa de que muchos de esos depósitos no fueron destinados a esta función originalmente; esto ocasiona deterioro de los documentos y riesgo de pérdida de la información, así como riesgo de desplome en algunos casos particulares.	Aspectos De Preservación	Condiciones De Edificios Y Locales Destinados A Archivos	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	42	Las unidades de conservacion como carpetas y cajas, no cuentan con las especificaciones técnicas requeridas, ocasionando deterioro para la documentación y por ende perdida de información.	Aspectos De Preservación	Unidades De Conservación	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	43	No se utilizan las referencias de las cajas según el fpo de archivo, esto hace que sean incontrolables los volumen identificados.	Aspectos De Preservación	Unidades De Conservación	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	44	Se evidencia que en varios depósitos las ventanas, puertas o celosías permiten el intercambio de aire, ocasionando deterioro en los soportes documentales.	Aspectos De Preservación	Condiciones Ambientales	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	45	Las claraboyas o rejillas que están en los depósitos de archivo no se encuentran acondicionadas con filtros que impidan la entrada de partículas o contaminantes a los depósitos, esto ocasiona altos niveles de polución que contaminan los documentos.	Aspectos De Preservación	Condiciones Ambientales	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	46	Los depósitos no cuentan con equipos de mediciones de condiciones ambientales que permitan establecer la fluctuación en temperatura, HR y polución a la que están expuestos los soportes documentales.	Aspectos De Preservación	Condiciones Ambientales	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	47	No se han instalado materiales o equipos de modificacion de condiciones ambientales en los depósitos de archivo	Aspectos De Preservación	Condiciones Ambientales	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	48	Las luminarias no son fluorescentes de baja intensidad, necesarias para disminuir la pigmentación de los soportes documentales. Tampoco se han instalado de forma correcta (archivo central)	Aspectos De Preservación	Condiciones Ambientales	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	49	En algunos depositо sobre todo los archivos de gestion se tienen ventanas que permiten la entrada de luz solar al depósito de archivo, esto deterioro en todo los aspectos los soportes documentales.	Aspectos De Preservación	Condiciones Ambientales	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	50	Se identifica que en algunas areas AG y archivo central se realiza la limpieza de las instalaciones, como pisos y estanterías, esto es favorable para la documentación. Pero se identifican tambien muchos fondos acumulados sin ningun tipo de limpieza y en ciertos puntos la documentación se encuentra pegada con baygon	Aspectos De Preservación	Mantenimiento	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	51	No se realiza la limpieza de las unidades de conservacion como carpetas, ni tampoco de las piezas documentales; esto pone en riesgo la perdurabilidad de soportes e información , así como la salud de los funcionarios.	Aspectos De Preservación	Mantenimiento	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	52	Los exdntores identificados no son de agentes limpios, ocasionando daño a los soportes documentales en caso de utilización.	Aspectos De Preservación	Seguridad Y Emergencias	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	53	Se identifica que los extintores son recargados anualmente, siendo esto favorable a la seguridad de la documentación, pero no se ha dado las capacitaciones necesarias para su uso a el personal encargado.	Aspectos De Preservación	Seguridad Y Emergencias	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	54	No se han instalado sistemas de alarma contra intrusiones, en los diferentes deposito, esto pone en riesgo la información y los derechos de los ciudadanos.	Aspectos De Preservación	Seguridad Y Emergencias	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	55	Se identifican algunos sistemas de alarma para la deteccion de incendios, los cuales no son convenientes para el material papel, ya que el activarse pueden deteriorar el soporte.	Aspectos De Preservación	Seguridad Y Emergencias	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	56	No se evidencian sistemas de alarma para la detección de inundaciones en los depósitos de archivo, aunque en algunos se encuentran cocinetas y baños.	Aspectos De Preservación	Seguridad Y Emergencias	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	57	Se identifica que se ha provisto la señalización para la identificacion de los equipos de atención de desastres y rutas de evacuación, establecidas dentro de los planes de contingencia de la entidad sobre todo para los archivos de gestión, mas ninguna señalización para los depositos de archivos.	Aspectos De Preservación	Seguridad Y Emergencias	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	58	Se identifica que se ha elaborado un Plan de prevención de desastres y situaciones de riesgo, sin el componente archivístico.	Aspectos De Preservación	Seguridad Y Emergencias	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			
Gestión de la información	59	En algunos depósitos se ha dispuesto de extintores en el área de archivo, aunque no cumplen con las condiciones técnicas necesarias para los soportes archivísticos.	Aspectos De Preservación	Seguridad Y Emergencias	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	De Integral de archivos	Secretario General	otro de mano	Reducir la cantidad de incidentes en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PGD y SIC y sus proyectos	3			

ANEXO 3
5. Mapa de riesgos Alcaldia de Bello

Proceso	No.	Riesgo	Clasificación		Causas	Consecuencias	Probabilidad	Impacto	Riesgo Inherente	Opción de manejo	N°	Actividad de Control	Soporte	Responsable	Tiempo	Indicador del control	Diseño del control	Ejecución del Control	Solidez del control	Solidez del conjunto	Probabilidad	Impacto	Riesgo Residual	Opción de manejo	Acciones de contingencia ante posible materialización	Evidencia-Registro de implementación de contingencia ante posible materialización	N°	Acción Preventiva	Responsable de la acción preventiva	Indicador de Acción Preventiva	Cantidad	COSTO	RECURSO HUMANO	TIEMPO
Gestión de la información	60	Se ha realizado el levantamiento y valoración del panorama de riesgo en la Entidad, sin el componente archivístico, esto ocasiona un riesgo en la seguridad de la información.	Aspectos De Preservación	Seguridad Y Emergencias	Desconocimiento normativo y aprobación e implementación del SIC	Ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.	CASI SEGURO	Mayor	Extremo	Reducir	C.1	Aprobar e implementar SIC y realizar auditorias internas a este sistema	Os Integral de archivos	Secretario General	dro de mand	Reducir la cantidad de incidentias en los aspectos de Gestión de la Información	Fuerte	Débil	Débil	Débil	CASI SEGURO	Mayor	Extremo	Prevenir	Auditorias internas, plan de mejoras; reportes SNA	Informe de hallazgo con plan de mejora	P.1	Implementar PINAR y todos sus proyectos	Secretario General	Indicadores formulados en el PINAR, PCD y SIC y sus proyectos	3			

ANEXO 4
6 Diagnóstico de depósitos de archivos

PROTOTIPO DE DIAGNÓSTICO INTEGRAL DE ARCHIVOS

El presente Modelo de Diagnóstico Integral de Archivos ha sido diseñado para recopilar información veraz frente a los asp
directamente en la implementación de la Función Archivística en los sujetos obligados de la Ley General de Archivos.

La relación de las preguntas con la normatividad vigente, permite a las personas que lo apliquen profundizar en los temas cuestionad
convierte también en una herramienta de sensibilización. Su alcance está definido en la identificación de situaciones problemáticas
de una matriz visual [1] , lo que evita el uso de herramientas complejas usadas en otros tipos de diagnósticos empresariales,
información y no son del resorte de este tipo de estudio.

No se incluye la evaluación de las necesidades y normatividad respecto los Sistemas de Gestión de Documentos Electrónicos de Arch
pretende afianzar los conceptos de la organización de los documentos en soportes físicos lo que a futuro facilitará la compresión de
de los SGDEA.

Como resultado de la aplicación de este modelo se espera que quienes lo apliquen redacten un informe acompañando de materia
indiquen las causas que impiden la implementación de la Función Archivística y se listen las necesidades que permitan a la Alta Dire
desarrollar o actualizar instrumentos Archivísticos como el Plan Institucional de Archivos y el Programa de Gestión Documental.

1. La metodología propuesta ha sido desarrollada en base al Modelo de Conservación Preventiva Para Museos, elaborado por la Facultad de Estudios del Patrimonio C
Externado de Colombia, como resultado del Convenio 1871 de 2005 con el Ministerio de Cultura.

NOTA: El presente es SÓLO un modelo de Diagnóstico Integral de Archivos y la entidad es autónoma de elegir la
considere pertinente, de acuerdo con sus necesidades actuales en materia de Gestión Documental.

Este documento es sólo un prototipo y no es de obligatorio cumplimiento ni es obligatorio elegir este modelo.

CHIVO
NERAL
A NACIÓN
OMBIA

)ectos que inciden

dos y por lo tanto se
ɔ de riesgos a través
ɥue abarcan mayor

ivo, debido a que se
ɛ la implementación

al gráfico, donde se
ɛcción de la Entidad

:ultural de la Universidad

herramienta que

PROTOTIPO DE DIAGNÓSTICO INTEGRAL DE ARCHIVOS

GLOSARIO

CONCEPTO	DEFINICIÓN
Archivo Central	Unidad administrativa que coordina y controla el funcionamiento de los archivos de gestión y reúne los documentos transferidos por los mismos una vez finalizado su trámite y cuando su consulta es constante.
Archivo de gestión	Archivo de la oficina productora que reúne su documentación en trámite, sometida a continua utilización y consulta administrativa.
Archivo histórico	Archivo al cual se transfiere del archivo central o del archivo de gestión, la documentación que por decisión del correspondiente Comité de Archivo, debe conservarse permanentemente, dado el valor que adquiere para la investigación, la ciencia y la cultura. Este tipo de archivo también puede conservar documentos históricos recibidos por donación, depósito voluntario, adquisición o expropiación.
Archivo total	Concepto que hace referencia al proceso integral de los documentos en su ciclo vital
Ciclo vital del documento	Etapas sucesivas por las que atraviesan los documentos desde su producción o recepción, hasta su disposición final.
Conservación de documentos	Conjunto de medidas preventivas o correctivas adoptadas para asegurar la integridad física y funcional de los documentos de archivo.
Conservación preventiva de documentos	Conjunto de estrategias y medidas de orden técnico, político y administrativo orientadas a evitar o reducir el riesgo de deterioro de los documentos de archivo, preservando su integridad y estabilidad
Depósito de archivo	Local especialmente equipado y adecuado para el almacenamiento y la conservación de los documentos de archivo.
Deterioro	Alteración o degradación de las propiedades físicas, químicas y/o mecánicas de un material, causada por envejecimiento natural u otros factores.
Diagnóstico de Archivos	Procedimiento de observación, levantamiento de información y análisis, mediante el cual se establece el estado de los archivos y se determina la aplicación de los procesos archivísticos necesarios
Función archivística	Actividades relacionadas con la totalidad del quehacer archivístico que comprenden desde la elaboración del documento hasta su eliminación o conservación permanente
Gestión Documental	Conjunto de actividades administrativas y técnicas, tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final con el objeto de facilitar su utilización y conservación.
Medición lineal	Estimación comparativa de la longitud ocupada por la documentación ubicada de canto o filo
Muestreo	Técnica estadística aplicada en la selección documental, con criterios cuantitativos y cualitativos.
Sistema Integrado de Conservación	Conjunto de estrategias y procesos de conservación que aseguran el mantenimiento adecuado de los documentos, garantizando su integridad física y funcional en cualquier etapa del ciclo vital.

Referencias	
Banco Terminológico AGN	http://banter.archivogeneral.gov.co/vocab/index.php

NOTA: El presente es **SÓLO** un modelo de Diagnóstico Integral de Archivos y la entidad es autónoma de elegir la herramienta que considere pertinente, de acuerdo con sus necesidades actuales en materia de Gestión Documental.

Este documento es solo un prototipo y no es de obligatorio cumplimiento ni es obligatorio elegir este modelo.

ANEXO 4

6 Diagnóstico de depósitos de archivos

DIAGNÓSTICO INTEGRAL DE ARCHIVOS IDENTIFICACIÓN DE LA ENTIDAD						
NOMBRE DE LA ENTIDAD	ALCALDIA MUNICIPAL DE BELLO					
NIT						
CIUDAD / MUNICIPIO	BELLO (ANTIOQUIA)					
CATEGORÍA DEL MUNICIPIO						
CARÁCTER DE LA ENTIDAD	PUBLICA	X	PRIVADA		PRIVADA CON FUNCIONES PÚBLICAS	
SECTOR - ORDEN	GUBERNAMENTAL					
DIRECCIÓN	Edificio Gaspar de Rodas - Cra 50 No. 51 00 Bello - Antioquia					
TELÉFONO	Conmutador - 6047944 - Fax(57-4)2750845 - Línea Gratuita 01 8000528228					
PAGINA WEB	https://bello.gov.co/					
CORREO ELECTRÓNICO INSTITUCIONAL	E-mail: contactenos@bello.gov.co - notificaciones@bello.gov.co					

ANEXO 4
6 Diagnóstico de depósitos de archivos

FORMATO DE DIAGNOSTICO

FECHA DE ELABORACIÓN DEL DIAGNOSTICO	Día 12 Mes 3 Año 2020

NOMBRE: MARIA EUGENIA BETANCURT PEREZ
CARGO: Directora administración gestión documental y atención al ciudadano

A. IDENTIFICACIÓN

AI. DATOS DEL ARCHIVO

DENOMINACIÓN O NOMBRE DEL ARCHIVO:			ARCHIVO CENTRAL		
FECHA DE CREACIÓN:	1959	ACTO LEGAL:	Acuerdo 46 de 13 de diciembre de 1959		
DIRECCIÓN:		TEL:		FAX:	
CORREO ELECTRÓNICO:		PÁG.. WEB:	https://bello.gov.co/		
MUNICIPIO:	Bello	CATEGORÍA:	1	DEPARTAMENTO:	Antioquia

NIVEL Y TIPO DE ARCHIVO

ENTIDAD U OFICINA	NIVEL				TIPO				
PRODUCTORA	NACIONAL	DEPTAL.	MUNICIPAL	DISTRITAL	GESTIÓN	CENTRAL	HISTÓRICO	GENERAL	OTRO
Alcaldia Municipal de Bello Archivo Central			X			X			

SISTEMA DE ARCHIVO DE LA ENTIDAD:

CENTRALIZADO:	X	CENTRAL:	X	GENERAL:	X	SATÉLITES:	X
ESPECIALIZADOS:							

		N° DE DEPÓSITOS:	
OTROS:			

OBSERVACIONES: Supresión del Archivo Municipal Acuerdo 64 de 06 de agosto de 1971

ANEXO 4
6 Diagnóstico de depósitos de archivos

A.2 IDENTIFICACIÓN DE LA ENTIDAD A LA QUE PERTENECE EL ARCHIVO

1.	NOMBRE	**Alcaldia Municipal de Bello**									
2.	NIVEL: NACIONAL		DEPTAL:		MUNICIPAL:	**X**	DISTRITAL:		EXTRANJERO:		
3.	SECTOR:	**Gubernamental**									
4.	ORGANISMO A QUE PERTENECE:	**Gobernación de Antioquia**									
5.	CARÁCTER DE LA ENTIDAD:										
	PUBLICA:	**X**	PRIVADA:		MIXTA:						
	PRIVADA/FUNCIONES PUBLICAS:			PRIVADA/INTERES CULTURAL:							
	FAMILIAR:		PERSONAL:		OTRA:						
6.	UBICACIÓN EN LA ESTRUCTURA DEL ESTADO (RAMA):		**Administrativa**								
7.	FECHA DE CREACIÓN DE LA ENTIDAD:	**1913**		ACTO LEGAL:	**Ordenanza 48 del 29 de abril de 1913.**						
8.	DIRECCIÓN:	**Edificio Gaspar de Rodas - Cra 50 No. 51 00 Bello - Antioquia**				TEL:	**Conmutador - 6047944 - Línea Gratuita 01 8000528228**				
9.	FAX:	**Fax(57-4)2750845**	E-MAIL:		**E-mail: contactenos@bello.gov.co - notificaciones@**	PAG.WEB:	https://bello.gov.co/				
10.	MUNICIPIO:	**Bello**		CATEGORÍA:	**1**		DPTO:	**Antioquia**			
11.	TIENE REGIONALES Y SUCURSALES:	SI:		NO:	**x**	ESPECIFIQUE:					
12.	N° DE DEPENDENCIAS:	**72**									
13.	**MISIÓN DE ENTIDAD: Fomentamos el desarrollo sostenible, con talento humano competente, administrando con eficiencia los recursos y prestando eficazmente los servicios para mejorar la calidad de vida de su población.**										
14.	REPRESENTANTE LEGAL:										
	NOMBRE:	**Oscar Andres Perez Muñoz**									
	PROFESIÓN:	**Administrador de empresas**									
	CARGO:	**Alcalde Municipal**									
	TIEMPO EN EL CARGO:	**Cuatro meses**									
	OBSERVACIONES:										

ANEXO 4

6 Diagnóstico de depósitos de archivos

A.3. ADMINISTRACIÓN DEL ARCHIVO

1. JEFE DEL ARCHIVO:

NOMBRE: **Maria Eugenia Betancurt Perez**

PROFESIÓN U OFICIO: **Psicologa**

CURSOS DE CAPACITACIÓN: **Curso en la Universidad de Antioquia**

2. EXISTE EN EL ORGANIGRAMA DE LA ENTIDAD LA SECCIÓN O DIVISIÓN DEL ARCHIVO: SI: **X** NO: — **Dirección administrativa de gestión documental y atención al ciudadano**

3. EXISTE EN EL ORGANIGRAMA DE LA ENTIDAD EL CARGO DE JEFE SI: — NO: **X**

4. EL RESPONSABLE ¿ESTA DEDICADO DE TIEMPO COMPLETO AL ARCHIVO? SI: — NO: **X**

FUNCIONES QUE DESEMPEÑA: **No se identifican en el manual de funciones; estan a cargo de la Secretaria General la gestión documental, sin detalle.**

5. CARGO QUE OCUPA EL RESPONSABLE DEL ARCHIVO: **Director**

TIEMPO EN EL CARGO: **1 año y medio** TIEMPO EN LA ENTIDAI **1 año y medio**

6. A QUE DEPENDENCIA PERTENECE EL ARCHIVO DENTRO DE **Secretaria General**

7. JEFE INMEDIATO DEL RESPONSABLE DE ARC **Secretaria General**

NOMBRE: **Lus Giovany Arias Tobón** CARGC **Secretario General**

8. PRESUPUESTO ANUAL DEL ARCHIVO:

PROPIO: ASIGNADO POR LA DEPENDENCIA: **807,916,669** SEGÚN NECESIDADES: OTRO:

- APROXIME LA CANTIDAD DEL PRESUPUESTO ANUAL: **807916669**

9. A QUE NECESIDADES SE DESIGNA LOS RUBROS DEL ARCHIVO:

Material de Consumo: Tipo: **X** MANTENIMIENTO: TIPO

PERSONAL: TIF CAPACITACIÓN: TIPO:

REPROGRAFÍA: TIPO EQUIPOS: TIPO

PRESERVACIÓN: TIPO: ORGANIZACIÓN: TIPO:

OTROS **Consultoria**

10. EL ARCHIVO INCIDE EN LA COMPRA DE MATERIALES Y EQUIPOS PARA PRODUCCIÓN, TRAMITE Y DISPOSICIÓN FINAL DE LA DOCUMENTACIÓN:

SI: — NO: **X** ESPECIFIQUE: **El archivo suministra cajas y carpetas, en lo demás las areas son autonomas**

11. EXISTE MANUAL DE FUNCIONE

ENTIDAD: SI: **X** NO: — ARCHIVO: SI: **X** NO: — **M-GI-02 / Decreto 11 de 2008**

12. LAS FUNCIONES DEL RESPONSABLE DEL ARCHIVO ¿ESTÁN DETERMINADAS POR EL MANUAL? SI: — NO: **X**

EN CASO CONTRARIO ESPECIFIQUE QUIEN ASIGNA SUS FUNCIONES: El Director del area y el Secretario General

13. EXISTE UN MANUAL DE GESTIÓN DOCUMENTAL: SI: — NO: **X**

14. EL ARCHIVO ¿ESTA ORGANIZADO SEGÚN EL MANUAL?: SI: — NO: **X**

¿DESDE CUANDO SE APLICA EL MANUAL?

¿COMPLETA ASPECTOS DE PRESERVACIÓN?

15. ¿EXISTEN TABLAS DE RETENCIÓN DOCUMENTAL? SI: **X** NO: —

16. ¿EXISTE TABLA DE VALORACIÓN DOCUMENTAL? SI: — NO: **X**

17. ¿EXISTE UN REGLAMENTO DE ARCHIVO? SI: NO: **X** DESDE CUANDO SE APLICA:

18. ¿EXISTE "COMITÉ DE ARCHIVO"? **SI** ACTO ADMINISTRATIVO Y FECHA **Resolución 2655 de 2018 y 1196 de 2019**

FUNCIONAMIENTO: Actas

19. NUMERO DE PERSONAS QUE TRABAJAN EN EL ARCHIVO:

PROFESIONAL (P): TÉCNICO (T): ASISTENCIAL (A):

P	T	A	CAPACITACIÓN				NOMBRADO		ASIGNADO		TIEMPO		VINCULACIÓN		DEDICACIÓN (TIEMPO)		
													CONTRATO	PLANTA	COMPLETO	MEDIO	PARCIAL
	1	**3**					**x**				**48**	**h**		**x**	**x**		

OBSERVACIONES:

ANEXO 4

6 Diagnóstico de depósitos de archivos

B.1 EL EDIFICIO

1.	ÉPOCA DE CONSTRUCCIÓN:		1576					
2.	FUNCIÓN ORIGINAL:	Casa						
3.	CONTEXTO CLIMÁTICO:	H.R.	64	(PROMEDIO)	TEMP:	25	(PROMEDIO)	
4.	CONTEXTO URBANO: Forma p	NORTE:	Limita por el norte con el municipio de San Pedro de los Milagros,		SUR:	por el sur con el municipio de Medellín		
	ORIENTE:	por el oriente con el municipio de Copacabana,			OCCIDENTE:	por el occidente con los municipios de Medellín y de San Jerónimo		
5.	NIVELES DEL EDIFICIO:	4			ÁREA CONSTRUIDA:			
6.	TIPO DE CONSTRUCCIÓN (ESTRUCTURA, CERRAMIENTO, ACABADOS):							
7.	ESTADO DEL INMUEBLE:	En buen estado						
8.	ESPACION QUE CONFORMAN LA ENTIDAD/CANTIDAD:							
9.	EXISTEN PLANOS ARQUITECTÓNICOS:				PLANOS TÉCNICOS:			
10.	OBSERVACIONES:							

ANEXO 4

6 Diagnóstico de depósitos de archivos

B.4 CONDICIONES DE PREVENCION DE DESASTRES Y MANTENIMIENTO

1. EXISTE UN PLAN DE PREVENCION DE DESASTRES PARA LA ENTIDAD: SI: X NO: ESCRITO X

PARA EL ARCHIVO: SI: NO: X ESCRITO:

EL EDIFICIO POSEE DETECTOR DE INCENDIOS: SI: X NO:

TIPO:

No. DE DETECTORES EN EL AREA DEL ARCHIVO: 0

FUNCIONAN: SI: X NO: LABOR DE MANTENIMIENTO: SI: X NO:

CUALES: barrer, aspirar

EL EDIFICIO POSEE EXTINTORES: SI: X NO: TIPO:

No. DE EXTINTORES EN EL AREA DEL ARCHIVO: 0

FUNCIONAN: SI: NO: LABOR DE MANTENIMIENTO: SI: NO:

CUALES:

2. CUENTA LA ENTIDAD CON CENTROS DE APOYO CERCANO EN CASO DE DESASTRE SI

TIPO:

3. CON COMITÉ PARITARIO DE SALUD OCUPACIONAL: SI

4. CON BRIGADAS: SI

5. MAPA DE RIESGOS: SI

6. PLANES DE EVALUACION: SI

7. SEÑALACION: SI

8. VIGILANCIA: SI

9. HAY ALGUNA DOTACION ESPECIAL PARA LOS FUNCIONAMIENTOS DE ARCHIVO O PARA FUNCIONARIOS QUE TRABAJAN CON DOCUMENTOS: SI: NO: X

ESPECIFIQUE: guantes, tapabocas y batas, se utilizan de manera voluntaria

10 RELACIONE LOS NUMERALES 6 AL 12 CON EL ARCHIVO:

6. PLANES DE EVALUACION: NO

7. SEÑALACION: NO

8. VIGILANCIA: NO

11. SABE QUE HACER CON LA DOCUMENTACION EN CASO DE DESASTRE: NO

CON AGUA: NO

CON FUEGO: NO

OBSERVACIONES:

12. **MANTENIMIENTO (LIMPIEZA): Solo pisos y escritorios**

	FRECUENCIA				EQUIPOS Y MATERIALES
	ANUAL	SEMESTRAL	MENSUAL	OTRO	
DEPOSITO	x				aspiradoras, escobas y traperas
DOCUMENTACION					

OBSERVACIONES: No hay limpieza de documentos

13. SE REALIZA ACCIONES DE CONTROL MICROBIOLOGICOEN AREAS Y/O EN DOCUMENTACION: Se programan fumigaciones según necesidad y en oficinas con los mismos quimicos en archivos

METODO, FRECUENCIA, PRODUCTOS:

14. INSPECCION DEPOSITO No hay plan de inspección y vigilancia de depositos de archivo

ELEMENTO	MATERIAL	ESTADO DE CONCERVACION			
		GRIETAS	HUMEDAD	ATAQ. INSECTOS	OTRO
PISOS					
MUROS					
TECHOS					
DIVISIONES					

BAJANTES: A LA VISTA: SI: NO: GRIETAS: SI: NO:

CONDUCTOS DE ENERGIA: A LA VISTA: SI: NO: DETERIORO: SI: NO:

OBSERVACIONES:

15. REALICE UN ESQUEMA DEL ARCHIVO Y SU DISTRIBUCION, IDENTIFICANDO AREAS, PUERTAS, VENTANAS Y UBICACIÓN DE ESTANTES:

CONVENCIONES:

16. RELACION DE REGISTRO FOTOGRAFICO:

OBSERVACIONES:

ANEXO 4
6 Diagnóstico de depósitos de archivos

MODELO DE DIAGNÓSTICO INTEGRAL DE ARCHIVOS

DEFINICIÓN EQUIPO DE TRABAJO

ENTIDAD: ALCALDIA MUNICIPAL DE BELLO

FECHA DE ELABORACIÓN:2020

Objetivo: Definir el equipo de trabajo que realizará el Diagnóstico Integral de Archivos. Es importante, que el equipo establecido sea interdisciplinario y se involucren todas las áreas de la entidad.

No	NOMBRE	AREA/DEPENDENCIA	PERFIL (PROFESION)	ROLL (CARGO)	RESPONSABILIDAD PRINCIPAL
1	Óscar Andrés Pérez Múñoz	Alcalde		Alcalde	
2	Diana Marcela Uribe Tobón	Primera Dama		Primera Dama	
3	Isabel Daniela Ortega Pérez	Secretario de Gobierno		Secretario de Gobierno	
4	Nubia del Socorro Valencia Montoya	Secretaria de Educación		Secretaria de Educación	
5	Óscar Hernán Orrego Gutierrez	Secretario Adulto Mayor		Secretario Adulto Mayor	
6	Eliana Restrepo Herrera	Secretaria de Recaudos y Pagos		Secretaria de Recaudos y Pagos	
7	Andrea Martinez Orjuela	Secretaria de Cultura		Secretaria de Cultura	
8	Carlos Alberto Pinto Santa	Secretario de Planeación		Secretario de Planeación	
9	Luis Giovany Arias Tobón	Secretario de la General		Secretario de la General	
10	Juan David Casas	Secretario de Medio Ambiente, Vivienda y Desarrollo Rural		Secretario de Medio Ambiente, Vivienda y Desarrollo Rural	
11	Juan Gabriel Rodríguez Díaz	Secretario de Tránsito y Movilidad		Secretario de Tránsito y Movilidad	
12	Rigoberto Arroyave Acevedo	Asesor de Movilidad		Asesor de Movilidad	
13	Jhon Harold Muñoz Restrepo	Secretario Obras Públicas		Secretario Obras Públicas	
14	Francisco Javier Echeverri Cárdenas	Secretario de Hacienda		Secretario de Hacienda	
15	Juan David Arango Peláez	Secretario Privado		Secretario Privado	
16	Rene Omar Jimenez Arango	Secretario de Salud		Secretario de Salud	
17	Julio Eduardo Muñoz Espinal	Secretario de Servicios Administrativos		Secretario de Servicios Administrativos	
18	Yulieth Andrea Sánchez Carreño	Secretaria de Deportes		Secretaria de Deportes	
19	Wber Zapata Lopera	Asesor de Gestión del Riesgo		Asesor de Gestión del Riesgo	
20	Estefan Valencia Palacio	Gerente de Proyectos Especiales		Gerente de Proyectos Especiales	
21	David Antonio Lopera Monsalve	Gerente de Inclusión Social		Gerente de Inclusión Social	
22	Natali Arredondo Villa	Asesora de Educación		Asesora de Educación	
23	Nestor David Restrepo Bonnett	Asesor de Educación		Asesor de Educación	
24	Edgar de Jesús Callejas Arango	Asesor Desarrollo Social		Asesor Desarrollo Social	
25	José Rolando Serrano Jaramillo	Asesor de Asuntos Corporativos		Asesor de Asuntos Corporativos	
26	Juan Pablo Castañeda Arango	Asesor de Asuntos Institucionales		Asesor de Asuntos Institucionales	
27	Jhon Jairo Cardona Tobón	Asesor del Despacho Asuntos Financieros		Asesor del Despacho Asuntos Financieros	
28	Julian Mauricio Montoya Cuartas	Director Administrativo de TIC y Soporte Tecnológico		Director Administrativo de TIC y Soporte Tecnológico	
29	Melissa Orrego Eusse	Comunicadora		Comunicadora	
30	Tania Gina Posada Alegarda	Directora Admiistrativa Para las Mujeres		Directora Admiistrativa Para las Mujeres	
31	Liliana Maria Alvarez	Asesoria juridica		Asesoria juridica	
32	Jorge ignacio rodriguez castrillon	Sisben		Sisben	
33	luis erasmo correa	rentas		rentas	
34	Adriana Maria Santos Bohorquez	Rentas (tramites de cambio propietario)		Rentas (tramites de cambio propietario)	
35	Gustavo Ernestop Gil Arenas	Alumbrado Público		Alumbrado Público	
36	daisse catalina moreno	movilidad para foto multas		movilidad para foto multas	
38	VICTOR AUGUSTO ARANGO	UMAT		UMAT	
40	Arley Montoya	transito		transito	

ANEXO 4
6 Diagnóstico de depósitos de archivos

DIAGNÓSTICO INTEGRAL DE ARCHIVOS

ASPECTOS ADMINISTRATIVOS

NORMATIVIDAD	INSTANCIAS ASESORAS	Si	No	TIPO	Parcial	Peso	OBSERVACIONES			
Decreto 1080 de 2015	La Entidad ha conformado el Comité Interno de Archivo? Si la respuesta es afirmativa indique el Acto Administrativo y su fecha.	X				1	Resolución 2655 de 2018 y 1196 de 2019			
	Los miembros del Comité Interno de Archivo son los enunciados en el artículo 2.8.2.1.15 del Decreto 1080 de 2015?		X			0				
	Las Funciones del Comité Interno de Archivos son las enunciadas en el artículo 2.8.2.1.16 del Decreto 1080 de 2015?		X			0				
	En el territorio (Municipio o Departamento) se ha creado el Archivo General Territorial?					0	No aplica			
	Están las funciones del Archivo General del Territorio acordes con las disposiciones del artículo 2.8.2.1.6 del Decreto 1080 de 2015?					0	No aplica			

NORMATIVIDAD	ASPECTOS ORGANIZACIONALES	Si	No	TIPO	Parcial	Peso	OBSERVACIONES			
Acuerdo 038 de 2002	En el Manual de Funciones y de procedimientos se ha regulado el recibo y la entrega de los documentos de archivo por parte de los servidores públicos?		x			0				
Decreto 1080 de 2015	La Entidad ha formulado una política de gestión Documental?		X			0				
Acuerdo 05 de 2013	La Entidad ha creado el Archivo Histórico?	X				1	Acuerdo 41 del 14 de septiembre de 1993	VERIFICAR SU FUNCIONAMIENTO		
	Indique el Acto Administrativo de creación de la Entidad.	X				N/A	Ordenanza 48 del 29 de abril de 1913.			
	Indique el número de dependencias de la Entidad	72				N/A				
	Tiene la Entidad el Organigrama por dependencias actualizado?	X				1	DECRETO 201904000120			
	Tiene la Entidad un manual de funciones actualizado?	X				1				
	La Entidad cuenta con el Mapa de Procesos actualizado?	X				1				
	Ha desarrollado la Entidad un Normograma de acuerdo a su contexto legal?		x			0	Actualizar normatividad de gestión documental			
	La entidad ha sufrido reestructuraciones, cuántas y cuándo fue la última?	59				N/A	DECRETO 201904000120			
	La entidad ha tenido cambios en la estructura orgánico-funcional de la entidad?	X				N/A				
	Existen actos administrativos u otras normas que indiquen la creación de dependencias o grupos con la respectiva asignación de funciones?	X				N/A				
	Se ha designado a una dependencia específica la función archivística de la Entidad o se ha creado la dependencia, sección o grupo de archivo? Indique acto administrativo	X				1	DECRETO 201904000120	Se requiere la norma		
Acuerdo 05 de 2013	La Entidad ha conformado el Archivo Central Institucional?		X			0	acuerdo 46 del 13 de diciembre de 1959, la creación del cargo del Secretario del Jefe del Archivo Municipal	DERROGADO POR EL Acuerdo 64 de 06 de agosto de 1971		
Acuerdo 04 de 2015	Tiene la Entidad funciones relacionadas con la garantía, protección y salvaguardia de los Derechos Humanos y el Derecho Internacional Humanitario?	X				N/A				

NORMATIVIDAD	ASPECTOS DE FINANCIACIÓN	Si	No	TIPO	Parcial	Peso	OBSERVACIONES			
	Cuál fue el presupuesto designado a las funciones de archivo durante la vigencia?	X				1	807,916,669			
	Cuánto presupuesto ha sido asignado como gastos de funcionamiento del archivo? Describa en qué se ha invertido.	x				0	807,916,669	Todo Consultoria y operación, cajas carpetas e insumos		
	Cuánto presupuesto ha sido asignado en gastos de inversión para el archivo? Describa en que ha sido invertido.		x			0				
	En vigencias anteriores se han contratado o ejecutado proyectos para el funcionamiento del archivo o en sistemas de información?		x			0				
	Ha sido suficiente el presupuesto asignado al área de archivo durante la vigencia para cumplir con el PINAR o el PGD? Explique		x			0	No se cuenta con PINAR y PGD			

NORMATIVIDAD	ASPECTOS DE FORMACIÓN Y CAPACITACIÓN	Si	No	TIPO	Parcial	Peso	OBSERVACIONES			
Ley 594 de 2000	Los funcionarios encargados de los archivos han sido capacitados en programas o áreas de su labor?				X	0	Se identifica poca capacitación, informal y formal nada			
Acuerdo 038 de 2002	Los servidores públicos han sido capacitados en temas relacionados al manejo y organización de los archivos?				X	0	Se identifica poca capacitación, informal y formal nada			
	Los servidores públicos reciben o entregan los documentos o archivos inventariados?		X			0	Se evidencia acumulación de documentos en archivos de gestión			
Acuerdo 050 de 2000	Los servidores públicos han sido capacitados y entrenados para la atención de emergencias?		X			0	El plan de emergencia de la entidad no contempla aspectos de archivo.			
Acuerdo 060 de 2001	La Unidad de Correspondencia cuenta con el personal suficiente y capacitado para recibir, enviar y controlar oportunamente el trámite de las comunicaciones de carácter oficial?	X				0	Hay que implementar indicadores de gestión para determinar su eficacia			

ASPECTOS ADMINISTRATIVOS	
ASPECTOS A EVALUAR	23
POSITIVOS	14
NEGATIVOS	9

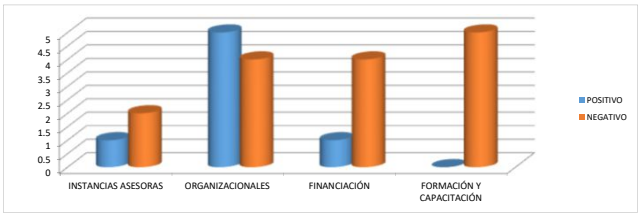
INSTANCIAS ASESORAS	
ASPECTOS A EVALUAR	3
POSITIVOS	1
NEGATIVOS	2

ASPECTOS ORGANIZACIONALES	
ASPECTOS A EVALUAR	9
POSITIVOS	5
NEGATIVOS	4

ASPECTOS DE FINANCIACIÓN	
ASPECTOS A EVALUAR	5
POSITIVO	1
NEGATIVO	4

ASPECTOS DE FORMACIÓN Y CAPACITACIÓN	
ASPECTOS A EVALUAR	5
POSITIVOS	0
NEGATIVOS	5

ASPECTOS ADMINIS	INSTANCIAS ASESORAS	ORGANIZAC	FINANCIAC	FORMACIÓN Y CAPACITACIÓN	
POSITIVO	1	5	1	0	7
NEGATIVO	2	4	4	5	15



ANEXO 4
6 Diagnóstico de depósitos de archivos

DIAGNÓSTICO INTEGRAL DE ARCHIVOS
ASPECTOS DE LA FUNCIÓN ARCHIVÍSTICA

	NORMATIVIDAD	INSTRUMENTOS ARCHIVÍSTICOS	Si	No	Parcial	Peso	OBSERVACIONES
1	Acuerdo 05 de 2013	La Entidad ha elaborado el Cuadro de Clasificación Documental	X			1	
2	Acuerdo 04 de 2013	La Entidad ha elaborado las Tablas de Retención Documental?	X			1	
3		Las Tablas de Retención Documental fueron aprobadas por la instancia competente? Indique acto administrativo	X			1	En construcción
4		Las Tablas de Retención Documental fueron convalidadas por la instancia competente? Indique acto administrativo		X		0	
5		Las Tablas de Retención Documental fueron implementadas por la instancia competente? Indique acto administrativo		X		0	
6		Las Tablas de Retención Documental fueron publicadas en la página web de la Entidad?		X		0	
7		Han sido actualizadas las Tablas de Retención Documental? Indique el motivo y la fecha	X			1	Las que se estan presentando
8	Decreto 1080 de 2015	La Entidad ha elaborado el Programa de Gestión Documental?		X		0	El que esta en intranet es un documento del AGN 2004 desactualizado
9		El Programa de Gestión Documental fue aprobado por la instancia competente? Indique acto administrativo		X		0	
10		Se ha realizado la implementación del Programa de Gestión Documental?		X		0	
11		Se ha realizado el seguimiento al Programa de Gestión Documental?		X		0	
12		Se ha publicado el Programa de Gestión Documental en la página web de la Entidad?		X		0	
13		La Entidad ha elaborado el Plan Institucional de Archivos?		X		0	
14	Acuerdo 04 de 2013	La Entidad ha elaborado las Tablas de Valoración Documental?	X			1	Esta en construcción
15		Las Tablas de Valoración Documental fueron aprobadas por la instancia competente? Indique acto administrativo		X		0	

ANEXO 4

6 Diagnóstico de depósitos de archivos

16		Las Tablas de Valoración Documental fueron convalidadas por la instancia competente? Indique acto administrativo		X		0	
17		Las Tablas de Valoración Documental fueron implementadas por la instancia competente? Indique acto administrativo		X		0	
18	Decreto 1080 de 2015	Ha implementado la Entidad la elaboración de los inventarios documentales en los archivos de gestión?		X		0	No se evidencia plan de transferencias documentales, por lo tanto se presume que los archivos de gestión no cumplen con la politica archivistica establecida por el AGN.
19		Ha elaborado la Entidad el Modelo de Requisitos para la gestión de documentos electrónicos?		X		0	
20		Ha elaborado la Entidad el banco terminológico de tipos, series y subseries documentales?	X			1	
21		Ha desarrollado la Entidad los mapas de procesos, flujos documentales, y la descripción de funciones de las unidades administrativas?		X		0	
22		Ha desarrollado la Entidad las Tablas de Control de Acceso para el establecimiento de categorías adecuadas de derechos y restricciones de acceso y seguridad aplicables a los documentos?		X		0	
23	Acuerdo 06 de 2014	Ha elaborado la Entidad el Sistema Integrado de Conservación?		X		0	
24		El Comité Interno de Archivo emitió concepto para la aprobación del Sistema Integrado de Conservación?		X		0	
25		Fue aprobado el Sistema Integrado de Conservación mediante acto administrativo?		X		0	
26							
27	NORMATIVIDAD	ORGANIZACIÓN Y DESCRIPCIÓN	Si	No	Parcial		OBSERVACIONES
28	Acuerdo 02 de 2014	Se están conformando los expedientes de acuerdo a los Cuadros de Clasificación adoptados por la Entidad?		X		0	Se presume que si apenas se esta entregando la TRD, los expedientes aún no cuentan con el amarre necesario para este instrumento.
29		Los expedientes son identificados de acuerdo al sistema de descripción adoptado por la Entidad?		X		0	No se evidencia sistema de descripción

ANEXO 4
6 Diagnóstico de depósitos de archivos

30	Acuerdo 42 de 2002	Las carpetas reflejan las series y subseries documentales correspondientes a la Unidad administrativa?	X			1	Respetan el principio de orden original VALIDAR
31	Acuerdo 05 de 2013	Se ha implementado la Hoja de Control de documentos al interior del expediente?		X		0	Solo para algunas series como las HV, los demas expedientes no llevan este control. VALIDAR
32		La Entidad ha desarrollado un programa de descripción documental?		X		0	
33		La Entidad ha elaborado instrumentos de descripción?			X	0	Solo inventarios en algunos casos, faltan catalogos, indices, censos, guias.
34	Acuerdo 02 de 2014	Se realiza la foliación de los expedientes en su etapa de gestión?		X		0	Se realiza en algunos casos al momento de la entrega. VALIDAR
35	Acuerdo 038 de 2002	La Entidad ha adoptado el Formato Único de Inventario Documental?	X			1	
36	Acuerdo 02 de 2014	Se realiza y mantiene actualizado el inventario de los expedientes en los archivos de gestión?		X		0	
37	Acuerdo 11 de 1996	El material gráfico (dibujos, croquis, mapas, planos, fotografías, ilustraciones, prensa, entre otros) es extraído y se deja en su lugar un testigo?		X		0	La información queda almacenada en la misma unidad documental. VALIDAR
38		El material gráfico es almacenado en la sección del archivo dispuesta para conservar distintos formatos?		X		0	
39	Acuerdo 042 de 2002	Se realiza préstamo de documentos para trámites internos?	X			1	
40		Las dependencias realizan registro de los préstamos y solicitan su devolución?		X		0	Algunas dependencias, no todas. VALIDAR
41	Acuerdo 02 de 2014	La Entidad realiza o ha realizado procesos de digitalización de los expedientes? Explique el motivo	X			0	Algunos, para tramite de documentos, y requerimientos de TRANSPARENCIA. VALIDAR
42		Se han realizado las transferencias primarias?			X	0	Algunas areas, VALIDAR
43	Acuerdo 042 de 2002	Las cajas usadas para la transferencia primaria se encuentran identificadas?	X			0	VALIDAR

ANEXO 4
6 Diagnóstico de depósitos de archivos

44	Acuerdo 04 de 2013	Se ha establecido un procedimiento para la Eliminación de documentos?	X			0	Se observa que no cumple con el acuerdo 04 de 2019 del agn y se permité la eliminación de documentos en el archivo de gestión. AJUSTAR EL PROCEDIMIENTO. Validar que no se hayan eliminado documentos con valores secundarios o sin cumplir tiempos de retención.
45		El procedimiento para eliminación de documentos está acorde con lo dispuesto en el Acuerdo 04 de 2019?		X		0	
46	Acuerdo 02 de 2004	Tiene la entidad documentos dispuestos sin ningún criterio de organización archivística (Fondos Acumulados)?	X			0	62,30 metros lineales de documentación para elaborar las Tablas de Valoración Documental. Revisando un total 4,518 unidades documentales ubicadas en 354 cajas. Segun Informe TVD. VALIDAR
47	Acuerdo 07 de 2015	Se han perdido parcial o totalmente uno más expedientes en la Entidad?	X			0	Segun informe de TVD. VALIDAR, recoger actas de archivo y eliminación de documentos, se debe cruzar con VALORACIÓN, para determinar perdida real.
48	Circular 04 de 2003	Las Historias Laborales son organizadas de acuerdo a lo dispuesto en la Circular 04 de 2003?	X			1	VALIDAR
49	Acuerdo 02 de 2014	En los archivos de gestión se utilizan unidades como AZ o carpetas argolladas?	X			0	VALIDAR
50							
51	NORMATIVIDAD	COMUNICACIONES OFICIALES	Si	No	Parcial		OBSERVACIONES
52	Acuerdo 060 de 2001	La Entidad ha creado o conformado la Unidad de Correspondencia? Indique acto administrativo		X		0	
53		La Entidad ha adoptado una política respecto las firmas responsables?		X		0	
54		Describa el procedimiento de radicación de documentos		X		0	

ANEXO 4
6 Diagnóstico de depósitos de archivos

55		Describa el procedimiento para la numeración de actos administrativos e indique la dependencia responsable.		X		0	
56		Se han desarrollado e implementado planillas, formatos o controles para certificar la recepción de los documentos a nivel interno?	X			1	VALIDAR, que cumplan con el acuerdo 060 de 2001
57		Se han dispuesto servicios de alerta para el seguimiento de tiempos de respuesta?		X		0	Validar con el aplicativo que utilizan
58		La entidad ha publicado el horario de atención al público de la unidad de correspondencia?	X			1	

ANEXO 4
6 Diagnóstico de depósitos de archivos

ASPECTOS DE FUNCION ARCHIVÍSTICA	53
POSITIVOS	10
NEGATIVOS	43
INSTRUMENTOS ARCHIVÍSTICOS	25
POSITIVOS	6
NEGATIVOS	19
ORGANIZACIÓN Y DESCRIPCIÓN	22
POSITIVOS	4
NEGATIVOS	18
COMUNICACIONES OFICIALES	7
POSITIVOS	2
NEGATIVOS	5

ASPEC	INSTRUMENTOS ARCI	ORGANIZACIÓN Y DESCRIPCIÓN		COMUNICACIONES OFICIALES	
POSIT	6	4	2	12	
NEGA	19	18	5	42	

DIAGNÓSTICO INTEGRAL DE ARCHIVOS
ASPECTOS DE PRESERVACIÓN A LARGO PLAZO

	NORMATIVIDAD	CONDICIONES DE EDIFICIOS Y LOCALES DESTINADOS A ARCHIVOS	Si	No	Parcial	Peso	OBSERVACIONES
6		Los depósitos presentan el espacio suficiente para		X		0	Se presume que no, porque mucha información reposa en las areas
10		El depósito fue diseñado y dimensionado teniendo en cuenta la manipulación, transporte y seguridad de los documentos?		X		0	Los depositos se eligieron según necesidad de custodia, y no se planificaron teniendo en cuenta condiciones de deposito establecidas por el AGN.
11		Fue adecuado el depósito climáticamente?		X		0	No existen equipos de control climatico
12		Las áreas destinadas a custodia cuentan con elementos de control y aislamiento?		X		0	No se respetan areas establecidas en la normativa
13		Las zonas técnicas o de trabajo archivístico, consulta, limpieza, entre otras actividades se encuentran fuera del área de almacenamiento?		X		0	No se respetan areas establecidas en la normativa
14		La estantería está diseñada para almacenar las unidades de conservación usadas por la Entidad?		X		0	Solo es estanteria fija abierta y otros muebles según las necesidades, los archivos de gestión utilizan archivadores de gavetas. VALIDAR
17		Se encuentran los parales de la estantería fijados al piso?		X		0	Se fijan en el aire. VALIDAR
18		La balda inferior se encuentra al menos a 10 cm del piso?		X	X	0	En algunos depositos. VALIDAR
19		Los acabados del mobiliario son redondeados?		X	X	0	En algunos mobiliarios. VALIDAR
20		Se utiliza el cerramiento superior para almacenar		X		0	Estos espacios son utilizados para almacenar. VALIDAR
21		Se encuentra la estantería recostada sobre los muros?	X		X	0	En la gran mayoria esta recostada. VALIDAR
22		Tiene la estantería un sistema de identificación visual?		X		0	No cuenta con ubicación topografica. VALIDAR
23		Presentan oxidación los elementos de la estantería?		X		1	No se identifica. VALIDAR
24		Las bandejas o parales de la estantería se encuentran deformados?	X		X	0	En algunos casos, por resistencias de laminas. VALIDAR
25		La Entidad usa planotecas?		X	X	0	No se sabe. VALIDAR
5		El espacio ofrece suficiente espacio para albergar la documentación acumulada y su natural incremento?		X		0	No se aplican instrumentos archivisticos. Hay mucha acumulación. VALIDAR
2	Acuerdo 049 de 2000	Indique el número total de depósitos de archivo	11			N/A	VALIDAR
26		Se encuentran las planotecas en buen estado?		X	X	0	No se identifica. VALIDAR
27		Se realiza mantenimiento periódico a los sistemas de rodaje de las bandejas de las planotecas?		X		0	No existe plan de mantenimiento para el archivo. VALIDAR
3		El terreno se presenta sin riesgos de Humedad subterránea o problemas de inundación y ofrece	X		X	1	En algunos depositos se identifican estos riesgos. VALIDAR
4		El terreno se encuentra situado lejos de industrias contaminantes o que presenten riesgos de un	X		X	1	En algunos depositos se identifican estos riesgos. VALIDAR

ANEXO 4
6 Diagnóstico de depósitos de archivos

7		Los pisos, muros, techos y puertas están construidos con materiales resistentes?	X		X	1	En algunos depositos se identifican estos riesgos. VALIDAR
8		Las pinturas empleadas presentan propiedades ignífugas?		X	X	0	En algunos depositos se identifican estos riesgos. VALIDAR
9		La resistencia de las placas es igual o mayor a 1200		X		0	No se identifica. VALIDAR
15		La estantería está elaborada en láminas metálicas,	X		X	1	En algunos depositos se identifican estos riesgos. VALIDAR
16		Las bandejas soportan al menos 100 Kg?	X		X	1	En algunos depositos se identifican estos riesgos. VALIDAR
28							
29	NORMATIVIDAD	UNIDADES DE CONSERVACIÓN	Si	No	Parcial	Peso	OBSERVACIONES
30	Acuerdo 049 de 2000	Las unidades de conservación están elaboradas en cartón neutro?		X		0	Muchas son unidades de cartulina. VALIDAR
31		Las unidades de conservación presentan un recubrimiento interno?		X		0	Muchas son unidades de cartulina. VALIDAR
32		Las Unidades de conservación presentan orificios?		X		0	VALIDAR
33		Las carpetas ofrecen protección a los documentos?		X	X	0	Muchas son unidades de cartulina. VALIDAR
34		Es necesario perforar los documentos?		X		0	Se hace por costumbre y la unidad de conservación que utilizan lo exige
35		Se desgastan o se deforman fácilmente las unidades de conservación como cajas y carpetas?	X			0	Mucha informacion no se encuentra en cajas. VALIDAR
36		Los diseños y tamaños son acordes al tipo de documentación que se almacena en ellas?		X		0	Se manejan medidas estandar. VALIDAR
37							
38	NORMATIVIDAD	CONDICIONES AMBIENTALES	Si	No	Parcial		OBSERVACIONES
41		Las ventanas, puertas o celosías permiten el intercambio de aire?	X		X	0	Se evidencian depositos cerrados completamente. VALIDAR
42		Estos vanos están acondicionados con filtros que impidan la entrada de partículas o contaminantes al depósito de archivo?		X		0	No se evidencia filtros de control de polución. VALIDAR
39	Acuerdo 049 de 2000	Se han realizado mediciones de condiciones ambientales en los depósitos de archivo?		X		0	No se lleva control de mediciones, ni existe programa. VALIDAR
40		Se han instalado materiales o equipos de modificación de condiciones ambientales en los depósitos de archivo?		X		0	No se han dotado los depositos de estos elementos. VALIDAR
43		Se utilizan luminarias fluorescentes de baja intensidad?		X		0	No se evidencia control de luminocidad. VALIDAR
44		Tiene ventanas que permiten la entrada de luz solar al depósito de archivo?	X		X	0	En algunos depositos. VALIDAR
45							
46	NORMATIVIDAD	MANTENIMIENTO	Si	No	Parcial		OBSERVACIONES
47	Acuerdo 049 de 2000	Se realiza la limpieza de las instalaciones? Indique cada cuanto y describa el cómo y los materiales que se utilizan.		X		0	Se barre y aspira, no existe plan de limpieza para los depositos de archivo. VALIDAR
48		Se realiza la limpieza de la estantería? Indique cada cuanto y describa el cómo y los materiales que se utilizan.		X		0	Se barre y aspira, no existe plan de limpieza para los depositos de archivo. VALIDAR
49		Se realiza la limpieza de las unidades de conservación? Indique cada cuanto y describa el cómo y los materiales que se utilizan.		X		0	Se barre y aspira, no existe plan de limpieza para los depositos de archivo. VALIDAR
50							

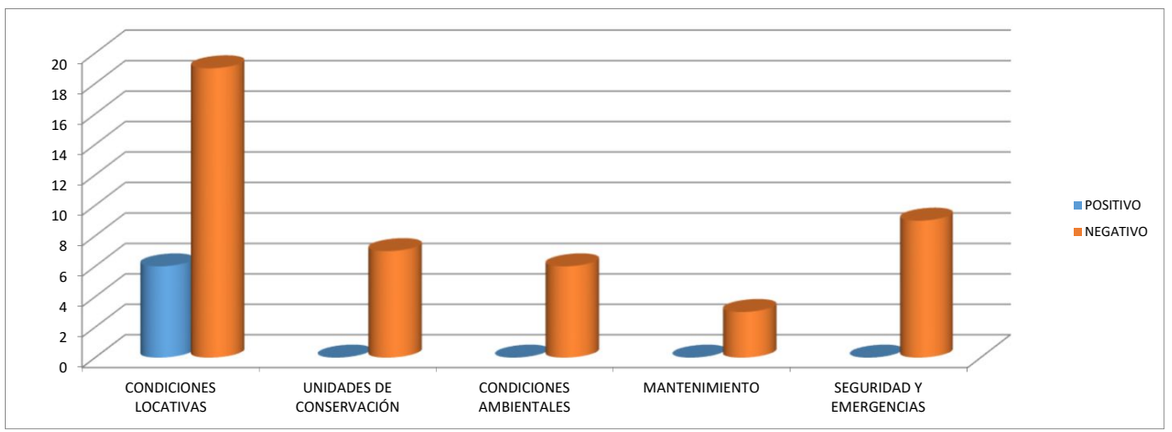
ANEXO 4
6 Diagnóstico de depósitos de archivos

51	NORMATIVIDAD	SEGURIDAD Y EMERGENCIAS	Si	No	Parcial		OBSERVACIONES
53		Los extintores son de agentes limpios?		X		0	Los extintores son de agua. VALIDAR
54		Los extintores son recargados anualmente?	X			0	VALIDAR
55		Se han instalado sistemas de alarma contra		X		0	Se utilizan las mismas cerraduras de las puertas de las instalaciones. VALIDAR
56		Se han instalado sistemas de alarma para la detección de incendios?		X	X	0	Las que tiene el edificio en sus oficinas. VALIDAR
57		Se han instalado sistemas de alarma para la detección de inundaciones?		X		0	VALIDAR
58		Se ha proveído la señalización para la identificación de los equipos de atención de desastres y rutas de	X		X	0	Las señalizaciones del sistema de seguridad y salud en el trabajo, según el programa, no incluye el componente de archivo. VALIDAR
59		Se ha elaborado un Plan de prevención de desastres y situaciones de riesgo?		X		0	No se tiene con componente de archivo. VALIDAR
52	Acuerdo 050 de 2000	Ha dispuesto la Entidad extintores en el área de archivo?	X		X	0	En algunos depositos. VALIDAR
60		Se ha realizado el levantamiento y valoración del panorama de riesgo en la Entidad?	X		X	0	Si, sin el componente de archivo. VALIDAR

ANEXO 4
6 Diagnóstico de depósitos de archivos

ASPECTOS DE PRESERVACION A LARGO PLAZO	50
POSITIVOS	6
NEGATIVOS	44
CONDICIONES DE EDIFICIOS Y LOCALES DESTINADOS A ARCHIVOS	25
POSITIVOS	6
NEGATIVOS	19
UNIDADES DE CONSERVACIÓN	7
POSITIVOS	0
NEGATIVOS	7
CONDICIONES AMBIENTALES	6
POSITIVOS	0
NEGATIVOS	6
MANTENIMIENTO	3
POSITIVOS	0
NEGATIVOS	3
SEGURIDAD Y EMERGENCIAS	9
POSITIVOS	0
NEGATIVOS	9

ASPECTOS DE PRESERVACION A LARGO PL	CONDICIONES LOCATI	UNIDADES DE CONSERVACIÓN	CONDICIONES AMBIENTAL	MANTENIMIEN	SEGURIDAD Y EMERGENCIAS		
POSITIVO	6	0	0	0	0		6
NEGATIVO	19	7	6	3	9		44



ANEXO 4
6 Diagnóstico de depósitos de archivos

MATRIZ DE ANÁLISIS

Entidad:	**ALCALDIA MUNICIPAL DE BELLO**
Fecha de elaboración	**Marzo 20 de 2020**

Objetivo: Realizar el análisis de los aspectos problemáticos que impiden la implementación de la Función Archivística.

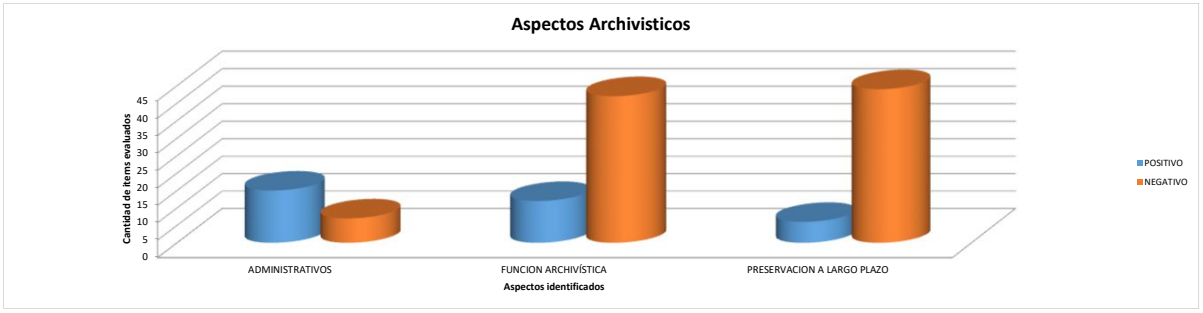
Instrucciones: De acuerdo a los datos recolectados en las hojas del modelo, sombree con color rojo las áreas que presentan riesgo o problemáticas para la implementación de la función archivística en la Entidad.

ASPECTOS ADMINISTRATIVOS			
INSTANCIAS ASESORAS	ASPECTOS ORGANIZACIONALES	ASPECTOS DE FINANCIACIÓN	ASPECTOS DE FORMACIÓN Y CAPACITACIÓN
Comité Interno de Archivo	Organigrama por dependencias	Presupuesto actual	Nivel de Estudios
	Manual de funciones		Cantidad de personal
	Normograma		
Archivo General del Territorio	Designación de funciones de archivo	Impacto de las inversiones anteriores	Capacitación y actualización
	Política de Gestión Documental		

ASPECTOS DE LA FUNCIÓN ARCHIVÍSTICA		
INSTRUMENTOS ARCHIVÍSTICOS	ORGANIZACIÓN Y DESCRIPCIÓN	COMUNICACIONES OFICIALES
Cuadro de Clasificación Documental	Conformación	Unidad de Correspondencia
Tablas de Retención Documental	Ordenación	
Programa de Gestión Documental	Identificación	
Plan Institucional de Archivos		Políticas de firmas responsables
Tablas de Valoración Documental	Hoja de Control	
Inventarios documentales		
Modelo de Requisitos para la gestión de documentos electrónicos	Foliación	
Banco terminológico de tipos, series y subseries documentales		Radicación de documentos
Mapas de procesos, flujos documentales,	Inventario de archivos de gestión	
Tablas de Control de Acceso		
Sistema Integrado de Conservación	Transferencias primarias	Horarios de Atención

ASPECTOS DE CONSERVACIÓN A LARGO PLAZO			
CONDICIONES DE EDIFICIOS Y LOCALES DESTINADOS A ARCHIVOS	UNIDADES DE CONSERVACIÓN	MANTENIMIENTO	SEGURIDAD Y EMERGENCIAS
Ubicación	Materiales adecuados	Instalaciones	Sistemas de Alarma
Resistencia de Materiales		Documentos de Archivo	Elementos para la atención de emergencias
Mobiliario	Diseño y función	Deterioros	Plan de Prevención de Desastres y situaciones de riesgo
Condiciones ambientales		Intervenciones anteriores	

ASPECTOS	ADMINISTRATIVOS	FUNCION ARCHIVÍSTICA	PRESERVACION A LARGO PLAZO
POSITIVO	15	12	6
NEGATIVO	7	42	44



ANEXO 5
8. Herramienta de estructura SIC

FICHA DE PROYECTO INTERNO

Nombre: Implementar Sistema Integrado de Conservación (SIC) en relación con • Programa de Inspección y mantenimiento de sistemas de almacenamiento e

Objetivo:

Alcance: El alcance del proyecto va desde la Aprobación del documento por parte del Comité interinstitucional hasta Actualización y seguimiento a los planes y programas,

Responsable del Plan: Despacho del Alcalde, Secretaría General, Dirección Administrativa de Gestión Documental y Atención al Ciudadano, Secretaría de Control Interno,

Programa del Plan de Desarrollo	Actividad	Responsable	Fecha de Inicio	Fecha Final	Entregable	Observaciones
Plan de Desarrollo Municipal "Por el Bello que Queremos, PACTO DOS "Por una ciudad educada y educadora", PACTO TRES "Por la calidad institucional y por el ordenamiento territorial", PACTO SEIS: "Por el emprendimiento, la innovación y las nuevas tecnologías, en el componente TIC´s	Aprobación del documento por parte del Comité de Desarrollo Administrativo	Despacho del Alcalde, Secretaría General, Dirección Administrativa de Gestión Documental y Atención al Ciudadano, Secretaría de Control Interno, Dirección Técnica de Formulación de Proyectos, Secretaría de Hacienda, Secretaría de Planeación, Dirección Técnica de TIC y Soporte Tecnológico	2021	2023	Acta de comité y acto administrativo de adopción.	
	Publicación del SIC				SIC publicado	
	Realizar cronograma e implementación del SIC				Cronograma y seguimiento	
	Seguimiento al cuadro de control de mando					
	Actualización y seguimiento a los planes y programas				Programas actualizados	

INDICADORES				
Nombre del Indicador	**Formula**	**Sentido**	**Meta**	**% de cumplimiento**
Implementación del Sistema Integrado de Conservación (SIC)	Implementación realizada / Implementación proyectada * 100	**Creciente**	**100%**	**100%**

RECURSOS		
TIPO	**CARACTERISTICAS**	**OBSERVACIONES**
Humano	Los Responsables	
Tecnicos, humanos, financieros, locativos entre otros	volumenes documentales y mejoras identi	

PRESUPUESTO: (0.000) Los recursos están asociados al presupuesto anual para el servicio de administración y gestión del archivo y correspondencia de la entidad.

ANEXO 5
8. Herramienta de estructura SIC

ASPECTOS CRÍTICOS - PINAR

ASPECTOS CRÍTICOS		RIESGO
Aspectos De Preservación	Condiciones De Edificios Y Locales Destinados A Archivos	Se evidencia poco espacio para almacenar la documentación existente, posible cusa que no se ha implementado TRD y TVD, tampoco se han hecho las proyecciones necesarias, para determinar el espacio en metros cuadrados necesario según el volumen documental generado anualmente; esto ocasiona deterioro de la documentación y perdida de la información.
		Los depósitos no están adecuados climáticamente; ocasionando deterioro de los documentos análogos y perdida de información.
		Los depósitos no se han diseñado teniendo en cuenta sus diferentes zonas de distribución (custodia, trabajo archivístico, consulta, limpieza, reprografía entre otras); ocasionando deterioro a los documentos y poniendo en riesgo la salud de sus empleados.
		Las estanterías que se utilizan no están diseñadas para los documentos dependiendo de sus formatos, tamaños y soportes; ocasionando deterioro de los mismos y perdida de información.
		Muchas estanterías metálicas identificadas no cuentan con requisitos técnicos de resistencia, ensamble y anclaje; así como de distribución y distancias mínimas entre ellas, pisos y paredes; ocasionando deterioro de los documentos y riesgos ocupacionales para los funcionarios.
		Se evidencia que no se tienen planes de mantenimiento para unidades de instalación como archivadores de gavetas, rodantes, fijos, plano tecas entre otros; ocasionando un riesgo para la conservación de los documentos y para la salud de los funcionarios.
		Se evidencia riesgo de humedad en los depósitos de archivo, provocado por baños y cocinetas en algunos de ellos; ocasionando riesgo para la documentación y la información.
		Los muros, techos y puertas de los depósitos de archivo no fueron construidos teniendo en cuenta los aspectos técnicos mínimos para ellos, es posible que sea a causa de que muchos de esos depósitos no fueron destinados a esta función originalmente; esto ocasiona deterioro de los documentos y riesgo de pérdida de la información, así como riesgo de desplome en algunos casos (archivo central)
	Unidades De Conservación	Las unidades de conservación como carpetas y cajas, no cuentan con las especificaciones técnicas requeridas, ocasionando deterioro para la documentación y por ende perdida de información.
		No se utilizan las referencias de las cajas según el tipo de archivo, esto hace que sean incontrolables los volumen identificados.
	Condiciones Ambientales	Se evidencia que en varios depósitos las ventanas, puertas o celosías permiten el intercambio de aire, ocasionando deterioro en los soportes documentales
		Las claraboyas o rejillas que están en los depósitos de archivo no se encuentran acondicionadas con filtros que impidan la entrada de partículas o contaminantes a los depósitos, esto ocasiona altos niveles de polución que contaminan los documentos.
		Los depósitos no cuentan con equipos de mediciones de condiciones ambientales que permitan establecer la fluctuación en temperatura, HR y polución a la que están expuestos los soportes documentales.
		No se han instalado materiales o equipos de modificación de condiciones ambientales en los depósitos de archivo
		Las luminarias no son fluorescentes de baja intensidad, necesarias para disminuir la pigmentación de los soportes documentales. Tampoco se han instalado de forma correcta (archivo central)
		En algunos deposito sobre todo los archivos de gestión se tienen ventanas que permiten la entrada de luz solar al depósito de archivo, esto deteriora en todo los aspectos los soportes documentales.
	Mantenimiento	Se identifica que en algunas areas AG y archivo central se realiza la limpieza de las instalaciones, como pisos y estanterías, esto es favorable para la documentación. Pero se identifican tambien muchos fondos acumulados sin ningun tipo de limpieza y en ciertos puntos la documentación se encuentra mezclada con basura.
		No se realiza la limpieza de las unidades de conservación como carpetas, ni tampoco de las piezas documentales; esto pone en riesgo la perdurabilidad de soportes e información , así como la salud de los funcionarios.
	Seguridad Y Emergencias	Los extintores identificados no son de agentes limpios, ocasionando daño a los soportes documentales en caso de utilización.
		Se identifica que los extintores son recargados anualmente, siendo esto favorable a la seguridad de la documentación, pero no se ha dado las capacitaciones necesarias para su uso a el personal encargado.
		No se han instalado sistemas de alarma contra intrusiones, en los diferentes deposito, esto pone en riesgo la información y los derechos de los ciudadanos.
		Se identifican algunos sistemas de alarma para la detección de incendios, los cuales no son convenientes para el material papel, ya que al activarse pueden deteriorar el soporte.
		No se evidencian sistemas de alarma para la detección de inundaciones en los depósitos de archivo, aunque en algunos se encuentran cocinetas y baños.
		Se identifica que se ha proveído la señalización para la identificación de los equipos de atención de desastres y rutas de evacuación, establecidas dentro de los planes de contingencia de la entidad sobre todo para los archivos de gestión, mas ninguna señalización para los depositos de archivos.
		Se identifica que se ha elaborado un Plan de prevención de desastres y situaciones de riesgo, sin el componente archivístico.
		En algunos depósitos se ha dispuesto de extintores en el área de archivo, aunque no cumplen con las condiciones técnicas necesarias para los soportes archivísticos.
		Se ha realizado el levantamiento y valoración del panorama de riesgo en la Entidad, sin el componente archivístico, esto ocasiona un riesgo en la seguridad de la información.

SISTEMA INTEGRADO DE CONSERVACIÓN - SIC
MATRIZ PARA LA FORMULACIÓN DE LINEAMIENTOS

COMPONENTE	ASPECTOS CRÍTICOS		OBJETIVOS	PLANES PROGRAMAS Y/O PROYECTOS	ACTIVIDADES	REQUISITOS DOCUMENTALES	REQUISITOS TECNOLÓGICOS	POLÍTICAS NORMAS Y ESTÁNDARES Y BUENAS PRÁCTICAS
Aspectos De Preservación	**Condiciones De Edificios Y Locales Destinados A Archivos**	Se evidencia poco espacio para	Aprobar e implementar el SIC	Programa de Inspección y	**Descritas en cada Programa**	**Elaboración, aprobación, implementación y seguimiento a cada programa.**	**Detallados en cada programa**	**Detallados en cada programa**
		Los depósitos no están adecuados	Elaborar, aprobar e implementar	Programa de Inspección y				
		Los depósitos no se han diseñado	Elaborar, aprobar e impremental	Programa de Inspección y				
		Las estanterías que se utilizan no están	Proyectar y acondicionar	Programa de Inspección y				
		Muchas estanterías metálicas	Acondicionar los depositos de	Programa de Inspección y				
		Se evidencia que no se tienen planes de	Implementar estanterías	Programa de Inspección y				
		Se evidencia riesgo de humedad en los	Implementar estanterías	Programa de Inspección y				
		Los muros, techos y puertas de los	Acondicionar los muros, techos	mantenimiento de sistemas				
	Unidades De Conservación	Las unidades de conservación como	Acondicionar ventanas, puertas	mantenimiento de sistemas				
		No se utilizan las referencias de las	acondicionar las claraboyas o	ambiental desinfección,				
	Condiciones Ambientales	Se evidencia que en varios depósitos las	Elaborar, aprobar e implementar	ambiental desinfección,				
		Las claraboyas o rejillas que están en	Elaborar el implementar plan de	Almacenamiento y re-				
		Los depósitos no cuentan con equipos	Implementar unidades de	Programa de				
		No se han instalado materiales o	Utilizar referencias de cajas	Programa de Monitoreo y				
		Las luminarias no son fluorescentes de	Instalar sistemas de alarma	Programa de Monitoreo y				
		En algunos deposito sobre todo los	Implementar sistemas de	Programa de Monitoreo y				
	Mantenimiento	Se identifica que en algunas areas AG y	Implementar sistemas de	Programa de Monitoreo y				
		No se realiza la limpieza de las unidades	Acondicionar climáticamente los	Programa de Monitoreo y				
	Seguridad Y Emergencias	Los extintores identificados no son de	Acondicionar los depósitos con	Programa de Monitoreo y				
		Se identifica que los extintores son	Acondicionar luminarias, las	Plan de Prevención y				
		No se han instalado sistemas de alarma	Implementar extintores de	Plan de Prevención y				
		Se identifican algunos sistemas de	Mantener los extintores	Plan de Prevención y				
		No se evidencian sistemas de alarma	Proveer los depositos de archivo	Plan de Prevención y				
		Se identifica que se ha proveído la	Elaborar, aprobar e implementar	Plan de Prevención y				
		Se identifica que se ha elaborado un	Elaborar el panorama de riesgo	Plan de Prevención y				
		En algunos depósitos se ha dispuesto						
		Se ha realizado el levantamiento y						

ANEXO 5
8. Herramienta de estructura SIC

	SISTEMA INTEGRADO DE CONSERVACIÓN - SIC **CRONOGRAMA DE IMPLEMENTACIÓN**	SC-CER143688

PLAN - ACTIVIDAD / TIEMPO	Corto plazo		Mediano plazo	Largo plazo
	2020	2021	2022	2023
PLAN DE CONSERVACION DOCUMENTAL.				
Programa de Capacitación y sensibilización				
Programa de Inspección y mantenimiento de sistemas de almacenamiento e instalaciones físicas				
Programa de Saneamiento ambiental desinfección, desratización y desinsectación				
Programa de Monitoreo y control de condiciones ambientales.				
Programa de Almacenamiento y re-almacenamiento.				
Plan de Prevención y atención de desastres para material documental				
PLAN DE PRESERVACIÓN DIGITAL A LARGO PLAZO				

ANEXO 5
8. Herramienta de estructura SIC

SISTEMA INTEGRADO DE CONSERVACIÓN - SIC

PLAN/ IMPLEMENTACIÓN	INDICADORES	META	Medicion trimestral				GRÁFICO	OBSERVACIONES
			1	2	3	4		
PLAN DE CONSERVACION DOCUMENTAL.	*Seguridad*	*100%*	25%	25%	25%	25%		
Programa de Capacitación y sensibilización	*Seguridad*	*100%*	25%	25%	25%	25%		
Programa de Inspección y mantenimiento de sistemas de almacenamiento e instalaciones físicas	*Seguridad*	*100%*	25%	25%	25%	25%		
Programa de Saneamiento ambiental desinfección, desratización y desinsectación	*Seguridad*	*100%*	25%	25%	25%	25%		
Programa de Monitoreo y control de condiciones ambientales.	*Seguridad*	*100%*	25%	25%	25%	25%		
Programa de Almacenamiento y re-almacenamiento.	*Seguridad*	*100%*	25%	25%	25%	25%		
Plan de Prevención y atención de desastres para material documental	*Seguridad*	*100%*	25%	25%	25%	25%		
	Seguridad	*100%*	25%	25%	25%	25%		
PLAN DE PRESERVACIÓN DIGITAL A LARGO PLAZO	*Seguridad*	*100%*	25%	25%	25%	25%		