GR-PG04

**PROGRAMA DE NORMALIZACIÓN DE FORMAS Y FORMULARIOS**



**CONTENIDO**

[**1.** **INTRODUCCIÓN** 3](#_Toc120612698)

[**2.** **OBJETIVOS** 3](#_Toc120612699)

[**2.1.** **OBJETIVO GENERAL** 3](#_Toc120612700)

[**2.2.** **OBJETIVOS ESPECIFICOS** 3](#_Toc120612701)

[**3.** **ALCANCE DEL PROGRAMA** 4](#_Toc120612702)

[**4.** **POLÍTICAS DE OPERACIÓN** 4](#_Toc120612703)

[**5.** **NORMATIVIDAD** 5](#_Toc120612704)

[**6.** **DEFINICIONES APLICABLES AL PROGRAMA** 6](#_Toc120612705)

[**7.** **MODELO DE REQUISITOS MÍNIMOS PARA EL PROGRAMA** 6](#_Toc120612706)

[**8.** **CARACTERISTICAS DEL PROGRAMA** 7](#_Toc120612707)

[**9.** **REQUISITOS DE ACCESO Y SEGURIDAD PARA EL SISTEMA SGDE** 8](#_Toc120612708)

[**10.** **COPIAS DE SEGURIDAD Y RECUPERACIÓN** 8](#_Toc120612709)

[**11.** **NIVELES DE SEGURIDAD Y ACCESO** 9](#_Toc120612710)

[**12.** **REQUERIMIENTOS FRENTE A LAS TABLAS DE RETENCION DOCUMENTAL (TRD)** 9](#_Toc120612711)

[**13.** **REQUISITOS DE CAPTURA** 9](#_Toc120612712)

[**14.** **REQUISITOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS** 10](#_Toc120612713)

[**15.** **FIABILIDAD** 12](#_Toc120612714)

[**16.** **INTEGRIDAD** 13](#_Toc120612715)

[**17.** **DISPONIBILIDAD** 15](#_Toc120612716)

[**18.** **TRANSFERENCIA DE DOCUMENTOS ELECTRÓNICOS** 16](#_Toc120612717)

[**19.** **METAS E INDICADORES DEL PROGRAMA** 16](#_Toc120612718)

[**20.** **DOCUMENTOS RELACIONADOS PARA LA EJECUCIÓN DEL PROCEDIMIENTO** 17](#_Toc120612719)

[**21.** **CONTROL DE CAMBIOS** 17](#_Toc120612720)

[**22.** **CONTROL DE FIRMAS** 17](#_Toc120612721)

# **INTRODUCCIÓN**

Dentro de los objetivos establecidos en la Unidad Administrativa Especial Cuerpo Oficial de Bomberos, se hace necesario ha diseñado el siguiente Programa de Normalización de Formas y Formularios para Documentos Electrónicos el cual permite realizar el análisis diplomático de los documentos cual sea su soporte, delimitando y fijando sus características y atributos, con el propósito de crear las formas, formatos y formularios, denominándolos con nombres propios; permitiendo con ello establecer la tradición documental, autenticidad, integridad, fiabilidad y disponibilidad de la tipología de los documentos, para facilitar la identificación, clasificación y descripción de los documentos.

Cada proceso institucional debe regirse por la unicidad de las formas y documentos que puedan hacer parte de procesos administrativos, internos y que se hacen indispensables en las acciones de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos con el fin de generar lineamientos claros que nutran el saber institucional y facilite el acceso, comprensión y desarrollo de cada acción emprendida.

# **OBJETIVOS**

# **OBJETIVO GENERAL**

Establecer acciones que permitan y aseguren el uso de los documentos internos y externos de forma unificada, controlada y actualizada, mediante un método estructurado y sistemático para la elaboración, edición, revisión, aprobación, manejo distribución, modificación y control de los documentos, con el fin de prevenir el uso no intencionado de documentos obsoletos en diversos aspectos dentro de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos, dando así cumplimiento y lugar a una adaptación exitosa de diversos estándares.

# **OBJETIVOS ESPECIFICOS**

▪ Realizar un análisis de la producción documental durante el ciclo de vida del documento y el tipo de soporte a fin de identificar las formas, formatos y formularios susceptibles de ser automatizados.

▪ Establecer las características de contenido y forma documental fija para los formatos y documentos electrónicos de la Unidad, de manera articulada con el Programa de Gestión Documental garantizando el cumplimiento de los requisitos establecidos en la normatividad vigente.

▪ Determinar y socializar las directrices de la producción de formatos, formularios y documentos electrónicos, para garantizar la disminución de copias físicas de documentos electrónicos contribuyendo al cumplimiento de la política Cero Papel de la UAECOB.

# **ALCANCE DEL PROGRAMA**

Dentro de la Unidad Administrativa Especial Cuerpo Oficial de bomberos, el siguiente Programa de Normalización de requisitos de Formas y Formularios para Documentos Electrónicos es un instrumento de referencia y validación de los sistemas de producción de documentos electrónicos que será implementado durante el ciclo vital en el manejo electrónico de documentos de archivo.

# **POLÍTICAS DE OPERACIÓN**

Es responsabilidad de cada líder de proceso:

* Consultar y verificar los nuevos documentos, como el presente programa, como parte fundamental del desarrollo de los procesos que hacen parte del área correspondiente a la asumida en el liderazgo.
* Socializar los documentos que aprueba, al personal que interactúa en el proceso.
* Notificar los elementos que crea convenientes para una aplicación de programa exitosa.
* Hacer cumplir los requisitos establecidos en los documentos aprobados.
* Revisar y/o actualizar la documentación asociada a los procesos en el marco del MIPG cada vez que se requiera, como mínimo cada 2 años.
* Es responsabilidad del Líder del Proceso revisar periódicamente la vigencia de la normatividad y documentos Externos aplicables.
* La organización de documentos producto de las actividades desarrolladas en este procedimiento deben quedar de acuerdo con las tablas de retención documental -TRD convalidadas.
* Los jefes de las dependencias de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos — UAECOB— son responsables por la producción, organización, trámite, consulta, conservación, custodia del archivo de gestión de su área o tema encomendado, y de la restricción de acceso a los documentos que tengan reserva legal, sin perjuicio de las responsabilidades señaladas en la Ley 1952 de 2019 para todos los Servidores Públicos y la Ley 594 de 2000 “Ley General de Archivos”.
* Todos los colaboradores de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos responden por la integridad, autenticidad, veracidad y fidelidad de la información a su cargo, y por la organización, conservación y custodia de los documentos, teniendo en cuenta la normatividad archivística vigente, sin perjuicio de las responsabilidades señaladas en la Ley 1952 de 2019 para todos los servidores públicos.
* Lo correspondiente a lo estipulado en las políticas de operación establecidas de comunicaciones oficiales en cuanto a producción y trámite de comunicaciones oficiales, sus tipos, radicación y distribución. GR-MN02, y la gestión de las mismas GR-PR20.
* Las firmas autorizadas para las comunicaciones oficiales son las designadas por el artículo segundo de la Resolución Interna No.453 de 2021.
* Para la elaboración de los documentos se debe tener en cuenta los lineamientos dados en la Guía de Elaboración y Control de Documentos GE-PR01-GA01.
* Para la elaboración, referido al contenido de los documentos, se debe tener en cuenta lo establecido en el procedimiento de información documentada GE-PR01 y la guía de Elaboración y Control de Documentos GE-PR01-GA01
* Un documento se considera parte del Sistema de Gestión y Desempeño cuando se encuentra publicado en la Página Web de acuerdo con el procedimiento de Información Documentada GE-PR01.

# **NORMATIVIDAD**

Se hace necesario partir de una base normativa aplicable para el Programa Normalización de requisitos de Formas y Formularios para Documentos Electrónicos, la cual se establece de la siguiente forma:

* Ley 594 de 2000, por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
* Decreto 1080 de 2015, Artículo 2.8.2.5.8. Instrumentos archivísticos para la gestión documental.
* Acuerdo 04 de 2013 AGN., por el cual se reglamentan parcialmente los decretos 2578 y 2609 de 2012, y se modifica el procedimiento para la elaboración, presentación, evaluación, aprobación e implementación de las Tablas de Retención Documental y las Tablas de Valoración Documental.
* Acuerdo 03 de 2015 AGN., por el cual se establecen los lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.
* Acuerdo 004 de 2019 AGN, por el cual se reglamenta el procedimiento para la elaboración, aprobación, evaluación y convalidación, implementación, publica- ción e inscripción en el Registro único de Series Documentales – RUSD de las Tablas de Retención Documental – TRD y Tablas de Valoración Documental – TVD
* ISO 15489 Información y documentación. Gestión de documentos.

# **DEFINICIONES APLICABLES AL PROGRAMA**

**Campo:** En informática es un registro, espacio usado para una categoría particular de datos (Real Academia Española de la Lengua, 2014). En las bases de datos un campo en la mínima unidad de información a la que se pueda acceder, un campo o un conjunto de ellos forman un registro.

**Formulario:** Un formulario es un documento, ya sea físico o digital, diseñado con el propósito de que el usuario introduzca datos estructurados como nombre, apellidos, dirección, teléfono, celular etc., en las zonas del documento destinadas para este propósito, para ser almacenados y procesados posteriormente. (Real Academia Española de la Lengua, 2014)

**Formulario electrónico:** Formatos que pueden ser diligenciados por cualquier ciudadano para realizar trámites en línea. Por ejemplo, Formularios para peticiones quejas y reclamos. (Archivo General de la Nación, 2012)

**Plantilla de Documentos:** Documento base sobre el cual se construyen varios documentos respetando su estructura y configuración. Los usuarios pueden ver siempre la versión más actualizada que ha sido normalizada al ver la última plantilla en uso.

# **MODELO DE REQUISITOS MÍNIMOS PARA EL PROGRAMA**

El programa se encuentra enmarcado en los requisitos que se pretenden para el Sistema de Gestión de Documentos Electrónicos (SGDE) que se encuentra en realización dentro de la entidad, además de que le da lugar a su conformación como tal. Se relacionarán un conjunto de aplicaciones que permitan la gestión de los documentos en formatos electrónicos y evidencien la trazabilidad y recuperación de los documentos de la entidad.

* Organizar los documentos físicos y electrónicos, según las Tablas de Retención Documental.
* Asignar metadatos de acuerdo con el Cuadro de Clasificación Documental, para la búsqueda y recuperación de los documentos.
* Incluir los tiempos de conservación a corto, mediano y largo plazo de los documentos electrónicos.
* Realizar la eliminación parcial o completa de los documentos electrónicos de archivo de acuerdo con los tiempos de retención establecidos en las tablas de retención documental (TRD).
* Garantizar la autenticidad de los documentos de archivo y la información conexa (metadatos) durante el ciclo de vida de los documentos electrónicos.
* Garantizar la integridad de los documentos electrónicos de archivo, mediante agrupaciones documentales, en series y subseries y las autorizaciones de modificaciones y la trazabilidad de adulteración.
* Garantizar la fiabilidad de los documentos electrónicos de archivo por sus creadores.
* Permitir la disponibilidad de los documentos electrónicos de archivo, cuando sean requeridos por los funcionarios, contratistas y la ciudadanía.
* Organizar los documentos electrónicos de archivo por series, subseries documentales según con la estructura orgánico-funcional de la Entidad.
* Realizar las migraciones correspondientes según las nuevas versiones de software y hardware para los diferentes soportes de almacenamiento electrónico existentes en el mercado para la recuperación y reproducción de la información en estos soportes magnéticos.

# **CARACTERISTICAS DEL PROGRAMA**

Dentro del desarrollo del programa se relacionan las características que se deben contemplar para la implementación del programa mediante los módulos del SGDE en la Unidad Administrativa Especial Cuerpo Oficial de Bomberos

**Conformidad:** Respaldar la gestión de la información disponible electrónicamente a partir de los procesos administrativos de la entidad.

**Interoperabilidad:** Permitir la interoperabilidad con los otros sistemas de información, a lo largo del tiempo, basado en el principio de neutralidad tecnológica, el uso de formatos abiertos y estándares nacionales o internacionales adoptados por las autoridades o instancias competentes.

**Seguridad:** Mantener la información administrativa en un entorno seguro.

**Adición de contenidos:** Agregados nuevos contenidos a los documentos, en forma de metadatos, sin que se altere la autenticidad, valor probatorio e integridad de los documentos.

**Diseño y funcionamiento:** Permitir la creación y captura de documentos con el fácil manejo para los usuarios, haciéndola tan simple como sea posible.

**Gestión Distribuida:** Ofrecer capacidades para importar y exportar masivamente los documentos agrupados en series, subseries, expedientes y metadatos asociados desde y hacia otros sistemas de gestión documental.

**Disponibilidad y acceso:** Asegurar la autenticidad, integridad, inalterabilidad, accesibilidad, interpretación y comprensión de los documentos electrónicos en su contexto original, así como su capacidad de ser procesados y reutilizados en cualquier momento.

**Neutralidad tecnológica:** Garantizar la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones para garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.

# **REQUISITOS DE ACCESO Y SEGURIDAD PARA EL SISTEMA SGDE**

El sistema de Gestión Documental Electrónico debe cumplir con los siguientes requisitos de seguridad para dar lugar al desarrollo exitoso de su intención:

* Permitir que el administrador restrinja el acceso a los documentos electrónicos de archivo, expedientes y metadatos a determinados usuarios o grupos de usuarios.
* Permitir que el administrador asocie al perfil del usuario ciertos atributos que determinarán las funciones, los campos de metadatos a los documentos electrónicos de archivo y los expedientes a los que el usuario tendrá acceso
* Permitir las mismas funciones de control para los perfiles y para los usuarios.
* Establecer grupos de usuarios asociados a un conjunto de expedientes o documentos electrónicos de archivo
* Permitir que un usuario pertenezca a más de un grupo.
* Permitir a los administradores la capacidad de establecer perfiles de usuarios y asignar usuarios a los grupos.

Por otra parte, al buscar un documento electrónico de archivo, volumen o expediente o solicita acceder a él sin tener derecho a consultarlo, el SGDE debe darle una de las siguientes respuestas que se seleccionarán cuando se configure el sistema:

* Visualizar los títulos y los metadatos de los documentos electrónicos de archivo.
* Reconocer la existencia del expediente o documento electrónico de archivo esto es, visualización del número del expediente o del documento de archivo, pero sin revelar su título ni ningún otro metadato.
* Ocultar toda información sobre el documento electrónico de archivo y de cualquier otra indicación que pueda sugerir su existencia.
* Realizar búsquedas de texto íntegro, nunca debe incluir en los resultados documentos electrónico de archivo a los que el usuario no tenga derecho a ac- ceder.
* Permitir que los usuarios intenten acceder a expedientes, volúmenes o documentos electrónico de archivo sin la autorización debida, debe quedar constancia de tales intentos en la pista de auditoría.

# **COPIAS DE SEGURIDAD Y RECUPERACIÓN**

Dentro de las acciones de respaldo y contingencia ante elementos de perdida que se puedan presentar, se hace necesario contar con protocolos de seguridad que involucre los siguientes tipos de copias de seguridad (Backups):

Copia de la programación de la aplicación SGDE Copia de la bodega de datos. De esta manera se garantizará que las copias de seguridad sean restablecidas desde diferentes posibles fallos que se puedan presentar.

La periodicidad de la información, que se registre y/o se almacene en la aplicación debe contar con una copia espejo garantizando que dicha copia se encuentre fuera de las instalaciones de la UAECOB garantizando su recuperación en caso de catástrofe.

# **NIVELES DE SEGURIDAD Y ACCESO**

Los niveles de seguridad del SGDE deben contar con las restricciones establecidas en el artículo 18 de la Ley 1712 de 2014 de transparencia el cual determina las excepciones que deben tener los documentos de carácter público. Los datos de acceso están relacionados con las Tablas de Control de Acceso.

# **REQUERIMIENTOS FRENTE A LAS TABLAS DE RETENCION DOCUMENTAL (TRD)**

El SGDE debe garantizar la conservación de los documentos electrónicos en cumplimiento del Acuerdo 004 de 2019 AGN con los tiempos de retención asignados y el soporte formato para cada tipo documental registrados en las Tablas de Retención Documental de la UAECOB.

De la misma manera el sistema debe cumplir con los siguientes requisitos:

* Asignar los tiempos de retención a los documentos por serie y subserie documentales establecidas en las Tablas de Retención Documental.
* Identificar los documentos electrónicos de archivo para la eliminación una vez se cumpla su periodo de retención en el archivo de gestión y archivo central por medio de la generación de inventario documental en el Formato Único de inventario documental FUID para publicación en la Página Web de la Entidad.
* Elaborar automáticamente inventarios de transferencias primarias y secundarias según los inventarios documentales y archivos electrónicos digitales para su conservación.
* Realizar las transferencias virtuales y/o alerta de transferencias automáticas al momento de cumplir con los periodos de retención establecidos en las Tablas de Retención Documental.
* Recuperar los expedientes de sistemas de archivo con búsqueda sencilla y estructurada que garantice la disponibilidad de la información.
* Soportar la búsqueda en texto completo de los documentos digitalizados asignándoles niveles de recuperación.

# **REQUISITOS DE CAPTURA**

El proceso de captura de documentos electrónico de archivo en el SGDE debe contar con los controles y la funcionalidad adecuados así:

* Registrar y gestionar todos los documentos electrónicos de archivo, con independencia del método de codificación empleado y de otras características tecnológicas.
* Garantizar que los documentos electrónicos de archivo se asocian con él un Cuadro de Clasificación Documental y a uno o más expedientes.
* Integrarse con el software de aplicaciones que genera los documentos electrónicos de archivo.
* Validar y controlar la entrada de metadatos en el SGDE.

# **REQUISITOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS**

Para un desarrollo exitoso del proceso, también se hace necesario establecer las características que deben tener un documento electrónico de archivo para su gestión y trámite en el sistema de archivos digitales, en este caso las tipologías y series documentales deben ser identificadas para determinar cuál es la forma idónea de producción y/o digitalización.

El primer nivel de información que se debe asociar a la gestión de documentos electrónicos de archivo está directamente relacionado con el valor probatorio que tenga un documento electrónico o digital con respecto del físico, por lo tanto, se debe identificar en las Tablas de Retención Documental cuando un documento es susceptible de digitalización y/o contiene valor probatorio.

Una vez identificados los tipos documentales de acuerdo con las Tablas de Retención Documental se procederá a establecer los mecanismos necesarios para la implementación de firmas digitales para los documentos electrónicos de archivo que por sus características sean requeridos.

Por otra parte, sobre los documentos electrónicos de archivo que se produzcan en la UAECOB en desarrollo de sus funciones estos deben cumplir con los elementos esenciales tales como: autenticidad, integridad, inalterabilidad, fiabilidad, disponibilidad y conservación, que garanticen que los documentos electrónicos mantienen su valor de evidencia a lo largo del ciclo de vida, incluyendo los expedientes mixtos (híbridos), digitales y electrónicos:

A continuación, se presentan las características que deben contener los documentos archivo según sea su soporte en cumplimiento de la Norma ISO 15489:

Autenticidad: Entendida como el efecto de acreditar que un documento es lo que pretende ser, sin alteraciones o corrupciones con el paso del tiempo. Es uno de los componentes que conforman la confianza del documento respecto al contexto, estructura y contenido:

Contexto: Tiene que ver con la actividad y con la entidad, por cuanto la actividad “per-se” sin un contexto administrativo identificable quedaría incompleta.

Estructura: Tiene que ver con la forma documental fija o la presentación del contenido, que en gran medida está dada por el software y hardware.

Contenido: La materia del documento. Tiene que ver con el entorno en el cual ha sido creado el documento de acuerdo con el marco jurídico, administrativo, procedimental y documental de la entidad, para lo cual se tendrán en cuenta los metadatos que permitan demostrar su procedencia.

Por lo anterior es importante que en un documento electrónico se pueda identificar:

* El software y hardware necesario para su representación.
* Que el documento es lo que afirma ser.
* La certeza sobre la persona que lo ha elaborado, enviado, firmado, o cuando exista evidencia respecto de la persona a quién se atribuya el documento.
* Que ha sido creado o enviado en el momento que se afirma.
* El documento electrónico es verídico y no ha sido alterado.

Requisitos para la presunción de autenticidad de los documentos electrónicos de archivo.

Se deben documentar e implementar procedimientos de seguridad y control durante todas las etapas del ciclo de vida del documento para evitar la pérdida o corrupción de los documentos de archivo o cualquier adición, supresión, modificación, utilización u ocultación no autorizadas, así como la protección de los medios de almacenamiento y la tecnología.

* Para el control de la creación, recepción, transmisión, mantenimiento, disposición y preservación de los documentos electrónicos de archivo, de manera que se asegure que los creadores de estos estén autorizados e identificados y que los documentos estén protegidos frente a cualquier adición, supresión, modificación, utilización u ocultación no autorizadas.
* Definir procedimientos para asegurar la cadena de preservación de los documentos electrónicos de archivo a lo largo del ciclo de vida, y en el transcurso del tiempo según con las Tablas de Retención Documental.

Para otorgar autenticidad a los documentos electrónicos de archivo el UAECOB puede hacer uso de las siguientes técnicas:

* **Estampas de tiempo:** Consiste en una secuencia de caracteres utilizada para certificar el momento específico en que se lleva a cabo un suceso sobre un documento electrónico o que éste no ha sido modificado en un espacio de tiempo determinado. La secuencia de caracteres está relacionada con la fecha y hora exacta en que ocurre dicho evento y específicamente cuando fue creado o firmado en un sistema de cómputo. Mediante la emisión de una estampa de tiempo es posible garantizar el instante de creación, modificación, recepción, firma de un determinado mensaje de datos impidiendo su posterior alteración, haciendo uso de la hora legal colombiana.
* **Firmas electrónicas**: Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.
* **Firmas digitales:** La firma digital se configura como un valor numérico que se asocia a un mensaje de datos y permite determinar que dicho valor ha sido generado a partir de la clave originaria, sin modificación posterior. La firma digital se basa en un certificado seguro y permite a la entidad receptora probar la autenticidad del origen y la integridad de los datos recibidos.

Como medida, en el marco de la conservación de los documentos electrónicos a largo plazo, se recomienda la actualización de la firma digital. Esta medida de control consiste en el resellado o la refirma, como medios para prevenir la obsolescencia o la vulneración del sistema de firma. La diferencia entonces es fundamentalmente probatoria, pues si bien la firma digital de manera automática incorpora la autenticidad, integridad y no repudio, en la firma electrónica es necesario probarla, además de determinar que se trata de un mecanismo confiable y apropiable. Si se trata de una firma biométrica electrónica o electrónica manuscrita, tendrá el mismo valor de una firma electrónica, siempre que cumpla con los requisitos exigidos por los arts. 3°8 y 5°9 del Decreto 2364 de 2012, sea o no emitida por una entidad certificadora. De lo contrario, si por ejemplo la firma es tomada en un “digital pad” y es fijada en un documento que es impreso, podrá ser tenida como una firma o rubrica común, impuesta mediante un mecanismo electrónico, es decir, una firma de puño y letra del autor, pero fijada, por decirlo así, con tinta electrónica.

* **Certificados digitales:** Los certificados digitales se conocen como una parte de la información que se asocia a un mecanismo para acreditar la validez de un documento perteneciente a un autor (autenticación), verificar que no ha sido manipulado ni modificado (integridad), al igual que impide que el autor niegue su autoría (no repudio) mediante validación de la clave pública del autor.
* **Código seguro de verificación (CSV):** Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente pueden tener la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

El Código seguro de verificación (CSV) es una comprobación de la autenticidad del documento ingresando un código alfanumérico en la sede electrónica correspondiente.

* **Marcas de agua digitales:** Corresponde a datos incrustados en documentos electrónicos tales como fotografías, películas, audios, y otros contenidos digitales y constituyen un medio seguro para certificar el origen, propiedad y autenticidad de los activos digitales.

# **FIABILIDAD**

Entendida como la capacidad de un documento para asegurar que su contenido es una representación completa, fidedigna y precisa de las operaciones, las actividades, los hechos que testimonia o se puede establecer, declarar o sostener el acto o hecho del que es relativo, determinando la competencia del autor y examinando tanto la completitud en la forma del documento como el nivel de control ejercido durante su proceso de producción.

Los requisitos para la presunción de fiabilidad de los documentos electrónicos deberán ser creados así:

* Dando testimonio de la operación o actividad que reflejan, declarando el acto o hecho del que es concerniente.
* Dando testimonio del lugar, estableciendo la competencia del autor.
* Dando certeza de estar completo en la forma del documento de archivo, incluyendo información de control de su producción.
* Manteniendo su identidad inequívoca, es decir los atributos de contexto y procedencia que le son propios, como evidencia electrónica de las transacciones, actividades o hechos a lo largo del tiempo.
* Mediante métodos seguros y verificables.
* Por individuos que dispongan de un conocimiento directo de los hechos o automáticamente por los instrumentos que se usen habitualmente para realizar las operaciones.

# **INTEGRIDAD**

Se puede entender como la cualidad de un documento electrónico de archivo para estar completo y sin alteraciones, con la cual se asegura que el contenido y atributos están protegidos a lo largo del tiempo. Es uno de los componentes que conforman la confianza del documento.

Requisitos para la presunción de integridad de los documentos electrónicos de archivo:

* Los documentos deben permanecer completos, protegidos contra modificaciones y alteraciones no autorizadas.
* Se deben especificar las adiciones o anotaciones pueden realizarse en un documento después de su creación, en qué circunstancias pueden autorizarse dichas adiciones o anotaciones y quién está autorizado para llevarlas a cabo. Cualquier anotación, adición o supresión autorizada que se realice en un documento debería indicarse de forma explícita y dejar traza.
* Analizar los casos especiales donde se puedan llevar a cabo estas actividades, los riesgos, las implicaciones jurídicas, dichas actividades deberá estar previamente autorizadas y documentadas.
* Conservar los metadatos de contexto, que den cuenta de la naturaleza procedimental, jurídica, administrativa y tecnológica (auditoria) que da origen al documento dándole la confiabilidad requerida.
* Mantener de manera permanente la relación entre el documento electrónico de archivo y sus metadatos.
* En caso de requerirse algún cambio por razones de obsolescencia tecnológica, preservación a largo plazo, se debe realizar por personal debidamente autorizado dejando evidencia en el documento (a través de metadatos) y en la documentación del procedimiento de los cambios realizados, conforme a reglas establecidas, limitadas y controladas por la entidad. (Esto debe previamente ser autorizado por una instancia de nivel decisorio; adicionalmente debe quedar reglamentado en el Sistema Integrado de Conservación.)
* Proporcionar y mantener pistas de auditoría u otros métodos de seguimiento que demuestren que los documentos de archivo están protegidos frente a la utilización, la modificación y la destrucción no autorizadas.
* Conservar los niveles de restricción de acceso, en caso de que el contenido de los documentos sea clasificado o reservado, según la Ley 1712 de 2014.
* Estas medidas de control pueden formar parte del sistema en el que se gestionan o producen los documentos o ser externas al mismo donde se pueda demostrar que la actualización, el mantenimiento habitual o cualquier fallo de funcionamiento del sistema no afectan a la integridad de los documentos.
* “La integridad de la información tiene que ver con que el contenido del documento transmitido por vía electrónica sea recibido en su integridad por el destinatario, tarea que puede cumplirse técnicamente utilizando el procedimiento conocido como “sellamiento” del mensaje, mediante el cual aquel se condensa de forma algorítmica y acompaña al mensaje durante la transmisión, siendo recalculado al final de ella en función de las características del mensaje realmente recibido; de modo, pues, que si el mensaje recibido no es exacto al remitido, el sello recalculado no coincidirá con el original y, por tanto, así se detectará que existió un problema en la transmisión y que el destinatario no dispone del mensaje completo. Incluso, la tecnología actual permite al emisor establecer si el receptor abrió el buzón de correo electrónico y presumiblemente leyó el mensaje”.

Esa característica guarda una estrecha relación con la “inalterabilidad”, requisito que demanda que el documento generado por primera vez en su forma definitiva no sea modificado, condición que puede satisfacerse mediante la aplicación de sistemas de protección de la información, tales como la criptografía y las firmas digitales.

Ejemplo: Un documento con criptografía solo puede ser visto por la persona que lo envió o lo recibió, y el destinatario puede verificar si el remitente es auténtico y si el documento ha sido modificado o alterado.

Mecanismos técnicos y tecnológicos de integridad:

Adicional a lo mencionado anteriormente, se debe establecer:

* Políticas y procedimientos para la administración de bases de datos, documentos electrónicos y demás registros de información.
* Integridad personal, responsabilidad, confianza del personal que maneja información sensible de la organización.
* Medidas de protección para evitar la pérdida o corrupción de los documentos de archivo y los medios de almacenamiento.
* Segregación de funciones, es decir asignar y monitorear los permisos de acceso a los datos y documentos electrónicos para que cada función tenga los privilegios que necesita y no abusen de los mismos. Este es un concepto de probada eficacia práctica, en el que seguramente harán hincapié las auditorías internas cuando se revisen sistemas y transacciones de carácter confidencial.
* Integridad en bases de datos, se establece desde la etapa de diseño de una base de datos mediante la aplicación de reglas y procedimientos estándar, y se mantiene a través del uso de rutinas de validación y verificación de errores. Esto incluye integridad de las entidades, la integridad de los dominios y la integridad referencial.

Para contribuir con la integridad en los documentos electrónicos la entidad pueden hacer uso de las siguientes técnicas:

* Controlar los privilegios y derechos de acceso para prevenir cambios no autorizados de la información.
* Autenticación, cuando se habla de la integridad del origen (Fuente de los datos). Ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.
* Parches de seguridad sobre el sistema operativo y software base para evitar mantener vulnerabilidades que puedan ser aprovechadas para afectar la integridad de los documentos electrónicos de archivo.

# **DISPONIBILIDAD**

Entendida en un documento electrónico de archivo, como la capacidad actual y futura de que tanto el documento como sus metadatos asociados puedan ser consultados, localizados, recuperados, presentados, interpretados, legibles, y por tanto estar en condiciones de uso.

Requisitos para la presunción de disponibilidad de los documentos electrónicos de archivo.

Cada documento deberá contener la información necesaria para identificar el contexto de las actividades administrativas que lo conforman y el vínculo archivístico, existentes entre los documentos de archivo y el expediente de acuerdo con lo establecido en las Tablas de Retención Documental (TRD).

La información debe estar disponible para consulta presente y en el futuro independientemente del sistema que la produjo, su estructura o medio de registro original.

Mantener el vínculo permanente entre el documento y sus metadatos.

Los documentos electrónicos y la información en ellos contenida, debe estar disponible en cualquier momento, mientras la entidad está obligada a conservarla, de acuerdo con lo establecido en las Tablas de Retención Documental (TRD).

# **TRANSFERENCIA DE DOCUMENTOS ELECTRÓNICOS**

Consiste en el proceso técnico, administrativo y legal mediante el cual se entregan, a los archivos centrales (transferencia primaria) o a los archivos históricos (transferencia secundaria), los documentos electrónicos de archivos que de conformidad con las tablas de retención documental han cumplido su tiempo de retención en la etapa de archivo de gestión o de archivo central respectivamente.

En cumplimiento de lo anterior la Unidad Administrativa deberá acoger los lineamientos emitidos por el Archivo General de la Nación para la generación de la transferencia de documentos electrónicos de archivo, de forma que se asegure su integridad, autenticidad, preservación y consulta a largo plazo.

Es importante destacar que el Archivo General de la Nación es el responsable de recibir las transferencias de los archivos de valor histórico en formato digital de entidades públicas del orden nacional del sector central de la Rama Ejecutiva, así como los organismos del orden nacional adscritos o vinculados a los ministerios, departamentos administrativos, agencias gubernamentales y superintendencias, para asegurar su protección, conservación y acceso a los ciudadanos.

# **METAS E INDICADORES DEL PROGRAMA**

Como meta estructural y transversal, se establece la actualización de las Tablas de Retención Documental como base, y respuesta a la vez, del desprendimiento de procesos, procedimientos y formatos correspondientes.

Tomando lo anterior como base, se establece:

* 1. Generar la articulación interna, requerida y necesaria, para poder establecer elementos de forma que procuren el cumplimiento del programa.
  2. Generar la articulación interna, requerida y necesaria, para poder establecer elementos de fondo que procuren el cumplimiento del programa.
  3. Generar la revisión interna de formas o formularios que no correspondan al programa en cuestión y que ya estén en uso dentro de la UAECOB.

Generar una priorización de las series o documentos que son base fundamental del desarrollo y proceder institucional, además que se implican de manera cotidiana.

Establecer un sistema o plataforma eficiente para la gestión, y demás conexos administrativos, de los documentos electrónicos identificados y establecidos.

# **DOCUMENTOS RELACIONADOS PARA LA EJECUCIÓN DEL PROCEDIMIENTO**

|  |  |
| --- | --- |
| **Código** | **Documento** |
| GR-PG01 | Programa de Gestión de Documental |
| GE-PR01 | Información documentada |
| GR-GA04 | Preservación Digital de Archivos |

# **CONTROL DE CAMBIOS**

|  |  |  |
| --- | --- | --- |
| **VERSIÓN** | **FECHA** | **DESCRIPCIÓN DE LA MODIFICACIÓN** |
| 01 | 24/01/2023 | Creación del Documento con accesibilidad |

# **CONTROL DE FIRMAS**

|  |  |  |
| --- | --- | --- |
| **Elaboró**  Juan Sebastián Párraga Abril | **Cargo**  Contratista de Gestión Documental | **Firmado Original** |
| **Revisó**  Yenis Alexandra Santamaría Mesa  Yecenia Cadena  Patricia Pacheco | **Cargo**  Líder de Gestión Documental  Contratista SGC  Contratista Mejora Continua de Oficina Asesora de Planeación  “Los arriba firmantes declaramos que hemos proyectado y/o revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales y/o técnicas vigentes aplicables a la Unidad Administrativa Especial Cuerpo Oficial de Bomberos y por lo tanto, lo presentamos para la firma del líder del proceso” | **Firmado Original** |
| **Aprobó**  Amalin Ariza Mahuad | Subdirector SGC | **Firmado Original** |