

– Guía –

Lineamientos para el uso de documentos electrónicos

En la contingencia generada por la emergencia sanitaria COVID-19



En Bogotá, nos cuidamos entre
todos, cuídate en casa.
#YoMeQuedoEnCasa

ALCALDÍA MAYOR DE BOGOTÁ
GESTIÓN PÚBLICA
Secretaría General

Alcaldesa Mayor de Bogotá
Claudia Nayibe López Hernández

Secretaria General
Margarita Barraquer Sourdis

Subsecretaria Técnica
Gloria Patricia Rincón Mazo

Alto Consejero Distrital de las TIC – ACDTIC
Felipe Guzmán Ramírez

Director Distrital de Archivo de Bogotá - DDAB
Álvaro Arias Cruz

Subdirector del Sistema Distrital de Archivos – SSDA
Julio Alberto Parra Acosta

Autores

Álvaro Arias Cruz, Director DDAB
Nelson Humberto León Acuña, Profesional Especializado
John Fredy Garzón Caicedo, Profesional Universitario
William Javier Patarroyo Baquero, Profesional Universitario

Colaboradores

Juan Carlos Parada Gallardo, Asesor Alta Consejería de TIC
María del Pilar Niño Campo, Profesional Alta Consejería de TIC
Nancy Angélica Rodríguez Marín, Profesional Universitaria
Marly Yolie Quintana Daza, Profesional Universitaria

Diseño y Diagramación

Juan Sebastián Torres Hernández, Profesional en comunicaciones



"Juntos – Seguros,
trabajamos con documentos electrónicos"

Tabla de Contenido

	Pág
Introducción	5
Alcance	7
Objetivos	8
I. Ambientes de trabajo seguro	9
II. Documentos electrónicos (E-Docs)	14
III. Autenticidad, integridad y fiabilidad de documentos electrónicos (E-Docs)	16
IV. Correos electrónicos	20
V. Documentos digitalizadas	23
VI. Plataformas de comunicación por Internet	25
VII. Ventanillas electrónicas	28
VIII. Almacenamiento de documentos electrónicos	30
Consideraciones finales	35
Glosario y lista de siglas	36
Bibliografía	38
Información adicional	42

Introducción

La Presente guía es un documento mediante la cual se establecen lineamientos técnicos para mitigar los riesgos asociados al uso documentos electrónicos en los ambientes de trabajo en casa en razón de la actual emergencia ocasionada por el COVID-19.

En vista a lo anterior, la Dirección Distrital de Archivo de Bogotá, en cumplimiento de las funciones asignadas mediante Decreto Distrital 425 de 2016⁽¹⁾, y el rol de Archivo General de Bogotá establecido en el Decreto Distrital 828 de 2018⁽²⁾ ha determinado la necesidad de elaborar la presente guía para orientar de manera urgente y temporal a las entidades y organismos del distrito en materia del uso de documentos electrónicos en ambientes de trabajo en casa. Cabe anotar que estas medidas si bien son temporales, una vez superada la emergencia se le deben dar continuidad a su aplicación.

Con el fin de propiciar un canal seguro para la conectividad y Gestión de Documentos Electrónicos de Archivo en condiciones de trabajo en casa y/o teletrabajo, se realizan una serie de recomendaciones con respecto al uso adecuado de canales electrónicos haciendo énfasis sobre la implementación de herramientas para seguridad informática, lo cual permitirá mitigar riesgos asociados al uso indebido y pérdida de información durante la gestión de Documentos Electrónicos de Archivo.

Así mismo, mediante el presente documento se socializa lineamientos para la producción de Documentos Electrónicos de Archivo garantizando características como su autenticidad, integridad, y fiabilidad y no repudio por parte de sus autores. Bajo las anteriores premisas se imparten lineamientos para el uso de firmas electrónicas, digitales, hash de archivos y otros mecanismos criptográficos.

1 | COLOMBIA. ALCALDÍA MAYOR DE BOGOTÁ, D.C. Decreto 425 de 2016. (03, octubre, 2016). Por medio del cual se modifica la Estructura Organizacional de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=67103>>

2 | COLOMBIA. ALCALDÍA MAYOR DE BOGOTÁ, D.C. Decreto 828 de 2016. (27, diciembre, 2018). Por el cual se regula el Sistema Distrital de Archivos y se dictan otras disposiciones [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=82128>>

En cuanto a correo electrónico, es necesario que las entidades distritales implementen medidas para su gestión como Documentos Electrónicos de Archivo teniendo en cuenta un uso adecuado herramientas complementarias como firmas digitales, mecanismo de encriptación y funciones como la confirmación de envío y lectura. Adicionalmente, se podrá utilizar servicios de correo electrónico certificado, siempre y cuando se de cumplimiento a la normativa vigente.

Con el fin de continuar prestando el servicio de radicación en las entidades y no afectar la continuidad en la prestación de servicios, se deberán implementar medidas para la conformación de ventanillas únicas electrónicas dando cumplimiento a lo estipulado Capítulo 7 del Decreto Nacional 1413 de 2017⁽³⁾ y el Acuerdo 060 de 2001⁽⁴⁾ del Archivo General de la Nación (AGN).

3 | COLOMBIA. PRESIDENCIA DE LA REPUBLICA. MINISTERIO DE HACIENDA., et al. Decreto 1413 de 2017. (25, agosto, 2017). Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales. [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=70951>>

4 | COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 060 de 2001. (30, octubre, 2001). por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas [en línea]. Disponible en: <<https://normativa.archivogeneral.gov.co/acuerdo-060-de-2001/>>

Alcance

La presente guía está dirigida a las entidades y organismos del distrito para implementar medidas en el uso de canales electrónicos y la gestión de documentos electrónicos en ambientes de trabajo en casa o teletrabajo en razón de la actual emergencia ocasionada por el COVID-19.

Así mismo, estas medidas y/o recomendaciones aplican a documentos que hoy requieren firma, contrafirma, coofirma y/o revisión o aprobación manuscrita; comunicaciones oficiales, correo electrónico y otros documentos que las entidades de acuerdo con sus necesidades, procedimientos y Programa de Gestión Documental-PGD u otros instrumentos archivísticos establezcan como documentos de archivo.

Objetivos

Objetivo General

Establecer y socializar a las entidades y organismos del distrito lineamientos, medidas y recomendaciones para el uso de canales y ambientes electrónicos seguros para la producción y gestión de Documentos Electrónicos de Archivo auténticos, íntegros y fiables durante el trabajo en casa o teletrabajo debido a la emergencia causada por el COVID-19.

Objetivos específicos

- Formular lineamientos para el uso de canales y ambientes electrónicos garantizando su adecuado uso y seguridad durante la gestión de Documentos Electrónicos de Archivo.
- Establecer medidas y lineamientos para la producción de Documentos Electrónicos de Archivo para garantizar su autenticidad, integridad, fiabilidad, disponibilidad y no repudio durante la emergencia causada por el COVID-19.
- Orientar a las entidades para la creación de Ventanillas Electrónicas con el fin de asegurar la continuidad del servicio de radicación de Comunicaciones oficiales acorde a lo establecido en el Acuerdo 060 de 2001⁽⁵⁾ del Archivo General de la Nación-AGN y lo estipulado en el Capítulo 7 del Decreto 1413 de 2017⁽⁶⁾.

5 | COLOMBIA. PRESIDENCIA DE LA REPUBLICA. MINISTERIO DE HACIENDA., et al. Decreto 1413 de 2017. (25, agosto, 2017) Op. Cit.

6 | COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 060 de 2001. Op. Cit.



I. AMBIENTES DE TRABAJO SEGURO



Ambientes de trabajo seguro

1.) Condiciones deseables para propender por un ambiente seguro en condiciones de trabajo en casa y/o teletrabajo.

En razón a la instrucción de establecer jornadas de trabajo en casa por parte de los servidores públicos haciendo énfasis en el uso de tecnologías de información y comunicación, en esta etapa de contingencia por el Covid -19 se ha determinado la necesidad de orientar de manera urgente a las entidades y organismos del distrito en materia del uso de documentos electrónicos.

Es por ello que deben tenerse en cuenta unas condiciones deseables para propender por un ambiente seguro de trabajo en casa y/o teletrabajo.

Con atención a lo anterior, las oficinas de tecnologías de la información de las entidades, con el fin de facilitar las actividades de teletrabajo, deben:



Oficina T.I.C

- Disponer de herramientas de conexión y canales virtuales seguros acordes con la arquitectura tecnológica institucional para asegurar el ambiente de trabajo.
- Definir los lineamientos para el aseguramiento del ambiente de trabajo.
- No sobre cargar los canales con conexiones, servicios o tareas innecesarias.



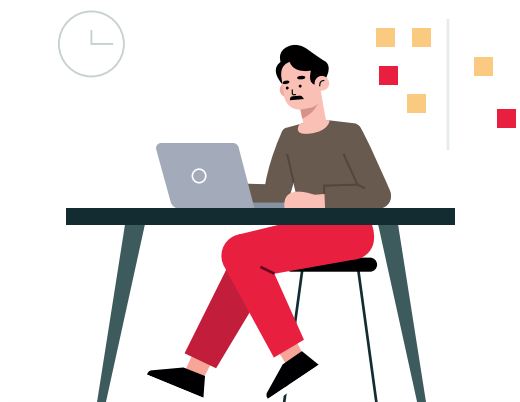
- Establecer cuáles son los datos que requieren mayores niveles de protección. Es primordial realizar la gestión adecuada de los roles, pues la información solo debería ser accesible para los perfiles de usuario que realmente necesiten visualizarla o modificarla.
- Conocer y poner en práctica la política de seguridad de la información de la entidad. Además de determinar los deberes y responsabilidades de los funcionarios, contratistas o terceros. Se recomienda que antes de entrar en temas técnicos como configuraciones, o salvaguardas para la información, ante un escenario de teletrabajo se debe establecer un marco normativo interno con el fin de estandarizar el modo y las condiciones bajo las cuales la dirección desea que se desarrolle el teletrabajo. Para aquellas entidades que aún no tengan adelantada dicha actividad, se deja a disposición el link con los documentos metodológicos de seguridad y privacidad de la información elaborados por la Alta Consejería TIC que les pueden servir como referencia.
<http://ticbogota.gov.co/seguridad>.
- Hacer uso de soluciones de seguridad actualizadas en los posible: Desde luego, uno de los puntos más fundamentales a la hora de proteger la información es tener un software de seguridad actualizado para que proteja la información de posibles amenazas, por consiguiente, configurar la ejecución y actualización periódica del antivirus.

En lo que corresponde a los servidores públicos, para el trabajo en casa y/o teletrabajo éstos deben:

- Contar con un antivirus y un firewall instalado, actualizado y activo, estos normalmente están incluidos en la suite de seguridad. Si no cuenta con uno, deberá descargarlo de un sitio seguro e instalarlo asegurándose que sea compatible con el equipo y sistema operativo. Muchos de ellos son gratuitos.
 - Conectarse a redes confiables, es decir, procurar no conectarse desde sitios públicos como café internet o desde la red de un vecino e incluso redes públicas.
 - Hacer uso adecuado de los canales y herramientas habilitados para desarrollar las actividades laborales evitando la sobrecarga de la red, esto es por ejemplo: evitar la descarga de
-



archivos o reproducción de contenidos que no sean necesarios para su trabajo, evitar el cargue o descargue e incluso la reproducción de videos a través de estos canales y utilizar el correo para reemplazar mensajería instantánea, entre otros casos.



Trabajador en casa

- Procurar el uso de servicios VPN (red privada virtual) de acuerdo con los lineamientos y protocolos emitidos por la Alta Consejería Distrital de las TIC- ACDTIC, toda vez que esto permite mayor seguridad al acceder a la infraestructura institucional.
- Cerrar adecuadamente las sesiones en las plataformas y herramientas utilizadas y no revelar usuarios y contraseñas a terceros.
- No descargar archivos que generen dudas, los cuales pueden ser propagación de ciberataques, antes de descargar un archivo evalúe su procedencia.
- No abrir link o descargar archivos de redes sociales o correos electrónicos que no sean de fuentes conocidas u oficiales.



Riesgo de seguridad



Medidas técnicas de seguridad recomendadas

Adicionalmente la Alta Consejería Distrital de las TIC, recomienda tener en cuenta lo siguiente:

- **Uso de llaves SSH.** Par de llaves criptográficas para autenticarse en un servidor SSH, este método alternativo al uso de contraseñas, requerirá la creación de una llave pública y una privada la cual es llevada a cabo como un paso anterior a la autenticación. La llave privada debe ser conservada por el usuario de manera secreta y segura, mientras que la llave pública puede ser compartida con otros usuarios sin restricción.



- **Infraestructura de llaves públicas y encriptación SSL/TLS** La Infraestructura de Llaves Públicas o PKI, por su sigla en inglés, se refiere a un sistema diseñado para crear, administrar y validar certificados que identifiquen individuos y encripta la comunicación. Los certificados SSL o TLS pueden ser usados para autenticar diferentes entidades entre sí. Cuando la autenticación se ha llevado a cabo, también pueden ser usados para establecer una comunicación encriptada.
- **Disponer de un software Cortafuegos** con el cual se puedan controlar los servicios que se encuentren expuestos a la red, bloqueando o restringiendo el acceso . Es decir, que bloquean o restringen el acceso a todo puerto exceptuando únicamente aquellos que deben estar habilitados para el público.
- **VPN y redes privadas.** Las redes privadas son las redes que se encuentran habilitadas únicamente para ciertos usuarios o servidores. Es una de las formas de crear conexiones seguras entre computadores remotos, presentándose como si éstos se encontraran en una red privada local.



II. DOCUMENTOS ELECTRÓNICOS (E-DOCS)

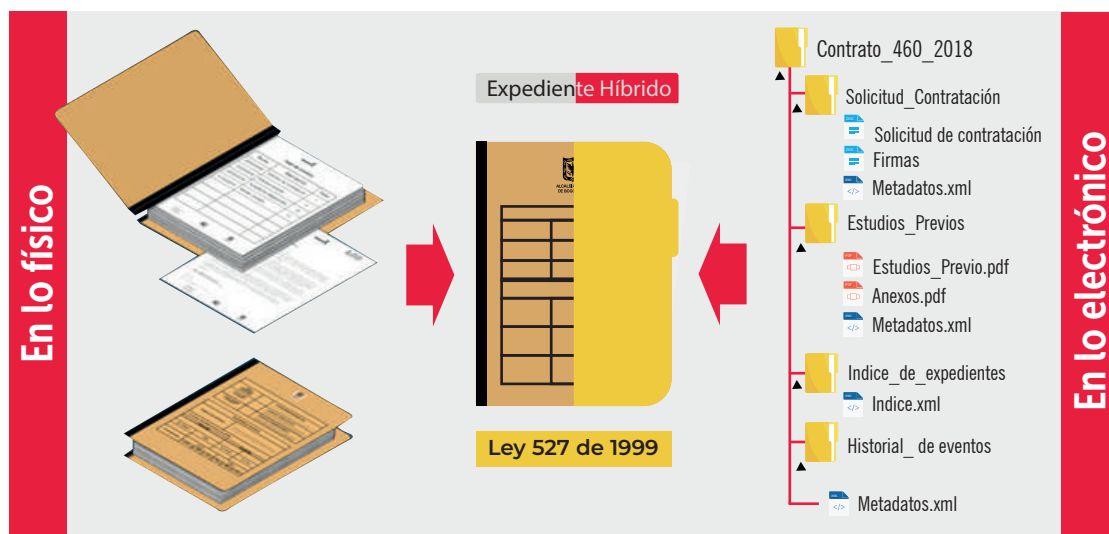


Documentos electrónicos (E-Docs)

Se entiende por documento electrónico de archivo “al registro de información generada, producida o recibida o comunicada por medios electrónicos, que permanece almacenada electrónicamente durante todo su ciclo de vida, producida, por una persona o entidad en razón a sus actividades o funciones, que tiene valor administrativo, fiscal, legal, ó valor científico, histórico, técnico o cultural y que debe ser tratada conforme a los principios y procesos archivísticos”⁽⁷⁾.

Por ello en la situación de emergencia actual y en aplicación del principio de equivalencia funcional en aquellos casos en que las normas así lo permitan⁽⁸⁾, los documentos electrónicos de archivo:

- Pueden producirse y/o capturarse en cualquier formato electrónico, asegurando que se trate de formatos sin obsolescencia tecnológica o que estén en desuso. En este sentido pueden utilizarse formatos como .pdf, .docx, xlsx o los que se hayan definido dentro del Programa de Gestión Documental o en el Plan de Preservación Digital de la Entidad.
- Deben incorporarse a los respectivos expedientes electrónicos, físicos o híbridos según sea el caso, así sea una vez se supere la emergencia.



7 | COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 002 de 2014. (14, marzo, 2014). Por medio del cual se establecen los criterios básicos para creación, conformación, organización, control y consulta de los expedientes de archivo y se dictan otras disposiciones [en línea]. Artículo 3º. Disponible en: <<https://normativa.archivogeneral.gov.co/acuerdo-002-de-2014/>>

8 | COLOMBIA. PRESIDENCIA DE LA REPUBLICA Y MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Ley 527 de 1999 (18, agosto, 1999). por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276>>



III. AUTENTICIDAD, INTEGRIDAD Y FIABILIDAD DE DOCUMENTOS ELECTRÓNICOS (E-DOCS)



Autenticidad, integridad y fiabilidad de documentos electrónicos (e-Docs)



Con el fin de mitigar riesgos sobre la autenticidad, integridad y fiabilidad de los documentos y procurando garantizar que estos no sean repudiados en virtud a posibles modificaciones por parte del creador y/o emisor ni por el receptor y/o destinatario, las entidades del distrito deberán establecer las medidas viables y bajo los recursos disponibles para el aseguramiento de tales características

De esta forma, uno de los métodos que coadyuvan a otorgar confiabilidad a los documentos electrónicos es la firma electrónica, la cual es definida legalmente en el Decreto 1074 de 2015 a través del artículo 2.2.2.47.1⁽⁹⁾ como:

“Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permiten 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”.

Ahora bien, el método de firmado electrónico adoptado por una entidad debe ser confiable y apropiado, en virtud al contexto legal y de producción de los documentos, así mismo, que dicho método permita identificar de manera inequívoca al creador de un documento con el fin de certificar su contenido.

Con base en lo expuesto, se observa que las firmas electrónicas confiables están compuestas por datos o códigos que identifican de manera segura al productor de un documento y que a partir de su uso es posible identificar posibles modificaciones o alteraciones no autorizadas al documento luego de haberse firmado.

La normativa colombiana contempla dos tipos de firmas las electrónicas y las digitales. En el primer caso, hace referencia a la idea más general de firma y la define como “métodos tales como contraseñas, datos biométricos o claves criptográficas privadas que permite identificar a una persona en relación con un mensaje de datos...”, por otra parte, la firma digital se considera como una especie de la firma electrónica definida como “un valor numérico que se adhiere a un mensaje de datos y que se genera utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje...”

En este contexto, con el fin de mitigar riesgos sobre la autenticidad, integridad y fiabilidad de los documentos y procurando garantizar que estos no sean repudiados las entidades y organismos distritales pueden implementar:



- ✓ Firmas electrónicas.
- ✓ Firma digitales.
- ✓ Mecanismos criptográficos.
- ✓ Plataformas de firmas gratuitas o licenciadas.



Oficina T.I.C

- ✓ Avala uso de firmas gratuitas o licenciadas.
- ✓ Asigna y custodia firmas o certificados digitales desarrollados por la propia entidad.
- ✓ Define lineamientos.
- ✓ Brinda apoyo.



Digitalizada o
escaneada



**Firma autógrafa mecánica,
Firma digitalizada o escaneada**

No se recomienda, ya que el uso de imágenes digitales de la firma autógrafa insertadas en el documento no cumple con las especificaciones de firma electrónica señaladas en la Ley 527 de 1999.

Ahora bien, bajo las actuales circunstancias de trabajo virtual y teletrabajo se debe contemplar que los documentos electrónicos se mantengan íntegros y auténticos, y de otro lado asegurar el no repudio ⁽¹⁰⁾.

De acuerdo con el artículo 11 del Decreto Nacional 491 de 2020 ⁽¹¹⁾ se establece la posibilidad de usar firma autógrafa mecánica, digitalizada o escaneada, indicando que cada autoridad es responsable de garantizar la seguridad de los documentos que se firmen por estos medios. Sin embargo, debe tenerse en cuenta que la inserción de una imagen de la firma autógrafa en los documentos, por sí misma, no hace que el documento goce de confiabilidad, en ese sentido, se recomienda que, para aquellas actuaciones que así lo requieran, las entidades definan un proceso para la firma electrónica que garantice el cumplimiento de los requisitos como autenticidad, e integridad, de tal manera que con ello se aseguren la confiabilidad, y seguridad jurídica de las actuaciones que se adelanten por medios electrónicos, esto de acuerdo a la normatividad vigente (artículo 7 de la Ley 527 ⁽¹²⁾ de 1999, reglamentado por el Decreto 2364 de 2012⁽¹³⁾ , el artículo 6 de la Ley 962 de 2005⁽¹⁴⁾ y artículo 53 y ss de la Ley 1437 de 2011⁽¹⁵⁾)

Por otra parte, se podrá implementar firmas electrónicas, digitales, hash de archivos, códigos seguros de verificación CSV y otros mecanismos criptográficos, entre otros, según sea requerido y previo aval de la oficina de TI de cada entidad.

10 | El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Existirán por tanto dos posibilidades: 1. No repudio en origen: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. 2. No repudio en destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción." Véase: <https://www.sede.fnmt.gob.es/preguntas-frecuentes/otras-preguntas/asset_publisher/1RphW9leUoAH/content/1034-que-significa-no-repudio-o-irrenunciabilidad-?inheritRedirect=false>

11 | COLOMBIA. PRESIDENCIA DE LA REPUBLICA. Decreto 491 de 2020. (28, marzo, 2020). Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica, Social y Ecológica [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=91670>>

12 | COLOMBIA. PRESIDENCIA DE LA REPUBLICA Y MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Ley 527 de 1999 (18, agosto, 1999). Op. Cit.

13 | COLOMBIA. PRESIDENCIA DE LA REPUBLICA Y MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 2364 (22, noviembre, 2012). Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50583>>

14 | COLOMBIA. CONGRESO DE COLOMBIA. Ley 962 de 2005. (8, julio, 2005). por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=17004>>

15 | COLOMBIA. CONGRESO DE COLOMBIA. Ley 1437. (18, enero, 2011) Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=41249>>



IV. CORREOS ELECTRÓNICOS (E-MAIL)



Correos electrónicos (E-mail)

El correo electrónico es considerado documento electrónico de archivo siempre que sea utilizado como comunicación oficial interna o externa o haga parte de un trámite en el cumplimiento de las funciones de la entidad, por tanto:



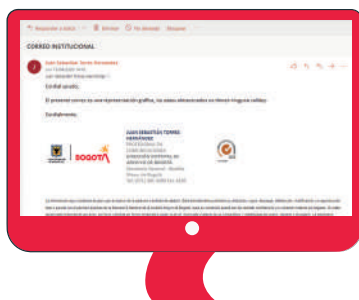
- Preferentemente se debe utilizar el correo institucional para el desarrollo de las funciones institucionales.
- Si cuenta con un servicio de correo electrónico certificado, este se usará con normalidad de acuerdo con el proveedor del servicio.
- Los correos electrónicos deben salir de las cuentas de los funcionarios que tengan autorizado el firmado de documentos de acuerdo con las políticas de cada entidad. Esto en el caso de tratarse de comunicaciones oficiales internas y enviadas, y aquellos correos que se constituyan como documento electrónico de archivo.
- En cuanto sea posible, los correos electrónicos deben ser radicados, aún si no se tiene la posibilidad de integrar el Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA o herramienta de radicación con la plataforma de correo, se deberán establecer mecanismos para la radicación según lo definido en el artículo quinto del Acuerdo 060 de 2001 expedido por el Archivo General de la Nación.



- Los correos electrónicos podrán ser firmados digitalmente y encriptados si es el caso, como mínimo se deberán habilitar las confirmaciones de entrega y lectura.
- En los casos que corresponda los correos deben ser radicados.
- Se deben establecer mecanismos para su radicación de acuerdo con el Acuerdo 060 de 2001⁽¹⁶⁾ del Archivo General de la Nación.
- Al igual que los documentos electrónicos y los físicos estos pueden ser archivados, atendiendo los cuadros de clasificación y tablas de retención del a entidad

Importante

Una impresión en papel, pdf o una captura de pantalla no reemplazan el correo original en su formato nativo, ya que esta operación puede perder entre otros los datos relacionados la producción y transmisión del mensaje. Sin embargo es de anotar que estos podrían tener valor como prueba dentro de un proceso administrativo o judicial.





V. DOCUMENTOS DIGITALIZADOS

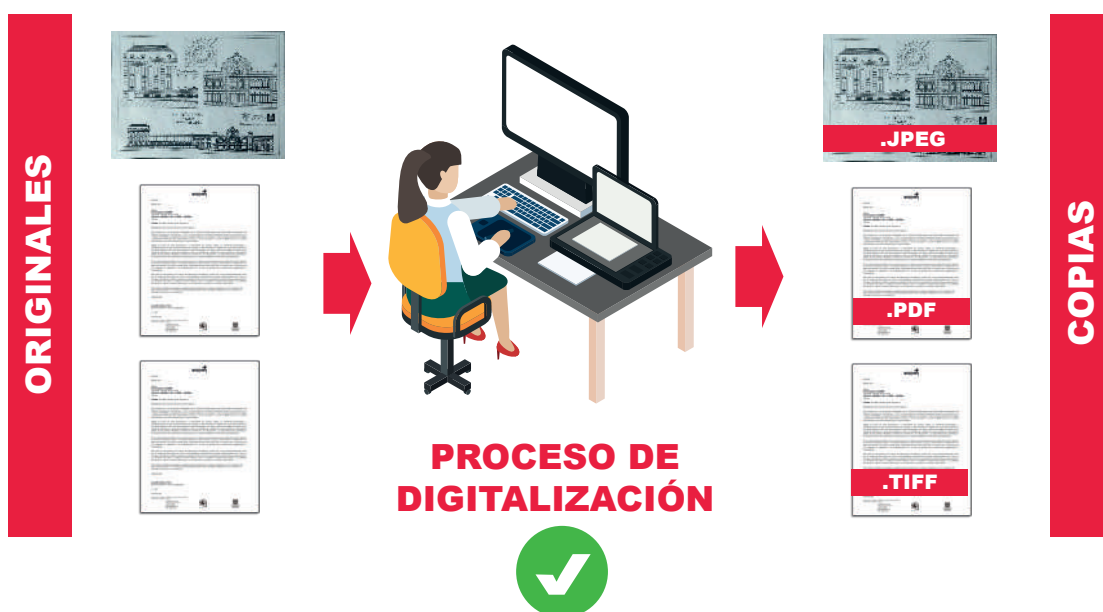


Documentos digitalizados

En virtud de lo señalado en el párrafo de artículo 18 del Acuerdo 003 de 2015⁽¹⁷⁾ Archivo General de la Nación.

X

Los documentos digitalizados no serán considerados como documentos electrónicos originales ni reemplazarán a los físicos originales.



La digitalización de documentos físicos se realizará con el fin de agilizar trámites durante la emergencia, una vez superada, los documentos originales, es decir en papel, deberán ser remitidos a las respectivas oficinas para su incorporación en los expedientes que corresponda.



Digitalizar no es sinónimo de eliminar o destruir el documento físico original, ni de reducir o ampliar los tiempos de retención documental, con lo que una entidad que haga uso de esta tecnología deberá garantizar los espacios de conservación de los documentos físicos y aplicar los tiempos que por TRD se han establecido.

17 | COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 003 de 2015. (17, febrero, 2017). Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012 [en línea]. Disponible en: <<https://normativa.archivogeneral.gov.co/acuerdo-003-de-2015/>>



VI. PLATAFORMAS DE COMUNICACIÓN POR INTERNET



Plataformas de comunicación por Internet

Con motivo de la situación especial que se está viviendo, las entidades pueden habilitar todos los canales de comunicación disponibles, entre los que se encuentran cuentan: **Chat (mensajería instantánea), Video Chat, Video Conferencias.**

! Chat (mensajería instantánea)

Los chats, video chats, entre otros, no se constituyen como documento electrónico de archivo toda vez que son plataformas de comunicación y adicionalmente no se cuenta con los mecanismos para su captura y gestión, garantizando su autenticidad, integridad, fiabilidad y disponibilidad, ni su preservación.

Las impresiones en papel o pdf o las capturas de pantalla de los chats, no se constituyen como documento electrónico de archivo y no reemplazan al chat en su forma nativa. Sin embargo, es de anotar que estos podrían tener valor como prueba dentro de un proceso.



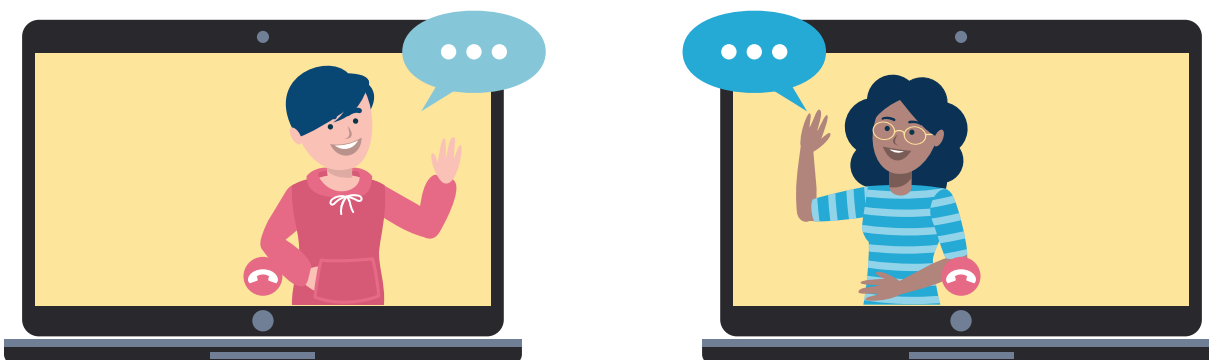
! Videoconferencia



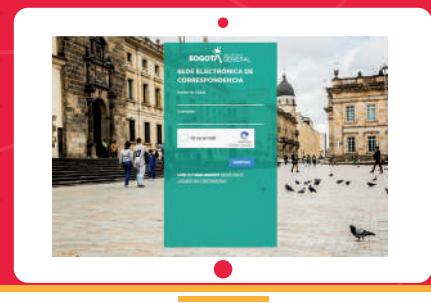
- Las video conferencias, video llamadas y similares no se constituyen como documento electrónico de archivo en razón a que no se cuenta con los mecanismos para su captura y gestión.
- Las grabaciones podrían ser consideradas como documento siempre y cuando se capturen en su formato electrónico original y se atienda lo señalado en las normas vigentes y los lineamientos dados en la presente circular. Deberá tenerse en cuenta en todo caso las normas de protección de datos personales y las autorizaciones requeridas en caso de grabar video conferencias.



- Las impresiones en papel o pdf o las capturas de pantalla, no se constituyen como documento electrónico de archivo y no reemplazan al chat en su forma nativa, toda vez que pierden, entre otros, sus datos de transmisión y sus impresiones son susceptibles de sufrir modificaciones por eliminación de mensajes.
- Es importante asegurarse que en la video conferencia no hayan intrusos o dependiendo de la importancia de los temas convocar solo a las personas requeridas.



VIDEOCONFERENCIA



VII. VENTANILLA ELECTRÓNICA



Ventanillas electrónicas

Emulando las condiciones del ambiente físico en el que se establecen las unidades de correspondencia ⁽¹⁸⁾, las cuales gestionan de manera centralizada y normalizada, los servicios de recepción, radicación y distribución de sus comunicaciones; se establecen las Ventanillas en ambiente electrónico, cumpliendo las mismas funcionalidades que sus pares físicos.

Estas Ventanillas Electrónicas, hacen parte de los servicios que las entidades deben implementar en lo que la Ley 1437 de 2011⁽¹⁹⁾ a través de su artículo 60 denomina “sedes electrónicas”.

Para su implementación las entidades y organismos del distrito deben:



En caso de no contar actualmente con una ventanilla electrónica, habilitar una cuenta de correo electrónico para recibir y enviar comunicaciones oficiales observando lo dispuesto en el artículo 61 del Ley 4137 de 2011⁽²⁰⁾ y los lineamientos de la política de Gobierno Digital.

Publicar a través de la página oficial de la institución u otros medios de comunicación oficiales, los horarios y las condiciones del servicio.

Garantizar la igualdad de acceso y habilitar los medios y procedimientos necesarios para que los ciudadanos se registren y puedan realizar sus tramites, particularmente los de radicación de correspondencia.

18 | COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 060 de 2001. Artículo 3 Op. Cit.

19 | COLOMBIA. CONGRESO DE COLOMBIA. Ley 1437. (18, enero, 2011) Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo [en línea] Artículo 60. Disponible en: <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=41249>

20 | Ibid. Artículo 61.



VIII. ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS



Almacenamiento de documentos electrónicos

La producción de documentos electrónicos al igual que los físicos, implican la necesidad de contar con unidades de almacenamiento adecuadas para garantizar su conservación o preservación.

Dicho esto, las entidades deben implementar sistemas de almacenamiento que les garanticen la protección y disponibilidad de los documentos, en este sentido es necesario tener en cuenta:

Desde las Oficinas de Tecnologías de la entidad y con el apoyo de los ingenieros de sistemas, se deben garantizar:

- Espacios seguros de almacenamiento.
- Formulación e implementación de políticas y lineamientos para almacenamiento de documentos electrónicos.
- En concordancia con lo señalado en el artículo 17 del Acuerdo 003 de 2015⁽²¹⁾ del Archivo General de la Nación, para el almacenamiento de los Documentos Electrónicos de Archivo, las áreas de Gestión Documental deberán coordinarse con las áreas de TIC de cada entidad, para asegurar los servicios tecnológicos necesarios, las condiciones de seguridad propicias de acuerdo a las políticas de seguridad y privacidad de la información de cada entidad y la conectividad para los usuarios de cada dependencia en trabajo en casa.

Oficina T.I.C



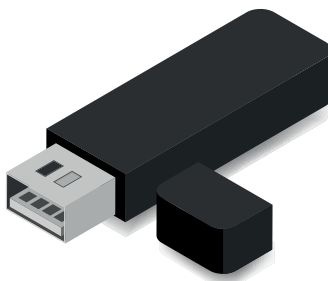
Gestión Documental



- Es posible hacer uso de diversos medios de almacenamiento tales como servidores locales, servicios de almacenamiento en nube, data center, sistemas de almacenamiento como NAS y SAN, entre otros.
- Los documentos catalogados como confidenciales pueden ser almacenados en herramientas como OneDrive – Google drive, siempre y cuando sean contratadas de forma institucional.
- Para el caso de uso de servicios en nube y correo electrónico, es necesario realizar la descarga de los documentos electrónicos de archivo incluyendo adjuntos referenciados, anexos, entre otros, para su integración a los respectivos expedientes respectivos.



En casos especiales, donde se requiera el uso de almacenamiento extraíble (USB, Tarjetas SD, MicroSD, entre otros) dado los altos riesgos asociados con su transporte y conexión en otros equipos, se recomienda su encriptado en función de la sensibilidad y criticidad de los documentos a almacenar.



La clasificación, ubicación e identificación de los documentos es primordial para garantizar el acceso y fácil recuperación de los mismos, es por esto que:

- Los documentos electrónicos de archivo se deben clasificar mediante una estructura de almacenamiento multinivel según el Cuadro de Clasificación Documental.
- La identificación de directorios y archivos (objetos digitales), deberá ser estandarizada y codificada para evitar y minimizar errores en procesos de migración, transferencia, backup, restauración del sistema, entre otros. Es recomendable el uso de nombres cortos y significativos y evitar espacios y caracteres especiales.
- Es importante recordar que una dirección o ruta de acceso a un objeto digital esta limitada a



ESTRUCTURA DEL DIRECTORIO		CARACTERES NOMBRE
	 INSTANCIA ALMACENAMIENTO SERVIDOR	5 a 30
NIVEL 1	 DEPENDENCIA	5 a 30
NIVEL 2	 SERIE	5 a 30
NIVEL 3	 SUBSERIE	5 a 30
NIVEL 4	 EXPEDIENTE O CARPETA	5 a 30
	 DOCUMENTOS	5 a 30



| Foto Archivo de Bogotá |

Consideraciones finales

Por último, es imprescindible al terminar las labores:

- Cerrar todas las conexiones con servidores y páginas web utilizando cuando sea posible la opción “desconectar” o “cerrar sesión”.
 - Eliminar información temporal prestando especial atención a la carpeta de descargas, papelera de reciclaje, o posibles carpetas perdidas que se dejen en “Mis documentos”.
 - Se recomienda no hacer copia local de la información sino hacer uso de herramientas colaborativas dispuestas por la entidad.
 - Utilizar herramientas de borrado seguro para eliminar los activos de información sensible o especialmente confidencial que hayan sido usados de forma local.
 - Si se han utilizado certificados digitales, estos deben ser borrados de forma segura. Asegurarse de retirar cualquier memoria USB, CD, o medio externo que se haya utilizado en el equipo.
 - Borrar el histórico de navegación, así como las cookies, y otros datos del navegador web, prestando especial atención a las contraseñas recordadas.
 - Si va a hacer uso de información crítica al conectarse con sistemas de información confidencial o clasificados como reservados, se recomienda no hacerlo desde redes de internet públicas.
-

Glosario y lista de siglas

Documento de archivo: Registro de información producida o recibida por una persona o entidad en razón a sus actividades o funciones, que tiene valor administrativo, fiscal, legal, científico, histórico, técnico o cultural y debe ser objeto de conservación en el tiempo, con fines de consulta posterior. (Acuerdo 002 de 2014, AGN)

Documento electrónico de archivo: Registro de información generada, producida o recibida o comunicada por medios electrónicos, que permanece almacenada electrónicamente durante todo su ciclo de vida, producida, por una persona o entidad en razón a sus actividades o funciones, que tiene valor administrativo, fiscal, legal, ó valor científico, histórico, técnico o cultural y que debe ser tratada conforme a los principios y procesos archivísticos. (Acuerdo 002 de 2014, AGN)

Expediente: Conjunto de documentos producidos y recibidos durante el desarrollo de un mismo trámite o procedimiento, acumulados por una persona, dependencia o unidad administrativa, vinculados y relacionados entre sí y que se conservan manteniendo la integridad y orden en que fueron tramitados, desde su inicio hasta su resolución definitiva. (Acuerdo 002 de 2014, AGN)

Expediente digital o digitalizado: Copia exacta de un expediente físico cuyos documentos originales, tradicionalmente impresos, son convertidos a formato electrónico mediante procesos de digitalización. (Acuerdo 002 de 2014, AGN)

Expediente electrónico de archivo: Conjunto de documentos y actuaciones electrónicos producidos y recibidos durante el desarrollo de un mismo trámite o procedimiento, acumulados por cualquier causa legal, interrelacionados y vinculados entre sí, manteniendo la integridad y orden dado durante el desarrollo del asunto que les dio origen y que se conservan electrónicamente durante todo su ciclo de vida, con el fin de garantizar su consulta en el tiempo. (Acuerdo 002 de 2014, AGN)

Expediente híbrido: Expediente conformado simultáneamente por documentos análogos y electrónicos, que a pesar de estar separados forman una sola unidad documental por razones del trámite o actuación. (Acuerdo 002 de 2014, AGN)

Firma digital: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la Transformación. (Ley 527 de 1999)

Firma electrónica: 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. (Decreto Nacional 1074 de 2015)

Co-firma o firma en línea: Es la firma múltiple en la que todos los firmantes están al mismo nivel y en la que no importa el orden en el que se firma. La co-firma se utiliza en la firma de documentos que son resultados de reuniones, conferencias o comités.

(veáse <https://firmaelectronica.gob.es/Home/Ciudadanos/Formatos-Firma.html>)

Contra-firma o firma en cascada: Firma múltiple en la que el orden en el que se firma es importante, ya que cada firma debe refrendar o certificar la firma del firmante anterior. La contra-firma se utiliza especialmente en aplicaciones como los Porta Firmas, en los que un documento debe seguir una línea específica a través de varios firmantes hasta que todo el proceso es aprobado.

(veáse <https://firmaelectronica.gob.es/Home/Ciudadanos/Formatos-Firma.html>)

Lista de siglas

- VPN.** Virtual Private Network (red privada virtual)
 - TRD.** Tabla de Retención Documental.
 - NAS.** Network Attached Storage (Sistema de almacenamiento)
 - SAN.** Storage Area Network (Sistema de almacenamiento).
 - SSH.** Secure Shell (protocolo para acceso remoto)
 - SSL.** Secure Sockets Layer (capa de sockets seguros)
 - TLS.** Transport Layer Security (seguridad de la capa de transporte)
 - PKI.** Public Key Infrastructure (infraestructura de clave pública)
 - CSV.** Códigos Seguros de Verificación
-

Bibliografía

ALTA CONSEJERIA DISTRITAL TIC. Guardianes de la Información [en línea]. Disponible en: <<http://ticbogota.gov.co/seguridad>>.

ARCHIVO GENERAL DE LA NACIÓN. G.INF.07 Guía para la gestión de documentos y expedientes electrónicos. Bogotá: Archivo General de la Nación, 2018. 129 p. Disponible en: <https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicaciones/DocumentoOficialV1_GuiaDocumentoYExpedienteElectronico26_ENE%202018_v3.pdf>

COLOMBIA. PRESIDENCIA DE LA REPUBLICA. Decreto 491 de 2020. (28, marzo, 2020). Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica, Social y Ecológica [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=91670>>

COLOMBIA. ALCALDÍA MAYOR DE BOGOTÁ, D.C. Decreto 425 de 2016. (03, octubre, 2016). Por medio del cual se modifica la Estructura Organizacional de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=67103>>

COLOMBIA. ALCALDÍA MAYOR DE BOGOTÁ, D.C. Decreto 828 de 2016. (27, diciembre, 2018). Por el cual se regula el Sistema Distrital de Archivos y se dictan otras disposiciones [en línea]. Disponible en: <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=82128>

COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 002 de 2014. (14, marzo, 2014). Por medio del cual se establecen los criterios básicos para creación, conformación, organización, control y consulta de los expedientes de archivo y se dictan otras disposiciones [en línea]. Disponible en: <<https://normativa.archivogeneral.gov.co/acuerdo-002-de-2014/>>

COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 003 de 2015. (17, febrero, 2017). Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012 [en línea]. Disponible en: <<https://normativa.archivogeneral.gov.co/acuerdo-003-de-2015/>>

COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 060 de 2001. (30, octubre, 2001). por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas [en línea]. Disponible en: <<https://normativa.archivogeneral.gov.co/acuerdo-060-de-2001/>>

COLOMBIA. CONGRESO DE COLOMBIA. Ley 1437. (18, enero, 2011) Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=41249>>

COLOMBIA. CONGRESO DE COLOMBIA. Ley 962 de 2005. (8, julio, 2005). por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos [en línea].
Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=17004>>

COLOMBIA. PRESIDENCIA DE LA REPUBLICA Y MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Ley 527 de 1999 (18, agosto, 1999). por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. [en línea]. Disponible en: <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276>

COLOMBIA. PRESIDENCIA DE LA REPUBLICA Y MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1074 (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62508>>

COLOMBIA. PRESIDENCIA DE LA REPUBLICA Y MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 2364 (22, noviembre, 2012). Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. [en línea] Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50583>>

COLOMBIA. PRESIDENCIA DE LA REPUBLICA. MINISTERIO DE HACIENDA., et al. Decreto 1413 de 2017. (25, agosto, 2017). Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales. [en línea]. Disponible en: <<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=70951>>

DIGICERT. ¿qué son SSL, TLS y HTTPS? [en línea]. Disponible en: <<https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https>>

GOBIERNO DE ESPAÑA. PORTAL ADMINISTRACIÓN ELECTRÓNICA. Formatos de firma [en línea]. Disponible en: <<https://firmaelectronica.gob.es/Home/Ciudadanos/Formatos-Firma.html>>

NETTIX. ¿Qué son las llaves SSH o SSH keys? [en línea]. Disponible en: <<https://www.nettix.com.pe/documentacion/soporte-documentacion/que-son-las-llaves-ssh-o-ssh-keys>>

REAL CASA DE LA MONEDA. SEDE ELECTRÓNICA. ¿Qué significa no repudio o irrenunciabilidad? [en línea]. Disponible en: <https://www.sede.fnmt.gob.es/preguntas-frecuentes/otras-preguntas/-/asset_publisher/1RphW9leUoAH/content/1034-que-significa-no-repudio-o-irrenunciabilidad-?inheritRedirect=false>

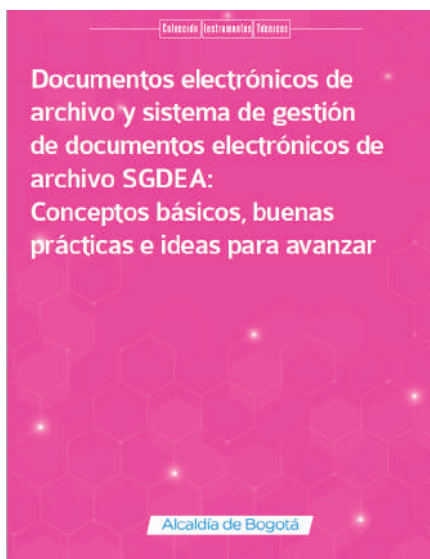
SECRETARÍA GENERAL DE LA ALCALDIA MAYOR DE BOGOTÁ. DIRECCIÓN DISTRITAL DE ARCHIVO DE BOGOTÁ. Documentos Electrónicos de Archivo y Sistema de Gestión de Documentos Electrónicos de Archivo SGDEA: conceptos básicos, buenas prácticas e Ideas para avanzar [en línea]. Bogotá D.C.: Secretaría General de la Alcaldía Mayor de Bogotá, 2019.

Disponible en:

<<https://secretariageneral.gov.co/transparencia/informacion-interes/publicacion/documentos-electronicos-archivo-y-sistema-gestion-documentos-electronicos-archivo-sgdaa-conceptos-basicos-buenas-practicas-e-ideas-avanzar>>

WIKIPEDIA. Infraestructura de clave pública [en línea]. Disponible en: <https://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica>

Información adicional



Consúltala en

<https://bit.ly/2XLynQL>

[Ingresa aquí](#)

Escanea el siguiente código QR



Visítanos

www.archivobogota.secretariageneral.gov.co

[Ingresa aquí](#)

"Juntos lo haremos"



Ciudadanos + Funcionarios + Ingenieros T.I.C

Funcionarios de
Gestión Documental



Archivo de
Bogotá



E-Docs fiables y seguros

¡Estamos para ayudar!

asistecnica-archivobogota@alcaldiabogota.gov.co
altaconsejeriadetic@alcaldiabogota.gov.co

© Secretaría General
2020

La presente guía está dirigida a las entidades y organismos del distrito para implementar medidas en el uso de canales electrónicos y la gestión de documentos electrónicos en ambientes de trabajo en casa o teletrabajo, en razón de la actual emergencia ocasionada por el COVID-19.

Desarrollada en un trabajo conjunto entre la Subsecretaría Técnica de Secretaría General de la Alcaldía Mayor de Bogotá, la Dirección Distrital de Archivo de Bogotá y la Alta Consejería Distrital TIC. Se pone a disposición tanto para la comunidad archivística de las entidades y organismos del distrito como para la ciudadanía en general.



SECRETARÍA
GENERAL

