CRITERIOS EN MATERIA DE DOCUMENTOS ELECTRÓNICOS DEL INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL DISTRITO FEDERAL.

1. Los presentes criterios establecen las disposiciones generales para la organización y conservación de los documentos electrónicos que detenta el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (INFODF), los cuales son de observancia obligatoria para las áreas y servidores públicos del INFODF.

2. Para los efectos de los presentes criterios se entenderá por:

Documento Electrónico. Información cuyo soporte durante todo su ciclo de vida se mantiene en formato electrónico y su tratamiento es automatizado, requiere de una herramienta específica para leerse o recuperarse.

Expediente electrónico. Conjunto de documentos electrónicos correspondientes a un procedimiento administrativo o a un asunto específico, cualquiera que sea el tipo de soporte en que se contengan.

Sistema automatizado de información. Conjunto de elementos informáticos orientados al tratamiento y administración de datos e información, organizados y disponibles para su posterior uso.

Soporte electrónico. Objeto electrónico sobre el cual o en el cual es posible grabar y recuperar datos.

3. Se deben organizar y conservar los documentos electrónicos cuyo contenido sea evidencia del ejercicio de las funciones y atribuciones de los servidores públicos del Instituto.

4. Los documentos deberán integrarse en expedientes y clasificarse de conformidad con el Cuadro General de Clasificación Archivística del Instituto.

5. Los documentos deben conservarse el plazo establecido en el Catálogo de Disposición Documental del Instituto.

6. Cuando no sea posible almacenar los documentos electrónicos en el formato original, deberá utilizarse un formato que asegure que la reproducción de la información con el mismo contenido.

7. La Dirección de Tecnologías de Información deberá elaborar la metodología técnica relativa al análisis de posibles riesgos informáticos de los diversos sistemas automatizados de información, orientada a generar un diagnóstico de

vulnerabilidad y estimación de posibles impactos y riesgos de pérdida de información.

8. Con base en los resultados del análisis referido en el numeral anterior, la Dirección de Tecnologías de Información desarrollará proyectos preventivos que permitan adoptar medidas técnicas para prevenir la pérdida de información.

9. Las áreas deberán contar con copias o respaldos de documentos referentes a sus funciones sustantivas, en soportes no reescribibles. La periodicidad de respaldos o copias estará determinada por el área respectiva en virtud de la temporalidad de la gestión documental de que se trate.

10. Se podrán reproducir los documentos que estén en soporte de papel a soporte electrónico (escaneado del original) mediante técnicas de reconocimiento de caracteres (OCR), y en un formato que permita su tratamiento automático, tal como buscar, copiar y extraer información.

11. Se deberá conservar y preservar la fiabilidad, autenticidad e integridad de los documentos electrónicos durante su existencia.

12. Los servidores públicos deberán mantener sus archivos electrónicos actualizados bajo la estructura de clasificación archivística institucional y gestionarlos preferentemente por medios electrónicos.

13. Los documentos electrónicos oficiales que ingresen a las áreas a través del correo electrónico institucional o por otro medio de transmisión electrónica, deben registrarse en el sistema automatizado respectivo, organizarse y conservarse de conformidad con su clasificación y plazo de conservación.

14. Cuando una aplicación informática sea sustituida por una nueva, se realizarán los procesos necesarios para incorporar todos los documentos existentes hasta ese momento a la nueva aplicación.

15. Si la aplicación informática deja de utilizarse y su funcionalidad no es sustituida por una nueva aplicación, se realizará cualquiera de las siguientes acciones:

a) Si el mantenimiento de los soportes y medios que ejecutan dicha aplicación se encuentra garantizado en el plazo en el que los datos deben ser conservados de conformidad con el Catálogo de Disposición Documental, tanto la aplicación como los soportes se mantendrán sin modificación.

b) Si el mantenimiento de los soportes y medios no se encuentra garantizado, entonces, al menos los datos básicos de la aplicación de carácter histórico se traspasarán a un nuevo formato cuya durabilidad se encuentre garantizada. Para evitar situaciones de ese tipo deben ser transferidos previamente todos los datos a un formato estandarizado.

16. Se deben transferir documentos electrónicos completos, auténticos y fiables, al archivo de Concentración e Histórico de acuerdo con las vigencias establecidas en el Catálogo de Disposición Documental del Instituto.

17. Se deben eliminar todos aquellos documentos que carecen de utilidad para el desarrollo de las funciones institucionales o sin valor administrativo.

18. La Dirección de Tecnologías de Información deberá realizar las copias y respaldos necesarios de los documentos que sean sustituidos con motivo de las actualizaciones derivadas de las obligaciones legales aplicables, así como de los relativos a la difusión institucional que se presenten en el portal de Internet, para esto deberá garantizar su preservación como información que debe mantenerse disponible para la consulta de los ciudadanos en formatos que puedan ser accedidos fácilmente por los usuarios.

19. Los soportes de la información a utilizarse deben seleccionarse del conjunto común de estándares de formato: gráfico, texto, datos, audio y video que faciliten el acceso y consulta de la información, y su posterior recuperación y conservación.

20. En la medida de lo posible, deberán utilizarse formatos con especificaciones públicas y libres de regalías y patentes.

Los formatos recomendados son los siguientes:

a) Formatos de texto:

MS WORD: Formato simple que permite su lectura a cualquier usuario.

TXT: Formato simple que permite su lectura a cualquier usuario.

PDF: Permite visualizar documentos reproduciendo todas las características del original en ficheros de menor tamaño, independientes de la aplicación y plataformas, su especificación es pública y también se encuentra extendido para la distribución y difusión formal de documentos y para su acceso y visualización.

RTF: Formato que constituye un mínimo común entre procesadores de texto diferentes.

SGML: norma internacional ISO 8879, del mundo editorial, que almacena el texto y su estructura, pero no tiene atributos de presentación.

XML: Dialecto del SGML adecuado para definir documentos independientes de la plataforma y procesarlos de forma automática pues distingue entre estructura, contenido y presentación, ofreciendo mayores posibilidades que HTML.

HTML: Versión simplificada del SGML que se utiliza en los servidores web, muy útil para la difusión de información.

SXW: Formato de los documentos de texto manejados por el software libre openoffice.org. Encapsulated PostScript: utilizado para enviar e imprimir documentos junto con su presentación, de forma que se asegure que la salida impresa es correcta con independencia del dispositivo utilizado.

b) Formatos de datos estructurados:

MS EXCEL: Utilización de hojas de cálculo.

HOJAS CÁLCULO OPEN OFICE: Utilización de hojas de cálculo.

XML: Dialecto del SGML adecuado para definir documentos independientes de la plataforma y procesarlos de forma automática pues distingue entre estructura, contenido y presentación, ofreciendo mayores posibilidades que HTML.

Bases de datos: Usar bases de datos relacionales conformes con las normas internacionales sobre SQL.

c) Formatos Gráficos:

Gráficos de mapa de puntos: imagen constituida por puntos y utilizada para posteriores codificaciones.

GIF: Mayormente utilizados en portales de Internet.

JPEG: ISO 10918. Hay que tener en cuenta que es destructivo con un nivel de compresión alto, por lo que se debe comprobar que la pérdida de imagen es aceptable. Soporta 16, 7 millones de colores 824 bits por pixel).

TIF: Utilizado en ficheros generados por escáneres con varias posibilidades según el número de colores elegido: blanco y negro; escala de grises y color. No es destructivo pero de nivel de compresión bajo.

PNG: Con características similares e incluso superiores a GIF, está libre de regalías y patentes. Soporta 16,7 millones de colores y se puede utilizar sin necesidad de licencias de software.

FAX: Formatos de ficheros fax: Grupo III y Grupo IV según el tipo de línea telefónica usada: normal y RDSI.

Gráficos vectoriales: gráfico que conserva las coordenadas de los vectores que lo componen, y es utilizado en la digitalización de planos.

CGM: Formatos para gráficos 2D, imágenes combinadas *raster* y vectoriales.

VML: *Vector Markup Language*.

d) Formatos comprimidos:

Especificación ZIP 2.0 para el intercambio de datos comprimidos.

21. En la medida de lo posible los documentos generados deberán utilizar las distintas modalidades lingüísticas del idioma español, para lo cual se deberán seleccionar los medios, equipos o sistemas que permitan la utilización de caracteres gráficos empleados por el idioma en referido.

22. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares, deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones informáticas.

23. Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos en cumplimiento de las garantías previstas en la Ley de Protección de Datos Personales para el Distrito Federal.

24. Los soportes de información deberán mantener una humedad entre 30% y un 50% y temperatura de 21º C.

25. Se deben realizar grabaciones periódicas de los archivos electrónicos, teniendo en cuenta la duración de los soportes y la evolución de su tecnología, ya sea reutilizando los mismos o migrando hacia otros más modernos.

26. Se preservará la información de los soportes electrónicos volviendo a grabar los soportes magnéticos y ópticos según los plazos recomendados para cada tipo de soporte.

27. Los plazos sugeridos para almacenamiento de información en soportes magnéticos y ópticos, son los siguientes:

Soporte magnético	**Capacidad**	**Plazo almacén**	**Consideraciones**
Disquete 3 1/2	1,44 a 120 MB	2 a 5 años	Regrabable +1.000 veces Norma ISO/IEC 9529
Cinta magnética 1.600 bpi		5 a 10 años	Regrabable + 1.000 veces Reescribir cada 10 años Rebobinar cada 2 años Norma ISO/IEC 3788
Cinta magnética 6.350 bpi	112,5 GB		
Cartucho 1/2" y ¼"	80 MB / 2 GB	5 a 10 años	Regrabable + 1.000 veces Reescribir cada 10 años Rebobinar cada 2 años Norma ISO 8462
Cinta DAT de 4 mm.	2 a 24 GB	5 a 10 años	Regrabable + 1.000 veces Reescribir cada 10 años Rebobinar cada 2 años Norma ISO/IEC 11319 Y 12246
Cinta de 8 mm.	3,5 a 25 GB		
Soportes ópticos	**Capacidad**	**Plazo almacén**	**Consideraciones**
CD-ROM, CD-R y CD-RW	0,65 GB	10 a 20 años	Regrabable (RW) + 1.000 veces Reescribir cada 10 años Normas ISO/IEC 9660 y 1014
DVD-ROM DVD RAM DVD-R y DVD RW	4,7 a 18 GB 4,7 A 9,4 GB 4,7 GB		Regrabable (RW) + 100 veces Reescribir cada 10 años Norma ISO/IEC 16824

28. Se realizarán controles periódicos del archivo de soportes electrónicos para protegerlos del deterioro físico.

29. Se deberá disponer de segundas copias del archivo de soportes electrónicos.

30. Para la protección de los soportes electrónicos se atenderán los aspectos siguientes:

a) Realizar copias de respaldo y recuperación;

b) Realizar la migración de soportes en función de su vida útil;

c) Realizar inventarios mensualmente de los contenidos del acervo electrónico; y

d) Especificar los plazos de tiempo de conservación de los soportes, su puesta fuera de servicio y borrado de la información.

31. La identificación y control de soportes electrónicos considerará los aspectos siguientes:

a) Se identificarán los soportes por su nombre, fecha de creación, durabilidad y periodo de retención;

b) Identificar y controlar la duración de los equipos y soportes;

c) Mantener registros de entrada y salida de los soportes recibidos y enviados;

d) Determinar el método para transferir los soportes a los archivos de Concentración e Histórico;

e) Autorización por parte del responsable, de la salida de soportes fuera de los locales en que están ubicados; y

f) Impedir cualquier recuperación de información mediante un método de borrado, esto para el caso de bajas documentales.

32. El control de cambios de soportes electrónicos considerará los aspectos siguientes:

a) Proteger los soportes de cambios no autorizados;

b) Documentar y justificar la necesidad del cambio;

c) Evaluar las consecuencias del cambio; y

d) Aprobar, implantar y verificar la realización de los cambios.

33. En función de los soportes informáticos que contengan datos de carácter personal les aplicará el nivel de seguridad básico, medio y alto contemplado en la Ley de Protección de Datos Personales para el Distrito Federal.

34. Los soportes electrónicos que contienen datos de carácter personal deberán estar ubicados en un área cuyo entorno tenga condiciones físicas de seguridad y restricción, de acceso solo al personal autorizado.

35. Se podrán utilizar otras instalaciones distintas para almacenar copias de seguridad y respaldo.

36. Para la gestión de soportes reescribibles se realizarán las siguientes acciones:

a) Deberán documentarse todos los procedimientos y niveles de autorización sobre el acceso a los responsables autorizados;

b) Se deberán retirar los soportes con autorización escrita y mantendrán su registro y seguimiento de salida;

c) Se deberá evitar identificar los datos almacenados a partir de la etiqueta del soporte;

d) Se deberán reutilizar y retirar los soportes eliminando su contenido con diferentes patrones de borrado; y

e) Realizar reparaciones de medios, equipos y sistemas, para evitar el riesgo de fuga de datos.

37. Para la manipulación de datos de carácter personal en soportes electrónicos se deberá:

a) Registrar la manipulación y esquema de etiquetado de todos los soportes;

b) Mantener un registro actualizado con el nombre de todas las personas autorizadas para el tratamiento en soporte electrónico;

c) Controlar los datos, acusar de recibo y marcar las copias remitidas a los receptores autorizados;

d) Registrar las operaciones de creación, modificación y borrado para su seguimiento respectivo;

e) Realizar revisiones periódicas para determinar el grado de cumplimiento de los procedimientos;

f) Cifrar la información de carácter sensible, como requisito de confidencialidad;

g) Firmar y fechar digitalmente la información sensible, como requisito de autenticidad; y

h) Ubicar de forma segura los soportes, para lo cual deberá disponerse de una caja de seguridad para el almacenamiento de los soportes electrónicos.

38. Para el traslado y tratamiento de los soportes electrónicos que contienen datos de carácter personal a los que se han de aplicar medidas de seguridad de nivel básico, deberá observarse lo siguiente:

a) La salida de soportes electrónicos que contengan datos de carácter personal, fuera de los locales en los que estén ubicados, únicamente podrá ser autorizada por el responsable de los mismos;

b) El responsable de los soportes electrónicos se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos;

c) Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la perdida o destrucción.

d) Deberán realizarse copias de respaldo al momento en que se produzca alguna actualización de los datos personales.

39. Para el traslado y tratamiento de los soportes electrónicos que contienen datos de carácter personal a los que se han de aplicar medidas de seguridad de nivel medio, deberá:

a) Registrarse la entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada;

b) Disponer de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada;

c) Observar que cuando un soporte vaya a ser desechado o reutilizado, se adopten las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario; y

d) Observar que cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados como consecuencia de operaciones de mantenimiento, se adopten las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

40. Para el traslado y tratamiento de los soportes electrónicos que contienen datos de carácter personal a los que se han de aplicar medidas de seguridad de nivel alto, se deberá:

a) Realizar la distribución de los soportes que contengan datos de carácter personal cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte; y

b) Conservar una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan.

41. La eliminación de soportes electrónicos deberá considerar las siguientes medidas técnicas:

a) Se eliminarán los soportes que contengan información de carácter sensible, o borrar sus datos para su reutilización, en consecuencia se destruirán mediante trituradoras o medios similares a los impresos;

b) Se deberán identificar de manera segura los soportes que deban destruirse, tales como cintas, discos reescribibles, casetes, listados de programas, datos de prueba y documentos del sistema;

c) Se realizará un registro actualizado de la destrucción de soportes con información sensible, a efectos de revisión; y

d) Se deberá evitar la acumulación de gran cantidad de información sensible para su destrucción.

Artículos Transitorios.

PRIMERO. Los presentes Criterios en Materia de Documentos Electrónicos del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, entrarán en vigor a partir del primero de mayo de 2012.

SEGUNDO. Durante los meses de enero a abril de dos mil doce, la Coordinación de Archivos y la Dirección de Tecnologías de Información impartirán la capacitación atinente a la aplicación del presente instrumento normativo.