PLAN DE PRESERVACIÓN DIGITAL A LARGO PLAZO (SUBSISTEMA DE SEGURIDAD EN LA INFORMACIÓN – DOCUMENTO ELECTRÓNICO DE ARCHIVO)

CONTENIDO

PLAN DE PRESERVACIÓN DIGITAL A LARGO PLAZO (SUBSISTEMA DE SEGURIDAD EN LA INFORMACIÓN – DOCUMENTO ELECTRÓNICO DE ARCHIVO)

1. OBLIGACIONES LEGALES

En el decreto 2609 del año 2012 en su artículo 9º se define la preservación a largo plazo como" el conjunto de acciones y estándares aplicados a los documentos durante su gestión para garantizar su preservación en el tiempo, independiente de su medio y forma de registro o almacenamiento".

En el capítulo IV del mismo decreto establece en el artículo 29 los requisitos para la preservación y conservación de los documentos electrónicos de archivo, con el objeto de asegurar su preservación y conservación en el tiempo.

En el año 2013 en el decreto 1515, modificado por el decreto 2758 de 2013 establece en su artículo 12 procedimientos y lineamientos generales para la transferencia secundaria de los documentos y archivo electrónicos declarados de conservación permanente, tanto al Archivo General de la Nación como a los archivos generales territoriales de forma que se asegure su integridad, autenticidad, preservación y consulta a largo plazo.

La preservación de los documentos y archivos electrónicos deben estar dentro del objeto del Sistema Integrado de Conservación, tal como se define en el acuerdo 006 de 2014."La implementación del SIC tiene como finalidad, garantizar la conservación y preservación de cualquier tipo de información, independientemente del medio o tecnología con la cual se haya elaborado."

En el capítulo III del acuerdo 006 de 2014 se formulan las disposiciones generales y los elementos mínimos que debe contener, en los artículos 19,20, 21, 23 y 24 se relaciona la estructura del plan de Preservación a largo plazo, los riesgos, los procesos y procedimientos y la adopción de estándares, normas técnicas internacionales y modelos de referencia para el acceso y preservación de los documentos.

2. POLITICA DE SEGURIDAD DE LA INFORMACION DE LA SECRETARIA DISTRITAL DE SALUD

Desde el año de 2011 la Secretaría Distrital de Salud por intermedio de la Dirección de Tecnologías de la Información y Comunicaciones(TIC) ha formulado la Política de Seguridad de la información actualizadas y complementadas hasta consolidar la versión de agosto año 2017 la cual se aplica actualmente.

La política plantea lineamientos para preservar y asegurar los datos informativos generados en el uso de las tecnologías y comunicaciones ante los riesgos de pérdidas, uso indebido, daño o alteración. Estas directrices por lo tanto obedecen a requerimientos de orden ético, legal y de buenas prácticas de los funcionarios y usuarios en las actividades cotidianas que derivan de las funciones de la entidad y en el uso adecuado de los recursos de la Dirección del TIC.

En consecuencia, el cubrimiento de la política tiene como finalidad abarcar de manera integral la seguridad de la información hacia los Datos de la entidad, las aplicaciones y los Sistemas operativos de la Secretaria Distrital de Salud; la seguridad de las comunicaciones (tecnologías de red, servidores de la entidad y redes de acceso), y la seguridad física o de las infraestructuras(centro de cómputo, centro de cableados y las estaciones de trabajo de los usuarios).

La política general comprende todas las reglas de seguridad para que todos los funcionarios de la entidad la conozcan y se cumplan ya que el impacto es hacia todos los usuarios del sistema.

El objetivo general es establecer lineamientos de seguridad de la información para los funcionarios y visitantes de la secretaria Distrital de Salud para permitir el uso y protección adecuada de los recursos de la información y las comunicaciones.
Para que se cumplan estos objetivos como primera medida se debe evitar que los datos informativos estén libres de modificaciones no autorizadas, y se debe permitir que la información sea accesible solo para usuarios autorizados, y por último se debe permitir el acceso a los sistemas de usuarios autorizados en el momento que se requiera.

La política establece un alcance para todos los funcionarios y contratistas, terceros e invitados, los cuales tienen la responsabilidad de conocer, entender y seguir todas las normas y procedimientos de seguridad de la información establecidos.

La dirección del TIC es el administrador de la plataforma Tecnológica y generador de la política de seguridad de la información de la Secretaria Distrital de Salud y se encarga de la adecuada gestión de la seguridad de la información procesada y almacenada por los sistemas y servicios.
Se exponen la normatividad, reglamento y disposiciones específicas de la política general. (ver anexo- Política de Seguridad de la información. SDS)

3.INTRODUCCIÓN

Este segundo componente del SIC está directamente relacionado con la gestión de documentos electrónicos de la entidad y se refiere a las acciones a corto, mediano y largo plazo que tienen como fin implementar los programas, estrategias, procesos, y procedimientos tendientes a asegurar la preservación a largo plazo de los documentos electrónicos de archivo. Al igual que el sistema de seguridad de la información, comprende un conjunto de prácticas destinadas a implementar, verificar, mantener y mejorar la protección de los activos de información críticos para la entidad y minimizar los riesgos por pérdida de confidencialidad, indisponibilidad y uso indebido de la información.

Por lo tanto el Plan de preservación a la largo plazo para medios digitales y electrónicos debe garantizar que la Política de Seguridad de la información de la entidad se cumpla, se desarrolle y actualice en el tiempo, por medio de la implementación de acciones, actividades y procedimientos tendientes a asegurar la preservación a largo plazo de los documentos electrónicos de archivo manteniendo las características de integridad, confidencialidad, inalterabilidad, fiabilidad, interpretación, comprensión y disponibilidad.

En el diagnóstico realizado a través de la información suministrada por los referentes de los archivos de gestión de las Subsecretarias de la entidad, se establece la carencia de un inventario de la información de datos generados en medios digitales y electrónicos y su correspondencia con las series y subseries establecidas en las tablas de retención.

Cada una de las oficinas productoras reciben, distribuyen y almacenan información de carácter misional y transversal, sin embargo no hay un cumplimiento de algunas oficinas productoras, de la política de seguridad de la información de la entidad para establecer los activos de información que necesitan ser preservados, y no hay información suficiente sobre el funcionamiento y alcances de los mecanismos tecnológicos para asegurar la integridad, confidencialidad y disponibilidad de la información, formuladas en la Política de seguridad de la información

Las oficinas productoras de la Secretaria Distrital de Salud presentan aplicativos electrónicos principalmente para la recepción, almacenamiento y distribución de correspondencia (Cordis). Los oficios producidos son digitalizados con las firmas correspondientes para ser enviados y almacenados, sin embargo la capacidad de almacenamiento no es suficiente cuando la producción de oficios es muy alta. Sin embargo el aplicativo para (Peticiones,quejas, reclamos y solicitudes(PQRS) utilizado en todas las oficinas presenta una gran capacidad para el almacenamiento de información. Esto significa que no existe una unificación en la capacidad de los aplicativos para almacenar información y por lo tanto no hay seguridad en la recuperación de la misma en los aplicativos utilizados.

La información misional de las Subsecretarias de Salud Pública, Servicios de Salud y Aseguramiento, Gestión Territorial, participación y Servicio a la Ciudadanía y Planeación y Gestión Sectorial se tramitan desde sus propios aplicativos creados para estructurar los datos específicos de cada oficina productora y para la migración respectiva hacia otras dependencias y hacia el usuario externo.

Así mismo, las oficinas con carácter legal o jurídico y administrativo como Asuntos Legales, Oficina Asesora jurídica del Despacho, Control Interno disciplinario y las oficinas de la Subdirección Corporativa presentan aplicativos para la correspondencia y para la información propia de la función de cada una, no obstante no se tiene el inventario de la información generada y los valores documentales que presentan, de acuerdo con la tabla de retención y valoración documental con fin de solicitar a la Dirección del TIC la generación de copias digitales y el procedimiento para asegurar su preservación en almacenamientos seguros.

La selección y respaldo de la información se realiza a criterio propio de cada oficina y es almacenada en la carpeta asignada a los usuarios(H: Home Dictory) a la cual la dirección de TIC le hace backup(copias) dentro de un esquema definido. Estos backups son transferidos a cintas de memoria y posteriormente enviados a una empresa externa para garantizar su conservación en depósitos especiales para este fin.

De acuerdo con la Política de Seguridad de la información, la oficina de Tecnología de la información y las Comunicaciones (TIC) tiene la función de prestar los servicios para la actualización o reemplazo de los aplicativos y sistemas operativos de las oficinas productoras, y mantenimiento de las redes y servidores de la entidad. Estos procedimientos están establecidos pero no se comunican periódicamente a las oficinas de la entidad.

En consecuencia, la Secretaria Distrital de Salud esta soportada por una política de seguridad de la Información con servidores y diversos aplicativos electrónicos para el manejo de la información, pero en términos de capacitación, seguridad y recuperación carece de un sistema operativo que articule y unifique la información de todas las oficinas productoras para garantizar una comunicación y preservación eficiente. Además el seguimiento para asegurar la preservación no está totalmente definido por un programa con acciones y actividades para el control de la información vital para la entidad.

4.ALCANCE

La preservación a largo plazo de la información debe asegurar la confiabilidad, integridad y disponibilidad de la información, necesaria para el desarrollo de los procesos de la entidad, por lo que la definición, aplicación, verificación y cumplimiento de los lineamientos para el buen uso de las herramientas informáticas debe ser de obligatorio cumplimiento en cada una de las etapas del ciclo vital de documento electrónico en todas las dependencias de la Secretaria Distrital de Salud y en el archivo central.

5.OBJETIVO

Evaluar, complementar y mejorar en la entidad las herramientas electrónicas y de preservación necesarias para garantizar las buenas prácticas en relación a la gestión y al plan seguridad de la información electrónica.

3. METODOLOGÍA- DESARROLLO DE LA ESTRUCTURA DE PRESERVACIÓN

- Armonizar las Tablas de Retención Documental convalidadas por el Archivo de Bogotá para los documentos físicos, y los demás instrumentos archivísticos de la entidad con los documentos de carácter electrónico y digital.

- Identificar y valorar los medios de almacenamiento y formatos digitales en los que se encuentra la información.

- Identificar documentos electrónicos.

- Identificar series o subseries híbridas (compuestas por documentos físicos y electrónicos) – metadatos.

Dentro de la actividad diaria de la entidad, se pueden identificar documentos que nacen electrónicos y tienen un trámite igualmente electrónico, dentro de ellos se encuentran hasta el momento, aquellos generados por los mecanismos de ayuda por medio de las cuales se reportan los inconvenientes en el funcionamiento de los sistemas, conocida como “soporte” y las necesidades de mejoramiento en la infraestructura conocida como “mantenimiento”.

Estos mecanismos generan un vestigio que permite verificar la trazabilidad del trámite. Si bien es importante la identificación de estos documentos electrónicos, es probable que sus tiempos de retención no sean extensos en el tiempo por lo que los temas de preservación a largo plazo probablemente no apliquen para estas series transversales.

- Evaluar riesgos y estrategias de preservación.

- Diseñar planes de información y capacitación en conjunto con la Dirección de TIC a todos los funcionarios y colaboradores de entidad sobre los temas técnicos, éticos y legales de la Seguridad de la información.

- Seleccionar y justificar la estrategia de preservación teniendo en cuenta las siguiente opciones formuladas en el Acuerdo 006 de 2014 del AGN:

a). Migración: Cambio a nuevos formatos/plataformas (hardware y software) o nuevos medios.

b). Emulación: Recreación en sistemas computacionales actuales del entorno software y hardware para permitir la lectura de formatos obsoletos.

c). Replicado: Copias de la información digital establecidas según la política de seguridad de la información que deberá ser diseñada en conjunto con la Oficina de Sistemas.

d). Refreshing: Actualización de software o medios.

La estrategia seleccionada para la preservación digital deberá estar soportada, documentada y justificada de acuerdo con los requisitos de preservación de los documentos, teniendo en cuenta los siguientes aspectos:

a). El registro histórico de todas las acciones de gestión y administración relativas a los documentos digitales y/o documentos electrónicos de archivo.

b). Llevar a cabo de manera regular la vigilancia de los desarrollos técnicos, las técnicas de conversión, migración y las normas técnicas pertinentes.

c). Elaborar un modelo aceptado de conceptos y utilizarlo como base para el plan de preservación digital a largo plazo.

d). Capturar todos los metadatos(campos específicos) asociados, transferirlos a los nuevos formatos o sistemas y asegurar su almacenamiento.

4. PROCESOS Y PROCEDIMIENTOS

Los procesos y procedimientos para la preservación digital deben tener en cuenta las siguientes actividades:

1) Identificar los documentos digitalizados y creados electrónicamente, desde el proceso de planeación y valoración de la gestión documental en todas las oficinas productoras de la entidad.
2) Establecer el cronograma de transferencias y eliminación de documentos de conformidad con las Tablas de retención y valoración documental
3) Identificar y valorar los formatos, Medios y soportes de almacenamiento en los documentos digitales.
4) Determinar los requisitos de los metadatos(campos específicos) asociados para documentos digitales
5) Establecer las acciones de preservación necesarias para garantizar la fiabilidad y autenticidad de los documentos digitales.
6) Determinar los requisitos legales y reglamentarios específicos para los documentos digitales en cada dependencia.
7) Establecer los requisitos de la Dirección de Auditoria
8) Establecer los procedimientos para la vigilancia tecnológica

5. CRONOGRAMA

ACTIVIDADES	CORTO PLAZO	MEDIANO PLAZO	LARGO PLAZO
Elaboración del cronograma del plan con el área de sistemas			
Socialización del plan.			
Identificación y valoración de información en medios digitales de acuerdo con las series y subseries			
Seleccionar y justificar las estrategias de preservación			
Elaborar informe de resultados y plan de ejecución			
Elaborar plan y ejecución del seguimiento			

6. RECURSOS:

Recurso humano:

- Servidores públicos de la Secretaria Distrital de Salud-
- Profesionales de la Oficina de Tecnología de la información y las Comunicaciones (TIC).
- Profesional en conservación y restauración documental
- Auxiliar técnico en sistemas de la información

Recursos financieros:

Vigencia: 1 año

Profesional especializado en conservación y restauración	$ 51`000.000
Profesional en sistemas de la información	$ 51´000.000
Auxiliar técnico	$ 19´200.000
Recursos dispuestos en el Subsistema de la información en equipos, procedimientos y medios digitales.	

7. RIESGOS DEL PLAN

Teniendo en cuenta la naturaleza única de los documentos digitales deben evaluarse los siguientes riesgos mínimos para la formulación de un plan de preservación a largo plazo.

1. Obsolescencia y degradación del soporte físico
2. Obsolescencia del formato del documento digital
3. Obsolescencia del software
4. Obsolescencia del hardware
5. Desastres naturales
6. Ataques deliberados a la información
7. Fallas organizacionales
8. Errores humanos que afectan la preservación de la información.

La política de seguridad de la información de la entidad considera estos aspectos y reglamenta las acciones para prevenir las amenazas y riesgos, no obstante en la entidad solamente existen acciones de respuesta ante accidentes puntuales, más no planes y procedimientos preventivos a largo plazo.

8.RESPONSABLES:

Todos los servidores públicos de la Secretaria Distrital de Salud deben estar comprometidos con el cumplimiento de los lineamientos para el buen uso de las herramientas informáticas de la entidad. Se contará con el apoyo permanente de la oficina de Tecnología de la información y las Comunicaciones (TIC) ya que de acuerdo con la Política de seguridad de la Información es la oficina encargada y responsable de los servicios para garantizar la seguridad de la información de la entidad

9.ANEXOS:

- Políticas de seguridad de la información de la Secretaria Distrital de Salud
- Formatos de vigilancia y seguimiento de la información digital, los sistemas operativos, redes, servidores e infraestructura. Estos deberán ser diseñados en conjunto con la Dirección de TIC.