POLÍTICA DE PROTECCIÓN DE REGISTROS

Sistema de Gestión de Seguridad de la Información
Secretaría de Educación Del Distrito

Vigencia 2025
Versión: 1.0

Tabla de Contenido

1. OBJETIVO 3
2. ALCANCE 3
3. PRINCIPIOS 3
4. LINEAMIENTOS GENERALES 4
4.1. Creación y Captura de Registros 4
4.2. Almacenamiento y custodia 4
4.3. Acceso y uso 4
4.4. Conservación y retención 4
4.5. Disposición final 5
4.6. Protección y seguridad 5
5. RESPONSABILIDADES Y MEJORA CONTINUA 5
6. CUMPLIMIENTO Y SANCIONES 6
7. REVISIÓN Y ACTUALIZACIÓN 6
8. REFERENCIAS NORMATIVAS 6

GLOSARIO

REGISTRO: Evidencia documentada que respalda actividades, decisiones, transacciones o procesos de la Entidad.

CICLO DE VIDA DEL REGISTRO: Etapas desde la creación, almacenamiento, uso, conservación y disposición final.

INFORMACIÓN PUBLICA: Aquella que puede ser conocida por cualquier persona sin restricciones.

INFORMACIÓN CLASIFICADA: Aquella cuya divulgación puede afectar derechos fundamentales o intereses legítimos de personas o la Entidad.

INFORMACIÓN RESERVADA: Información restringida por mandato legal o constitucional.

RIESGO: efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo.

SENSIBILIDAD: nivel de impacto que una divulgación no autorizada podría generar.

SERVICIO: es cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

1. OBJETIVO

Establecer lineamientos para la creación, gestión, almacenamiento, protección, acceso, conservación y disposición final de los registros de la Entidad, garantizando su integridad, disponibilidad, confidencialidad y trazabilidad, en cumplimiento con la norma ISO/IEC 27001:2022 (control 5.33), la Ley 1581 de 2012, la Ley 1712 de 2014 y demás disposiciones normativas aplicables.

2. ALCANCE

Esta política aplica a:

- ✓ Todos los servidores públicos, contratistas y terceros que generen, procesen o custodien registros de la Entidad.
- ✓ Todos los tipos de registros en formatos físicos y digitales, incluyendo información pública, clasificada y reservada.
- ✓ Sistemas de información, bases de datos, archivos físicos y electrónicos.

3. PRINCIPIOS

Los principios que rigen la definición del presente documento están alineados con:

- ✓ Legalidad: se refiere a la cualidad de estar en conformidad con la ley o el derecho vigente. Implica que todas las acciones, decisiones y normas deben estar basadas en la ley, y que ninguna autoridad o individuo puede actuar de manera arbitraria o contraria a la misma.
- ✓ Transparencia: se refiere a la cualidad de ser visible, comprensible y accesible, especialmente en el contexto de la información y las acciones de gobiernos, organizaciones o individuos.
- ✓ Seguridad: se refiere a las prácticas y tecnologías diseñadas para proteger la información confidencial de acceso no autorizado, uso indebido, divulgación, interrupción o destrucción.
- ✓ Trazabilidad: se refiere a la capacidad de rastrear el origen, uso y recorrido de la información dentro de un sistema o proceso. Esto implica poder identificar quién accedió a la información, cuándo y cómo se modificó, y dónde se encuentra en cada momento.
- ✓ Confidencialidad: se refiere a la capacidad de rastrear el origen, uso y recorrido de la información dentro de un sistema o proceso. Esto implica poder identificar quién accedió a la información, cuándo y cómo se modificó,

y dónde se encuentra en cada momento.

- ✓ Autenticidad: asegura que la información provenga de una fuente legítima y no haya sido alterada o falsificada.

4. LINEAMIENTOS GENERALES

4.1. Creación y Captura de Registros

- Todos los procesos y acciones realizadas por la Entidad deberán documentarse con registros claros, precisos y verificables.
- Los registros deberán contener metadatos que permitan su identificación, fecha, responsable y propósito.
- Las definiciones de los datos relacionados con los registros deben gobernarse y contar con un dueño y un custodio dentro de la Entidad, estas designaciones se harán en el marco del modelo de gobierno de datos institucional que se irá implementando paulatinamente en la SED

4.2. Almacenamiento y custodia

- Los registros físicos se almacenarán en espacios seguros con control de acceso.
- Los registros electrónicos se almacenarán en sistemas con respaldo, cifrado y control de acceso basado en roles.

4.3. Acceso y uso

- El acceso se otorgará según el principio de mínima autoridad y necesidad de conocer.
- La información pública se divulgará de acuerdo con la Ley 1712 de 2014, mientras que la clasificada o reservada tendrá restricciones definidas por ley.

4.4. Conservación y retención

- Se aplica la Tabla de Retención Documental (TRD) aprobada y definidas por la entidad[1].

[1] https://www.educacionbogota.edu.co/portal_institucional/transparencia/tablas-de-retencion-documental

- Los registros se conservarán durante el tiempo mínimo requerido por la ley o normatividad interna.

- Se deben garantizar mecanismos que impidan la modificación o remplazo de la información de forma no autorizada o siguiendo los mecanismos adecuados.

4.5. Disposición final

- La eliminación de registros se hará de manera segura (triturado, borrado seguro, sobreescritura o destrucción física) acorde con los tiempos establecidos en las tablas de retención documental.

- Todo proceso de disposición final será documentado y aprobado por el responsable designado.

4.6. Protección y seguridad

- Se aplicarán controles técnicos (cifrado, autenticación, respaldos) y administrativos (procedimientos, capacitación, auditorías) para proteger los registros.

- Los incidentes que comprometan registros deberán reportarse al Oficial de Seguridad de la Información, siguiendo el Procedimiento Modelo de Enfoque Gestión de Incidentes de Seguridad[2].

5. RESPONSABILIDADES Y MEJORA CONTINUA

- **Comité Interno de Archivo**

  - Aprobar, actualizar y vigilar el cumplimiento de la TRD.
  - Revisar periódicamente la pertinencia de los tiempos de retención.
  - Promover acciones de mejora continua en los procesos archivísticos y de disposición final.

- **Jefe de Archivo / Gestión Documental**

  - Liderar la implementación de la TRD en todas las áreas de la entidad.
  - Coordinar la capacitación del personal en gestión documental.
  - Realizar auditorías internas de cumplimiento.

---

2 https://sig.educacionbogota.edu.co/Isolucion/Administracion/frmFrameSet.aspx?Ruta=Li4vRnJhbWVTZXRBcnRpY3Vsby5hc3A/UGFnaW5hPUJhbmNvQ29ub2NpbWllbnRvNFNFRFByby9hL2E0ZTEzNjE4YWZkYzQyNWQ4NDQzYWY0ZjBmMzg0MjVkL2E0ZTEzNjE4YWZkYzQyNWQ4NDQzYWY0ZjBmMzg0MjVkLmFzcCZJREFSVElDVUxPPTYxOTk=

- Proponer mejoras basadas en hallazgos, auditorías y cambios normativos.

- **Oficial de Seguridad de la Información**

  - Garantizar que la disposición final cumpla con la política de seguridad y protección de datos.
  - Supervisar la aplicación de controles de seguridad en el ciclo de vida documental.
  - Incorporar mejoras derivadas de incidentes de seguridad o brechas identificadas.

- **Jefes de Proceso / Área**

  - Asegurar que la documentación de su área esté clasificada y retenida según la TRD.
  - Reportar inconsistencias o dificultades en la aplicación de la TRD.
  - Retroalimentar al Comité de Archivo con propuestas de mejora basadas en la experiencia operativa.

- **Todos los funcionarios y contratistas**

  - Cumplir con la TRD en la creación, manejo y disposición de documentos.
  - Reportar anomalías o hallazgos en el proceso documental.
  - Participar en actividades de mejora continua y adopción de nuevas prácticas archivísticas.

6. CUMPLIMIENTO Y SANCIONES

El incumplimiento de esta política podrá dar lugar a sanciones disciplinarias, contractuales y legales, según la normatividad vigente.

7. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada como mínimo una vez al año o cuando se presenten cambios normativos, tecnológicos u organizacionales que lo requieran.

8. REFERENCIAS NORMATIVAS

- ✓ ISO/IEC 27001:2022, Control 5.33 – Protección de registros.

- ✓ Ley 1581 de 2012 – Protección de datos personales.

- ✓ Ley 1712 de 2014 – Transparencia y acceso a la información pública.
- ✓ Decreto 1377 de 2013 – Reglamenta parcialmente la Ley 1581.
- ✓ Acuerdo 060 de 2001 – Archivo General de la Nación.

MILENA DEL PILAR SANDOVAL GOMEZ
Jefe Oficina de las Tecnologías de la Información y Las Comunicaciones

Elaboró: Juan Carlos Parra Moreno – Oficial Seguridad Informática

Reviso: Henry Alexander Moyan Montenegro – Oficial Seguridad de la Información

Reviso: Jasson Smit Castro León – Profesional Especializado OTIC

Reviso: Luz Dary Vargas Suarez – Profesional OTIC

Reviso: Álvaro Echeverry Salcedo – Contratista Especializado