Circular OTTD - 02 de 2026

Junio 18 de 2026

PARA: Despacho, Subsecretarios, Directores, Jefes de Oficina, Funcionarios y Contratistas

DE: Oficina de Tecnología y Transformación Digital (OTTD)

ASUNTO: Lineamientos en Materia de Seguridad de la Información y Gestión Tecnológica.

Con el fin de fortalecer la seguridad de la información, garantizar el cumplimiento normativo y asegurar el uso adecuado de los recursos tecnológicos de la Secretaría Distrital del Hábitat - SDHT, y en cumplimiento de la normatividad vigente y aplicable, particularmente las siguientes normas:

Fundamento Constitucional.

- Constitución Política de Colombia (artículos 15, 209 y 269).

Contratación Pública.

- Ley 80 de 1993 (Estatuto General de Contratación de la Administración Pública).

Seguridad de la Información y Protección de Datos.

- Ley 1581 de 2012 (Protección de datos personales).
- Decreto 1377 de 2013 (reglamenta parcialmente la Ley 1581 de 2012, protección de datos personales).
- Decreto 886 de 2014 (Registro Nacional de Bases de Datos).
- Decreto 1074 de 2015 (Decreto Único Reglamentario del Sector Comercio, Industria y Turismo; instrucciones sobre el Registro Nacional de Bases de Datos).
- CONPES 3995 de 2020 (Política Nacional de Confianza y Seguridad Digital).
- Manual de Políticas de Seguridad de la información SDHT 2025.
- Procedimientos y lineamientos de seguridad de la SDHT Mapa SIG.

Transparencia, Acceso a la Información y Derechos de Autor.

- Ley 23 de 1982 (Derechos de autor y derechos conexos).
- Ley 1712 de 2014 (Transparencia y derecho de acceso a la información pública).
- Resolución 1519 de 2020 (directrices publicación de información, accesibilidad web, seguridad digital y datos abiertos).

Tecnologías de la Información y las Comunicaciones (TIC).

- Ley 1341 de 2009 (Sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC, principios para el uso eficiente de las TIC.)
- Decreto 1078 de 2015 (Decreto Único Reglamentario del sector TIC).
- Ley 1978 de 2019 (por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones –TIC).

Comercio Electrónico y Medios Digitales.

- Ley 527 de 1999 (comercio electrónico y medios digitales)

Transformación Digital y Gobierno Digital.

- Ley 2052 de 2020 (Racionalización de trámites y transformación digital).
- Resolución 2893 de 2020: (lineamientos ventanillas únicas, sedes electrónicas, trámites, OPA de MinTIC).
- Decreto 767 de 2022 (Política de Gobierno Digital).
- Decreto 1083 de 2015 (políticas de Gestión y Desempeño Institucional, incluidas las políticas de Gobierno Digital y de Seguridad Digital).
- Decreto 1008 de 2018 (lineamientos generales de la Política de Gobierno Digital).
- Documento Maestro de Lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC, basado en el estándar ISO/IEC 27001:2022.

Diseño Institucional.

- Decreto 653 de 2025 (Decreto único del Sector Hábitat).

Se establecen los siguientes lineamientos de obligatorio cumplimiento:

1. Políticas de Seguridad de la Información.

Se reitera la obligatoriedad del cumplimiento de la Política de Seguridad de Información de la Secretaría Distrital del Hábitat. Al respecto, se ha indicado que (…) *"La SECRETARÍA DISTRITAL DEL HÁBITAT entendiendo la importancia de la adecuada gestión de la seguridad de la información, se ha comprometido con la implementación de buenas prácticas para la gestión de seguridad de la información y/o el Modelo de Seguridad y Privacidad de la Información, con un compromiso total de la alta dirección, manteniendo la confidencialidad, integridad y disponibilidad de sus activos de información mediante una gestión del riesgo continua, la adopción de buenas prácticas en el uso y gestión de los activos de información, así como la mejora de las competencias y conciencia de los servidores públicos y colaboradores de la entidad, con criterios de decisión aprobados y cumpliendo las normas legales, reglamentarias y contractuales adoptadas por la Secretaria Distrital del Hábitat.*

Los servidores públicos, proveedores, usuarios o terceras partes son responsables por el adecuado manejo y aseguramiento de la información utilizada en el desarrollo de sus actividades, en el cumplimiento de los lineamientos, requisitos, controles y buenas prácticas de seguridad de la información definidas por la entidad, así como la prevención, detección y reporte de cualquier incidente relacionado con la seguridad de la información."

2. **Protocolo de seguridad para equipos de cómputo e información institucional.**

Controles obligatorios:

A. Seguridad física del equipo

Todo equipo de cómputo susceptible a movimientos o desplazamientos deberá contar con las medidas de protección física necesarias, garantizando su integridad y continuidad operativa. Estas medidas deberán incluir, como mínimo, mecanismos de anclaje, fijación, protección contra golpes, barreras físicas y cualquier otro elemento que mitigue riesgos asociados al uso, manipulación o exposición del equipo de la siguiente manera:

1. Uso de guaya de seguridad en el caso de computadores portátiles.
   - Los portátiles deben asegurarse con guaya cuando estén en oficina, sala de juntas, eventos o espacios compartidos.
   - La guaya debe fijarse a un punto sólido del escritorio o mobiliario.
   - No debe dejarse el equipo sin guaya durante pausas, reuniones o almuerzos.
2. No dejar equipos desatendidos.
   - No debe dejar portátil, o Tablet sin supervisión en lugares públicos.
   - En vehículos, los equipos no deben quedar visibles.
3. Seguridad de equipos portátiles.
   - Al finalizar la jornada, los portátiles deben permanecer con guaya o bajo llave.
   - Las llaves no deben dejarse sobre el escritorio ni en lugares visibles.
4. Control de acceso a oficinas.
   - Las oficinas deben permanecer cerradas cuando no estén ocupadas.
   - Visitantes, proveedores o personal externo no deben permanecer solos en oficinas.
5. Todo cambio, movimiento o desplazamiento de equipos deberá ser coordinado previamente con el área de Bienes y Servicios de la Dirección Administrativa, en cumplimiento de los procedimientos establecidos. La mesa de ayuda de la OTTD y su equipo de trabajo, no realizarán movimientos

físicos de equipos de cómputo que no estén coordinados con el área de Bienes y Servicios y orientarán a los usuarios hacia dicha área o quien haga sus veces como custodio de los bienes físicos de la Entidad para la gestión correspondiente.

B. Política de escritorio limpio.

Se debe mantener el escritorio libre de información sensible expuesta.

1. Documentos físicos
   - No dejar contratos, actas, informes, datos personales, estrategias o documentos confidenciales sobre el escritorio.
   - Todo documento sensible debe guardarse al terminar su uso.
2. Tableros y salas
   - Después de reuniones, deben borrarse tableros, recoger documentos y cerrar sesiones en pantallas compartidas.

C. Seguridad lógica del equipo de cómputo.

- Se debe bloquear manualmente el equipo al retirarse del puesto usando Windows + L o equivalente.
- Al finalizar la jornada se deben cerrar las sesiones de correo, SharePoint, OneDrive, VPN, sistemas misionales y aplicativos institucionales, luego realizar el apagado de los equipos de cómputo.

D. Manejo de información.

1. Clasificación de información
   - Toda información debe manejarse según su nivel: pública, interna, confidencial o restringida.
   - Información estratégica, financiera, legal, datos personales y credenciales deben tratarse como confidenciales o restringidas.
2. Almacenamiento autorizado
   - La información corporativa debe guardarse en repositorios oficiales: nube corporativa, servidor, SharePoint, OneDrive institucional o sistema aprobado por la Oficina de Tecnología y Transformación Digital.
3. Prohibición de medios no autorizados
   - No se deben usar USB personales, discos externos no cifrados ni servicios personales como correos privados, WhatsApp personal, Google Drive personal o Dropbox personal para información corporativa.
4. Envío de información
   - Validar destinatarios antes de enviar correos.
   - No reenviar información estratégica a cuentas personales.

E. Gestión de contraseñas y control de acceso.

El acceso a los sistemas y servicios institucionales se otorga bajo el principio de mínimo privilegio, de acuerdo con el rol del usuario, y debe protegerse mediante credenciales seguras:

- Las contraseñas deben ser robustas (mínimo doce caracteres, combinando mayúsculas, minúsculas, números y símbolos), de uso personal e intransferible.
- No se deben compartir, reutilizar ni almacenar contraseñas en archivos, navegadores no autorizados o notas visibles.
- Debe activarse el doble factor de autenticación (MFA) en los servicios institucionales que lo dispongan.
- La asignación y el uso de accesos privilegiados son controlados por la Oficina de Tecnología y Transformación Digital (OTTD).
- Cualquier sospecha de compromiso de credenciales debe reportarse de inmediato a la OTTD.
- Todos los usuarios administradores, así como quienes gestionen sistemas de información, bases de datos, servicios de interoperabilidad o cualquier otro activo tecnológico de la Entidad que requiera el uso de credenciales de gestión y/o administración, deberán cumplir estrictamente con los lineamientos establecidos en el documento *PG07-PR07 Procedimiento de Gestión de Contraseñas de Administrador*. Este cumplimiento es obligatorio para garantizar la seguridad, trazabilidad, integridad y adecuada protección de los activos de información bajo su responsabilidad, en concordancia con las políticas del SGSI y los estándares institucionales de control y acceso.

F. Copias de respaldo de la información.

La información institucional debe estar respaldada para garantizar su disponibilidad e integridad:

- La información corporativa crítica debe almacenarse en los repositorios oficiales que garantizan respaldo (SharePoint, OneDrive institucional, servidores o sistemas aprobados por la OTTD).
- No debe conservarse como única copia la información guardada en el disco local del equipo.
- Las copias de respaldo de los sistemas de información son responsabilidad de la OTTD, conforme a los procedimientos del Mapa SIG.

G. Protección contra software malicioso.

Todos los equipos deben mantener activas las medidas de protección contra código malicioso:

- No se debe deshabilitar el antivirus o antimalware institucional.
- No se debe instalar software no autorizado ni descargar programas de fuentes no confiables.
- No se deben abrir archivos adjuntos ni enlaces de remitentes desconocidos o sospechosos (phishing).
- Cualquier alerta o comportamiento anómalo del equipo debe reportarse a la OTTD.

H. Cifrado de la información.

La información clasificada como confidencial o restringida debe protegerse mediante cifrado:

- La información confidencial o restringida debe cifrarse al almacenarse o transmitirse por medios externos.
- Los medios removibles autorizados deben estar cifrados.
- No se debe transmitir información sensible por canales no cifrados o no institucionales.

Cualquier inquietud al respecto, comunicarse con la OTTD por los medios disponibles establecidos.

I. Trabajo remoto y uso de VPN.

El acceso remoto a los recursos institucionales debe realizarse de forma segura:

- El acceso remoto debe efectuarse únicamente a través de la VPN autorizada por la OTTD.
- Debe mantenerse el equipo actualizado y protegida la red doméstica con contraseña.
- Debe evitarse el uso de redes Wi-Fi públicas o no confiables para acceder a información institucional.
- Al finalizar la jornada deben cerrarse la sesión de la VPN y los aplicativos institucionales.

J. Gestión y reporte de incidentes de seguridad de la información.

Todo evento o incidente de seguridad debe gestionarse de manera oportuna:

- Los incidentes (pérdida o robo de equipos, acceso no autorizado, fuga de información, infección por malware o intentos de phishing) deben reportarse de manera inmediata a la OTTD a través de la mesa de ayuda o el canal dispuesto para tal fin.

- No se debe intentar resolver el incidente por cuenta propia ni alterar las evidencias.
- Deben atenderse las instrucciones de la OTTD para la contención y recuperación.

K. Capacitación y concientización en seguridad de la información.

El fortalecimiento de la cultura de seguridad es responsabilidad de todos:

- Es obligatoria la participación en las jornadas de sensibilización y capacitación en seguridad de la información que programe la entidad.
- Deben aplicarse de manera permanente las buenas prácticas divulgadas por la OTTD.

L. Vigencia, seguimiento y actualización.

La presente circular rige a partir de su expedición y complementa el Manual de Políticas de Seguridad de la Información SDHT 2025 y los procedimientos del Mapa SIG:

- La OTTD verificará el cumplimiento de los presentes lineamientos; su inobservancia podrá dar lugar a las acciones disciplinarias, administrativas o contractuales a que haya lugar conforme a la normativa vigente.
- Estos lineamientos podrán ser actualizados o complementados mediante futuras circulares o insumos técnicos expedidos por la OTTD, los cuales se entenderán incorporados a este marco.

Cordialmente,

CARLOS GABRIEL GUTIERREZ PACHECO
Jefe de Oficina de Tecnología y Transformación Digital

Elaboró: Khaanko Norberto Ruiz Rodríguez - Contratista OTTD
Revisó: Jose Luis Daza Pérez – Contratista OTTD