DIRECTIVA No. 003

24 FEB 2017

PARA SUBSECRETARIO GENERAL Y DE CONTROL DISCIPLINARIO, ASESORES, DIRECTORES, SUBDIRECTORES, JEFES DE OFICINA, FUNCIONARIOS Y CONTRATISTAS DE LA SECRETARÍA DISTRITAL DE AMBIENTE.

DE FRANCISO JOSE CRUZ PRADA
Secretario Distrital de Ambiente

ASUNTO Lineamientos para el control y la implementación del Subsistema de Gestión de Seguridad de la Información en la SDA.

FECHA

La Ley 87 de 1993, por la cual se dictan normas para el ejercicio del Control Interno en las entidades y organismos del Estado Colombiano, en su artículo 6° determina que: *"El establecimiento y desarrollo del Sistema de Control Interno en los organismos y entidades públicas será responsabilidad del Representante Legal o máximo directivo correspondiente"*.

El Decreto Distrital 680 de 2001, modificó el Decreto 443 de 1990, por el cual se creó la Comisión Distrital de Sistemas, en el sentido de asignarle funciones en materia de: Coordinación de la gestión informática y de comunicaciones de las entidades del Distrito Capital; políticas y estándares informáticos y de comunicaciones; apoyo a la formulación y desarrollo de proyectos informáticos y de comunicaciones.

Por su parte, el Acuerdo Distrital 57 de 2002, por el cual se implementó el Sistema Distrital de Información SDI y se organizó la Comisión Distrital de Sistemas, estableció que las políticas, estrategias y recomendaciones de la Comisión Distrital de Sistemas, son de obligatorio cumplimiento por parte de las entidades del Distrito Capital por ser el organismo rector en materia de tecnología informática y de comunicaciones en la ciudad capital.

Al paso el Acuerdo 257 de 2006, por el cual se reformó la estructura, organización y funcionamiento de las entidades del Distrito Capital, en su artículo 5° dispone que:

> *"Las actuaciones administrativas serán públicas, soportadas en tecnologías de información y comunicación, de manera que el acceso a la información oportuna y confiable facilite el ejercicio efectivo de los derechos constitucionales y legales y los controles ciudadanos, político, fiscal, disciplinario y de gestión o administrativo, sin perjuicio de las reservas legales."*

Así las cosas, la Comisión Distrital de Sistemas de Bogotá, mediante la Resolución 305 de 2008, expidió políticas de seguridad de la información en el Distrito Capital, en tal sentido dispuso:

"Artículo 9. Objetivo. La utilización creciente de las Tecnologías de la Información y las Comunicaciones –TIC, genera beneficios para las entidades, organismos y órganos de control del Distrito Capital, mejorando el cumplimiento de la misión y la prestación de servicios a la ciudadanía. Sin embargo, por ser la información el activo más importante de la organización, es necesario protegerla frente a los posibles riesgos derivados del uso de las nuevas tecnologías, para garantizar la seguridad de la información, en aspectos tales como disponibilidad, confiabilidad, accesibilidad e integridad de la misma, en los términos de la Directiva 05 de 2005 del Alcalde Mayor de Bogotá.

Artículo 10. Definiciones.

10.1 Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.
10.1.1 Confidencialidad: Aseguramiento de que la información es accesible sólo para quienes están autorizados.
10.1.2 Integridad: Salvaguardia de la exactitud y completitud de la información y sus métodos de procesamiento.
10.1.3 Disponibilidad: Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando se requiera.
10.2 Activos de información: Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano y organismo.

Artículo 11. Marco Legal. Las entidades, organismos y órganos de control del Distrito Capital disponen de un marco de referencia de las mejores prácticas para el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información, basados en las recomendaciones de las normas internacionales: NTC ISO/IEC 27001 que establece los requisitos del Sistema de Gestión de Seguridad de la Información (...) y demás normas concordantes, las cuales son de obligatoria observancia por parte de los entes públicos distritales.

Artículo 13. Las directrices y lineamientos definidos deben ser difundidos, incorporados y acogidos al interior de cada una de las entidades, organismos y órganos de control del Distrito Capital, que junto con las normas internacionales generalmente aceptadas, son la base para que se implemente el Sistema de Gestión de Seguridad de la Información (SGSI), el cual debe estar alineado con el Sistema Integrado de Gestión, en cada uno de sus componentes, esto es, los Sistema de Gestión de Calidad, Control Interno, Desarrollo Administrativo y Gestión Ambiental."

Siguiendo esta misma línea, la aludida Resolución 305 de 2008, establece que la política de seguridad es de obligatorio cumplimiento para todos los servidores públicos y particulares que accedan a la información del respectivo ente público, así como a los espacios físicos del mismo que conlleven un componente de seguridad de información, de tal manera, en el artículo 16 prescribe:

"Las entidades, organismos y órganos de control del Distrito Capital deben adoptar políticas de seguridad y custodia de los datos y la información, y establecer los procedimientos para el adecuado uso y administración de los recursos informáticos de los cuales se valgan para cumplir con sus funciones administrativas, operativas y misionales."

El Decreto 176 del 12 de mayo de 2010, por el cual se dictaron lineamientos para la conformación articulada de un Sistema Integrado de Gestión en el Distrito Capital, dispuso el sistema como el conjunto de orientaciones, procesos, políticas, metodologías, instancias e instrumentos orientados a garantizar un desempeño institucional articulado y armónico, conformado por los siguientes subsistemas:

"Subsistema de Gestión de la Calidad (SGC); Subsistema Interno de Gestión Documental y Archivo (SIGA); Subsistema de Gestión de Seguridad de la Información (SGSI); Subsistema de Seguridad y Salud Ocupacional (S&SO); Subsistema de Responsabilidad Social (SRS); Subsistema de Gestión Ambiental (SGA); Subsistema de Control Interno (SCI), y adicionalmente para los Hospitales del Distrito Capital, el Subsistema único de Acreditación (SUA)."

De conformidad con el Decreto Nacional 2482 de 2012, por el cual se establecieron los lineamientos para la integración de la planeación y la gestión en la Administración Pública, se adoptó entre otras, la política de eficiencia administrativa:

"Orientada a identificar, racionalizar, simplificar y automatizar trámites, procesos, procedimientos y servicios, así como optimizar el uso de recursos, con el propósito de contar con organizaciones modernas, innovadoras, flexibles y abiertas al entorno, con capacidad de transformarse, adaptarse y responder en forma ágil y oportuna a las demandas y necesidades de la comunidad, para el logro de los objetivos del Estado. Incluye, entre otros, los temas relacionados con gestión de calidad, eficiencia administrativa y cero papel, racionalización de trámites, modernización institucional, gestión de tecnologías de información y gestión documental."

La norma NTC-ISO-IEC 27001:2013 es una norma internacional para la seguridad de la información, avalada por el Instituto Colombiano de Normas y Técnicas y Certificación ICONTEC, acogida por la Secretaría Distrital de Ambiente con sujeción a los dictados de la Comisión Distrital de Sistemas de la Alcaldía Mayor, especialmente en los Anexo A, numeral A.11.2.9 *"Política de Escritorio Limpio y Pantalla Limpia"* y Anexo A, numeral A.6.2.1 *"Política para Dispositivos Móviles"*, sobre los cuales se fijarán los presentes lineamientos para el control y la implementación del Subsistema de Gestión de Seguridad de la Información en la Secretaría Distrital de Ambiente en lo que corresponde a estos dos componentes.

A tono con lo anterior, el 11 de abril de 2016 el Consejo Nacional de Política Económica y Social –CONPES- a través del Documento CONPES 3854, aprobó la nueva *"Política de Seguridad Digital"* en el país, convirtiendo a Colombia en el primer país de Latinoamérica, en incorporar plenamente las recomendaciones y mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas por la Organización para la Cooperación y el Desarrollo Económico (OCDE), en vía de fortalecer el enfoque de la política de

ciberseguridad y ciberdefensa debido a las sofisticadas formas de afectar el avance normal del entorno digital en el desarrollo de las actividades económicas y sociales del país.

En el marco de sus competencias, el Secretario Distrital de Ambiente el 22 de abril de 2016 mediante la Resolución 363, como líder del proceso de Direccionamiento Estratégico actualizó el proceso 126MSIG Manual del Sistema Integrado de Gestión en términos de actualizar los objetivos estratégicos incluyendo lo referente al Subsistema de Gestión de Seguridad de la Información incorporando las políticas de seguridad de la información, así mismo, con Resolución 2269 del 20 de diciembre de 2016 se actualizaron los requisitos de la norma ISO14001 versión 2015.

Bajo el esquema funcional del Sistema Integrado de Gestión y acorde con las Resoluciones expedidas por la Secretaría Distrital de Ambiente 362/2016 y 291/2017, la Dirección de Planeación y Sistemas de Información Ambiental, será la encargada de administrar el directorio activo de red e implementar las directrices de seguridad definidas para el manejo y protección de la información. De igual forma, esta Dirección con el apoyo del equipo implementador del SGSI, será la encarga de determinar los requisitos de Seguridad en lo atinente al tratamiento de la información y la correcta aplicación de la presente directiva.

En consideración a todo lo anterior, la presente directiva fija los lineamientos para el control y la implementación del Subsistema de Gestión de Seguridad de la Información en la Secretaría Distrital de Ambiente e insta a todos los funcionarios y contratistas de la entidad y a aquellos particulares que ejerzan labores de la entidad, para que en adelante y en cumplimiento de sus obligaciones constitucionales y legales den cumplimiento a las siguientes políticas institucionales.

ESCRITORIO LIMPIO Y PANTALLA LIMPIA

La política específica del Subsistema de Gestión de Seguridad de la Información sobre *Escritorio limpio y pantalla limpia* considera, entre otros puntos, que la Secretaría Distrital de Ambiente promoverá la cultura de escritorio y pantalla limpios, donde cada servidor público de la entidad se compromete a mantener protegida la información en sus áreas de trabajo a través de la correcta custodia y disposición de documentos, CD, dispositivo USB y cualquier otro medio de almacenamiento, así como bloqueando la sesión de su estación de trabajo en el momento en que se ausente.

La norma NTC-ISO-IEC 27001:2013, contempla en el Anexo A, numeral A.11.2.9 Política de escritorio limpio y pantalla limpia "*Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de la información.*"

Con el objetivo de reducir el riesgo y probabilidades de fuga, pérdida de información y acceso no autorizado durante y fuera de las horas de trabajo, mediante la organización de los archivos, documentos en el escritorio del sistema operativo del computador y memorias USB, CD, DVD, notas tipo post-it, artículos personales o de dotación que el usuario genere y ubique en su mesa de escritorio o pantalla física.

Pantalla Limpia

- La pantalla de autenticación a la red de la Secretaría Distrital de Ambiente debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información.

- En el escritorio de Windows solo deberá tener los accesos directos a los programas más frecuentes, es decir aquellos que use diariamente, no deberá tener archivos ni accesos directos a archivos ya sean de trabajo o asuntos personales.

- Está prohibida la instalación de programas informáticos o almacenamiento de información para uso personal o que no estén asociados a las labores propias dentro de la entidad, lo anterior en procura de mantener un ecosistema de licenciamiento de software sano para la entidad y un uso apropiado de los recursos informáticos suministrados para sus labores diarias.

- En el evento en el que el usuario deba retirarse de su puesto de trabajo o desatender su computador, está en la obligación de bloquear su sesión en la red, por ninguna razón deberá dejar su sesión abierta, esto lo podrá realizar de la siguiente manera:

COMANDO	FUNCIÓN
Tecla Windows + tecla L	Bloquea la sesión del usuario en el equipo de cómputo, seguidamente el usuario debe loggearse con usuario y contraseña.
Tecla Windows + tecla m:	Combinación de teclado en Windows que permite rápidamente minimizar todas las ventanas para permitir la visualización rápida del escritorio de Windows.
Ctrl + Alt + Del y luego Enter	Evento en el cual el usuario presiona simultáneamente las teclas conocidas comúnmente como Control + Alt + Delete, seguidamente las libera y por último presiona la tecla enter, el efecto de este procedimiento es bloquear la sesión del usuario en la red de cómputo de la entidad; solo tiene efecto en el Sistema Operativo Windows.
Ctrl + Alt + Del	Procedimiento similar al anterior, lo usa el usuario para desbloquear el computador y así poder continuar con su sesión en Windows.

Tabla 1. Comandos de acceso rápido

- Una vez bloqueada la sesión, deberá apagar la pantalla como lineamiento de eficiencia del uso de energía. Esto garantiza que el riesgo de que personas no autorizadas o que no tengan competencia accedan a su sesión en red.

- Al final de la jornada todos los usuarios deberán apagar el computador, sin perjuicio de aquellos casos que por razones asociadas exclusivamente a sus labores podrá dejar encendida la CPU, pero la sesión bloqueada como se explicó en un lineamiento anterior.

- Con el fin de proteger la información de las terminales de cómputo de la entidad, la DPSIA determina el bloqueo automático de las sesiones después de diez (10) minutos de inactividad con la finalidad de brindar seguridad a la información en puestos de trabajo sin atención.

- Los fondos de pantalla y salva pantallas son exclusivamente institucionales, evite usar fotos familiares, personales o en general información ajena a la entidad para la cual usted presta sus servicios, como regla general la entidad controla que los fondos y los bloqueos de pantalla sean administrados a partir de las políticas del Directorio Activo de la red, sin que medie la intervención de los usuarios finales.

Escritorio Limpio

- Cada usuario es responsable de su espacio o puesto de trabajo. Deberá encargarse de mantener de forma segura y a su alcance visual todos los objetos propios para desarrollar sus funciones diarias, asegurándolos una vez que ha finalizado su labor o incluso en ausencias cortas durante la jornada laboral.

- Evitar el consumo de alimentos o bebidas cerca de los equipos de cómputo que pongan en riesgo los mismos.

- Los usuarios serán autoresponsables respecto de la ubicación física de los equipos de cómputo asignados para sus labores.

- Para el caso de los equipos que están ubicados en dependencias de acceso al público, todas las pantallas se ubicarán preferiblemente de forma tal que los ciudadanos no puedan tener contacto visual directo con la misma. El funcionario o contratista por ninguna razón deberá girar o mostrar la pantalla a los ciudadanos ya que para efectos de suministrar o exhibir la información al público la entidad tiene otros procedimientos establecidos.

- El tratamiento de memorias USB, medios como CD, DVD o similares son de estricto uso para tareas propias de la entidad, una vez usadas el usuario deberá retirar estos medios del computador y su puesto de trabajo. Cuando el funcionario o contratista deba ausentarse de su puesto de trabajo, no deben dejar conectados al ordenador los referidos dispositivos de almacenamiento externo, puesto que es un riesgo a la pérdida de información por extracción de estos elementos.

- Todos los usuarios sin excepción procurarán no dejar notas, post-it, hojas impresas medios magnéticos al alcance de cualquier persona en su puesto de trabajo o pantalla del computador, indistintamente de la información que contengan y mucho menos si se trata de información corporativa; si requiere de disposición especial y segura para almacenar información impresa o en medios magnéticos, notifique formalmente a su jefe inmediato o jefe de área para tomar las medidas formales y respectivas.

- El usuario deberá enviar impresión confidencial asignado una clave de impresión y es el encargado de retirar sus impresiones, esto en procura de mitigar el acceso a información por parte de otras personas ajenas a su dependencia o que no requieran el conocimiento de la misma, sin desmedro de las disposiciones que regulan la política de Cero Papel.

- No dejar el teléfono celular sobre el escritorio sin estar bloqueado, esto podría revelar información confidencial.

- Al finalizar la jornada de trabajo, los funcionarios y contratistas deben guardar en un lugar seguro los documentos, medios y dispositivos que contengan información confidencial o de uso interno de la entidad.

DISPOSITIVOS MÓVILES

La política específica del Subsistema de Gestión de Seguridad de la Información sobre *Dispositivos móviles* considera, entre otros puntos, que "*Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la SDA con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad.*"

La norma NTC-ISO-IEC 27001:2013, contempla en el Anexo A, numeral A.6.2.1 Política para dispositivos móviles "*Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.*"

La Dirección de Planeación y Sistemas de Información Ambiental (DPSIA) instruye sobre el uso apropiado de los dispositivos móviles de propiedad de la entidad asignados al servicio de los funcionarios y contratistas de la Secretaría Distrital de Ambiente para el cumplimiento de sus labores con el fin de proteger la información de la entidad de daño, perdida, modificación accidental o intencional.

Dentro del marco de lo anteriormente dicho, la DPSIA determina los siguientes lineamientos básicos para la correcta administración y manejo de los dispositivos móviles.

- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto al momento de su entrega.

- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

- Cada vez que el sistema de los dispositivos móviles institucionales notifique de una actualización disponible, los usuarios deben aceptar y aplicar la nueva versión.

- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como, deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador de establecimiento público (hoteles, cafés internet, entre otros).

- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

- Los usuarios deben utilizar el plan de datos asignado por la entidad en los dispositivos móviles institucionales, únicamente para el acceso a herramientas, programas y páginas de Internet relacionadas con sus labores.

- No está permitido en la Secretaría Distrital de Ambiente ni en los dispositivos móviles el acceso a páginas relacionadas con pornografía, drogas y/o cualquier otra que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

- No se permite el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Twitter, WhatsApp, Tango, Viber, Skype, Net2phone y otros similares. En el evento de ser requerido el acceso a estas aplicaciones por la naturaleza de sus labores, deberá solicitar autorización expresa a través de la dependencia a la que pertenezca la cual se comunicará a la Dirección de Planeación y Sistemas de Información Ambiental para efectos de su activación.

- No se permite la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y confidencialidad de los activos de información de la Secretaría Distrital de Ambiente.

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares donde no realice labores propias de sus funciones u objetos contractuales y que no ofrezcan garantías de seguridad física para evitar pérdida o robo de estos.

El incumplimiento de las previsiones aquí dispuestas dará lugar a sanciones administrativas sin perjuicio de las demás acciones a que haya lugar.

La presente Directiva es de obligatorio cumplimiento a partir de la fecha de su expedición y deberá será publicada en el Boletín Legal de la Secretaría Distrital de Ambiente.

FRANCISCO JOSÉ CRUZ PRADA
Secretario Distrital de Ambiente

Aprobó: Viviana Carolina Ortiz Guzmán –Directora Legal Ambiental.
Revisó: Shirley Andrea Zamora Mora –Directora de Planeación y Sistemas de Información Ambiental.
Proyectó: Sandra Patricia Mora Escalante –Equipo SIG.
Yeandri Natalia Moreno López DPSIA
Ma Concepción Osuna Ch –DLA.