Que en mérito de lo expuesto,

DECRETA:

ARTÍCULO 1. Modificar el numeral 5 del artículo 7 del Decreto Distrital 557 de 2018, el cual quedará así:

"ARTÍCULO 7. Funciones. Son funciones del Consejo Distrital del DRAFE:

(…)

5. Adoptar, modificar y dar cumplimiento a su reglamento.

(…)".

ARTÍCULO 2. Modificar el numeral 7 y adicionar el numeral 8 del artículo 11 del Decreto Distrital 557 de 2018, los cuales quedarán así:

"ARTÍCULO 11. Funciones. Son funciones de los Consejos Locales del DRAFE:

(…)

7. Adoptar, modificar y dar cumplimiento a su reglamento.

8. Reemplazar a los consejeros que presentan renuncia y suplir las vacantes de los sectores donde fueron declaradas desiertas las elecciones realizadas de conformidad con lo dispuesto en el artículo 14A del presente decreto, teniendo en cuenta los mecanismos dispuestos para el efecto en el reglamento interno del Consejo Local."

ARTÍCULO 3. Adicionar el artículo 14A al Decreto Distrital 557 de 2018, el cual quedará así:

*"**ARTÍCULO 14A. Elección Atípica.** Cada Consejo Local del DRAFE podrá reemplazar a los consejeros que presentan renuncia y suplir las vacantes de los sectores donde fueron declaradas desiertas las elecciones realizadas, mediante un proceso simplificado de elecciones, los cuales podrán ser mediante asambleas, análisis de experiencia, estudio de hojas de vida u otro mecanismo que se haga a través de convocatoria pública y cuente con el aval previo de la Secretaría Distrital de Cultura, Recreación y Deporte, el Instituto Distrital de Recreación y Deporte -IDRD y la Alcaldía Local respectiva, garantizando los principios de transparencia y eficacia.*

***PARÁGRAFO.** Previo al aval, las citadas entidades verificarán como mínimo: que la solicitud del proceso contenga la justificación y el mecanismo de elección seleccionado por el Consejo Local, que se hayan determinado el lugar y la forma de recepción de los documentos de los candidatos, así como el cronograma que señale las actividades y fechas que garanticen el cumplimiento del mecanismo seleccionado y las formas de divulgación de la convocatoria".*

ARTÍCULO 4. Vigencia y derogatoria. El presente decreto rige a partir del día siguiente a la fecha de su publicación.

PUBLÍQUESE Y CÚMPLASE.

Dado en Bogotá, D.C., a los veintidós (22) días del mes de octubre de dos mil diecinueve (2019).

ENRIQUE PEÑALOSA LONDOÑO
Alcalde Mayor

MARÍA CLAUDIA LÓPEZ SORZANO
Secretaria Distrital de Cultura, Recreación y Deporte

RESOLUCIONES DE 2019

SECRETARÍA DE HACIENDA

Resolución Número SDH-000316
(Octubre 17 de 2019)

"Por medio de la cual se adopta un nuevo Protocolo de Seguridad para las tesorerías de órganos y entidades que hacen parte del Presupuesto Anual del Distrito Capital y los Fondos de Desarrollo Local".

LA SECRETARIA DISTRITAL DE HACIENDA
En uso de las facultades que le confieren el artículo 62 del Acuerdo 257 de 2006, los artículos 2 y 4 del Decreto Distrital 601 de 2014, modificado por el artículo 1 del Decreto Distrital 364 de 2015, y

CONSIDERANDO:

Que de conformidad con el artículo 62 del Acuerdo 257 de 2006, el literal e) del artículo 2 y literal a) del artículo 4, ambos del Decreto Distrital 601 de 2014, modificado por el artículo 1º del Decreto Distrital 364 de 2015, corresponde a la Secretaría Distrital de Hacienda formular, orientar, coordinar y ejecutar las políticas tributaria, presupuestal, contable y de tesorería del Distrito Capital.

Que según el artículo 5 del Decreto Distrital 216 de 2017, reglamentario del Estatuto Orgánico del Presu-

puesto Distrital, corresponde a la Secretaría Distrital de Hacienda, por medio de la Dirección Distrital de Tesorería, aplicar el mecanismo de la Cuenta Única Distrital, mediante el cual debe recaudar, administrar, invertir, pagar, trasladar y/o disponer los recursos correspondientes al Presupuesto Anual del Distrito Capital y los Fondos de Desarrollo Local. No obstante, la misma norma prevé que, hasta tanto se implemente en su totalidad la Cuenta Única Distrital, los establecimientos públicos podrán continuar transitoriamente con las funciones de recaudar, administrar, invertir, pagar, trasladar o disponer respecto de sus recursos administrados.

Que la Secretaría Distrital de Hacienda, mediante Resolución SDH-314 de 2009 adoptó el *"Protocolo de Seguridad para las tesorerías de las entidades descentralizadas que conforman el Presupuesto Anual del Distrito Capital",* documento que se estima conveniente actualizar y sustituir integralmente mediante la presente Resolución.

Que en cumplimiento del artículo 8 de la Ley 1437 de 2011, el proyecto de resolución se publicó en el Portal Web de la Secretaría Distrital de Hacienda desde el día 25 de septiembre hasta el 1º de octubre de 2019, sin que se hubieran recibido comentarios por parte de la ciudadanía.

RESUELVE:

ARTÍCULO 1. Adopción del Protocolo de Seguridad: Adóptese el "Protocolo de Seguridad para las tesorerías de órganos y entidades que hacen parte del Presupuesto Anual del Distrito Capital", documento anexo que forma parte integral de la presente Resolución, contentivo de lineamientos y buenas prácticas enmarcados en la normatividad nacional y distrital aplicable, en los estándares de las instituciones financieras y en la experiencia que desde las entidades del Distrito Capital se ha recogido para la seguridad de los recursos administrados.

ARTÍCULO 2. Ámbito de aplicación: El Protocolo de Seguridad que se adopta mediante la presente Resolución es aplicable a todas las entidades que conforman el Presupuesto Anual del Distrito Capital y los Fondos de Desarrollo Local. Los representantes Legales y los servidores públicos competentes de dichas entidades tendrán la responsabilidad exclusiva de implementar, fortalecer, hacer seguimiento y supervisar permanentemente las buenas prácticas, procedimientos y controles adoptados para la seguridad y la prevención de riesgos en la gestión de tesorería y manejo de recursos del presupuesto.

PARÁGRAFO 1: La gestión integral de tesorería a cargo de la Dirección Distrital de Tesorería de la Secretaría Distrital de Hacienda continuará rigiéndose, en materia de seguridad, por la política establecida mediante Resolución SDH-324 de 2017 y demás normas y políticas aplicables.

PARÁGRAFO 2: El presente Protocolo de Seguridad podrá ser utilizado como referencia, en forma voluntaria, por las entidades distritales que no hacen parte del Presupuesto Anual del Distrito Capital. No obstante, los representantes legales en cada una de estas entidades en el marco de su autonomía y responsabilidad legal, administrativa y financiera y normas generales y especiales aplicables y en sus servidores públicos competentes tienen la responsabilidad exclusiva de definir, implementar y controlar sus respectivas políticas, protocolos, procedimientos y controles para la seguridad de sus tesorerías.

ARTÍCULO 3. Para efectos de la aplicación de esta Resolución, la remisión hecha a normas jurídicas se entenderá realizada a las que las modifiquen, adicionen o sustituyan.

ARTÍCULO 4. Vigencia y derogatorias: La presente Resolución rige a partir del día siguiente a la fecha de su publicación en el Registro Distrital y deroga la Resolución SDH-314 de 2009.

PUBLÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los diecisiete (17) días del mes de octubre de dos mil diecinueve (2019).

BEATRIZ ELENA ARBELÁEZ MARTÍNEZ
Secretaria Distrital de Hacienda

PROTOCOLO DE SEGURIDAD PARA LAS TESORERÍAS DE ENTIDADES Y ÓRGANOS QUE HACEN PARTE DEL PRESUPUESTO ANUAL DEL DISTRITO CAPITAL Y LOS FONDOS DE DESARROLLO LOCAL

CAPÍTULO 1
OBJETO Y PRINCIPIOS PARA LA SEGURIDAD EN LA GESTIÓN TESORAL

1.1. OBJETO

Mediante este Protocolo se establecen lineamientos y buenas prácticas que la Secretaría Distrital de Hacienda recomienda aplicar a las entidades y órganos que

hacen parte del Presupuesto Anual del Distrito Capital, así como a los Fondos de Desarrollo Local, en adelante las entidades destinatarias, con el fin de fortalecer la seguridad de su gestión de tesorería y minimizar riesgos en el manejo de los recursos del presupuesto distrital. Lo anterior, teniendo en cuenta la normatividad nacional y distrital aplicable, los estándares de las instituciones financieras y la experiencia que desde las entidades del Distrito Capital se ha recogido para la seguridad de los recursos administrados.

En el marco de su autonomía administrativa, responsabilidad, funciones y competencias cada entidad distrital sujeta a la presente Resolución y sus servidores públicos competentes serán los exclusivos responsables de desplegar, formalizar, fortalecer, hacer seguimiento y controlar las buenas prácticas, procedimientos, controles y demás medidas adoptados para la seguridad y la prevención de riesgos en su gestión de tesorería y manejo de recursos del presupuesto distrital. En ese orden, las prácticas recomendadas en el presente documento deberán adecuarse, bajo exclusiva responsabilidad de cada entidad y de sus servidores públicos, a las características, recursos disponibles y riesgos financieros y operativos propios de cada entidad destinataria.

1.2. COMPROMISO INSTITUCIONAL

La seguridad e integridad de las operaciones de tesorería a cargo de los órganos y entidades que conforman el Presupuesto Anual del Distrito Capital y los Fondos de Desarrollo Local se fundan en el compromiso y el concurso efectivo y permanente de todos los servidores públicos de cada entidad, en el marco de los principios éticos y del conocimiento y el cumplimiento riguroso de las normas nacionales y distritales y de los procedimientos aplicables.

1.3. INTEGRACIÓN CON EL SISTEMA DE GESTIÓN DE CALIDAD

De conformidad con las normas y principios del Sistema Integrado de Gestión, las directrices, mejores prácticas y controles que las entidades destinatarias adopten en el marco del presente protocolo o de manera autónoma deberán reflejarse en el contenido de los procesos, procedimientos, instructivos, guías, formatos y demás documentos que conforman el Sistema de Gestión de Calidad de cada entidad destinataria.

1.4. SEGURIDAD DE LA INFORMACIÓN

En cada entidad destinataria la gestión de tesorería se desarrollará con estricta observancia de las políticas y manuales de seguridad de la información del Subsistema de Gestión de la Seguridad de la Información de cada entidad.

Por ser la información el activo más importante de la organización, esta deberá protegerse frente a posibles riesgos derivados del uso de la tecnología. Por lo tanto, cada entidad deberá analizar las particularidades de su funcionamiento y adoptar las políticas de protección y mitigación de riesgos que resulten pertinentes a sus condiciones y necesidades, adoptando el enfoque de gestión de riesgos y las normas o lineamientos que al respecto expidan las autoridades.

1.5. SEGREGACIÓN FUNCIONAL Y CONTROL DUAL

La gestión de tesorería deberá soportarse en una estructura y operación con segregación funcional y esquemas operativos de control dual, tanto administrativo como transaccional, siempre que sean aplicables y viables.

1.6. CONFIDENCIALIDAD

Sin perjuicio del cumplimiento de las normas sobre transparencia y acceso a la información pública, los servidores públicos de las entidades destinatarias cumplirán con el deber de confidencialidad respecto de la gestión de tesorería, absteniéndose de brindar información interna o privilegiada asociada a operaciones o estrategias de negociación, así como información ficticia o incompleta, que pueda provocar errores o favorecer indebidamente intereses particulares en la gestión de tesorería.

La información que deba suministrarse se entregará a los solicitantes por parte de los directivos y servidores públicos competentes de las entidades destinatarias, cumpliendo con la normativa y formalidades previstas para la atención de solicitudes y peticiones, o según los procedimientos para la rendición de cuentas o reporte a autoridades y entes de control, según sea el caso.

1.7. DEL RECURSO HUMANO

Frente al manejo del recurso humano vinculado a las labores de tesorería de las entidades destinatarias se tendrá en cuenta lo siguiente:

- Se definirán claramente el perfil, la experiencia y las competencias adecuadas para todos los cargos vinculados a la gestión de tesorería.
- Los cargos a los que se asigna el manejo de recursos públicos en las áreas de tesorería se consideran de confianza. Por esto se recomienda que en lo posible estos cargos se provean con personal de Libre Nombramiento y Remoción.
- Se realizarán estudios de seguridad dentro de los procesos de vinculación y contratación para

proveer los cargos vinculados a la gestión de tesorería, teniendo en cuenta garantías de confidencialidad de la información personal del candidato, de conformidad con la normativa aplicable.

- Se contará con póliza de manejo que ampare los actos de los servidores públicos que en las respectivas tesorerías se encarguen de la negociación, aprobación, cierre y registro de la operación de tesorería, de tal forma que se mitiguen los riesgos derivados de esas actividades.

- Se realizará capacitación y contacto permanente con las empresas proveedoras de servicios administrativos en las áreas de tesorería, de manera que realicen seguimiento sobre la observancia de las condiciones especiales de seguridad por parte del personal de apoyo a su cargo.

CAPÍTULO 2
SEGURIDAD FINANCIERA

Las operaciones de tesorería de las entidades destinatarias se llevarán a cabo en condiciones óptimas para la gestión del riesgo financiero y con cumplimiento estricto del marco legal y reglamentario. En especial se sujetarán a lo previsto en la Resolución SDH-73 de 2018, *"Por medio de la cual se establecen las políticas y lineamientos de inversión y de riesgo para el manejo de recursos administrados por las entidades que conforman el Presupuesto Anual del Distrito Capital y los Fondos de Desarrollo Local.*

Lo anterior, en concordancia con las normas contenidas en el Decreto Único Reglamentario del Sector Hacienda y Crédito Público 1068 de 2015; en el Decreto Distrital 714 de 1996, Estatuto Orgánico del Presupuesto Distrital, y en su reglamentación, contenida en el Decreto Distrital 216 de 2017.

En las operaciones de inversiones autorizadas por la normativa vigente se aplicarán y mantendrán debidamente documentados los controles para seguridad en las cotizaciones, cierres y registro de las operaciones, administración de recursos en cuentas y traslados, límites de administración de riesgos, perfiles y límites de las personas que intervienen en los procesos de negociación según la segregación de funciones.

Las inversiones en títulos se realizarán preferiblemente en forma desmaterializada, según los montos y condiciones de cada entidad destinataria.

Para la custodia de los títulos desmaterializados podrá contratarse sociedades fiduciarias autorizadas, previa suscripción del correspondiente contrato de custodia, en los términos del Libro 37 de la Parte 2 del Decreto Nacional 2555 de 2010.

CAPÍTULO 3
SEGURIDAD TECNOLÓGICA

En las operaciones de tesorería de las entidades destinatarias se fortalecerá la utilización de banca electrónica mediante recursos y controles tecnológicos.

3.1. SEGURIDAD INFORMÁTICA EN TESORERÍA

Directrices generales:

- Las redes de voz y datos se inhabilitarán durante los horarios y períodos distritales y nacionales no hábiles.

- Para proteger la confidencialidad, autenticidad y/o integridad de los archivos que ordenan operaciones de tesorería, se observarán lineamientos para uso adecuado y efectivo de la criptografía y el uso de técnicas de cifrado adoptadas en la entidad, teniendo en cuenta que esas operaciones corresponden a información sensible y restringida.

- En lo posible la tesorería se apoyará en una red privada de trasmisión de datos y conexión por canales dedicados, que permita la conexión con los bancos a través de Portal, sitios que deben estar debidamente avalados como seguros por un ente certificador autorizado. La conexión se protegerá con firewall preventores de intrusos, controles de contenido, antikeyloggers, antivirus, entre otros, para garantizar la seguridad en las comunicaciones y la confidencialidad de las operaciones.

- La conexión a las entidades financieras para la realización de operaciones se efectuará únicamente desde las direcciones IP fijas que la entidad autorice para transar, las cuales se recomienda que se asocien a la MAC del equipo. Estas direcciones IP fijas deben ser inscritas previamente en la entidad financiera.

- Se definirá y utilizará un número limitado de equipos de cómputo y de comunicaciones para la ejecución de las transacciones y en lo posible éstos se destinarán exclusivamente para ese efecto. Igualmente se establecerán, según los requerimientos de las entidades financieras, aquellas restricciones especiales en: conectividad, comunicaciones, software financiero autorizado, programas de seguridad informática y financiera y su respectivo mantenimiento y soporte, bajo estándares de seguridad y prevención del riesgo y demás restricciones necesarias para los equipos

destinados a la preparación, ejecución, control o cumplimiento de las transacciones.

- Los equipos también deben contar con herramientas de control de software malicioso: anti-virus, anti-keylogger, anti-spyware; activas y actualizadas. Se debe garantizar la continua actualización de los parches de seguridad del sistema operativo.

- Se bloquearán o controlarán los puertos USB, quemadoras de CD y DVD en los equipos dedicados a las transacciones con bancos.

- Se deben definir cronogramas de monitoreo para verificar periódicamente las condiciones de seguridad de los equipos utilizados para el ingreso de transacciones.

- Por lo menos una vez al año, el representante legal de la entidad destinataria o el servidor público en quien éste delegue formalmente, revisará los usuarios, roles y privilegios de los aplicativos de tesorería y su acceso a la información financiera. Permanentemente deberán velar por la actualización de éstos, de forma que garanticen que los usuarios y roles activos sean los correctos. En periodos de ausencia por alguna situación administrativa consagrada en la ley vigente, los servidores públicos responsables de cada entidad tramitarán la desactivación temporal del usuario. Cuando un usuario se retire de una entidad o cuando haya cambio de funciones, el responsable deberá solicitar de manera inmediata la inactivación del usuario y desactivación de roles según las directrices establecidas para el efecto y usando los formatos asociados a los procedimientos de administración de cuentas de usuario.

- Cada entidad solicitará la asignación, modificación o desactivación de roles con la debida anticipación, de forma que garantice su normal operación. Así mismo, debe revisar periódicamente que tenga suficientes usuarios activos y con los roles necesarios, que le permita garantizar la continuidad de la prestación del servicio.

- Se debe contar con una clara definición de perfiles relacionados con la administración, operación y autorización de operaciones financieras. La configuración de usuarios se debe realizar en relación con: estado, montos máximos, número de procesos, horarios y días de operación, productos autorizados y novedades posibles.

- Previa solicitud, el acceso remoto a los aplicativos transaccionales de tesorería, restringidos por medio de redes privadas de trasmisión de datos, sólo podrá ser autorizado por el representante legal o servidor público competente. De este trámite se deberá dejar constancia escrita de la solicitud y autorización, incluyendo la motivación de la solicitud.

- Cada usuario será responsable de aplicar rigurosamente las buenas prácticas definidas en este protocolo, así como en las políticas, procedimientos y demás documentos pertinentes para la navegación adecuada en los portales bancarios, aplicativos de comunicación financiera y pagos, así como en los demás aplicativos de información de la entidad.

- De conformidad con el inciso 3 del artículo 8 del Decreto Distrital 216 de 2017, *"Los servidores públicos que suscriban las órdenes de pago y las órdenes de devolución deberán registrar sus firmas en la Dirección Distrital de Tesorería. En caso de modificación del registro de los funcionarios, la respectiva entidad responsable deberá informarlo y actualizar las firmas correspondientes en la Dirección Distrital de Tesorería, de acuerdo con los procedimientos que se establezcan".*

  El Tesorero Distrital, con apoyo de la Dirección de Informática y Tecnología de la Secretaría Distrital de Hacienda informará sobre los requerimientos para que el mecanismo digital o firma electrónica sean reconocidos por el sistema de información de esta Entidad.

3.2. PORTALES BANCARIOS

En el uso de portales bancarios se observarán las siguientes directrices específicas:

- El acceso a los portales bancarios y aplicativos de comunicación financiera y pagos será controlado, de forma que pueda autenticarse y verificarse la identidad de la persona que se registra en el sistema. De acuerdo con los mecanismos de seguridad adoptados por cada entidad financiera, se establecerán los procedimientos operativos que garanticen la custodia y efectividad de los controles adoptados.

- En la administración y registro de transacciones en portales bancarios y aplicativos de comunicación financiera y pagos se aplicarán controles duales y se solicitará la opción de confirmación de transacciones, siempre que el respectivo banco lo permita.

- Se debe contar con una clara definición de perfiles relacionados con la administración, operación y autorización de operaciones financieras.

- Se definirán y registrarán en el respectivo portal o sistema los topes transaccionales máximos para cada usuario y tiempos máximos para aprobar las transacciones, cuando el portal lo permita, y se informará a los usuarios transaccionales sobre los límites por entidad financiera y por tipo de operación.

- La configuración de usuarios debe realizarse en relación con: estado, montos máximos, número de procesos, horarios y días de operación, productos autorizados y novedades posibles. Se definirán, registrarán e informarán las horas y días específicos en los que los usuarios transaccionales tendrán acceso a los portales. En ningún caso se permitirá dicho acceso en días no hábiles (nacionales o distritales).

- Se revisarán diariamente los egresos de las cuentas bancarias para verificar que no existan operaciones o transacciones financieras no autorizadas.

- Se deben parametrizar en los portales bancarios y de forma inmediata todos los eventos relacionados con los usuarios administradores y transaccionales, tales como situaciones administrativas contempladas en la normativa vigente, reemplazos, cambios de perfil o cualquier otra situación que signifique su actualización o inactivación.

3.3. SEGURIDAD EN EL MANEJO DE CLAVES BANCARIAS

Los usuarios responsables de claves bancarias deben observar las siguientes medidas de seguridad:

- Las claves de acceso son personales y de uso exclusivo para los roles, operaciones y transacciones que la entidad le autoriza a realizar.

- Las claves asignadas deben ser cambiadas periódicamente por el usuario autorizado para tal fin.

- Se debe solicitar a la entidad financiera la asignación de mecanismos fuertes de autenticación (token, tarjeta de claves, entre otros). Este mecanismo de autenticación asignado contará con protocolos de custodia y se deben tener claros los procedimientos para los casos de extravío o pérdida.

3.4. POLÍTICA DE PAGOS ELECTRÓNICOS

En materia de pagos electrónicos, las tesorerías suscribirán los contratos, convenios u otrosí necesarios con las entidades financieras. Se propenderá por rotar el pago en diferentes entidades financieras, con el fin de garantizar transparencia y reducir el riesgo operativo.

La Secretaría Distrital de Hacienda, mediante Resoluciones SDH-243 de 2016 y SDH-304 de 2017, adoptó la "Política Distrital de Pagos Electrónicos con Recursos del Tesoro Distrital", de obligatoria observancia para las entidades que administran recursos de la Cuenta Única Distrital correspondientes al Presupuesto Anual Distrital.

Estas resoluciones, cuyo texto se puede consultar en la Web de la Secretaría Distrital de Hacienda (Ruta: http://www.shd.gov.co/ nuestra entidad / Contratación, Normatividad y Defensa Judicial / normativa / normatividad misional), tienen como objetivo fortalecer el servicio a través del uso de la tecnología, la seguridad y el control de riesgos; cumplir con criterios de austeridad en el gasto y eficiencia de la administración pública, y promover la política estatal de formalización de la economía y bancarización.

Corresponde a los representantes legales, ordenadores de gasto, responsables de presupuesto y servidores públicos de las áreas financieras, administrativas y contables en cada entidad destinataria, conocer y aplicar lo previsto en estas Resoluciones y en las demás normas y directrices distritales y nacionales aplicables.

CAPÍTULO 4
SEGURIDAD FÍSICA Y OPERACIONAL

4.1. ACCESO RESTRINGIDO Y CONTROL EN ÁREAS DE LA TESORERÍA

Para cumplir con la gestión de recaudo, administración, inversión, pagos, traslados y/o disposición de recursos de la Cuenta Única Distrital, las entidades que administran información reservada propia y de terceros, elementos de seguridad física y tecnológica y activos de información con carácter restringido que ameritan niveles de seguridad acordes con los estándares de las instituciones financieras.

Se implementarán controles y medidas de seguridad suficientes para brindar protección, control e integridad física a las instalaciones, bienes y elementos requeridos para ejecutar sus operaciones de tesorería.

En consecuencia, dependiendo de la estructura y las competencias funcionales de cada entidad, las siguientes áreas en donde se cumple la gestión de tesorería serán de acceso físico restringido:

- La mesa o área de inversiones

- El Back Office o área de valoración del portafolio, liquidación y compensación de operaciones.

- El área de Home Banking, banca electrónica y/o

de giros, en donde se ejecuten las transacciones de transferencia y/o distribución de fondos.

4.2. DIRECTRICES GENERALES PARA LA SEGURIDAD DE LAS ÁREAS RESTRINGIDAS DE TESORERÍA

- En concordancia con este carácter restringido, los servidores públicos competentes definirán y comunicarán las restricciones y controles especiales para el acceso físico al área de tesorería.
- Las áreas responsables de la Gestión Corporativa y de Informática y Tecnología de cada entidad destinataria prestarán el apoyo necesario en materia de controles y seguridades de acceso, cámaras de seguridad; cajas fuertes; seguridad en las áreas restringidas internas de back office y banca electrónica; adquisición y control de elementos de seguridad bancaria, custodia y manejo de títulos, arqueos y controles.
- El área de tesorería deberá ubicarse en zonas adecuadamente construidas, protegidas contra acceso indebido y factores ambientales externos.
- Se debe contar con un punto de control permanente contratado con una empresa autorizada de vigilancia. Las áreas permanecerán cerradas y aseguradas en horas no hábiles, según los calendarios laborales nacional y distrital. Estas áreas deben ser controladas mediante métodos electrónicos de control de acceso, los funcionarios deben poseer y portar su carné de acceso (debidamente marcado con nombre y fotografía); los visitantes deben ser autorizados por el servidor público que los va a atender y siempre deben estar acompañados. Se recomienda tener un área para atención de dichos visitantes.
- Se restringirá el acceso de dispositivos electrónicos no institucionales (celulares, beeper, USB, etc.), a las zonas de mayor seguridad y para dicho efecto se ubicarán casilleros a la entrada del área para que se puedan guardar dichos dispositivos.
- La entidad destinataria deberá contar con recursos informáticos suficientes para controlar el acceso a Internet. Los servidores públicos no podrán tener acceso dentro de las áreas restringidas a servicios no institucionales que posibiliten la comunicación con el exterior de dichas áreas.
- En los equipos de cómputo para preparación y autorización de operaciones se deshabilitará la funcionalidad de copiar a mecanismos de memoria externos como USBs, CDs, DVDs.
- Dependiendo de las condiciones físicas de cada entidad, las instalaciones de la tesorería contarán con cámaras de video ubicadas en la entrada, pasillos y áreas internas con acceso restringido. Estas áreas serán monitoreadas permanentemente mediante cámaras de seguridad de alta definición y se garantizará mantener copias de los archivos de video según los tiempos definidos en las tablas de retención de cada entidad. Las cámaras de video deben ser ubicadas de forma que no permitan visualizar el accionar de teclados y monitores, pero que identifiquen a la persona que hace uso de los mismos.
- Se recomienda contar con un sistema de grabación de llamadas y correos para monitorear las comunicaciones asociadas a las operaciones bancarias y de inversiones.
- En protección de los derechos, el sistema informará al transmisor que la llamada va a ser grabada o monitoreada.
- Desde la Alta Dirección se definirán los cargos, equipos de comunicación y direcciones de correo electrónico que estarán sujetos a ese seguimiento y monitoreo, teniendo en cuenta su relación directa o indirecta, permanente u ocasional, con las mencionadas operaciones. Las personas objeto de seguimiento deberán ser informadas del mismo y firmar formatos en señal de aceptación.
- Dicho sistema de grabación debe ser monitoreado técnicamente por el área de tecnología con el fin de garantizar su adecuada operación. Se almacenarán copias de las llamadas y correos por el tiempo previsto en las tablas de retención documental. Las distintas operaciones realizadas y grabadas deben ser revisadas periódicamente por funcionarios con roles de control ajenos a la operación.
- No podrá utilizarse el material grabado de las llamadas de las áreas mencionadas para efectos diferentes a los estrictamente relacionados con la verificación de la integridad de las operaciones de tesorería por parte de las instancias de control y supervisión competentes.
- Las cajas fuertes deben contar con mecanismos temporizadores que permitan el bloqueo de las mismas en horarios no hábiles y deberán ser vigiladas las 24 horas por medio de las cámaras de video. Se deben implementar claves duales para la apertura de las cajas fuertes. Periódicamente se cambiarán las claves, dependiendo de las necesidades, ya sea por simple control o por novedades

administrativas. Las claves respectivas - una vez efectuado el cambio - deben ser enviadas en sobre cerrado para custodia en otra área y solamente pueden ser retiradas por el tesorero.

4.3. APERTURA, CONTROL Y MANEJO DE CUENTAS BANCARIAS

La apertura, manejo, seguimiento y control de las cuentas bancarias de caja menor y demás cuentas bancarias de titularidad de las entidades destinatarias se sujetará a lo previsto en la Resolución SDH-323 de 2018, *"Por la cual se dictan directrices para la apertura, manejo, control y cierre de cuentas bancarias de las entidades que forman parte del Presupuesto Anual del Distrito Capital y los Fondos de Desarrollo Local",* así como las normas complementarias.

4.4. SEGURIDAD EN EL MANEJO DE CHEQUES Y VALORES

- No se podrá autorizar mediante cartas o notas débito aquellas operaciones y transacciones que puedan ser realizadas a través del Portal Empresarial, salvo cuando el portal falle y el uso de esas comunicaciones especiales sea requerido como plan de contingencia.
- La confirmación de las operaciones se hará únicamente por los servidores públicos que las firman o los servidores autorizados y previamente registrados ante la entidad financiera, validando los datos tanto de la operación como los de quien confirma cada operación.
- En aplicación de la política distrital de pagos electrónicos mencionada en el punto 3.4. de este protocolo, el giro de cheques sólo procederá en casos excepcionales.
- Para los diferentes cheques girados se llevará un control detallado y actualizado a través de aplicativos informáticos, que permita conocer su estado.
- Cada vez que se gire un cheque, el mismo será revisado por personas diferentes antes de ser firmado; de esta manera, en cada una de estas revisiones se van agregando los elementos de seguridad ya definidos.
- Todos los cheques girados tendrán sellos restrictivos.
- Todos los cheques llevarán dos firmas, de acuerdo con las atribuciones de cada servidor público para autorizar movimientos de recursos, o dar instrucciones sobre las cuentas bancarias, las cuales deben ir acompañadas de su respectivo sello.
- Los cheques llevarán protectógrafo mecánico y sello.
- Se pueden utilizar hologramas.
- Todas las condiciones de seguridad, como firmas, sellos, protectógrafos y condiciones serán previamente informadas y registradas ante cada entidad financiera, desde la apertura de las cuentas bancarias. Dichas condiciones se actualizarán periódicamente para asegurar su vigencia y además, cuando se requiera.
- Una vez los cheques que estén listos para ser entregados al beneficiario serán custodiados en la caja fuerte, a cargo del servidor público designado, el cual será el encargado de verificar que quien retira los cheques cumpla con los requisitos legales mínimos para reclamarlos.
- Los cheques sin uso (formas continuas y chequeras), deben ser custodiados en la caja fuerte con manejo dual de claves y temporizador. Los protectógrafos y los sellos también deben ser custodiados en caja fuerte.
- Se requiere mantener un stock mínimo de cheques por banco girador, equivalente al promedio de cheques girados en un mes y en consideración del tiempo que tarda una entidad bancaria en producir un nuevo pedido.
- Se realizará un arqueo mensual de cheques en blanco y se elaborará un acta firmada por cada uno de los servidores públicos que participan en esta labor.
- Mensualmente se realizará el arqueo de los cheques girados que se encuentran pendientes de ser entregados.
- Se deben realizar arqueos al cierre de cada mes sobre cheques y si se maneja, de papel de seguridad.
- Mensualmente se debe levantar un acta de anulación de cheques, incluyendo aquellos en los cuales la fecha de expedición supera 90 días sin haber sido cobrados.
- Dependiendo de la fecha de caducidad de la obligación de pagar y de su concepto, cada entidad realizará las gestiones necesarias para depurar, sanear o legalizar los cheques pendientes de cobro de conformidad con las normas y directrices pertinentes.
- En caso de extravío de cheques la entidad distrital procederá a:

(a) Emitir de manera inmediata orden de no pago y remitirlo al banco en oficio físico y mediante correo electrónico o mecanismo que disponga la entidad financiera. Se requiere obtener ACUSE de recibo del banco.

(b) Presentar denuncia de extravío en el sitio Web dispuesto para el efecto por la Policía Nacional.

(c) En caso de conocer de indicios de comisión de delito, los servidores públicos tiene el deber de presentar la correspondiente denuncia penal.

- Además de lo anterior, en caso de extravío de cheques se recomienda:

(a) Publicar aviso en prensa: *"Se informa al público: que el cheque No. xxxxxxx del banco xxxxxxx se encuentra extraviado, tiene orden de no pago y carece de toda validez. Se solicita abstenerse de negociar con este cheque."*

(b) Adelantar proceso verbal de cancelación de título valor. Por ser un cheque emitido contra recursos de la cuenta única distrital, el riesgo por extravío puede ser similar al de un cheque de gerencia, caso para el cual la Superintendencia Financiera de Colombia exigió a los bancos adelantar siempre dicho proceso judicial verbal - Concepto 2011058699-001 del 16-09-2011.

CAPÍTULO 5
SEGUIMIENTO Y CONTROL

5.1. AUTOCONTROL Y AUTOEVALUACIÓN

Cada entidad destinataria y sus servidores públicos competentes realizarán las actividades de autocontrol necesarias para verificar la permanente observancia de las prácticas, controles y procedimientos adoptados en desarrollo de estas directrices, en lo de su competencia, dejando de ello evidencia escrita.

5.2. MONITOREO, SEGUIMIENTO, EVALUACIÓN Y AUDITORÍA

En el Programa Anual de Auditoría de cada entidad se incorporarán las actividades necesarias para cumplir con el monitoreo, seguimiento, evaluación y/o auditoría que permitan establecer la conformidad con las normas y estándares vigentes, en las labores de las dependencias responsables de ejecutar o apoyar la gestión de tesorería y mantener las condiciones de seguridad de los recursos y las transacciones.

INSTITUTO DE DESARROLLO URBANO –IDU

Resolución Número 006678
(Octubre 2 de 2019)

"Por la cual se modifica la delegación consagrada en el artículo 5° de la Resolución 2307 de 2019 del IDU"

LA DIRECTORA GENERAL DEL INSTITUTO DE DESARROLLO URBANO –IDU;
en ejercicio de sus facultades legales y en especial las conferidas por los artículos 209 y 211 de la Constitución Política, artículos 9, 10 y 11 de la Ley 489 de 1998, Acuerdo Distrital 19 de 1972 y los Acuerdos 01 y 02 de 2009 del Consejo Directivo del IDU, y

CONSIDERANDO:

Que de conformidad con el artículo 209 de la Constitución Política "La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones".

Que los artículos 9, 10 y 11 de la Ley 489 de 1998 señalan los requisitos de la delegación.

Que los artículos 29 y 30 del Acuerdo del Consejo Directivo 01 del 3 de febrero de 2009 *"Por el cual se expiden los Estatutos del Instituto de Desarrollo Urbano, IDU"*, establecen las funciones generales de la Directora General del Instituto de Desarrollo Urbano y la facultan para delegar las que considere convenientes en los servidores públicos del nivel directivo y asesor, conforme a los criterios establecidos en la Ley 489 de 1998.

Que de conformidad con la Resolución 2307 de 2019 del IDU, la Directora General del Instituto estableció las delegaciones vigentes.

Que en la Directiva 06 del 16 de Agosto de 2019 expedida por la Secretaría Jurídica Distrital en relación con las "Garantías y Tratamiento en la Contratación Estatal", señaló en lo relativo a la Estabilidad y Calidad de la Obra, que el amparo de los perjuicios ocasionados después de la entrega a satisfacción por daño o deterioro, se determina de acuerdo al objeto, valor, naturaleza y obligaciones del contrato, en un término de vigencia de (5) años a partir del recibo a satisfacción, o en un plazo menor previa justificación técnica, y su procedimiento estará consagrado en el artículo 34 y siguientes de la Ley 1437 de 2011.