



PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

| | |
|--|----|
| 1. OBJETIVO | 2 |
| 2. SEGURIDAD Y GESTION DEL RIESGO:..... | 2 |
| 2.1. COMPONENTES GENERALES DE SEGURIDAD. | 3 |
| Cámaras de Seguridad..... | 3 |
| Grabación de Llamadas..... | 3 |
| Caja Fuerte..... | 4 |
| 2.2 . COMPONENTES ESPECÍFICOS..... | 4 |
| El talento Humano..... | 4 |
| Áreas Físicas Restringidas de la tesorería..... | 4 |
| Seguridad Lógica de la Red Restringida de la Tesorería..... | 4 |
| 2.3 SEGURIDAD EN LAS OPERACIONES | 5 |
| Gestión de Cheques..... | 5 |
| Canales Electrónicos..... | 5 |
| Seguridad en el Manejo de Claves Bancarias..... | 6 |
| Conexión con las Entidades Financieras..... | 7 |
| Cartas de Autorización y Notas Débito..... | 7 |
| 2.4 Custodia y Manejo De Títulos Valores..... | 7 |
| Seguridad en Manejo de Cheques..... | 8 |
| Custodia de cheques | 8 |
| Arqueos de cheques y Actas de Anulación | 8 |
| 3. MANEJO, CONTROL Y CIERRE DE CUENTAS..... | 8 |
| 3.1. Finalidad exclusiva de las cuentas bancarias..... | 8 |
| 3.2. Autorización previa de la Dirección Distrital de Tesorería para apertura de cuentas bancarias..... | 9 |
| 3.3. Trámite para identificación de Cuentas bancarias como exentas de GMF:..... | 9 |
| 3.4. Seguridad y gestión del riesgo:..... | 10 |



PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

| Firma de Autorizaciones | | |
|--------------------------------|--|----------------------------------|
| Elaboró | Revisó | Aprobó |
| Administrador Financiero | Representante Legal | Presidente del Concejo Directivo |
| Control de Cambios | | |
| Fecha | Descripción | |
| 02 de mayo de 2020 | Se crea de acuerdo a la normatividad legal vigente y operatividad vigente del proceso Gestión Financiera-Tesorería | |

1. OBJETIVO

El objetivo del presente documento es establecer los lineamientos y procedimientos que permiten fortalecer y asegurar el manejo de los recursos financieros depositados en la cuenta bancarias, para minimizar la probabilidad de fraude en la gestión de las operaciones de liquidez y de las transacciones y pagos, tomando como criterio la política anti fraude y los lineamientos para el manejo de los recursos.

2. SEGURIDAD Y GESTION DEL RIESGO:

En cumplimiento de lo anterior se establece el Protocolo de Seguridad para el manejo de las cuentas bancarias y en general el efectivo y equivalentes de la Corporación.

De acuerdo con la estructura organizacional, las condiciones físicas de las instalaciones en las que funciona Cormepaz (Sede física entregada en comodato por la Diócesis de Buenaventura en cabeza de Mons. Rubén Darío Jaramillo), realizado el análisis de los

Cra. 19 N° 1 b 73 Barrio Alberto Lleras, “Casa Social Cultural y Memoria”

Teléfono 24 21150, Celular 321 970 9253

cormepaz@gmail.com

Buenaventura



PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

procedimientos y riesgos asociados a al Área Financiera a continuación se establecen las condiciones y procedimientos que se deben seguir en Cormepaz orientadas a mitigar los riesgos asociados a la gestión de la tesorería, en especial las relacionadas con el fraude en la gestión de las operaciones de liquidez y de las transacciones bancarias.

2.1. COMPONENTES GENERALES DE SEGURIDAD.

Cámaras de Seguridad.

La oficina financiera está ubicada actualmente en la oficina 301 del tercer piso de a Casa Social Cultural donde funciona la el Área Administrativa y Financiera, está oficina cuenta con una (01) cámara de seguridad que están configuradas para realizar grabación por movimiento desde la entrada a la oficina. Lo que permite tener registro de las personas que ingresan al área.

Específicamente para la oficina asignada a la financiera se cuenta con una cámara de seguridad que está ubicada de forma que no permite la visualización simultánea de teclado y monitor del equipo asignado para realizar las transacciones bancarias y no se logra identificar a la persona que hace uso de este equipo.

Las grabaciones producidas por esta cámara quedan almacenadas en un dispositivo de grabación tipo DVR ubicado en el data center de la entidad y el tipo de archivo que se genera solamente permite su consulta y no su modificación o eliminación.

La Entidad en ningún caso podrá utilizar el material grabado para efectos diferentes a los estrictamente relacionados con la gestión de las operaciones. Este sistema debe informar al transmisor que la llamada va a ser grabada o monitoreada

Nota: 1: Las cámaras de video deben ser ubicadas de forma tal que no permitan visualizar teclados y monitores, pero que permitan identificar al funcionario que hace uso de los mismos.

Grabación de Llamadas.

En el marco de aumentar los niveles de seguridad y de acuerdo con las operaciones que a la fecha realiza se realizó la evaluación de grabar las llamadas del área, sin embargo, dado que a la fecha de elaboración del presente documento no se cuenta con presupuesto disponible para gastos de comunicaciones no es posible adquirir este servicio.



PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

Adicionalmente dado que el Cormepaz no realiza inversiones, tampoco se considera como un gasto indispensable para la operación.

Caja Fuerte.

No es permitida la existencia de caja fuerte

2.2 . COMPONENTES ESPECÍFICOS.

El talento Humano.

Para el Talento Humano que deba desarrollar funciones financieras, se tendrá en cuenta:

- Título profesional en Economía Contaduría Pública o Administración de Empresas
- Tarjeta o Matrícula Profesional en los casos reglamentados por la ley.
- Treinta (30) meses de experiencia profesional relacionada con las funciones del cargo...

El Financiero se consideran como “**Cargo de Confianza**”, su provisión se realiza como de Libre Nombramiento y Remoción.

Áreas Físicas Restringidas de la tesorería.

Teniendo en cuenta que en la administración financiera se realizan operaciones relacionadas con liquidación y compensación de operaciones, transacciones de transferencia y/o distribución de fondos, el área se considera con acceso restringido. Adicionalmente, esta área debe permanecer cerrada y asegurada en horas no hábiles.

La administración debe estar ubicada en un área cerrada, con puerta con llave la cual es administrada únicamente por el personal autorizado y la copia de la llave la tiene Servicios Generales la cual puede ser solicitada exclusivamente.

Seguridad Lógica de la Red Restringida de la Tesorería.

En lo que tiene que ver con la red de datos el equipo desde el que se realizan las transacciones Financieras son restringidos los días, domingos y festivos. En caso de que se requiera trabajar en ese equipo en dichos días el Administrativo y Financiero debe solicitarlo.



PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

El equipo desde el que se realizan las transacciones de Tesorería tiene acceso a páginas de internet que posibiliten la comunicación vía correo electrónico personal (hotmail, yahoo, facebook); chat's (Messenger MSN, Yahoo Messenger, etc.). Se permite el acceso a Gmail debido a que el servicio de correo electrónico institucional funciona a través de este proveedor.

2.3 SEGURIDAD EN LAS OPERACIONES

Gestión de Cheques.

El uso de este medio de pago se realizará únicamente cuando los canales virtuales presenten fallas prolongadas; Para los diferentes cheques girados producto de la ordenación, se deberá llevar un control en el talonario al momento del giro y un control en hoja electrónica, que permita conocer su estado. Los cheques girados y firmados deben ser custodiados en la caja fuerte.

Canales Electrónicos.

Seguridad Lógica y física del equipo donde se realizan los giros de tesorería:

- Contar con acceso físico restringido al personal no autorizado al área de ubicación de este equipo.
- El equipo desde el que se realizan las transacciones, cuenta con herramientas de control de software malicioso: anti-virus, anti-keylogger, anti-spyware; activas y actualizadas a través de un antivirus local y el firewall tipo appliance perimetral.
- Contar con una cuenta de usuario de dominio para el acceso al equipo, programada para que se solicite el cambio de contraseña periódicamente y con uso de contraseña segura.
- Acceso controlado a páginas de internet que posibiliten la comunicación vía correo electrónico personal (hotmail, gmail, yahoo, facebook); chat's (Messenger MSN, Yahoo Messenger, etc.) o portales similares.
- El Financiero debe contar con una cuenta de correo institucional
- Contar con una unidad de red con acceso exclusivo para el almacenamiento de los documentos de este equipo, a la que se le realizará copia de respaldo semanalmente. - Debe tener la dirección IP estática.



PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

- El área de ubicación del equipo debe contar con una cámara de seguridad con monitoreo 7x24 y grabado por movimiento en una unidad central.
- El equipo desde el que se realizan las transacciones de Tesorería, tiene inhabilitado el quemador de CD y DVD. Así mismo el puerto USB.
- El equipo desde el que se realizan las transacciones de Tesorería se le realiza actualización de los parches de seguridad del sistema operativo cada vez que realiza la jornada de mantenimiento del equipo por parte de la Oficina Asesora de Planeación.
- La configuración de usuarios se debe realizar con cada entidad financiera y debe contar con la aprobación de la Dirección General en relación con: estado, montos máximos, número de procesos, horarios y días de operación, productos autorizados y novedades posibles.
- Los giros se realizan a través del portal de los bancos con los que se tiene suscrito el contrato, estos portales hacen uso de protocolos de seguridad de cifrado de comunicaciones por lo cual todos los archivos transmitidos o recibidos, son encriptados y desencriptados automáticamente.

Seguridad en el Manejo de Claves Bancarias.

El Administrador Financiero y Representante Legal y/o quienes hagan sus veces, son las personas encargadas del manejo de claves bancarias y deben tener en cuenta las siguientes medidas de seguridad:

- Las claves de acceso son personales y de uso exclusivo para las 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 algún mecanismo fuerte de autenticación (token). Este mecanismo de autenticación asignado debe ser custodiado por el funcionario responsable y en caso de extravío o pérdida debe reportarlo por escrito al banco a través del Portal, solicitar su des habilitación al Usuario Primario e interponer la denuncia correspondiente.



PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

- Para el caso de las cuentas bancarias de giro se deben contar con dos mecanismos de autenticación (token) uno para el Administrador y otro para el Director.
- Se deben notificar a las entidades financieras, eventos como retiros, vacaciones reemplazos, encargos, cambios de cargo o cualquier situación que signifique la inactivación de cualquiera de los usuarios encargados de claves de acceso. Lo anterior, en un plazo oportuno, no mayor a 48 horas.
- Todas las transacciones del Portal se deben realizara desde los equipos asignados en los horarios establecidos de trabajo.

Conexión con las Entidades Financieras

Para las transacciones o giros con bancos se debe registrar la IP pública de la entidad desde donde se autorizan los giros.

La conexión con los bancos se realiza únicamente desde del equipo de transacciones de la Administración a través del Portal Web del banco con el que se tienen suscrito el contrato. La conexión con las entidades financieras para la realización de operaciones se realiza desde la dirección IP fija que tiene la entidad autorizada para transar, la cual es informada al banco en el momento de la suscripción del contrato.

Cartas de Autorización y Notas Débito

Para todas las operaciones y transacciones que puedan ser realizadas a través del Portal Empresarial, no se deben utilizar cartas ni notas débito para su autorización.

Para los casos en los que se deban utilizar estos mecanismos de aprobación, se deben tener en cuenta las siguientes medidas:

- Se deben respetar las mismas condiciones de manejo que se utilizan para los cheques. Tales como firmas, sellos y protectógrafo de los cheques
- La confirmación de las operaciones se hará únicamente por los funcionarios que la firman, validando los datos tanto de la operación como los del funcionario que confirma cada operación.

2.4 Custodia y Manejo De Títulos Valores



PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

Seguridad en Manejo de Cheques

Los cheques girados deben tener:

- Para cualquier monto, Sello restrictivo "**Para Consignar únicamente a la Cuenta del Primer Beneficiario**"
- Todos los cheques deben llevar dos firmas, siempre serán firmados por el Director General y una de las otras firmas registradas; además deben ir acompañadas de su respectivo sello.
- Los cheques llevarán protectógrafo mecánico
- Todas las condiciones de seguridad como firmas, sellos protectógrafos y condiciones son registradas ante cada entidad financiera, cuando se lleva a cabo la apertura de las cuentas bancarias.

Custodia de cheques

Las chequeras, y los sellos deben ser custodiados bajo llave con manejo dual de claves.

Arqueos de cheques y Actas de Anulación

Mensualmente el Administrador Financiero deberá realizar un arqueo de los cheques girados que se encuentran pendientes de entrega, lo mismo de cheques en blanco y se elaborará un acta firmada por cada uno de los funcionarios que participan en esta labor.

En el caso de haber existido cheques anulados en el mes, se realizará un acta de anulación de cheques, incluyendo aquellos en los cuales la fecha de expedición supera 90 días sin haber sido cobrados. Estos dineros son registrados contablemente en Acreedores Varios.

Dependiendo de la fecha de caducidad de la obligación de pagar y de su concepto, se elaborará un acta de depuración, para retirar y/o legalizar de la cuenta de Acreedores Varios lo correspondiente a cheques no cobrados.

3. MANEJO, CONTROL Y CIERRE DE CUENTAS

3.1. Finalidad exclusiva de las cuentas bancarias.

Para el correcto manejo del recurso recibido para cooperación, convenios, gestión propia y demás; se establecen directrices para la apertura, manejo, control y cierre de cuentas bancarias de las entidades financieras

Cra. 19 N° 1 b 73 Barrio Alberto Lleras, "Casa Social Cultural y Memoria"
Teléfono 24 21150, Celular 321 970 9253
cormepaz@gmail.com
Buenaventura



PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

- Cada proyecto deberá tener asignada una cuenta bancaria exclusiva para el manejo de los recursos recibidos.
- Los aportes de recurso propios se manejarán desde las cuentas institucionales.
- Cualquier cuenta bancaria que no se ajuste a dichas condiciones deberá ser cerrada de manera inmediata y definitiva por parte de la entidad.

3.2. Autorización previa de la Dirección Distrital de Tesorería para apertura de cuentas bancarias.

Para la apertura de cuentas bancarias **CORMEPAZ** deberá solicitar, mediante oficio suscrito por el Director General, la autorización previa y expresa de la Dirección Distrital de Tesorería para abrir cualquier cuenta bancaria.

En dicha solicitud se deberá indicar, para cada cuenta bancaria:

- El banco Seleccionado
- El titular de la cuenta y NIT
- El propósito de la cuenta.
- El origen de los recursos que se manejarán.

Cuando se sustituya una cuenta precedente, debe apartarse el soporte de cierre o se expresará el compromiso de cierre inmediato, una vez se abra la nueva cuenta. Hasta la fecha CORMEPAZ no ha considerado la apertura de una cuenta bancaria para el manejo de la caja menor debido a que el monto mensual máximo de un millón ciento cincuenta mil pesos (\$1.150.000), los reducidos reembolsos y la escasa reciprocidad no justifican su apertura. En todo en caso de considerar su apertura la solicitud de autorización de apertura de cuentas bancarias de caja menor deberá anexarse –adicionalmente - copia del acto administrativo expedido al tenor del **artículo 3 del Decreto Distrital 61 de 2007**.

El Director General de CORMEPAZ es el exclusivo responsable de seleccionar el establecimiento bancario en la cual se realizará la apertura de cada cuenta, el cual debe corresponder a una de las entidades bancarias que cuenten con cupo de inversión vigente publicado por la Secretaria Distrital de Hacienda.

3.3. Trámite para identificación de Cuentas bancarias como exentas de GMF:

El Director General de CORMEPAZ es exclusivamente responsable de tramitar oportunamente ante la Dirección Distrital de Tesorería la solicitud para que el (la) Administrador Financiero (a) Distrital identifique ante los bancos aquellas cuentas exentas del



PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

Gravamen a los Movimientos Financieros, en las cuales se manejen en forma exclusiva recursos correspondientes a la ejecución del presupuesto general del Distrito Capital, de acuerdo con lo previsto en el numeral 9 del artículo 879 del Estatuto Tributario, en concordancia con el artículo 9 del Decreto Reglamentario 405 de 2001.

Con tal fin, estas entidades deben remitir a la Dirección Distrital de Tesorería - Subdirección de Operación Financiera, los siguientes soportes:

- Oficio suscrito por el representante legal solicitando la marcación de la cuenta bancaria como exenta del Gravamen a los Movimientos Financieros.
- Certificación expedida por la respectiva entidad bancaria con antelación no mayor a un (1) mes a la fecha de solicitud, que permita a la Dirección Distrital de Tesorería verificar: el nombre y NIT del titular; la fecha de apertura, el número y tipo de cuenta bancaria y la dirección de correspondencia.
- Certificación suscrita por el responsable de presupuesto y el ordenador del gasto de la respectiva entidad o localidad, en la cual deberá constar que, en la cuenta, cuya identificación se solicita tramitar como exenta del GMF, se manejarán exclusivamente recursos provenientes del presupuesto general del Distrito Capital, debiendo detallar el(los) respectivo(s) rubro(s) presupuestal(es), y declarando que en ningún caso se manejarán allí recursos propios.
- Para los convenios mediante los cuales se ejecutan recursos provenientes del presupuesto general del Distrito Capital, además de los documentos anteriores, se deberá remitir copia del respectivo convenio y del documento que acredite la incorporación de estos recursos al presupuesto de la entidad solicitante.

3.4. Seguridad y gestión del riesgo:

Es responsabilidad exclusiva del CORMEPAZ y de sus servidores públicos competentes preservar las condiciones para el correcto manejo y debida seguridad de las cuentas bancarias, cumpliendo rigurosamente con las normas de gestión de riesgo y administración de recursos públicos, y protocolos bancarios de seguridad.

Desde la apertura de la cuenta y en forma actualizada, las entidades distritales deberán establecer y comunicar por escrito al respectivo banco cuales son las condiciones y procedimientos en materia de:

- Manejo y custodia de chequeras.
- Firmas registradas y servidores públicos autorizados.

Cra. 19 N° 1 b 73 Barrio Alberto Lleras, "Casa Social Cultural y Memoria"
Teléfono 24 21150, Celular 321 970 9253
cormepaz@gmail.com
Buenaventura



CORPORACIÓN MEMORIA Y PAZ – CORMEPAZ
901.283.250-7

PROTOCOLO DE SEGURIDAD MANEJO DE CUENTAS BANCARIAS Y EFECTIVO

- Uso y custodia de sellos restrictivos, tokens, cajillas u otros medios de seguridad.
- Instrucciones para confirmaciones telefónicas.
- Correos institucionales, horarios y demás instrucciones generales y de carácter operativo para garantizar la seguridad en el cierre, cumplimiento y seguimiento de las operaciones.
- Roles y claves para ingreso a portales bancarios; seguimiento y control de las cuentas y su cierre en los casos previstos en el artículo octavo.

Página | 11