

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
	Versión: 1	Página 1 de 26	
	Vigente desde: 25-09-2016		

CAJA DE LA VIVIENDA POPULAR - CVP

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 2 de 26
	Vigente desde: 25-09-2016		

1. INTRODUCCIÓN

La seguridad informática dispone de lineamientos técnicos y legales para preservar la confidencialidad, integridad y disponibilidad de la información de la Caja de la Vivienda Popular - CVP, incluye la adopción de controles que respondan a las necesidades de la entidad y que contribuyan al alcance de las metas institucionales.

Esta política debe ser aplicada por todos los (as) funcionarios (as), contratistas, proveedores, consultores y todo personal externo que utilice los servicios informáticos que ofrece la Entidad, deben conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

Esta política se actualizará por parte de la Dirección de Gestión Corporativa y CID, de acuerdo con las disposiciones legales, técnicas o institucionales que defina el Estado colombiano, el Distrito Capital y/o la CVP.

2. OBJETIVO

Proteger, preservar y administrar los activos de información que interactúan para el acceso a la información institucional de la Caja de la Vivienda Popular y el uso de los servicios TICs frente a amenazas y vulnerabilidades internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

2.1 Objetivos Específicos

- ✓ Definir, comunicar y generar la cultura de buenas prácticas para el acceso, uso y manejo de los servicios informáticos que tiene a disposición la Entidad, por parte de todos los funcionarios, contratistas y terceros relacionados con la CVP. Salvaguardar la plataforma tecnológica en aras de proteger la imagen, los intereses y el buen nombre de la Entidad.
- ✓ Actualizar los procedimientos, instructivos, manuales y formatos relacionados con la gestión de los servicios tecnológicos.
- ✓ Comprometer a todo el personal de la Entidad con la aplicación de los lineamientos de la seguridad informática.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 3 de 26
	Vigente desde: 25-09-2016		

- ✓ Comunicar a la alta dirección a través del Comité de Seguridad de la Información sobre los riesgos y mal uso de los activos de información y acciones tomadas para su mitigación y corrección.
- ✓ Gestionar las amenazas y vulnerabilidades en los activos de información para reducir los riesgos asociados con la seguridad de la información
- ✓ Incorporar el cumplimiento de las normas relacionadas con la privacidad de la información y la propiedad intelectual.

3. ALCANCE Y APLICABILIDAD

Esta política aplica para los activos de información definidos por la CVP y es de obligatorio cumplimiento por parte de toda persona natural o jurídica que tenga relación con la entidad.

La política pretende garantizar la satisfacción de las partes interesadas priorizando la confidencialidad, integridad y disponibilidad de la información, bajo un enfoque de mejora continua y autocontrol en los procesos y en la prestación de los servicios, con base en la sensibilización de cada uno de los servidores de la CVP y el apoyo del equipo humano de sistemas, de manera que el acceso a la información oportuna y confiable facilite el ejercicio efectivo de los derechos constitucionales y legales, además de los controles ciudadano, político, fiscal, disciplinario y de gestión o administrativo, sin perjuicio de las reservas legales.

4. DEFINICIONES

Política: Son instrucciones mandatorias que indican la intención y la directriz de la alta gerencia respecto a la operación de la entidad.

Servidor: En redes locales se entiende como el software que configura un PC u otro computador como servidor para facilitar el acceso a la red y sus recursos.

Firewall: Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Logs: Registro oficial de eventos, durante un rango de tiempo en particular, en donde se almacena toda actividad que se hace en el equipo monitoreado.

Parches: Actualizaciones que se aplican a un programa para corregir o mejorar su funcionalidad.

Sistema Operativo (SO): Es el software básico de un computador que provee una interface entre el resto de programas, los dispositivos de hardware y el usuario.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 4 de 26
	Vigente desde: 25-09-2016		

Servicios de Servidores: son todas aquellas herramientas o aplicaciones de software que están disponibles para apoyar la gestión de la entidad, algunos servicios disponibles son: Servicios de dominio de Active Directory, Servidor de aplicaciones, Servidor DHCP, Servidor DNS, Servicios de archivos, Hyper-V, Servicios de acceso y directivas de redes.

Base de datos: Conjunto de archivos de datos recopilados, definidos, estructurados y organizados con el objeto de brindar información.

Afinamiento de bases de datos: Son las actividades relacionadas con mantener el desempeño y la eficiencia de la base de datos. Estas actividades se realizan cuando las necesidades del negocio requieren mayor rendimiento en sus transacciones y/o almacenamiento.

Licencias de tipo GNU (General Public License): Es la licencia más usada en el mundo del software y garantiza a los usuarios finales (personas, organizaciones, compañías) la libertad de usar, estudiar, compartir y modificar el software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

Software Licenciado: Es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciario del programa informático (usuario consumidor /usuario profesional o empresa), para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

Log de transacciones: Es un archivo, donde se registran todas las transacciones de las bases de datos.

Back-up (copia de respaldo): Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos o CDs), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto.

Plan de Contingencia: Procedimientos alternativos de una entidad cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aun cuando alguna de sus funciones se vean afectadas por un accidente interno o externo.

Plan de Pruebas de Recuperación: Pruebas de recuperación de copias de respaldo programadas con el fin de verificar la consistencia e integridad de las copias de respaldo.

Back ups incrementales: Una operación de back up incremental sólo copia los datos que han variado desde la última operación de back up de cualquier tipo. Se suele utilizar la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último back up.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 5 de 26
	Vigente desde: 25-09-2016		

Niveles de respaldo de información: Hace referencia a los diferentes ambientes en los cuales las copias de seguridad se guarda de manera oportuna con el fin de tener varios niveles de recuperación de la información en caso de desastre. Actualmente la entidad cuenta con dos niveles de respaldo, las unidades de cinta y replicación de las bases de datos en el data center externo.

Cuenta de Usuario: Credencial que identifica a un usuario para autenticarse sobre una plataforma tecnológica.

Contraseña: Cadena de caracteres que permite validar la autenticidad de una cuenta de usuario.

Desactivación de cuenta de usuario: Es un estado de la cuenta de usuario que se asigna cuando el propietario de la cuenta termina definitivamente su vínculo con la Entidad.

Plataforma Tecnológica: Una plataforma tecnológica es una agrupación de equipamientos técnicos y humanos destinados a ofrecer unos recursos tecnológicos de elevado nivel acompañados de excelentes conocimientos científicos a una comunidad de usuarios, públicos y privados, tanto a nivel local, regional como nacional.

Software de Monitoreo: Herramienta que constantemente vigila los dispositivos de una red de datos para informar a los administradores de redes mediante correo electrónico y/o alarmas el estado de los mismos.

Software Antivirus: Herramienta cuyo objetivo es detectar y eliminar virus informáticos.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información, además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (accountability), no repudio y fiabilidad.

TI: se refiere a tecnologías de la información

TIC: se refiere a tecnologías de la información y comunicaciones

Vulnerabilidad: debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 6 de 26
	Vigente desde: 25-09-2016		

5. NORMATIVIDAD

La Caja de la Vivienda Popular acoge las normas vigentes de seguridad de información, protección de datos personales y directrices de ciberseguridad a nivel nacional y territorial aplicando las prácticas y estándares recomendados para su cumplimiento.

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Otras
Ley	1266	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.	2008	X		
Resolución	305	Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre	2008		X	
Decreto	1227	Por la cual se crea el Comité de Seguridad de la Información (CSI) de la Caja de Vivienda Popular	2008			X
Ley	1273	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".	2009	X		
Decreto	235, Art.1-4	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones pública	2010	X		

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 7 de 26
	Vigente desde: 25-09-2016		

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Otras
Directiva	22	Estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos y ciudadanas que capturan las entidades del Distrito Capital.	2011		X	
Ley	1581	Por el cual se dictan disposiciones generales para la protección de datos personales.	2012	X		
Decreto	1377	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.	2013	X		
Ley	1712	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.	2014	X		
Decreto	886	Reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los Responsables del Tratamiento	2014	X		
Decreto	2573	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones	2014	X		
Decreto	103	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.	2015			
Decreto	415	Por el cual se adiciona el Decreto único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de información y las comunicaciones.	2016			

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 8 de 26
	Vigente desde: 25-09-2016		

5.1. DOCUMENTOS DE REFERENCIA

Tipo de documento	Título del documento	Código	Origen	
			Externo	Interno
Norma Técnica Distrital	Norma Técnica Distrital SIG 001:2011. Capítulo 6 Seguimiento y Monitoreo del Desempeño de la Seguridad de la Información.	SIG 001:2011	X	
Conpes 3701	Lineamientos de Política para Ciberseguridad y Ciberdefensa	N.A.	X	
Norma Técnica Internacional ISO 27001, 27002, 27005	Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información en una organización pública o privada	ISO 27001, 27002, 27005	X	

6. RESPONSABILIDADES

- La Dirección de Gestión Corporativa y CID – Sistemas es la responsable de la elaboración y/o modificación y/o actualización y/o eliminación e implementación, monitoreo y seguimiento de la Política de Seguridad de la Información, asegurando así los recursos adecuados y promoviendo así una cultura activa de seguridad en la entidad.
- La Alta Dirección a través del Comité de Seguridad de la Información es la responsable de la aprobación y de la verificación del cumplimiento de la política de seguridad de la información.
- Los (as) funcionarios(as) que realicen labores en o para la Caja de la Vivienda Popular tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.
- El director y/o jefe de área es el responsable de hacer cumplir las normas y políticas de seguridad de la información establecidas por la alta dirección en la CVP.
- La Dirección de Gestión Corporativa lidera la definición de parámetros para el establecimiento de hardware, software y comunicaciones, así como de la arquitectura tecnológica. Sin embargo, la administración de la información en la fase de registro tanto en aplicativos como bases de datos, es responsabilidad de cada área, con el fin de evitar modificación no autorizada o intencional o el uso indebido de los activos de la organización.
- Las auditorías y seguimientos a los sistemas de información se realizarán de manera preventiva por la Oficina de Control Interno con el acompañamiento del área de

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 9 de 26
	Vigente desde: 25-09-2016		

sistemas. Los usuarios de los sistemas y aplicativos deberán reportar a la Dirección de Gestión Corporativa las inconsistencias, anomalías y nuevos requerimientos.

7. ACTIVOS DE INFORMACIÓN

La Dirección de Gestión Corporativa y CID identificó los activos de información y han sido inventariados para su control y administración. Estos recursos están compuestos por medios físicos (archivo documental), digitales (bases de datos digitales y manuales técnicos y de sistema, sistemas de información, aplicaciones de software, sistemas de back up) electrónicos (servidores, computadores personales y de comunicaciones (redes LAN y Wifi, firewall, sistemas de control de comunicaciones), recurso humano con roles y responsabilidades para acceso a la información sobre los cuales se aplicarán regulaciones internas para el uso controlado y seguro de la misma.

Todos los servidores, contratistas y terceras partes, que usen activos de información de propiedad de la CVP son responsables de cumplir y acoger con integridad la Política de Seguridad para dar un uso racional y eficiente a los recursos asignados con las siguientes directrices:

7.1 Equipos - Servidores

Objetivo: Definir las actividades que son necesarias para realizar la administración segura de los equipos servidores, de forma tal que pueda garantizarse su estabilidad, disponibilidad e integridad de los recursos de red.

Condiciones Generales:

- ✓ Los servidores deben estar ubicados en el centro de datos con perfiles administrativos de acceso lógico y físico restringido a personal no autorizado.
Todo el software instalado en los servidores debe ser licenciado y aprobado por el administrador de la plataforma tecnológica. No aplica software de licenciamiento GNU.
- ✓ Los servidores de la entidad deben estar protegidos en todo momento con una plataforma actualizada de antivirus licenciado con el fin de garantizar la integridad y disponibilidad de los servicios suministrados.
- ✓ El acceso físico y lógico a los equipos servidores de la entidad solo serán autorizados por la Dirección de Gestión Corporativa y CID – Sistemas.
- ✓ Todo equipo servidor debe disponer del formato código 208-DGC-ft-05 Asignación y Hoja de vida de equipos, debidamente actualizado.
- ✓ Durante la configuración de los servidores deben cumplirse las normas y/o requisitos mínimos para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y software a ser ejecutados por los usuarios y mantener la documentación actualizada.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 10 de 26
	Vigente desde: 25-09-2016		

- ✓ Los servidores que proporcionen servicios a través de la red e Internet deben incluir en el formato Asignación y su hoja de vida el registro de los mantenimientos preventivos y/o correctivos, actualizaciones de software que se realicen.
- ✓ Cada servidor debe contar con un documento guía de instalación y recuperación de entorno tecnológico.
- ✓ El personal del área de sistemas es responsable de acompañar a todos los visitantes, proveedores, personal de soporte y otras personas no autorizadas, en el ingreso a las áreas seguras cuando sea necesario, registrando el ingreso en la bitácora. Se entiende como área segura el centro de cómputo, subcentros de distribución de cableado de piso, cuartos de UPS y acceso restringido a la oficina del Área de Sistemas.
- ✓ El acceso no autorizado a los servidores debe ser sancionado por la CVP en su facultad legal de protección a la información pública.

Responsables:

El administrador de la Plataforma Tecnológica es el responsable de la seguridad y aplicación de las políticas sobre los servidores.

7.2 Centro de Cómputo y Centros de Cableado.

Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de la red cableada.

- ✓ El acceso al Centro de Cómputo y Centros de Cableado de la CVP debe ser controlados a través de un registro o bitácora obligatoria de cada ingreso y salida del personal el cual será controlado, verificado y preservado por el administrador de la plataforma tecnológica
- ✓ El centro de cómputo debe cumplir con las condiciones físicas y de seguridad acordes con los estándares establecidos por la CVP. La Dirección de Gestión Corporativa es responsable de velar por el cumplimiento de este requerimiento.
- ✓ Las puertas del Centro de Cómputo y Centros de Cableado deben permanecer cerradas.

Responsables:

La Dirección de Gestión Corporativa y CID junto con el Administrador de la red y el grupo de Profesionales y Técnicos de Sistemas son los responsables del cumplimiento y aplicación de esta política

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 11 de 26
	Vigente desde: 25-09-2016		

7.3 Equipos de cómputo de escritorio

Objetivo: Asegurar la protección de la información administrada por usuarios que utilicen o tengan asignado un equipo de cómputo de escritorio.

- ✓ Los computadores de la CVP son de uso institucional, razón por la cual no se permite el acceso o uso por parte de personal ajeno a la entidad, incluyendo proveedores, familiares de funcionarios o contratistas, beneficiarios o visitantes.
- ✓ Todo equipo debe estar conectado a una toma de corriente de energía regulada (tomas de color anaranjado).
- ✓ Todo equipo de cómputo de la entidad (propio o en alquiler) debe disponer de un cable patch cord conectado a la salida lógica de datos de color azul, dispuesta sobre la canaleta.
- ✓ La CVP no permite la instalación de software personal y/o que no esté licenciado por la entidad. Los únicos funcionarios autorizados para instalar software en los equipos de la CVP es el personal técnico de sistemas.
- ✓ La entidad debe contemplar e incluir actividades de mantenimiento preventivo y/o correctivo para los computadores de escritorio de uso institucional.
- ✓ Los usuarios deben contar con la autorización del respectivo directivo o jefe de la dependencia para movilizar o cambiar de equipo de cómputo y debe ser notificado al área de sistemas mediante correo electrónico, el cual debe provenir del director, jefe o secretaria del área.
- ✓ No está permitido manipular, extraer o cambiar componentes y/o la configuración de los equipos de escritorio. Cualquier falla o anomalía debe ser notificada al área de sistemas quien tiene la responsabilidad exclusiva de estas actividades.
- ✓ Los equipos que ingresan temporalmente a la entidad que son de propiedad de terceros deben ser registrados en la portería de la entidad para poder realizar su retiro sin formato de autorización de la CVP.
- ✓ La entidad no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya ingresado a sus instalaciones.
- ✓ El Área de Sistemas no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo de información) a equipos que no sean de la Entidad.
- ✓ Todos los usuarios deben bloquear el equipo de cómputo con protector de pantalla que exija la contraseña de acceso a la sesión ante la ausencia temporal del puesto de trabajo.

7.4 Impresoras, scanner y plotter

Objetivo: Garantizar el buen uso, funcionamiento y seguridad de activos de apoyo para el desarrollo de funciones misionales.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 12 de 26
	Vigente desde: 25-09-2016		

- ✓ Estos activos de apoyo son de uso compartido en las áreas y por lo tanto no es permitido su traslado, manipulación de componentes e insumos, acciones que son ejecutadas exclusivamente por personal técnico del área de sistemas.
- ✓ Los insumos (toner, papel, tintas) son solicitados por las áreas correspondientes a la Subdirección administrativa. La instalación de los toner, y tintas están a cargo del área técnica de sistemas por solicitud registrada en el correo electrónico soporte@cajaviviendapopular.gov.co.
- ✓ Los documentos que se impriman y/o digitalicen en equipos de la entidad deben ser de carácter institucional.
- ✓ Los usuarios son responsables de salvaguardar y conservar la confidencialidad de documentos impresos y no deben ser desatendidos en los plotters e impresoras de la entidad.
- ✓ Ningún usuario debe desarrollar labores de reparación o mantenimiento de estos equipos, en caso de falla se debe avisar al área de sistemas. Los costos de reparación ocasionados por la manipulación indebida de estos equipos serán asumidos por el usuario que ocasionó el daño. En caso de no identificarse un responsable lo asumirá el grupo de usuarios asignados al equipo en servicio.

Responsables: El personal técnico del área de sistemas es responsable de la ubicación, instalación, mantenimiento y capacitación sobre el uso de activos de apoyo. Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión y digitalización para que no se afecte su adecuado mantenimiento.

7.5 Bases de Datos

Objetivo: Lograr y mantener la protección adecuada de estos activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones, garantizando la integridad, confiabilidad y disponibilidad de la información.

- ✓ Las aplicaciones de software de motores de bases de datos objeto de la administración deben estar bajo un licenciamiento a nombre de la entidad. No aplica para licencias de tipo GNU
- ✓ Las bases de datos deberán alojarse en equipos autorizados por el administrador de la red de la CVP.
- ✓ Los acceso a la base de datos, deben ser controlados con políticas de perfil asignadas por el administrador de la red.
- ✓ Las bases de datos deben contar con copias de seguridad y con un procedimiento de recuperación en caso de contingencias y continuidad.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 13 de 26
	Vigente desde: 25-09-2016		

- ✓ Las bases de datos deben disponer un log de transacciones que evidencie la trazabilidad de los datos. La Entidad debe contar con un diccionario de datos en el cual se identifiquen los datos sensibles de sus instancias de bases de datos.

Responsables:

La Dirección de Gestión Corporativa y CID es la responsable de formular, establecer las políticas y ejecutar la administración de las bases de datos de la entidad descritas en el procedimiento según sus funciones y competencias. Las direcciones misionales y las dependencias que utilicen aplicativos o sistemas de información institucionales como medio de registro de su operación son los responsables por la calidad de los datos, su registro, modificación y utilización, así como del debido uso de la información en términos de protección de datos personales e información institucional.

7.6 Copias de Seguridad y Restauración

Objetivo: Determinar las acciones que garanticen la administración de las copias de seguridad y las restauraciones de copias de información para asegurar que toda la información esencial y el software se pueda recuperar después de una falla.

- ✓ Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los computadores de escritorio. Por lo tanto es obligación de los usuarios almacenar la información institucional en la unidad Z asociada a la cuenta de usuario del dominio de la Entidad. La DGC y CID no garantiza la copia o restauración de información que se encuentre en los computadores personales o portátiles de la entidad.
- ✓ Se determina que la periodicidad de la copia de seguridad sobre la unidad Z, bases de datos y carpetas compartidas de área en el servidor se realiza así:
 - Diaria incremental
 - Semanal
 - Mensual

La copia de seguridad se realiza a partir de las 10:00 pm de lunes a viernes.

Si la periodicidad indicada no se ajusta a la necesidad de la dependencia, mediante correo electrónico al buzón suporte@cajaviviendapopular.gov.co soportaran el requerimiento indicando la modificación.

- ✓ Cada dependencia debe solicitar al área de sistemas la creación de carpetas compartidas en los servidores de la entidad, con los respectivos permisos de lectura y/o escritura, para almacenar de forma segura información compartida de carácter institucional mediante notificación al buzón de correo electrónico suporte@cajaviviendapopular.gov.co.
- ✓ Las copias de respaldo de los servidores no incluyen archivos de audio y video. Si

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 14 de 26
	Vigente desde: 25-09-2016		

alguna información institucional se encuentra en estos formatos se debe dar aviso al área de sistemas para incluirlo en el backup mediante notificación al buzón de correo electrónico soporte@cajaviviendapopular.gov.co.

- ✓ El retiro de un funcionario o contratista obliga a la entrega efectiva de la información física y digital al jefe directo o supervisor del contrato, quien decidirá la disposición final, el tiempo, la carpeta de la dependencia, quién tiene el acceso y copia de la información digital. Determinará la valoración de la información como activo. La información física requiere entrega oficial al archivo documental con visto bueno del jefe directo o supervisor del contrato.
- ✓ Cualquier alteración en la seguridad de la información de los equipos y medios dispuestos por la entidad deben ser reportados a la Dirección de Gestión Corporativa y CID, como un incidente de seguridad.
- ✓ Para las solicitudes de copias de respaldo y de restauración de copias debe aplicarse lo enunciado en el instructivo 208-DGC-In-03 MEDIDAS TECNOLÓGICAS Y ADMINISTRATIVAS DE PROTECCIÓN DE DATOS

Responsables:

La Dirección de Gestión Corporativa y CID definirá los periodos, los servidores y los medios de almacenamiento y ejecutará el procedimiento para la realización de las copias de seguridad de la información institucional.

El Data Center es el único centro replicador de información para bases de datos de la política de backup mencionada anteriormente.

Los directores y/o jefes son los responsables de la información física y digital de cada dependencia y contarán con el apoyo técnico del área de archivo y sistemas para consolidar procedimientos efectivos de resguardo, recuperación y procesamiento.

7.7 Cuentas de usuario

Objetivo: Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daños de la información durante y fuera del horario de trabajo normal de los usuarios..

- ✓ Las cuentas de usuario son propiedad de la CVP, asignadas de forma individual e intransferible, para uso exclusivo de información institucional. Por lo tanto, cada usuario asume la responsabilidad del buen uso de su contenido, usuario y contraseña, so pena de las sanciones legales a que haya lugar.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 15 de 26
	Vigente desde: 25-09-2016		

- ✓ Para la creación o modificación de cuentas de usuario se debe tener en cuenta lo enunciado en el instructivo 208-DGC-In-03 MEDIDAS TECNOLÓGICAS Y ADMINISTRATIVAS DE PROTECCIÓN DE DATOS.
- ✓ Todas las contraseñas de los sistemas (administrador de red, cuentas de administración de aplicaciones, cuentas de usuario etc...) deben cambiarse con una periodicidad mensual.
- ✓ El usuario responde por el uso que se dé a su cuenta, se prohíbe el préstamo de la cuenta a otro usuario.
- ✓ Ningún usuario deberá intentar obtener contraseñas de otros usuarios para acceder a sistemas o información institucional.
- ✓ Es deber y responsabilidad de los usuarios asignar contraseñas fuertes, es decir, que contengan la combinación de números, letras y caracteres especiales. (Los caracteres especiales cuando sea permitido por la plataforma donde se esté asignando la credencial). Política implementada en el Directorio Activo.
- ✓ En caso que exista una prórroga para un contratista, el supervisor(a) del contrato debe enviar a la cuenta de soporte institucional la solicitud de ampliación de uso de la respectiva cuenta de red, incluyendo el número del contrato y la fecha hasta la cual se hace la prórroga.
- ✓ El área de gestión de humana debe reportar mediante correo electrónico al buzón soporte@cajaviviendapopular.gov.co, de manera oportuna todos los cambios significantes (traslados, suspensiones, vacaciones, desvinculación) en las responsabilidades de un usuario (personal de planta), de su estado laboral, de su ubicación dentro de la entidad con el fin de mantener el principio de seguridad de la información.
- ✓ Para la creación de cuentas de usuario de sistemas de información, se debe contar con el usuario de red creado en el dominio de la Entidad y el buzón de correo electrónico institucional, aplicando el procedimiento \\serv-cv11\calidad\10. PROCESO ADMINISTRACIÓN DE LA INFORMACIÓN\PROCEDIMIENTOS\208-DGC-Pr-06 CREACIÓN Y DESACTIVACIÓN DE USUARIOS\208-DGC-Pr-06 ADMINISTRACIÓN DE CUENTAS DE USUARIO

Responsables:

El responsable para la gestión (creación, modificación, suspensión y/o desactivación de cuentas de usuarios) del procedimiento es el Profesional designado de la Dirección de Gestión Corporativa y CID – Sistemas y el líder de gestión humana.

Los supervisores de los contratos deberán reportar al área de sistemas, con anticipación al vencimiento del mismo las novedades de terminación, suspensión, terminación anticipada, por sanción o sesión de un contrato con el fin de actualizar el control de acceso a los sistemas en el que el contratista figura como activo.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 16 de 26
	Vigente desde: 25-09-2016		

Para el caso de los sistemas de información se hace responsable de la gestión de este procedimiento al encargado o administrador del sistema de información del área.

7.8 Red Wifi y Acceso a Internet

Objetivo: Establecer lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales.

- ✓ Ningún equipo de cómputo o de comunicaciones ajeno a la CVP o de propiedad de los funcionarios o contratistas debe ser conectado a la red institucional. En caso de ser necesario el acceso a internet para este tipo de equipos se ha dispuesto una red WiFi de uso exclusivo para visitantes y ciudadanos.
- ✓ Solo se instalarán computadores personales u otros dispositivos con la autorización de la Dirección de Gestión Corporativa y CID – Sistemas y previo análisis y verificación de la situación de vulnerabilidad de la entidad.
- ✓ La contraseña de acceso a la red Wifi es enviada mensualmente a los buzones de correo de los cargos directivos de la CVP. Los encargados o coordinadores de las reuniones pueden solicitar esta contraseña de manera presencial en la oficina de sistemas para uso exclusivo en el espacio de la reunión.
- ✓ La identificación de conexiones permanentes por parte de un dispositivo que no es de la entidad en la red wifi genera un cambio de contraseña en la misma y un llamado de atención al usuario que hace un uso continuo del servicio.
- ✓ Los encargados del soporte técnico deben desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado mediante correo electrónico al buzón del administrador de la red.
- ✓ La descarga de archivos de internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de internet/intranet. Por lo tanto no se permite la descarga de música, conexión a medios de comunicación vía internet como emisoras, canales de televisión, youtube, redes sociales y sitios de entretenimiento virtual, actualmente implementada por política en el Firewall de la entidad.
- ✓ Está prohibido el uso de software malintencionado para acceder a privilegios de navegación no autorizados.
- ✓ La conexión de internet estará controlada de acuerdo con las categorías de navegación definidas para los usuarios; sin embargo en ningún caso se considerarán aceptables los siguientes usos:
 - Navegación en sitios de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 17 de 26
	Vigente desde: 25-09-2016		

- Publicación o envío de información confidencial de funcionarios, beneficiarios o información institucional sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.
 - Utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados.
 - Publicación de anuncios comerciales o material publicitario, salvo las oficinas que dentro de sus funciones así lo requieran. Lo anterior deberá contemplar una solicitud previa, la cual debe ser justificada por el jefe de la oficina.
 - Utilizar la plataforma tecnológica para hacer ofertas fraudulentas de compra o venta, así como conducir cualquier tipo de fraude financiero, tales como "cartas en cadena" o "pirámides", son faltas y se constituyen como violaciones a esta Política.
 - No está permitido personificar o intentar personificar a otra persona a través de la utilización de encabezados falsificados o el uso de otra información personal.
 - Utilizar la plataforma tecnológica para promover o mantener asuntos o negocios personales.
 - Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el licenciamiento y/o procesamiento del equipo de cómputo o de la red.
- ✓ Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los funcionarios y terceros autorizados. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.
 - ✓ Para acceder a las páginas web que por política general están restringidas el (la) funcionario(a) debe solicitar el acceso a través del correo electrónico suporte@cajaviviendapopular.gov.co, previa autorización del superior inmediato.
 - ✓ La CVP cuenta con un servicio de telefonía IP y su conexión es exclusivamente para el servicio de voz. La detección de conexiones de computadores personales u otros dispositivos a esas salidas lógicas generará un incidente de seguridad que será reportado e investigado con los respectivos llamados de atención a los responsables.

Responsables:

La Dirección de Gestión Corporativa y CID junto con el grupo de Profesionales de Sistemas son los responsables del monitoreo, diseño de mecanismos e implementación de protocolos de seguridad y reporte de incidentes en el uso de internet y red wifi.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 18 de 26
	Vigente desde: 25-09-2016		

Los funcionarios y contratistas de la CVP son responsables del buen uso de internet y red wifi, así como correo informativo de incidentes de seguridad de la información al administrador de la red.

7.9 Soporte Técnico

Objetivo: Apoyar técnicamente la plataforma tecnológica de la Caja de la Vivienda Popular (CVP) mediante actividades de mantenimiento correctivo y preventivo, soporte técnico de hardware y software e incidentes informáticos para garantizar la seguridad y disponibilidad de las herramientas tecnológicas en los diferentes procesos de la Entidad.

- ✓ El soporte técnico es un servicio orientado a atender los incidentes relacionados con el funcionamiento de la plataforma tecnológica de la CVP, incluyendo el sistema de telefonía. Este servicio se presta de lunes a viernes en la jornada laboral establecida por la administración.
- ✓ Las solicitudes de soporte técnico **sólo serán atendidas** si están registradas en el correo institucional suporte@cajaviviendapopular.gov.co o en la plataforma de servicio dispuesta por la Dirección de Gestión Corporativa y CID.
- ✓ El soporte técnico no contempla equipos de uso personal de los funcionarios y contratistas vinculados a la CVP. No se recibe atención de solicitudes de soporte verbales.
- ✓ Las áreas que tienen como responsabilidad el servicio al ciudadano, la dirección general y las direcciones misionales, tienen prioridad para la prestación del servicio de soporte técnico. Esta condición no exime el registro de la solicitud en el correo de soporte o la plataforma establecida para ello.
- ✓ Es responsabilidad de cada funcionario y contratista realizar un buen uso de los equipos, dispositivos y herramientas tecnológicas entregadas por la CVP para el desarrollo de sus funciones. Cualquier alteración, daño o inconsistencia presentada en el hardware como en el software debe ser reportada al área de sistemas. En este orden, no está permitido la manipulación correctiva de los equipos de cómputo, escáner e impresoras por parte del personal no autorizado. En estos casos sólo está autorizada la revisión por parte de personal de soporte técnico del área de sistemas.
- ✓ Los puntos de red, cambio de teléfonos y movilización de equipos requieren la intervención de un funcionario de soporte técnico y la aprobación del directivo o jefe del área.
- ✓ Las solicitudes de acceso a la información de otro funcionario (ubicada en el equipo o correo institucional) y copias de información de un contratista o funcionario diferente al usuario que hace la solicitud, deben realizarse al correo suporte@cajaviviendapopular.gov.co con la autorización del director de área.
- ✓ Algunos computadores personales de uso en la CVP están en condición de alquiler, por lo tanto el personal de sistemas realizará el correspondiente diagnóstico con el

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 19 de 26
	Vigente desde: 25-09-2016		

fin de escalar el problema al proveedor, con base en el acuerdo de nivel de servicio contratado.

- ✓ Las solicitudes de carpetas compartidas, buzones de correo, accesos a sitios específicos en internet deben ser revisadas y evaluadas por el área de sistemas y estar sujetos a los recursos técnicos institucionales.
- ✓ Los equipos portátiles están destinados para uso temporal en reuniones de los usuarios internos de la CVP. Por lo tanto el personal de sistemas no responde por información almacenada en ellos. Por seguridad de la información se recomienda liberar o borrar cualquier archivo almacenado antes de su entrega y no modificar la configuración inicial de los mismos como asignación de claves.
- ✓ Los responsables de la atención del soporte técnico deben generar mensualmente un reporte discriminado de la atención al usuario, caracterizando el servicio y las acciones correctivas tomadas o propuestas para subsanar los incidentes.
- ✓ La Dirección de Gestión Corporativa y CID – Sistemas debe mantener una hoja de vida de cada equipo, que contemple las revisiones efectuadas, cambios de piezas, modificaciones realizadas y las estadísticas de su rendimiento.
- ✓ La Dirección de Gestión Corporativa y CID – Sistemas debe informar a los usuarios de la CVP, por medio escrito o telefónico, sobre las jornadas de mantenimiento preventivo y/o correctivo.
- ✓ La CVP no realiza mantenimiento preventivo y/o correctivo a elementos de cómputo que no sean de propiedad de la entidad.
- ✓ Los equipos y medios suministrados en préstamo no deben dejarse desatendidos en sitios públicos durante el tiempo de préstamo y son responsabilidad del usuario que hizo la solicitud de préstamo.
- ✓ En el caso de requerir el apoyo de funcionarios de soporte técnico como acompañamiento para eventos o reuniones externas, se debe realizar la solicitud con antelación al correo soporte@cajaviviendapopular.gov.co, para programar los recursos del área de sistemas. La atención estará enfocada a la instalación y desinstalación de los equipos en el sitio. El área de sistemas no se responsabiliza del transporte, seguridad y devolución de los equipos.
- ✓ Los equipos audiovisuales o de cómputo que van a ser retirados de la entidad deben solicitarse mediante los formatos **208-DGC-ft_04 Préstamo de equipos audiovisuales** y el **208-SADM-ft-19 Único Ingreso y salida de elementos** dispuestos en la carpeta Calidad, con mínimo 24 horas de anticipación.
- ✓ El usuario que firma la solicitud de préstamo de equipos es el responsable del mismo desde el momento que recibe el insumo hasta el momento de su devolución al área de Sistemas. Además es el responsable del traslado, custodia y buen uso del equipo.
- ✓ Los equipos y medios que sean retirados de la entidad deben contar con una autorización del jefe del área y el responsable del área de sistemas. No deben dejarse desatendidos en sitios públicos durante su uso; los computadores y

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 20 de 26
	Vigente desde: 25-09-2016		

dispositivos portátiles deben transportarse como equipaje de mano y contar con un seguro que cubra casos de robo, daño parcial o total.

- ✓ Todos los equipos reservados y retirados de la oficina de sistemas en calidad de préstamo deben ser devueltos exclusivamente al personal de soporte técnico en el tiempo previsto y en las mismas condiciones en que se recibieron. En caso de pérdida o daño se reportará por escrito como un incidente para investigación disciplinaria y se realizarán las acciones pertinentes como denuncia por robo y trámite ante la compañía aseguradora, previa la investigación respectiva. Los trámites de denuncia los adelanta el funcionario responsable del préstamo ante la instancia policial respectiva.
- ✓ No se recomienda dejar equipos de la CVP en condición de préstamo guardados en los escritorios de los funcionarios o contratistas. Tampoco sacarlos de la entidad si no están destinados a actividades institucionales.
- ✓ Los responsables de soporte técnico deben generar un reporte mensual de la actividad, caracterizando el servicio e incluyendo los incidentes, soluciones registradas y sugerencias para la mejora del mismo.

Responsables:

La Dirección de Gestión Corporativa y CID junto con el grupo de Profesionales de Sistemas son los responsables del monitoreo, diseño de mecanismos e implementación de protocolos de atención y seguridad en el soporte técnico.

Los funcionarios y contratistas de la CVP son responsables del buen uso de los equipos entregados como herramienta para el desarrollo de sus funciones, de reportar daños, mal uso o funcionamiento de los equipos e incidentes que afecten la seguridad de los mismos y por consiguiente de la información institucional.

7.10 Desarrollo y Mantenimiento de Software

Objetivo: Definir los lineamientos técnicos y operativos para el desarrollo de software de acuerdo con las necesidades y recursos de la CVP, así como el mantenimiento de aplicaciones que se encuentran en ambiente de producción en la Entidad.

- ✓ Todos los desarrollos de software y las nuevas aplicaciones que se implementen en la entidad deben estar autorizados por la Dirección de Gestión Corporativa y CID.
- ✓ La plataforma tecnológica, las bases de datos y aplicaciones institucionales están bajo la responsabilidad del área de sistemas de la Dirección de Gestión Corporativa. Por lo tanto, las demás dependencias deben atender las políticas institucionales definidas para el uso, desarrollo y seguridad de las mismas.
- ✓ Las herramientas de desarrollo de software utilizadas deben contar con una licencia

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 21 de 26
	Vigente desde: 25-09-2016		

- adquirida legalmente por la entidad solo para las que apliquen.
- ✓ La Dirección de Gestión Corporativa- Sistemas debe mantener una copia de los archivos fuentes de las aplicaciones de acuerdo con políticas y procedimientos de copias de seguridad.
 - ✓ Todo desarrollo que se realice debe generar los siguientes entregables:
 - 208-DGC-Ft-14 Formato Solicitud Mantenimiento de Software
 - Documento de Pruebas Funcionales
 - Manual de Usuario
 - Manual de instalación y operación
 - Archivos con el Código fuente e inventario de componentes del sistema debidamente documentados
 - Archivos ejecutables
 - 208-DGC-Ft-15 Formato Paso a producción de aplicación o componentes de software
 - Diccionario de Datos
 - Modelo Entidad - Relación de la BD
 - ✓ Es función del responsable de infraestructura, el responsable del desarrollo y mantenimiento establecer la separación de los ambientes de desarrollo, pruebas y producción, para minimizar los riesgos de acceso no autorizado o de cambios al sistema operacional.
 - ✓ El administrador de la red, en conjunto con el responsable del desarrollo, y de infraestructura, definirán el proceso administrativo de claves, así como la administración de las técnicas criptográficas que deban utilizarse.
 - ✓ Debe verificarse que los desarrollos o mantenimientos al software contemplen los estándares del entorno tecnológico de la entidad y los objetivos estratégicos de la misma.
 - ✓ El responsable del desarrollo y el responsable de infraestructura deberán documentar y mantener actualizado quienes obtienen acceso a los datos de prueba, y quienes acceden a los datos reales (en caso de necesitarse).
 - ✓ En la etapa de despliegue, se deben asignar los roles para el acceso a la información.
 - ✓ Las funciones de desarrollo de aplicaciones, prueba, aceptación y producción de aplicaciones, y la custodia del software e información ligada, deben estar separadas y ser realizadas por funcionarios distintos entre sí, a efecto de asegurar una adecuada segregación de funciones.
 - ✓ Cualquier modificación al software, debe ser probado previamente antes de ser desplegado.
 - ✓ Todo sistema de información debe contar con un esquema de contingencias el cual debe contemplar aspectos de software, hardware y recurso humano necesario para la continuidad del servicio.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 22 de 26
	Vigente desde: 25-09-2016		

- ✓ Todo sistema de información debe tener asignado un administrador del sistema responsable de actividades de operación, manejo, cumplimiento de la seguridad establecida
- ✓ El acceso a los archivos fuente de las aplicaciones está limitado únicamente al personal autorizado por la Dirección de Gestión Corporativa y CID.
- ✓ La Dirección de Gestión Corporativa como encargada de los sistemas de información brindará la custodia y realizará las copias de los archivos fuente de las aplicaciones de propiedad de la entidad.
- ✓ La Dirección de Gestión Corporativa y CID debe supervisar y monitorear el desarrollo del software subcontratado por la Entidad.

Responsables:

La Dirección de Gestión Corporativa y CID es la responsable de formular y establecer las políticas para el desarrollo, documentación y mantenimiento de software de la entidad. Las direcciones misionales y la dirección de Gestión Corporativa y CID deben desarrollar las actividades descritas en el procedimiento según sus funciones y competencias.

8. LINEAMIENTOS GENERALES PARA TODA LA ENTIDAD

- ✓ Durante la configuración de los servidores el administrador de servidores debe generar las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y software a ser ejecutados por los usuarios.
- ✓ Debe realizarse un estudio y/o diagnóstico que determinen las necesidades y/o requerimientos de software y/o hardware.
- ✓ La CVP debe contemplar que el proveedor deba realizar mantenimiento preventivo y/o correctivo a los equipos las veces que sea requerido por la CVP a través de la Dirección de Gestión Corporativa y CID – Sistemas.
- ✓ Debe definirse igualmente que el proveedor deba suministrar los equipos con el software preinstalado y sus respectivas licencias y medio de instalación.
- ✓ El proveedor debe informar a la Dirección de Gestión Corporativa y CID cualquier anomalía de fabricación del que llegare a expedir el distribuidor y suministrar los correctivos necesarios.
- ✓ Toda adquisición de tecnología informática y de sistemas que se haga en la CVP debe contarse con el concepto técnico de la Dirección de Gestión Corporativa y CID – Sistemas.
- ✓ La selección del modelo y capacidades del hardware requerido por determinada dependencia, debe ir de acuerdo con el plan estratégico de sistemas y sustentado por un estudio elaborado por la Dirección de Gestión Corporativa y CID, en el cual se enfatizan las características y volumen de información que ameritan

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 23 de 26
	Vigente desde: 25-09-2016		

sistematización y diferencian los tipos de equipos que se adjudican a las diversas áreas usuarias

9. MONITOREO Y SEGUIMIENTO

La Dirección de Gestión Corporativa y CID – Sistemas debe realizar el monitoreo y seguimiento a la implementación y/o mantenimiento de la política de seguridad de la información

10. PROCESO DISCIPLINARIO

El desconocimiento de la política de seguridad de la información de la Caja de la Vivienda Popular, podría generar acciones disciplinarias de aquellos funcionarios que puedan cometer alguna violación de la Política de Seguridad de la Información, por lo tanto, es importante conocer las políticas y los procedimientos de seguridad de la información, así, como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de gestión de la Dirección de Gestión Corporativa y CID.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por la Caja de la Vivienda Popular

- ✓ No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- ✓ Ingresar a carpetas de otros procesos, unidades, grupos o áreas, sin autorización y no reportarlo al punto único de contacto o al GRUPO DE SOPORTE.
- ✓ No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- ✓ No actualizar la información de los activos de información a su cargo.
- ✓ Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- ✓ No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, de documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada).
- ✓ Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- ✓ Dejar las gavetas abiertas o con las llaves puestas en los escritorios,
- ✓ Dejar los computadores encendidos en horas no laborables.
- ✓ Permitir que personas ajenas a la Caja de la Vivienda Popular, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
- ✓ Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 24 de 26
	Vigente desde: 25-09-2016		

- ✓ Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- ✓ Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico u ofensivo, cadenas de correos y correos masivos no autorizados.
- ✓ Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- ✓ Recepcionar o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la Entidad.
- ✓ Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- ✓ Utilizar equipos electrónicos o tecnológicos desatendidos o que a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recepcionar y almacenar datos.
- ✓ Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el Área de Sistemas de la Caja de la Vivienda Popular.
- ✓ Permitir el acceso de exfuncionarios a la red corporativa, sin la autorización del Área de Sistemas de la Caja de la Vivienda Popular.
- ✓ Utilización de servicios disponibles a través de internet, como FTP, Telnet y accesos remotos, no permitidos por la Caja de la Vivienda Popular o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- ✓ Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Caja de la Vivienda Popular.
- ✓ No cumplir con las actividades designadas para la protección de los activos de información de la Caja de la Vivienda Popular.
- ✓ Destruir o desechar de forma incorrecta la documentación institucional.
- ✓ Descuidar documentación con información pública reservada o clasificada de la institución, sin las medidas apropiadas de seguridad que garanticen su protección.
- ✓ Registrar información pública reservada o clasificada, en pos-it, apuntes, agendas, libretas, etc., sin el debido cuidado.
- ✓ Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no pertenezca a la Caja de la Vivienda Popular o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la Caja de la Vivienda Popular, sin la debida autorización.
- ✓ Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de la Caja de la Vivienda Popular para beneficio personal.
- ✓ El que sin autorización acceda en todo o parte de la infraestructura informática o se mantenga dentro del mismo en contra de la voluntad de la Caja de la Vivienda Popular.
- ✓ El que impida u obstaculice el funcionamiento o el acceso normal a la infraestructura informática, los datos informáticos o las redes de telecomunicaciones de la Caja de la Vivienda Popular, sin estar autorizado.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 25 de 26
	Vigente desde: 25-09-2016		

- ✓ El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de la Caja de la Vivienda Popular.
- ✓ El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de la Caja de la Vivienda Popular.
- ✓ El que modifique, altere datos personales de las bases de datos de la Caja de la Vivienda Popular sin la debida autorización.
- ✓ El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por la Caja de la Vivienda Popular.
- ✓ No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la Caja de la Vivienda Popular o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- ✓ Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la Caja de la Vivienda Popular a personas no autorizadas.
- ✓ Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de la Caja de la Vivienda Popular o de terceros.
- ✓ Ejecutar acciones tendientes a eludir o variar los controles establecidos por la Caja de la Vivienda Popular.
- ✓ Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- ✓ Sustraer de las instalaciones de la Caja de la Vivienda Popular, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- ✓ Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
- ✓ No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de la Caja de la Vivienda Popular, para traslado, reasignación o para disposición final.
- ✓ Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la Caja de la Vivienda Popular o de alguno de sus funcionarios.
- ✓ Realizar cambios no autorizados en la plataforma tecnológica de la Caja de la Vivienda Popular.
- ✓ Acceder, almacenar o distribuir pornografía infantil.
- ✓ Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el Área de Sistemas de la Caja de la Vivienda Popular.
- ✓ Copiar sin autorización las aplicaciones de software de la Caja de la Vivienda Popular, o violar los derechos de autor o acuerdos de licenciamiento.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA CAJA DE LA VIVIENDA POPULAR		Código: 208-DGC-Mn-07
			Versión: 1 Página 26 de 26
	Vigente desde: 25-09-2016		

11. ACUERDO DE CONFIDENCIALIDAD

Todos los funcionarios y terceros deben firmar la cláusula y/o acuerdo de confidencialidad que deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación temporal o de prestación de servicios, o cuando se permita el acceso a información y/o a los recursos a personas o entidades externas.

12. CONTROL DE CAMBIOS

Versión	Fecha Aprobación (dd-mm-aaaa)	Cambios	Revisó (Nombre y Cargo)
01	25-09-2016	Creación del documento	Camilo Augusto Ramos Beltrán Silenia Neira Torres Sandra Lorena Guacaneme Urueña

Elaboró:	Revisó:	Aprobó:
Camilo Augusto Ramos Beltrán Contratista	Silenia Neira Torres Profesional - Dirección Gestión Corporativa y CID Claudia Marcela García Profesional - Oficina Asesora de Planeación	Sandra Lorena Guacaneme Urueña Directora de Gestión Corporativa y CID Richard Eduardo López Jefe Oficina Asesora de Planeación
Fecha: 29/08/2016	Fecha: 22/09/2016	Fecha: 25/09/2016