1. MISIÓN Y ALCANCE

Este procedimiento permite asegurar que los recursos del sistema de información (material informático o programas) de la Caja de la Vivienda Popular sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren avaladas y dentro de los términos de su autorización.

El Procedimiento es aplicado por el área de sistemas y comprende las actividades de defensa del perímetro, autenticación y gestión y control.

2. NORMATIVIDAD

TIPO	No.	TEMA	FECHA	ORIGEN		
				NACIONAL	DISTRITAL	INTERNA
Constitución Nacional			1991	X		
Directiva	005	Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital Mediante Decreto Distrital Número 680 del 31 de agosto de 2001, se estableció a la Comisión Distrital de Sistemas como organismo rector y asesor de las políticas y estrategias que se adopten en todas las entidades integrantes de la Administración Distrital en tecnología informática y comunicaciones, asignándole como una de sus funciones, la de establecer políticas y estándares para lograr el desarrollo armónico y coordinado de la informática y las comunicaciones de los entes del Distrito Capital y verificar su cumplimiento.	2004		**X**	
Acuerdo	017	Por el cual se ordena la	2002		**X**	

		Inscripción en registro de Instrumentos Públicos actos administrativos que afectan Bienes Inmuebles en el Distrito Capital y se dictan otras disposiciones."				
Decreto	680	Por el cual se modifica la Comisión Distrital de Sistemas -CDS-	2001		**X**	
Acuerdo	057	"Por el cual se dictan disposiciones generales para la implementación del sistema distrital de información -sdi-, se organiza la comisión distrital de sistemas, y se dictan otras disposiciones".	2002		**X**	
Circular	066	Formulación de proyectos informáticos y de comunicaciones Ver Circular Secretaría General 66 de 2002 Mediante Decreto 680 del 31 de agosto 2001 se redefinió la Comisión Distrital de Sistemas, convirtiéndola en el organismo rector de las políticas y estrategias que se adopten en todas las entidades del Distrito Capital en tecnología informática y comunicaciones y como asesor de la Administración Distrital en dichas materias.	2002		**X**	
Directiva	002	Formulación de proyectos informáticos y de comunicaciones Ver Circular Secretaría General 66 de 2002 Mediante Decreto 680 del 31 de agosto 2001 se redefinió la Comisión	2002		**X**	

		Distrital de Sistemas, convirtiéndola en el organismo rector de las políticas y estrategias que se adopten en todas las entidades del Distrito Capital en tecnología informática y comunicaciones y como asesor de la Administración Distrital en dichas materias.				
Decreto	397	Delega en el Secretario General de la Alcaldía Mayor de Bogota las atribuciones conferidas al Alcalde Mayor en el Acuerdo 57 de 2002 como presidente de la Comisión Distrital de Sistemas, y las demás funciones que se requieran en el ejercicio de esta atribución	2002		**X**	
Resolución	001	Por la cual se establece el reglamento interno de la Comisión Distrital de Sistemas.	2003		**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**	

3. CONDICIONES GENERALES

- Los usuarios son responsables de entender y seguir los procedimientos administrativos establecidos para la utilización y el mantenimiento de los recursos informáticos de la entidad.
- Los funcionarios tienen la responsabilidad de resguardar el acceso a los recursos informáticos mediante la utilización de contraseñas confidenciales, personales e intransferibles.
- Todas las acciones realizadas bajo los auspicios de un identificador de usuario y sus consecuencias legales son responsabilidad del usuario titular del identificador.

4. DOCUMENTOS DE REFERENCIA

Tipo de documento	Titulo del documento	Código	Origen	
			Externa	Interna
N/A				

5. GLOSARIO

Antivirus: son programas cuya función es detectar y eliminar Virus informáticos y otros programas maliciosos *(a veces denominados malware).*
Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado.
Firewall: Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas
Usuario: es la persona que utiliza o trabaja con algún objeto o que es destinaría de algún servicio público o privado, empresarial o profesional.
Logs: es un registro oficial de eventos durante un periodo de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why, W5) un evento ocurre para un dispositivo en particular o aplicación.
Backup: Las copias de seguridad son un proceso que se utiliza para salvar toda la información, es decir, un usuario, quiere guardar toda la información, o parte de la información, de la que dispone en el PC hasta este momento, realizará una copia de seguridad de tal manera, que lo almacenará en una *cinta, DVD, BluRay*,en Internet o simplemente en otro Disco Duro, para posteriormente si pierde la información, poder restaurar el sistema.

6. DESCRIPCIÓN DEL PROCEDIMIENTO

No.	Actividad	Responsable	Observaciones y/o registros relacionados
¿Se puede prestar 3 clases de servicios: Defensa del perímetro o Autenticación o Gestión y control?			
DEFENSA PERÍMETRO			
Se puede realizar firewall ó administración del antivirus o sistema de detección de intrusos			
Firewall			
1.	Configurar y administrar el firewall	Profesional Universitario	De acuerdo con procesos propios del firewall, a través del cual se generan los informes y se realizan los ajustes quedando como evidencia el buen funcionamiento del mismo
2.	Realizar pruebas de seguridad al firewall	Profesional Universitario	
3.	Elaborar informe de la prueba donde se evidencia las acciones a seguir	Profesional Universitario	
4.	Implementar las acciones correctivas	Profesional Universitario	
5.	Realizar seguimiento a las acciones periódicamente.	Profesional Universitario	
6.	Elaborar informe del seguimiento. Y fin del procedimiento	Profesional Universitario	
Administración del antivirus			
7.	Verificar que el antivirus se esté actualizando. Y fin del procedimiento	Profesional Universitario	Se verifica semanalmente que se encuentre actualizado, de acuerdo con los parámetros del software utilizado
Sistema de detección de intrusos			
8.	Verificar los informes de detección de intrusos que emite el sistema	Profesional Universitario	
9.	Diseñar e implementar acciones correctivas Y fin del procedimiento	Profesional Universitario	
AUTENTICACIÓN			
Se realiza creación o eliminación de cuentas de usuario ó paz y salvo			
Creación, eliminación de cuentas de usuarios			

10.	Enviar solicitud de creación o eliminación de cuenta de usuario al correo electrónico soporte.cvp@habitatbogota.gov.co del área de sistemas	Dependencia correspondiente	Correo electrónico
11.	Recibir la solicitud de la dependencia.	Profesional Universitario	Correo electrónico
12.	Crear o eliminar usuario y asignar o eliminar contraseña segura.	Profesional Universitario	Correo electrónico
13.	Mantener confidencialidad de la contraseña	Profesional Universitario	Correo electrónico
14.	Solicitar el cambio de la contraseña de acuerdo a los lineamientos de la política de seguridad de la información. Y fin del procedimiento	Profesional Universitario	Correo electrónico
Paz y salvos			
15.	Enviar solicitud vía correo a sistemas informando la terminación de las actividades del contratista que laboran en la dependencia.	Director de la dependencia o quien haga sus veces	
16.	Verificar la entrega del estado de equipo y la información.	Profesional Universitario del área de sistemas o quien realice la verificación	
17.	Elaborar y firmar paz y salvo de sistemas	Profesional Universitario del área de sistemas o quien realice la verificación	
18	Eliminar la cuenta del usuario. Y fin del procedimiento	Profesional Universitario del área de	
GESTIÓN Y CONTROL			
Se realiza creación segura o logs de auditoria o Backups			
Creación segura			
19.	Elaborar documento estándar de instalación de estación de trabajo y de servidor (Estándar)	Profesional Universitario	
20.	Implementar el estándar	Profesional	

		Universitario	
21.	Realizar seguimiento, monitoreo y control al estándar. Y fin del procedimiento	Profesional Universitario	
Logs de auditoria			
22.	Diseñar documento donde se normatice dónde van a hacer implementados los logs de auditoria	Profesional Universitario	
23.	Implementa los logs	Profesional Universitario	
24.	Realizar seguimiento a los logs para búsqueda de comportamientos anormales en la operación.	Profesional Universitario	
25	Preservar los logs de auditoria	Profesional Universitario	
26	Presentar informe al coordinador de sistemas acorde a cronograma establecido. Y fin del procedimiento	Profesional Universitario	
BACKUPS			
Creación de backups			
27	Diseñar documento donde se normatice que tipo de información, frecuencia, el medio y el método con el cual se va a realizar el backup.	Coordinador de la dependencia de sistemas	
28	Implementar el documento acorde a las necesidades previstas.	Coordinador de la dependencia de sistemas	
29	Realizar el backup en dos copias.	Coordinador de la dependencia de sistemas	
30	Realizar seguimiento a los logs de backups para verificar la integridad de la operación.	Coordinador de la dependencia de sistemas	
31.	Preservar los logs de backups	Coordinador de la dependencia de sistemas	
Almacenamiento de backups			
32.	Almacenar la primera copia en la dependencia encargada bajo la seguridad adecuada.	Profesional Universitario del área de sistemas	

33.	Almacenar la segunda copia fuera de la entidad	Profesional Universitario del área de sistemas	
¿Se requiere restaurar la información?			
Restauración de información			
34.	Recibir solicitud de restauración de la información a través de correo institucional por parte del jefe de la dependencia o quien haga sus veces.	Coordinador de la dependencia de sistemas	
35.	Aprobar o rechazar la solicitud de restauración de la información	Coordinador de la dependencia de sistemas	

7. DIAGRAMA DE FLUJO

Ver diagrama de flujo del procedimiento de Seguridad Informática

8. ANEXOS

N/A

9. CONTROL DE CAMBIOS

VERSIÓN ANTERIOR	VERSIÓN ANTERIOR ELABORADA POR	VERSIÓN ANTERIOR REVISADA POR	MOTIVO DE LA ACTUALIZACIÓN	HOJAS A REEMPLAZAR
1	Mauricio Duque y Andrea Quimbayo Chávez	Mauricio Duque y Camilo Ramos	Se modifico la normatividad agregando la resolución 305 y se actualizó la plantilla del procedimiento.	La totalidad del documento.

Elaboró: Enrique Lara	Revisó: Gina Alexandra Vaca – Directora de Gestión Corporativa y CID	Aprobó: COMITÉ SISTEMA INTEGRADO DE GESTIÓN P/ Yeny Carolina Tiria Medina
Fecha: 14/10/2011	Fecha: 26/10/2011	Fecha: 28/10/2011