CAJA DE LA VIVIENDA POPULAR

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Calle 54 N° 13-30
Código Postal : 110231, Bogotá D.C.
PBX: 3494520
Fax: 3105884
www.cajaviviendapopular.gov.co
soluciones@cajaviviendapcpular.gov.co

Tabla de Contenido

1. INTRODUCCIÓN

La seguridad de la información 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.

La Alta Dirección de la Caja de la Vivienda Popular, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para la CVP, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés que se identifiquen en la Entidad.

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 de este no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

Es de destacar que a través de la Resolución 1550 del 14/12/2007 “Por medio de la cual se establecen las Políticas de Informática y Sistemas para la Caja de la Vivienda Popular” se dictan las primeras directrices relacionadas con seguridad informática en la CVP, así mismo para el 12/09/2016 se oficializó la versión uno (1) de la política de seguridad informática a través de la Resolución 4664 “Por medio de la cual se adopta la Política de Seguridad Informática de la Caja de la Vivienda Popular”, luego se actualiza este documento a través de la Resolución 3332 del 16 de agosto de 2019 "Por la cual se actualiza la Política de Seguridad de la Información de la Caja de la Vivienda Popular” donde se oficializa el documento de la política de seguridad de la información en su versión dos (2) este contempla actualizaciones y modificaciones en el contenido del documento.

Esta política se actualizará por parte de la Oficina TIC, 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 TIC frente a amenazas y vulnerabilidades internas o externas, deliberadas o accidentales, teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la entidad alineados con el contexto de direccionamiento estratégico y de gestión del riesgo 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

- ✓ Consolidar la seguridad de la información como una línea estratégica en la Caja de La Vivienda Popular definiendo, comunicando y generando la cultura de buenas prácticas para el acceso, uso y manejo de los activos de información, por parte de todos los funcionarios, contratistas y terceros relacionados con la Caja de la Vivienda Popular.

- ✓ Proteger los activos de información, y salvaguardar la plataforma tecnológica en aras de proteger la imagen, los intereses y el buen nombre de la Entidad, gestionando las amenazas y vulnerabilidades en los activos de información para reducir los riesgos asociados con la seguridad de la información y dar cumplimiento a los lineamientos establecidos en la Política de Gobierno Digital y Seguridad Digital respecto a la Seguridad de la Información.

3. ALCANCE Y APLICABILIDAD

Esta política aplica a los activos de información definidos por la Caja de la Vivienda Popular 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 Caja de la Vivienda Popular y el apoyo del equipo de la Oficina de las Tecnologías de la Información y las Comunicaciones, 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 la reservas legales.

4. MARCO LEGAL Y/O NORMATIVO

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.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
CONSTITUCIÓN POLÍTICA DE COLOMBIA	1991	1991	Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Disponible en Línea: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15	X		
Ley Estatutaria	1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.	X		
Ley	23	1982	Sobre Derechos de Autor. Congreso de la República. Disponible en Línea http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431	X		
Ley	527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276.	X		
Ley	1266	2008	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. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488	X		

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
Ley	1273	2009	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". Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492	X		
Ley	1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43292.	X		
Ley	1712	2014	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. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882.	X		
Decreto	235, Art.1-4	2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones pública	X		
Decreto	4632	2011	Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones. Disponible en Línea: http://wsp.presidencia.gov.co/Normativa/Decretos/2011/Documents/Diciembre/09/dec463209122011.pdf	X		
Decreto	2609	2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado". Disponible en Línea: http://www.mintic.gov.co/portal/604/articles3528_documento.pdf.	X		
Decreto	1377	2013	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5364.	X		

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
Decreto	886	2014	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. Disponible en línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57338.	X		
Decreto	103	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556.	X		
Decreto	1494	2015	Por el cual se corrigen yerros en la Ley 1712 de 2014. Disponible en Línea: http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201494%20DEL%2013%20DE%20JULIO%20DE%202015.pdf.	X		
Decreto	415	2016	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.	X		
Decreto	1499	2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.	X		
Decreto	1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Disponible en Línea: https://www.mintic.gov.co/portal/604/articles-74903_documento.pdf. Expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones	X		

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
Directiva	22	2011	Estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos y ciudadanas que capturan las entidades del Distrito Capital. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45545. Expedida por el Alcalde Mayor de Bogotá.		X	
Directiva	02	2019	Simplificación de interacción digital los ciudadanos y el estado. Expedida por Presidente de la Republica.	X		
Resolución	305	2008	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. Expedida por: la Comisión Distrital de Sistemas (CDS) de Bogotá.		X	
Resolución	197	2019	Por la cual se crea el Comité Institucional de Gestión y Desempeño de la Caja de Vivienda Popular. Expedida por el Director General de la Caja de la Vivienda Popular.			X

4.1. Documentos de Referencia

Tipo de documento	Título del documento	Código	Origen	
			Externo	Interno
Decreto Distrital	Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión Nacional y se dictan otras disposiciones	591 de 2018	X	
Conpes 3701	Lineamientos de Política para Ciberseguridad y Ciberdefensa.	N.A.	X	

Tipo de documento	Título del documento	Código	Origen	
			Externo	Interno
Conpes 3854	Política nacional para abordar la seguridad digital.	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	
MANUAL DE GOBIERNO DIGITAL	Para la Implementación de la Política de Gobierno Digital, entidades del orden nacional; Modelo de Seguridad y Privacidad de la Información-MSPI; Formato Política SGSI – MSPI para la Política de Gobierno Digital. Disponible en Línea: file:///E:/CVP/2019/Gobierno%20Digital/Manual-GD-V7.pdf.	Versión 7	X	

5. DEFINICIONES

Acceso a la Información: Conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema de bases de datos, bibliotecas, archivos e Internet.

Activos de información: Corresponde a elementos tales como bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.

Activos de software: Son elementos tales como: Aplicaciones de software, herramientas de desarrollo, y utilidades adicionales.

Activos físicos: Se consideran activos físicos elementos tales como: Computadores, portátiles, módems, impresoras, máquinas de fax, equipos de comunicaciones, PBX, cintas, discos, UPS, muebles etc.

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.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

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.

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.

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

Clave: Contraseña o password, es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La clave debe mantenerse en secreto ante aquellos a quien no se le permite el acceso.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados[1].

Correo Electrónico Institucional: Es el servicio basado en el intercambio de información a través de la red y el cual es provisto por la Caja de la Vivienda Popular, para los funcionarios, contratistas y terceros autorizados para su acceso. El propósito principal es compartir información de forma rápida, sencilla y segura. El sistema de correo electrónico puede ser utilizado para el intercambio de información, administración de libreta de direcciones, manejo de contactos, administración de agenda y el envío y recepción de documentos, relacionados con las responsabilidades institucionales.

Cuarto de Comunicaciones: Es un área utilizada para el uso exclusivo de equipos asociados con el sistema de cableado de telecomunicaciones de la Entidad. El cuarto de telecomunicaciones debe ser capaz de albergar los equipos de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado.

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

[1] NTC-ISO/IEC 27000, pág. 2.

Custodio de la información: es el encargado de la administración de seguridad de información. Dentro de sus responsabilidades se encuentra la gestión del Plan de Seguridad de Información, así como la coordinación de esfuerzos entre el personal de sistemas y los responsables de las otras áreas de la Entidad, siendo estos últimos los responsables de la información que utilizan. Asimismo, es el responsable de promover la seguridad de información en toda la Entidad con el fin de incluirla en el planteamiento y ejecución de los objetivos institucionales.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información de la Entidad, después del resultado de los procesos de evaluación y tratamiento de riesgos.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

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.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad autorizada[2].

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Firewall: Un cortafuego (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.

Freeware: Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.

Hacking ético: Es una forma de referirse al acto de una persona, conocido como hacker, que utiliza sus conocimientos de informática y seguridad para encontrar vulnerabilidades o fallas de seguridad en el sistema, con el objetivo de reportarlas en la organización para que

[2] NTC-ISO/IEC 27000, pág. 2.

se tomen todas las medidas necesarias que posibilite prevenir una catástrofe cibernética, como el robo de información[3].

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento los cuales deben ser exactos.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal[4].

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley[5].

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley[6].

Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Intranet: Es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.

Inventario Tecnológico: Se refiere al inventario de dispositivos electrónicos que hacen parte de los activos de la Entidad.

3https://www.iniseg.es/blog/ciberseguridad/que-es-el-hacking-etico/?gclid=EAIaIQobChMItNm_gp-84wIVioCfCh1qrAGJEAAYAiAAEgIcrPD_BwE
[4] Ley No.1712 DE 2014
[5] Ley No.1712 DE 2014
[6] Ley No.1712 DE 2014

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[7].

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.

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

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse.

Mecanismos de bloqueo: Son los mecanismos necesarios para impedir que los usuarios, tanto de los sistemas de información como de los servicios, tengan acceso a estos sin previa autorización, ya sea por razones de seguridad, falta de permisos, intentos malintencionados o solicitud de los propietarios de la información.

Memoria USB: La memoria USB (Universal Serial Bus) es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información. Se le denomina también lápiz de memoria, lápiz USB o memoria externa, siendo innecesaria la voz inglesa pen drive o pendrive.

Mensajería Instantánea Institucional: Comúnmente conocido como “Chat”, es un canal de comunicación provisto por la Caja de la Vivienda Popular para facilitar una forma de comunicación en tiempo real entre los funcionarios, contratistas creando un espacio virtual de encuentro específico.

Niveles de respaldo de información: Hace referencia a los diferentes ambientes en los cuales las copias de seguridad se guardan 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 datacenter externo.

7 https://es.wikipedia.org/wiki/GNU_General_Public_License

OTP (One Time Password): Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.

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

Phishing (cosecha y pesca de contraseñas): Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándolas a que visiten páginas web falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás información confidencial.

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 vea 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.

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.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Política de Gobierno Digital: Con la transformación de la Estrategia de Gobierno en Línea a política de Gobierno Digital, se genera un nuevo enfoque en donde no sólo el Estado sino también los diferentes actores de la sociedad son actores fundamentales para un desarrollo integral del Gobierno Digital en Colombia y en donde las necesidades y problemáticas del contexto determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público[8].

Propiedad intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias

[8] http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html

o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas[9].

Propietario de la información: En tecnologías de la información y la comunicación (TIC) es el responsable de preservar y disponer de la información de acuerdo a los lineamientos de la Entidad.

Puntos de entrada y salida: Cualquier dispositivo (distinto de la memoria RAM) que intercambie datos con el sistema lo hace a través de un "puerto", por esto se denominan también puertos de E/S ("I/O ports"). Desde el punto de vista del software, un puerto es una interfaz con ciertas características; se trata por tanto de una abstracción (no nos referimos al enchufe con el que se conecta físicamente un dispositivo al sistema), aunque desde el punto de vista del hardware, esta abstracción se corresponde con un dispositivo físico capaz de intercambiar información (E/S) con el bus de datos.

Rack: Soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. También son llamados bastidores, cabinas, gabinetes o armarios.

Roles y Privilegios: La autenticación para verificar la identidad, para demostrar que una persona es quien dice ser y también para permitir una política de autorización con el fin de definir qué es lo que determinada identidad puede "ver y hacer" con la información.

Red de datos: Una red de datos es un conjunto de ordenadores que están conectados entre sí compartiendo recursos, información, y servicios.

Repositorio de documentos: Sitio centralizado donde se almacena y mantiene información digital actualizada para consulta del personal autorizado.

Requerimiento: Necesidad de un servicio TIC que el usuario solicita a través del mecanismo definido por la organización en los procedimientos normalizados.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

RSS (Really Simple Syndication): RSS son las siglas de Really Simple Syndication, un formato XML para sindicar o compartir contenido en la web. Se utiliza para difundir información actualizada frecuentemente a usuarios que se han suscrito a la fuente de contenidos. El formato permite distribuir contenidos sin necesidad de un navegador,

9 https://www.wipo.int/edocs/pubdocs/es/intproperty/450/wipo_pub_450.pdf

utilizando un software diseñado para leer estos contenidos RSS tales como Internet Explorer, entre otros.

Scanner: Es un periférico que permite transferir una imagen desde un papel o superficie y transformarlos en gráficos digital (proceso también llamado digitalización). Existen actualmente escáneres que capturan objetos en tres dimensiones. Suelen utilizar un haz de luz o láser para realizar el proceso.

Seguridad de Comunicaciones: Consiste en prevenir que alguna entidad o persona no autorizada pueda interceptar comunicaciones o acceder de forma inteligible a información.

Seguridad de la información: Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información.

Seguridad Física: Consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas ante amenazas a los recursos y la información confidencial, se refiere, a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

Seguridad Lógica: Medidas establecidas por la administración de usuarios y administradores de recursos de tecnología de información para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando los recursos tecnológicos y medios de información.

Servicio: Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.

Servicios de almacenamiento de archivos "On line": Un servicio de alojamiento de archivos, servicio de almacenamiento de archivos online, o centro de medios online es un servicio de alojamiento de Internet diseñado específicamente para alojar contenido estático, mayormente archivos grandes que no son páginas web.

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.

Servicios TIC: El concepto de Servicio TIC consiste en dar soporte, de forma integrada y personalizada, a todas estas herramientas que necesita hoy en día el profesional de empresa para realizar su trabajo. Los elementos del Servicio TIC son:

- Los dispositivos: PC, portátiles, agendas electrónicas, impresoras, teléfonos, sistemas de videoconferencia, etc.
- La Red de Área Local corporativa (LAN). Así como las comunicaciones de voz incluyendo el teléfono y ahora llega el momento de proporcionar y gestionar los PC y la electrónica de red necesarios para las comunicaciones de datos.
- Las comunicaciones de voz y datos WAN (Red de Área Remota), que incluyen tanto las redes privadas corporativas como el acceso a redes públicas como Internet. La integración de las comunicaciones WAN y estas cada vez se requieren con las comunicaciones LAN.
- Los servicios y aplicaciones desde la red.

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.

SGSI - Sistema de Gestión de Seguridad de la Información: Consiste en un conjunto de políticas, procedimientos, directrices y recursos y actividades asociados, que son gestionados de manera colectiva por una organización con el fin de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio[10].

Shareware: Clase de software o programa, cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. para adquirir el software de manera completa es necesario un pago económico.

Sistemas de Información: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo[11].

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

Smartphone: El teléfono inteligente (en inglés: smartphone) es un tipo teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de almacenar

[10] NTC-ISO/IEC 27000, pág. 12.
[11] https://es.wikipedia.org/wiki/Sistema_de_informaci%C3%B3n

datos y realizar actividades, semejante a la de una minicomputadora, y con una mayor conectividad que un teléfono móvil convencional[12].

Sniffer: Es una aplicación especial para redes informáticas, que permite como tal capturar los paquetes que viajan por una red.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

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

Software de Dominio Público: es un software libre que no tiene un propietario, por ende, no existen derechos de autor, licencias o restricciones de distribución. Por este concepto, el software de dominio público se diferencia de un freeware, el cual conserva los derechos de autor[13].

Software Licenciado: Es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario 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[14].

Software pirata: Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.

Soporte Técnico: Rango de servicios por medio del cual se proporciona asistencia a los usuarios al tener algún problema al utilizar un producto o servicio, ya sea este el hardware o software de una computadora de un servidor de Internet, periféricos, artículos electrónicos, maquinaria, o cualquier otro equipo o dispositivo.

Spam: Es la denominación del correo electrónico no solicitado que recibe una persona. Dichos mensajes, también llamados correo no deseado o correo basura, suelen ser publicidades de toda clase de productos y servicios[15].

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 estos.

[12] https://sites.google.com/site/sectorandroid217/historia-de-los-dispositivos-moviles/smart-phone
[13] http://www.cavsi.com/preguntasrespuestas/que-es-software-de-dominio-publico/
[14] https://es.wikipedia.org/wiki/Licencia_de_software
[15] https://definicion.de/spam/

Tecnología de la información T.I.: Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

TI: Se refiere a tecnologías de la información.

TIC: Se refiere a tecnologías de la información y comunicaciones

Tipos de información: cualquier tipo de información producida y/o recibida por las entidades públicas, sus dependencias y servidores públicos, y en general por cualquier persona que desarrolle actividades inherentes a la función de dicha entidad o que hayan sido delegados por esta, independientemente del soporte y medio de registro (análogo o digital) en que se produzcan, y que se conservan en:

a) Documentos de Archivo (físicos y electrónicos).
b) Archivos institucionales (físicos y electrónicos).
c) Sistemas de Información Corporativos.
d) Sistemas de Trabajo Colaborativo.
e) Sistemas de Administración de Documentos.
f) Sistemas de Mensajería Electrónica.
g) Portales, Intranet y Extranet.
h) Sistemas de Bases de Datos.
i) Disco duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc.
j) Cintas y medios de soporte (back up o contingencia).
k) Uso de tecnologías en la nube.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento

Topología de Red: Se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados".

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Usuario: Persona que utiliza los recursos TIC y que interactúan de forma activa en un proceso, secuencia, código etc.

Usuario de la información: Es un usuario aquella persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos. A menudo es un usuario aquel que adquiere una computadora o dispositivo electrónico y que lo emplea para comunicarse con otros usuarios, generar contenido y documentos, utilizar software de diverso tipo y muchas otras acciones posibles.

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

Webcam - Cámara Web: Una cámara web o cámara de red (en inglés: webcam) es una pequeña cámara digital conectada a una computadora la cual puede capturar imágenes y transmitirlas a través de Internet, ya sea a una página web o a otra u otras computadoras de forma privada.

6. RESPONSABILIDADES

COMPROMISO DE LA DIRECCIÓN

La Alta Dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar información:

- A través del Comité Institucional de Gestión y Desempeño De La CVP es la responsable de la aprobación y de realizar el seguimiento a la estrategia de la implementación de la política de seguridad de la información.
- Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y las necesidades de la mejora continua.

COMPROMISO COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO DE LA CVP

- Actualizar y presentar la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.

- Analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- Verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.
- 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 Caja de la Vivienda Popular.

COMPROMISO OFICINA CONTROL INTERNO

- Las auditorías y seguimientos a los sistemas de información se realizarán de manera preventiva por la Oficina de Control Interno con el acompañamiento de la Oficina TIC.
- La Oficina de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de la Caja de la Vivienda Popular a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
- La Oficina de Control Interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
- La Oficina de Control Interno debe informar a las áreas responsables los hallazgos de las auditorías.

COMPROMISO OFICINA TIC

- La Oficina TIC 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.
- Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información y todos sus capítulos, el uso de los servicios tecnológicos en toda la entidad de acuerdo a las mejores prácticas y lineamientos de la Dirección General de la Caja de la Vivienda Popular y directrices del Gobierno Nacional.
- La Oficina TIC 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.

- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Institución.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la entidad al Comité Institucional de Gestión y Desempeño de la CVP, las diferentes Oficinas, Direcciones y Subdirecciones de la Caja de la Vivienda Popular, así como a los entes de control e investigación que tienen injerencia sobre la Entidad.
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la Entidad.
- Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de la Caja de la Vivienda Popular.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la Entidad.
- Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la entidad. Esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.
- Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Dirección General y las diferentes direcciones.
- Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.

COMPROMISO DEL GRUPO DE SOPORTE TECNOLÓGICO

- Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de estos; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes Oficinas, Direcciones o Subdirecciones siguiendo el procedimiento establecido.
- Establecer, mantener y divulgar las políticas y procedimientos de los servicios de tecnología, incluidos todos los capítulos que hacen parte de esta Política, en toda la entidad de acuerdo a las mejores prácticas y directrices de la Entidad y del Gobierno.

- Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado.
- Brindar el soporte necesario a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la entidad.

RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN

Son propietarios de la información cada uno de los directores, así como los jefes de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.

- Valorar y clasificar la información que está bajo su administración y/o generación. Autorizar, restringir y delimitar a los demás usuarios de la entidad el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas o terceros que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
- Determinar los tiempos de retención de la información en conjunto con él grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.
- Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de esta.
- Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y terceros en las diferentes dependencias de la entidad.

RESPONSABILIDADES DE LOS FUNCIONARIOS, CONTRATISTAS Y TERCEROS USUARIOS 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.
- Los usuarios de los sistemas y aplicativos deberán reportar a la Oficina TIC las inconsistencias, anomalías y nuevos requerimientos.
- Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones, Código Disciplinario Único – Ley 734 de 2002 o Contrato.

- Manejar la Información de la entidad y rendir cuentas por el uso y protección de tal información, mientras que esté bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual acceden y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Evitar la divulgación no autorizada o el uso indebido de la información.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de esta.
- Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
- Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
- Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos a la Caja de la Vivienda Popular a la red Institucional ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Oficina TIC.
- Usar software autorizado que haya sido adquirido legalmente por la entidad. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno de la Oficina TIC.
- Divulgar, aplicar y el cumplir con la presente Política.
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección General de la entidad puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad de la entidad, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la entidad. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.
- Proteger y resguardar su información personal que no esté relacionada con sus funciones en la entidad. La Caja de la Vivienda Popular no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito.

7. GESTIÓN DE ACTIVOS

La Caja de la Vivienda Popular es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios de la Caja de la Vivienda Popular y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

La Caja de la Vivienda Popular es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la Caja de la Vivienda Popular (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).

La Oficina TIC es la responsable de realizar el inventario de los activos de información para su control y administración, de acuerdo al formato que esta Oficina determine para tal fin. Estos recursos deben estar compuestos por medios físicos (archivo documental), digitales (bases de datos digitales y manuales, 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.

La información registrada en el formato en comento queda bajo la responsabilidad de cada propietario de información y centralizado por la Oficina TIC, el cual se publicará en la página web de la Caja de la Vivienda Popular.

La Caja de la Vivienda Popular implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter institucional.

Todos los servidores, contratistas y terceras partes, que usen activos de información de propiedad de la Caja de la Vivienda Popular son responsables de cumplir y acoger con integridad la Política de Seguridad para dar un uso racional y eficiente a los recursos asignados.

7.1 Equipos - Servidores

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

- ✓ Los servidores deben estar ubicados en el centro de datos con 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 para el 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 sólo serán autorizados por la Oficina TIC.
- ✓ Todo equipo servidor debe disponer del formato de 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.
- ✓ 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 y backups que se realicen.
- ✓ Cada servidor debe contar con un documento guía de instalación y recuperación de entorno tecnológico.
- ✓ El personal de soporte de la Oficina TIC es responsable de acompañar a todos los visitantes, vendedores, personal de soporte y otras personas no autorizadas, en el ingreso a las áreas seguras. Se entiende como área segura el centro de cómputo, subcentros de distribución de cableado de piso y cuartos de UPS.
- ✓ El acceso no autorizado a los servidores debe ser sancionado por la Caja de Vivienda Popular en su facultad legal de protección a la información pública.

Responsables:
El administrador de la Plataforma Tecnológica de la Oficina TIC 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 Caja de la Vivienda Popular 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 de la Caja de la Vivienda Popular debe cumplir con las condiciones ambientales, físicas y de seguridad acordes con los estándares establecidos, acorde a la disposición del espacio del sitio destinado para albergar los servidores y centros de distribución de cableado horizontal. La Oficina TIC 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 Oficina TIC junto con el grupo de Profesionales y Técnicos de Sistemas son los responsables del cumplimiento y aplicación de esta política.

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 Caja de la Vivienda Popular 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 Caja de la Vivienda Popular 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 Caja de la Vivienda Popular es el personal técnico de la Oficina TIC.
- ✓ 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

a la Oficina TIC mediante correo electrónico, el cual debe provenir del director, jefe o secretaría 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 a través del correo electrónico de soporte de la Oficina TIC 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 autorización; la entidad no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.
- ✓ El Oficina TIC no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e 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.

Responsables:
Todos los funcionarios y contratistas de la Caja de la Vivienda Popular son los responsables del cumplimiento y aplicación de esta política.

7.4 Impresoras, scanner y plotter

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

- ✓ 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 de la Oficina TIC.
- ✓ La solicitud de insumos como tonner, papel, tintas, debe realizarse a la Subdirección Administrativa –servicios generales. La Oficina TIC solamente aprobará la pertinencia del cambio del tonner y/o tinta.
- ✓ 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 que queden 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 reportar a través del correo electrónico de soporte de la Oficina TIC. 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 o dependencia que tenga asignado el equipo en servicio.

Responsables:
El personal técnico de la Oficina TIC 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
- ✓ La administración de los motores de las bases de datos debe ser asignada mediante obligación contractual a un contratista o función a un servidor de la Entidad que cumpla con los requerimientos de administrador de bases de datos. Las bases de datos deben contar con copias de seguridad y un con un procedimiento de recuperación en caso de contingencias y continuidad.
- ✓ 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 identifique los datos sensibles de sus instancias de bases de datos.

Responsables:
La Oficina TIC es la responsable de formular, establecer las políticas y ejecutar la administración de las bases datos de la entidad. Las demás 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 Oficina TIC no garantiza la copia o restauración de información que se encuentre en los computadores personales o portátiles de la entidad.
- ✓ Cada dependencia y/o dirección o grupo administrador de la información define la periodicidad de las copias de seguridad de para sus recursos de información, acción que deberá concertarse con la Oficina TIC.
- ✓ Cada dependencia debe solicitar a la Oficina TIC 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.
- ✓ Las copias de respaldo de los servidores no incluyen archivos de audio y video. Si alguna información institucional se encuentra en estos formatos se debe dar aviso a la Oficina TIC para incluirlo en el backup.
- ✓ El Oficina TIC no garantiza la recuperación y/o copia de información personal almacenada en los portátiles y computadores de escritorio.
- ✓ El retiro de un funcionario o contratista obliga a que realice la entrega efectiva de la información física y digital al jefe directo o supervisor del contrato, quien decidirá la disposición final.
- ✓ Cualquier alteración en la seguridad de la información de los equipos y medios dispuestos por la entidad deben ser reportados a través del correo electrónico de soporte de la Oficina TIC, 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 Oficina TIC 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 a partir del requerimiento que realice el dueño de la información.

El Data Center será el único centro replicador de información autorizado por la entidad dado

el caso que se presente algún tipo de contingencia.

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 de la Oficina TIC 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 Caja de la Vivienda Popular, asignadas de forma individual e intransferible, para uso exclusivo de información institucional y es utilizada para validarse en el dominio de la red, identificándose como usuario válido. Por lo tanto, cada usuario asume la responsabilidad del buen uso de su contenido, usuario y contraseña, sopena de las sanciones legales a que haya lugar.
- ✓ 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.
- ✓ Es responsabilidad del usuario aplicar la normatividad vigente en el manejo de contraseñas en donde se define:
  - No usar palabras comunes que se puedan encontrar en los diccionarios.
  - La clave no debe contener caracteres idénticos consecutivos.
  - La clave de acceso a la red debe tener como mínimo ocho (8) caracteres.
  - No revelar las contraseñas a nadie.
- ✓ El usuario responde por el uso que se dé a su cuenta, por tal motivo, se prohíbe el préstamo de la cuenta a otro usuario, el Oficial de Protección de datos o quien haga sus veces, en conjunto con el Responsable del tratamiento de datos podrán revocar y solicitar la cancelación parcial o definitiva de la cuenta de usuario.
- ✓ Ningún usuario deberá intentar obtener contraseñas de otros usuarios para acceder a recursos tecnológicos 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).
- ✓ En caso que exista una prórroga para un contratista, el supervisor(a) del contrato

o a través del correo electrónico asignado a la Secretaria de la dirección/subdirección/oficina 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 por medio de correo electrónico a la Oficina TIC, de manera oportuna todos los cambios significantes en las responsabilidades de un usuario, 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.
- ✓ Mientras los aplicativos o sistemas de información no dispongan de un log de usuarios y perfiles que permita determinar el control de acceso, el administrador asignado deberá llevar un registro o bitácora de activación, desactivación y derechos de acceso de todos los usuarios del sistema correspondiente.
- ✓ Los responsables y administradores de los sistemas de información deben revisar los derechos de acceso de los usuarios semestralmente.

Responsables:
El responsable para la gestión (creación, modificación, suspensión y/o desactivación de cuentas de usuarios) del procedimiento es el Profesional designado de la Oficina TIC y el líder de gestión humana.

Los supervisores de los contratos o secretarias de las direcciones / subdirecciones / oficinas deberán reportar a la Oficina TIC, con anticipación al vencimiento de este 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.

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.

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 (red

cableada). 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 Oficina TIC 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 Caja de la Vivienda Popular. Los encargados o coordinadores de las reuniones pueden solicitar esta contraseña de manera presencial en la Oficina TIC para uso exclusivo en el espacio de la reunión.
- ✓ La identificación de conexiones permanentes por parte de un mismo dispositivo 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.
- ✓ 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. (Se exceptúa de esta política la Oficina de Comunicaciones).
- ✓ Está prohibido el uso de software malintencionado para acceder a privilegios de navegación a través de túneles.
- ✓ La Oficina TIC no se hace responsable por conductas difamatorias, obscenas u ofensivas que se realicen a través de los servicios que proporciona.
- ✓ Es responsabilidad de los usuarios contar con el software y configuración de seguridad en su equipo para minimizar el riesgo al que se puede ver expuesto a un ataque al encontrarse conectado sobre esta red.
- ✓ De ninguna forma ni caso específico la Oficina TIC será responsable por cualquier daño que pueda sufrir el equipo o dispositivo usado para establecer conexión a la red inalámbrica.
- ✓ El usuario es responsable de toda actividad que se lleve desde su equipo o dispositivo mientras esté conectado a la red inalámbrica.
- ✓ Es obligación del usuario informar a la Oficina TIC la violación de alguna de las normas descritas en este documento tanto por personas ajenas o funcionarios de la entidad.
- ✓ Es responsabilidad del usuario estar enterado de los cambios de las presentes políticas.
- ✓ Es responsabilidad del usuario la seguridad física de su equipo, por lo que la Oficina TIC no es en ninguna forma responsable por robo o daños al equipo del usuario. El usuario acepta y reconoce que la Oficina TIC sólo provee el servicio de acceso a red.

- ✓ Los incidentes o errores que se presenten durante el uso de los servicios de red inalámbrica, deberán ser reportados a la Oficina TIC a través de la mesa de servicio.
- ✓ 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.
  - 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.
  - Hacer ofertas fraudulentas de compra o venta, así como conducir cualquier tipo de fraude financiero, tales como "cartas en cadena" o "pirámides", son faltas 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.
  - 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.
- ✓ La Oficina TIC no asume responsabilidad alguna frente al usuario respecto de los usos que éste haga del servicio de la Zona WiFi, ni de los datos o informaciones transferidas desde Internet.
- ✓ Por el hecho de ingresar al portal cautivo (red inalámbrica) y a las Páginas Web y para garantizar el buen y adecuado uso de la misma, el Usuario deberá cumplir con lo siguiente:

  - Ser responsable por cualquier actividad que se lleve a cabo bajo su registro.
  - No abusar, acosar, amenazar o intimidar a otros usuarios en los Sitios Web ya sea a través de los chats, foros, blogs o cualquier otro espacio de participación.

- No usar los Sitios Web como medio para desarrollar actividades ilegales o no autorizadas tanto en Colombia, como en cualquier otro país.
- Ser el único responsable por su conducta y por el contenido de textos, gráficos, fotos, videos o cualquier otro tipo de información de la cual haga uso o incluya en cualquier Sitio Web solicitado.

✓ 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 soporte@cajaviviendapopular.gov.co, previa autorización del superior inmediato.

Responsables:
La Oficina TIC 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.

Los funcionarios y contratistas de la Caja de la Vivienda Popular son responsables del buen uso de internet y red wifi, así como del reporte de incidentes de seguridad de la información a través de estos servicios.

7.9 Soporte Técnico

Objetivo: Apoyar técnicamente la plataforma tecnológica de la Caja de la Vivienda Popular mediante actividades de mantenimiento correctivo y preventivo, soporte técnico de hardware y software 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 Caja de la Vivienda Popular, 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 soporte@cajaviviendapopular.gov.co o en la plataforma de servicio (mesa de ayuda) dispuesta por la Oficina TIC.
✓ El soporte técnico no contempla equipos de uso personal de los funcionarios y contratistas vinculados a la CVP. No se garantiza la atención de solicitudes 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 a la Oficina TIC. 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 de la Oficina TIC
- ✓ 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 soporte@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 la Oficina TIC realizará el correspondiente diagnóstico con el 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 la Oficina TIC y estar sujetos a los recursos técnicos institucionales.
- ✓ Los equipos portátiles están destinados para uso temporal en reuniones de los usuarios internos de la Caja de la Vivienda Popular. Por lo tanto, el personal de la Oficina TIC 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 Oficina TIC 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 Oficina TIC debe informar a los usuarios de la Caja de la Vivienda Popular, 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 de la Oficina TIC. La atención estará enfocada a la instalación y desinstalación de los equipos en el sitio. El Oficina TIC 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 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 a la Oficina TIC. 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 de la Oficina TIC. No deben dejarse desatendidos en sitios públicos durante su uso; los computadores y 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 TIC 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 denuncio por robo y trámite ante la compañía aseguradora, previa la investigación respectiva. Los trámites de denuncio los adelanta el funcionario responsable del préstamo ante la instancia policial respectiva.
- ✓ Los equipos de sonido requieren una manipulación cuidadosa por parte de los usuarios. El personal de soporte técnico puede apoyar la instalación en el sitio de uso y orientar a los responsables del préstamo sobre su manejo.
- ✓ No dejar equipos de la Caja de la Vivienda Popular 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.
- ✓ La Oficina TIC divulgará periódicamente en los medios de comunicación internos, las situaciones de fallas o incidentes frecuentes en su plataforma tecnológica y la forma de solucionarlas o posibles acciones que pueden realizar los usuarios para el correcto funcionamiento de los equipos.

- ✓ 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 Oficina TIC 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 Caja de la Vivienda Popular 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 Caja de la Vivienda Popular, 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 Oficina TIC.
- ✓ La plataforma tecnológica, las bases de datos y aplicaciones institucionales están bajo la responsabilidad de la Oficina TIC. Por lo tanto, las demás dependencias deben atender las políticas institucionales definidas para el uso, desarrollo y seguridad de estas.
- ✓ Las herramientas de desarrollo de software utilizadas deben contar con una licencia adquirida legalmente por la entidad.
- ✓ La Oficina TIC 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 entregables establecidos en el procedimiento Desarrollo y Mantenimiento de Software
- ✓ 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 responsable de Gestión de Seguridad, 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, y quienes acceden a los datos reales (en caso de necesitarse).
- ✓ El usuario final de la aplicación deberá participar en el análisis de requisitos, así como en el entrenamiento en el uso de la aplicación.
- ✓ Al inicio de la fase de diseño del proyecto deberá realizarse un análisis de riesgos del nuevo sistema por parte del "Gerente de Proyecto", a fin de clasificarlo de acuerdo con su continuidad, confiabilidad y confidencialidad. Para esta evaluación se utilizará un esquema de valoración del Riesgos elaborado por el grupo de Sistemas de Información con el apoyo del Grupo de Planeación y Control Interno.
- ✓ Con base en el análisis y clasificación del riesgo del sistema y durante la fase de diseño del proyecto, los requerimientos de seguridad deberán ser definidos formalmente por parte del "usuario" del sistema o un representante del mismo. Las medidas de seguridad deben ser definidas a partir de los requerimientos de seguridad establecidos.
- ✓ 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.
- ✓ Las herramientas y privilegios propios del ambiente de desarrollo, que favorecen un ambiente y facilidades para las pruebas, no deben ser traspasados al ambiente de producción debido a que comprometen la seguridad de la operación normal; éstas deberán de realizarse en un ambiente de prueba o en paralelo.
- ✓ El proceso de puesta en producción de las aplicaciones, de los sistemas o de sus actualizaciones, debe realizarse de tal forma que no deteriore los servicios a los usuarios o la operación normal, por tanto, debe coordinarse adecuadamente y realizarse con cronogramas y horarios preestablecidos.
- ✓ 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.
- ✓ Todo sistema de información debe tener asignado un administrador del sistema responsable de actividades de operación, manejo, cumplimiento de la seguridad establecida
- ✓ Todo desarrollo o mantenimiento de software debe contar con un manual técnico que incluye la descripción, alcance, versiones de las herramientas utilizadas, forma de instalación y recomendaciones técnicas. Además, debe entregarse a sistemas y al área que va a utilizar el desarrollo, el manual de usuario, con las pruebas respectivas y con el acta de aprobación del desarrollo de acuerdo con el formato establecido en el procedimiento Soporte y Mantenimiento de Software.

- ✓ La Oficina TIC sólo autoriza la realización de soporte técnico al software y aplicaciones definidas institucionalmente como herramientas de producción
- ✓ El acceso a los archivos fuente de las aplicaciones está limitado únicamente al personal autorizado por la Oficina TIC.
- ✓ La Oficina TIC 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 Oficina TIC debe supervisar y monitorear el desarrollo del software subcontratado por la Entidad

Responsables:
La Oficina TIC 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 Oficina TIC deben desarrollar las actividades descritas en el procedimiento según sus funciones y competencias.

7.11 Clasificación de la información

La Caja de la Vivienda Popular, consciente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley y la Caja de la Vivienda Popular, define reglas de cómo clasificar la información, liderado por el proceso de Gestión Documental de la Entidad.

- ✓ Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel visual u otro que genere la Caja de la Vivienda Popular como, por ejemplo:

  - Formularios/ comprobantes propios o de terceros.
  - Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
  - Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
  - Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.

- ✓ Los usuarios responsables de la información de la Caja de la Vivienda Popular, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

- ✓ Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como "Valiosa" para

la Caja de la Vivienda Popular; Independiente del tipo de activo, se deben considerar las siguientes características:

- El activo de información es reconocido como valioso para la Caja de la Vivienda Popular.
- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
- Forma parte de la identidad de la organización y sin el cual la Caja de la Vivienda Popular puede estar en algún nivel de riesgo. (La determinación del nivel y tipo de riesgo se estima sobre la base del modelo MECI de la Caja de la Vivienda Popular).
- Los niveles de clasificación de la información valiosa que se ha establecido son:
    - Información pública reservada,
    - Información pública clasificada (privada y semi-privada),
    - Información pública.

8. GESTIÓN LIGADA A LOS RECURSOS HUMANOS

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad, disponibilidad y accesibilidad por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación laboral con la entidad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información, tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello, que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Objetivo:

✓ Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

- ✓ Ser explícito con las responsabilidades en materia de seguridad en la etapa del ingreso de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado o contratista según el caso.
- ✓ Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para cumplir las Políticas de Seguridad de la Información de la Caja de la Vivienda Popular en el transcurso de sus tareas normales.
- ✓ Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones relacionados con el manejo de la información de la Caja de la Vivienda Popular.
- ✓ Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

8.1. Antes del empleo

La Caja de la Vivienda Popular realiza los controles previos de verificación del personal en el momento en que se solicita el cargo/contratista. Estos controles incluyen antecedentes disciplinarios, procuraduría, personería y judiciales y todos los aspectos que a tal efecto requiere a la entidad.

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas de Seguridad de la información.

Todos los usuarios de bienes y servicios informáticos de la Caja de la Vivienda Popular deben firmar la aceptación del Acuerdo de confidencialidad y uso adecuado de los recursos informáticos y de información de la Caja de la Vivienda Popular.

Todo empleado llámese funcionario, contratista o terceros nuevo de la Caja de la Vivienda Popular deberá de contar con la inducción sobre las Políticas de Seguridad de la Información, a través de la Oficina TIC, Recursos Humanos y Contratación, donde se den a conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento.

8.2. Durante el empleo

Todos los servidores públicos de la Caja de la Vivienda Popular y cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la entidad, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la Caja de la Vivienda Popular.

Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Área de Talento Humano debe ser el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada tiempo determinado (no mayor a seis meses) se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado de ese momento.

Al personal que ingrese a la Caja de la Vivienda Popular se le indicará el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se habilitarán los medios técnicos necesarios para comunicar y socializar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

8.3. Proceso Disciplinario

La Oficina TIC publicará en la Intranet el documento Política de Seguridad de la Información, socializará su contenido y hará cumplir su alcance. El desconocimiento de la política de seguridad de la información de la Caja de la Vivienda Popular, por parte de funcionarios, contratistas y terceros puede generar acciones disciplinarias. Las investigaciones disciplinarias y las respectivas sanciones le corresponden a la Oficina TIC y Control Interno Disciplinario.

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 a la mesa de ayuda.
- ✓ 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).
- ✓ No guardar la información digital, producto del procesamiento de la información perteneciente a la Caja de la Vivienda Popular.
- ✓ Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- ✓ 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.
- ✓ 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 (exceptuando el penalizado por la ley) 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 Oficina TIC de la Caja de la Vivienda Popular.
- ✓ Permitir el acceso de funcionarios a la red corporativa, sin la autorización de la Oficina TIC de la Caja de la Vivienda Popular.
- ✓ Utilización de servicios disponibles a través de internet, como FTP y Telnet, 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 permanezca 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.
- ✓ 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 de la información 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 Oficina TIC 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.

8.4. Cese del empleo o cambio de puesto de trabajo

Todos los servidores públicos al finalizar su relación contractual con la Caja de la Vivienda Popular, deberán tramitar el formato de paz y salvo correspondiente mediante el diligenciamiento del documento 208-DGC-Ft-25 ENTREGA DE BIENES Y CREDENCIALES V4.

Los administradores de los diferentes sistemas de información, deberán desactivar las cuentas de usuario.

El administrador del dominio, deberá verificar el vencimiento de la cuenta e inactivar las credenciales, con el fin de asegurar, que el usuario no pueda iniciar una sesión con las credenciales que en su momento le fueron otorgadas.

El administrador de la plataforma del correo electrónico designado para la Caja de la Vivienda Popular, procederá a generar una copia del contenido del buzón del correo y de la información que tenga almacenada en la unidad de drive sobre el correo. Una vez tenga almacenada la copia del buzón, procederá a eliminar la cuenta.

El supervisor del contrato y/o Jefe y/o Director y/o subdirector, deberá recibir copia de la información generada por el servidor público en la cual debe incluir los usuarios y contraseñas para archivos que haya generado y estén protegidos para su apertura.

Responsables:
El Responsable de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los funcionarios, informará a todo el personal que ingresa, sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto a la Política.

El Responsable de contratación incluirá las obligaciones relativas a la seguridad de la información en las descripciones de las actividades de los contratistas, informará a todo el personal que ingresa, sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el contratista y coordinará las tareas de capacitación de usuarios respecto a la Política.

El Responsable de Seguridad de la Información tendrá a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité Institucional de Gestión y Desempeño de la CVP, a los propietarios de la información.

El Comité Institucional de Gestión y Desempeño de la CVP debe ser responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad de la Información maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

9. SEGURIDAD FÍSICA Y DEL ENTORNO

La Caja de la Vivienda Popular debe garantizar la protección del perímetro de seguridad de las instalaciones físicas, controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como mitigar los riesgos y amenazas externas y ambientales, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información de la Entidad.

9.1. Áreas seguras

Todos los sitios en donde se encuentren sistemas de procesamiento informático o de almacenamiento, deben ser protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo y registro de entradas y salidas.

El centro de cómputo, los cuartos de distribución del cableado lógico y eléctrico y el cuarto de ubicación de las UPS en el sótano deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá estar acompañada permanentemente por el personal profesional y/o técnico de la Oficina TIC, motivo por el cual, la entrada o salida a cada uno de los recintos mencionados deben quedar registrados en el Formato Ingreso a Áreas Seguras de Tecnología.

El acceso a esos sitios, deben contar con una puerta metálica de acceso, la cual debe permanecer cerradas con llave. Las llaves de acceso deberán reposar en la caja de llaves (llavero) ubicado en el espacio para desarrollo de las funciones de la Oficina TIC.

Responsables:
El Responsable del ingreso a las áreas seguras, está a cargo de los profesionales y técnicos de la Oficina TIC.

9.1.1. Perímetro de seguridad física.

Las instalaciones de la Caja de la Vivienda Popular tienen definida un área de recepción a la entrada del edificio. El edificio está dotado de cámaras de seguridad, las cuales se encuentran monitoreadas por el personal de la empresa de vigilancia, con grabación permanente en discos duros.

Responsables: El Responsable del aseguramiento físico de las instalaciones, está a cargo de la Subdirección Administrativa.

9.1.2. Controles físicos de entrada.

En la recepción del edificio hay torniquetes de acceso, donde se accede por tarjeta de proximidad y en dado caso de ser un visitante, se permite el acceso con autorización de un servidor público de la Entidad registrando el ingreso en el software de control de visitantes, el cual expide un sticker y fotografía identificando el visitante y a la dependencia a la cual se dirige.

Con el fin de prevenir la pérdida de información física o digital, los servidores de la Caja de la Vivienda Popular y terceros que presten servicios para la Caja de la Vivienda popular deberán seguir las siguientes normas:

- ✓ El porte del carnet de identificación en un lugar visible es de uso obligatorio dentro de las instalaciones de la Entidad.
- ✓ Está prohibido prestar el carnet de identificación, se considera como suplantación de identidad por parte de la persona que lo usa sin ser la persona autorizada.
- ✓ La pérdida del carnet de identificación debe ser reportado al Grupo de talento humano por medio de correo electrónico.
- ✓ La pérdida de la tarjeta de proximidad debe ser reportada al Grupo de Servicios Generales, por medio del documento "Constancia por pérdida de documentos de la policía nacional" y debe ser autorizada para la entrega de la nueva tarjeta y debe ser tramitada ante la Subdirección Administrativa.
- ✓ El ingreso de computadores que no sean de propiedad de la Caja de la Vivienda Popular deben ser registrados en el LIBRO DE REGISTRO DE EQUIPOS, que destine para tal fin la empresa de vigilancia indicando la fecha, hora de entrada, hora de salida, nombre y apellido, marca, serial y firma; de igual manera a la hora de salida se debe verificar que el equipo que está saliendo sea el mismo número de serie del que entró con la persona responsable.

Responsables:
El Responsable de garantizar los controles físicos de entrada es la Subdirección Administrativa.

9.1.3. Seguridad de oficinas, despachos e instalaciones

Todo servidor público de la Caja de la Vivienda Popular, debe acatar los siguientes lineamientos:

- ✓ Todo ingreso de contratistas o visitantes para los fines de semana o días no hábiles deberá ser solicitado previamente al Profesional de Servicios Generales, indicando el motivo del requerimiento, en caso de ser autorizado se informará vía correo electrónico a la vigilancia del edificio el ingreso del personal.
- ✓ El personal externo debe devolver el sticker de identificación personal en la recepción del edificio, al salir de la Entidad.
- ✓ El personal de vigilancia de la Entidad, así como el personal de vigilancia del edificio, deben revisar todo bolso o paquetes del personal al ingresar o salir de las instalaciones.
- ✓ No se permite el ingreso de armas a las instalaciones de la Entidad, salvo los expresamente autorizados.

Responsables:
El Responsable de asegurar el ingreso a las oficinas de la entidad, está a cargo de la Subdirección Administrativa a través de la empresa de vigilancia.

9.1.4. Trabajo en áreas seguras

Se debe garantizar el mantenimiento de los extintores contra incendios, la red contra incendios, entre otros controles que permitan la actuación en caso de emergencia.

- ✓ La responsabilidad del ingreso a áreas denominadas como seguras será exclusiva del responsable de dicha área.
- ✓ El responsable del área segura o a quien éste designe debe supervisar los trabajos realizados por terceros en el área segura a su cargo.
- ✓ La Subdirección Administrativa garantizará el funcionamiento de cada uno de los controles de seguridad establecidos para cada una de sus áreas a cargo, como, por ejemplo, controles de acceso, puertas cerradas, extintores entre otros.
- ✓ El responsable del área segura o quién este delegue debe proporcionar los requisitos de seguridad de su área en particular y garantizar su cumplimiento, en caso de que la información que se maneje en el área sea clasificada o reservada debe procurar por la implementación de las prohibiciones del uso de dispositivos fotográficos.
- ✓ Se deben usar los elementos de protección personal que el área segura requiera.
- ✓ Está prohibido fumar y el consumo de bebidas alcohólicas en toda la entidad de la Caja de la Vivienda Popular.

9.1.5. Áreas de acceso público y de carga y descarga

- ✓ El acceso a las zonas de despacho y carga debe ser autorizado por la Administración del edificio por solicitud directa del Grupo de Recursos físicos.
- ✓ Todo vehículo que ingrese a dejar o retirar elementos de la Entidad debe estar previamente autorizada por el Grupo de Recursos Físicos.

9.2. Seguridad de los equipos

Todos los computadores portátiles, módems y equipos de comunicación se deben registrar al ingreso y a la salida, y no debe abandonar la entidad a menos que esté acompañado por la autorización respectiva.

Los equipos de cómputo (PCs, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa.

Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no deberían estar autorizados para utilizar los recursos informáticos de la Entidad.

9.2.1. Emplazamiento y protección de equipos

Los equipos de cómputo de la Caja de la Vivienda Popular deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades, teniendo en cuenta los siguientes puntos:

Ubicar los equipos de cómputo en un sitio donde se minimice el acceso innecesario y se proporcione control de acceso adecuado.

Limitar actividades tales como comer, beber y manipular líquidos o alimentos, en la proximidad de los equipos de cómputo.

9.2.2. Instalaciones de suministro

Los equipos tecnológicos de la Caja de la Vivienda Popular están protegidos contra posibles fallas en el suministro de energía u otras anomalías eléctricas. Para asegurar la continuidad del suministro de energía, se dispone de:

- ✓ Múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- ✓ Suministro de energía interrumpida mediante UPS para asegurar el apagado regulado y sistemático.
- ✓ Equipos de UPS inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
- ✓ Interruptores de emergencia ubicados en sitios estratégicos a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica.
- ✓ Múltiples fuentes de alimentación eléctrica.

9.2.3. Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones está protegido contra interceptación o daño, mediante las siguientes acciones:

- ✓ Uso de conductos independientes para separar el cableado eléctrico del cableado de comunicaciones, evitando interferencias.
- ✓ Acceso controlado a los módulos y cuartos de cableado.
- ✓ Protección del tendido del cableado troncal (vertical) mediante la utilización de ductos blindados.
- ✓ Inspecciones físicas en busca de dispositivos no autorizados conectados al cableado.
- ✓ Uso de rotulado de equipos y de cables claramente identificables.
- ✓ Plano actualizado del cableado y puestos identificados por piso, esto último es una responsabilidad compartida con la Subdirección Administrativa.

9.2.4. Mantenimiento de los equipos

Se realizará el mantenimiento periódico de los equipos informáticos para asegurar su disponibilidad e integridad permanentes. Para ello se debe tiene en cuenta:

- ✓ Se cuenta con un listado actualizado de los equipos tecnológicos y registro de los mantenimientos preventivos y/o correctivos realizados.
- ✓ Únicamente el personal calificado y autorizado puede realizar actividades de mantenimiento y llevar a cabo reparaciones o modificaciones en los equipos tecnológicos.
- ✓ Se registrarán todos los mantenimientos preventivos y las acciones correctivas que se realicen en los equipos tecnológicos.
- ✓ Se eliminará toda la información que contenga cualquier equipo informático que se requiera retirar, realizando previamente las respectivas copias de resguardo.

9.2.5. Salida de elementos tecnológicos fuera de la Entidad

Los activos no serán retirados de las instalaciones de la Caja de la Vivienda Popular y/o sus sedes anexas, sin una autorización formal de la Oficina TIC y la Subdirección Administrativa.

Se deberán llevar a cabo verificaciones periódicas para detectar el retiro no autorizado de elementos tecnológicos de la Entidad y se notificará a la Subdirección Administrativa de los hallazgos encontrados.

9.2.6. Seguridad de los equipos fuera de las instalaciones

El uso de equipos tecnológicos fuera de la Entidad deberá ser autorizado por la Subdirección Administrativa y la Oficina TIC. En el caso de que almacenen información clasificada, deberá ser aprobado, además, por el Propietario de esta.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipo. Así mismo, se mantendrá una adecuada cobertura de seguro para proteger el equipo fuera de las sedes de la entidad.

9.2.7. Reutilización o retirada segura de equipos

La mala manipulación de los equipos tecnológicos podrá comprometer la información almacenada en los mismos. Los medios de almacenamiento que contienen material crítico, como discos rígidos no removibles, serán físicamente destruidos o sobrescritos de forma segura, en lugar de utilizar las funciones de borrado estándar, según corresponda.

9.2.8. Restricciones en la instalación de software

La instalación de software por parte de los usuarios está totalmente prohibida. La instalación no controlada de software en equipos de cómputo puede dar pie a la introducción de vulnerabilidades y a la fuga de información, a la falta de integridad u otros incidentes de seguridad de información o bien a la transgresión de derechos de propiedad intelectual.

Está prohibido realizar las siguientes acciones por parte de los funcionarios y/ contratistas de la CVP:

- Proveer copias de software licenciado a contratistas, empleados temporales, amigos, parientes o cualquier otra tercera persona.
- Instalar software en cualquier computador o servidor de la Entidad.
- Descargar ssoftware de Internet u otro servicio en línea a cualquier computador o servidor de la Entidad.
- Modificar, revisar, transformar o adaptar cualquier software.
- Descompilar o reversar la ingeniería en cualquier software.
- Para el uso de sniffer debe existir una autorización por parte de la Oficina TIC, dependencia responsable de verificar la necesidad de la instalación de dicho software.

De conformidad con lo anterior, única y exclusivamente el personal de la Oficina TIC está autorizado a realizar la instalación de software licenciado y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado y justificado por la Oficina TIC, previa solicitud expresa del director o jefe de dependencia.

La Oficina TIC podrá en cualquier momento realizar una inspección del software instalado en los equipos de cómputo.

Los Usuarios deberán informar a través del correo de soporte@cajaviviendapopular.gov.co de cualquier conocimiento que tengan de violación al uso adecuado y legal del software o de los derechos respectivos del autor.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Los sistemas de información están comunicados entre sí con otros sistemas internos, así como con terceros fuera de la Entidad. Por lo tanto, es necesario establecer criterios de seguridad en las comunicaciones que se constituyan.

Las comunicaciones establecidas permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

10.1. Responsabilidades y procedimientos de operación

Con el propósito de asegurar la operación correcta y segura de los medios de procesamiento de la información, se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los elementos tecnológicos y de procesamiento de información. Esto incluye el desarrollo de los procedimientos de operación apropiados.

10.1.1. Documentación de los procedimientos de operación

Se documentarán y mantendrán actualizados los procedimientos necesarios para implementar esta Política. Dichos procedimientos y sus actualizaciones serán revisados al menos anualmente por el responsable del proceso.

10.1.2. Gestión de cambios

Existen procedimientos para el control de los cambios en el ambiente productivo. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El responsable del desarrollo e implementación de los Sistemas de Información controlará que los cambios en los ambientes productivos no afecten la seguridad de estos ni de la información que soportan.

10.1.3. Segregación de tareas

Se separará en caso de corresponder la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o el mal uso de la información y/o los servicios, por falta de independencia en la ejecución de funciones críticas.

Si este método de control no se pudiera cumplir en algún caso, la Oficina TIC deberá implementar otros controles como:

- ✓ Monitoreo de las actividades.
- ✓ Registros de auditora y control periódico de las actividades.
- ✓ También se podrá solicitar supervisión por parte de una unidad de auditora interna y/o externa.

Se debe asegurar la independencia de las funciones de auditoría de seguridad, tomando precauciones para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización.

10.1.4. Separación de los recursos de desarrollo, prueba y operación

Para el desarrollo de sistemas de información, se contará con ambientes separados de desarrollo, pruebas y producción, estableciendo procedimientos que aseguren la calidad de los desarrollos que se implementen, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Para ello, se tendrá en cuenta los siguientes lineamientos:

- ✓ Separar las actividades de desarrollo y prueba en entornos diferentes.

- ✓ Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción cuando no sean indispensables para su funcionamiento.
- ✓ Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.
- ✓ Prohibir a los usuarios compartir contraseñas en estos sistemas.
- ✓ Las interfaces de los sistemas identificaran claramente a que instancia se está realizando la conexión.
- ✓ se establecerá un procedimiento para la autorización, documentación y registro de acceso del personal de desarrollo a los ambientes de producción.

10.1.5. Gestión de capacidades

La Oficina TIC, con el insumo que entreguen los dueños de los diferentes Sistemas de Información, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados.

Para ello tomará en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información para el periodo estipulado de vida útil de cada componente.

10.2. Protección contra el código malicioso y descargable

Se deben tomar las precauciones necesarias para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados.

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos, tales como virus Troyanos, bombas lógicas, etc.

La Oficina TIC definirá e implementará controles de detección y prevención para la protección contra software malicioso. Así mismo, se desarrollarán procedimientos adecuados de sensibilización de usuarios en materia de seguridad y se definirán las pautas y los criterios para el control de acceso a los sistemas de información.

Estos controles deberán tener en cuenta lo siguiente:

- ✓ Prohibir el uso de software no autorizado por la entidad.
- ✓ Construir procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde redes externas o a través de ellas, o por cualquier otro medio, señalando las medidas de protección a tomar.

- ✓ Instalar y actualizar periódicamente software de detección y reparación de virus, examinando computadoras y medios informáticos, como medida preventiva.
- ✓ Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente, si es que constituyen cambios críticos a los sistemas).
- ✓ Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la entidad, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- ✓ Verificar, antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto o en archivos recibidos a través de redes no confiables o unidades extraíbles.
- ✓ Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
- ✓ Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a ellos.
- ✓ Capacitar a los usuarios para que puedan identificar posibles eventos de riesgo que puedan afectar la información.

10.3. Copias de seguridad

Con el propósito de mantener la integridad y disponibilidad de la información y los medios tecnológicos para el procesamiento de información, se deben establecer los procedimientos para implementar la política de respaldo acordada y la estrategia para tomar copias de respaldo de los datos y practicar su restauración oportuna.

10.3.1. Copias de seguridad de la información

La Oficina TIC determinará sobre la base de la criticidad de la información de que se trate, un esquema de resguardo. Así mismo, dispondrá y controlará la realización de dichas copias, y las pruebas periódicas de su restauración.

Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de la entidad. Los sistemas de resguardo deberán probarse periódicamente, asegurándose de que cumplen con los requerimientos de los planes de continuidad de la entidad.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

- ✓ Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- ✓ Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo con lo indicado por el proveedor, y asegurar la destrucción de los medios desechados.
- ✓ Almacenar en una ubicación remota copias recientes de información de resguardo, junto con sus registros exactos y completos, y los procedimientos documentados de restauración, a una distancia suficiente que permita evitar daños provenientes de un desastre en el sitio principal.
- ✓ Se deberá retener la información y el software esenciales para la Entidad, de acuerdo con la periodicidad que determine la normatividad aplicable.
- ✓ Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad, y los requisitos legales a los que se encuentre sujeta.
- ✓ Asignar a la información de resguardo un nivel de protección física y ambiental, según las normas aplicables.
- ✓ Probar periódicamente los medios de resguardo.
- ✓ Verificar y probar periódicamente los procedimientos de restauración, garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

10.4. Gestión de la seguridad de las redes

Con el fin de asegurar la protección de la información en redes y la protección de la infraestructura de soporte, la gestión segura de las redes debe considerar el flujo de datos, implicaciones legales, monitoreo y protección. Así mismo, se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

Para esto, la Oficina TIC definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Caja de la Vivienda Popular, así como el acceso no autorizado, teniendo en cuenta las siguientes acciones:

- ✓ Procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias.
- ✓ Definición de controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
- ✓ Implementar controles especiales para mantener la disponibilidad de los servicios de red y equipos de cómputo conectados.

- ✓ Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura tecnológica de la entidad.

10.5. Intercambio de información

Con el propósito de mantener la seguridad en el intercambio de información dentro de la Entidad y con cualquier otra entidad externa, se propenderá a proteger la información y los medios físicos que contiene la información en tránsito.

10.5.1. Políticas y procedimientos de intercambio de información

Se establecerán procedimientos y controles formales para proteger el intercambio de información a través del uso de elementos de comunicación, considerando lo siguiente:

- ✓ Protección de la información intercambiada de la intercepción, copiado, modificación, dirección equivocada y destrucción.
- ✓ Detección y protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas.
- ✓ Definición del uso aceptable de los elementos de comunicación electrónicas.
- ✓ Uso seguro de comunicaciones inalámbricas.
- ✓ Responsabilidades de funcionarios, contratistas y cualquier otro usuario de no comprometer a la entidad, por ejemplo, a través de la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación, compras no autorizadas y cualquier otro medio (ej.: redes sociales).
- ✓ Uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información.
- ✓ Sensibilización a personal sobre las precauciones que deben tomar a la hora de transmitir información de la Entidad.

10.5.2. Acuerdos de intercambio

Cuando se realicen acuerdos entre entidades para el intercambio de información digital y software, se especificará el grado de sensibilidad de la información de la entidad involucrada y las consideraciones de seguridad sobre la misma.

Se deberán tener en cuenta los siguientes aspectos:

- ✓ Responsabilidades sobre el control y la notificación de transmisiones, envíos y recepciones.
- ✓ Procedimientos de notificación de emisión, transmisión, envío y recepción.

- ✓ Normas técnicas para el empaquetado y la transmisión.
- ✓ Responsabilidades y obligaciones en caso de pérdida, exposición o divulgación no autorizada de datos.
- ✓ Uso de un sistema para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.
- ✓ Términos y condiciones de la licencia bajo la cual se suministra el software.
- ✓ Información sobre la propiedad de la información suministrada y las condiciones de su uso.
- ✓ Normas técnicas para la grabación y lectura de la información y del software.
- ✓ Controles especiales que puedan requerirse para proteger ítems sensibles (claves criptográficas, etc).

10.5.3. Mensajería electrónica

La mensajera electrónica como el correo electrónico, el intercambio de datos electrónicos (EDI por sus siglas en ingles), la mensajería instantánea y las redes sociales juegan un papel muy importante en las comunicaciones de la Entidad. La mensajera electrónica tiene diferentes riesgos que las comunicaciones basadas en papel.

Se considerarán las siguientes medidas de seguridad en los mensajes electrónicos:

- ✓ Protección de mensajes por el acceso no autorizado, modificaciones o denegación de servicio.
- ✓ Correcta asignación de la dirección y el transporte del mensaje.
- ✓ Confiabilidad y disponibilidad general del servicio.
- ✓ Consideraciones legales, por ejemplo, requerimientos para firmas electrónicas.
- ✓ Obtención de aprobación previa al uso de los servicios públicos externos tales como mensajera instantánea o el compartir archivos.
- ✓ Niveles altos de controles de autenticación para los accesos desde las redes públicamente accesibles.

10.6. Supervisión

Para detectar las actividades de procesamiento de información no autorizadas, se deben monitorear los sistemas y se deben reportar los eventos de seguridad de la información utilizando bitácoras de operador y registrando las fallas para asegurar que se identifiquen los problemas en los sistemas de información.

Así mismo, se debe utilizar el monitoreo del sistema para verificar la efectividad de los controles adoptados y la conformidad con un modelo de política de acceso.

10.6.1. Registros de auditoría

Se deberán producir y mantener los registros de auditora en los cuales se detallen las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un periodo acordado para permitir la detección e investigación de incidentes.
Se debe tener en cuenta como mínimo la siguiente información:

- ✓ Identificación de los usuarios;
- ✓ Fechas, tiempos, y detalles de los eventos principales, por ejemplo, inicio y cierre de sesión.
- ✓ Identidad del equipo o la ubicación si es posible.
- ✓ Registros de intentos de acceso al sistema exitosos y fallidos.
- ✓ Cambios a la configuración del sistema.
- ✓ Archivos accedidos y el tipo de acceso.
- ✓ Direcciones de redes y protocolos.

10.6.2. Protección de la información de los registros

Se deberán implementar controles para la protección de los registros de auditoria contra cambios no autorizados y problemas operacionales, incluyendo alteraciones de los tipos de mensajes, eliminación de archivos de registro, fallas para registrar o sobrescribir eventos registrados en el pasado, etc.

10.6.3. Registros de administración y operación

Se deberán registrar y revisar periódicamente las actividades de los administradores y operadores de sistema incluyendo:

- ✓ Cuentas de administración u operación involucrada.
- ✓ Momento en el cual ocurre un evento (éxito o falla).
- ✓ Información acerca del evento o las fallas.
- ✓ Procesos involucrados.

10.6.4. Sincronización del reloj

Con el propósito de garantizar la exactitud de los registros de auditora, al menos los equipos que realicen estos registros, se debe tener una correcta configuración de sus relojes.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier; variación significativa.

11. CONTROL DE ACCESO

El control de accesos mediante sistemas de restricciones y excepciones a la información es la base de todo sistema de seguridad. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y contralados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la restricción final de derechos de los usuarios que ya no requieren el acceso.

11.1. Requisitos para el control de acceso

Se debe controlar el acceso a la información, equipos tecnológicos para el procesamiento de la información y procesos sobre la base de los requerimientos de la entidad y de seguridad. Las reglas de control del acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información.

11.1.1. Política de control de acceso

En la aplicación de gestión de accesos, se tendrán en cuenta los siguientes aspectos:

- ✓ Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- ✓ Identificar toda la información relacionada con las aplicaciones.
- ✓ Establecer criterios coherentes entre la Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes
- ✓ Identificar la normatividad aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.

- ✓ Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo y/o de acuerdo con sus obligaciones contractuales.

11.2. Gestión de acceso de usuario

Con el fin de evitar el acceso no autorizado a la información de la entidad, se implementarán procedimientos para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Los procedimientos deben abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la baja final de los usuarios que ya no requieren acceso a los sistemas y servicios de información.

11.2.1. Registro de usuario

Se cuenta con un procedimiento de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual incluye:

- ✓ Uso de identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo usuario. El uso de identificadores grupales solo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- ✓ Verificación de la autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- ✓ Verificación del nivel de acceso otorgado coherente con la Política de Seguridad de la Información de la entidad
- ✓ Mantenimiento de un registro formal de todas las personas registradas para utilizar el servicio.
- ✓ Cancelación inmediatamente de los derechos de acceso para los usuarios que cambiaron sus tareas o de aquellos a los que se les revocó la autorización, se desvincularon de la entidad o sufrieron la pérdida de sus credenciales de acceso.

Adicionalmente se deben contemplar revisiones periódicas que permitan:

- ✓ Cancelar identificadores y cuentas de usuario redundantes;
- ✓ Inhabilitar cuentas inactivas por más de 60 días, o el periodo que se estipule.
- ✓ Eliminar cuentas inactivas por más de 180 días, o el periodo que se estipule.

- ✓ En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas. Las excepciones deberán ser solicitadas por director o jefe de área correspondiente.
- ✓ Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
- ✓ Incluir cláusulas de confidencialidad en los contratos de personal y de servicios.

11.2.2. Gestión de privilegios

Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas, como la instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, entre otros. Dichas cuentas no serán de uso diario, sino que solo serán utilizadas ante la necesidad expedida de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

- ✓ La Oficina TIC definirá procedimientos para la administración de dichas contraseñas críticas, que contemplen lo siguiente:
- ✓ Causas que justifiquen el uso de contraseñas críticas, así como el nivel de autorización requerido.
- ✓ Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
- ✓ La utilización de las contraseñas criticas deberá ser registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con ellas.
- ✓ Cada contraseña critica se renovará una vez utilizada, y se definirá un periodo luego del cual esta será renovada, en caso de que no se haya utilizado.
- ✓ Se deberán registrar todas las actividades que se efectúen con las cuentas críticas para luego ser auditadas.

11.2.3. Gestión de contraseñas de usuario

Para una correcta gestión de contraseñas, se deben contemplar los siguientes pasos:

- ✓ Sensibilizar a los usuarios para que se comprometan a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo.
- ✓ Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema.

- ✓ Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña.
- ✓ Almacenar las contraseñas solo en sistemas informáticos protegidos.
- ✓ Configurar los sistemas de tal manera que las contraseñas cumplan con parámetros seguros de configuración tales como:
  - Contener 8 caracteres alfanuméricos, como mínimo.
  - Suspender o bloquear permanentemente al usuario luego de 3 intentos para acceder al sistema con una contraseña incorrecta (deberá pedir solicitar la reactivación a la Oficina TIC mediante correo a soporte@cajaviviendapopular.gov.co)
  - Solicitar el cambio de la contraseña cada 90 días.
  - Impedir que sean reutilizadas las ultimas 6 contraseñas.

11.2.4. Revisión de los derechos de acceso de usuario

Se debe identificar y autenticar a cualquier usuario que, de manera local o remota, requiera utilizar los recursos tecnológicos de la Caja de la Vivienda Popular, para lo cual se requiere contar con sistemas de seguridad que cumplan al menos con las siguientes características:

- ✓ Cada usuario que requiera acceder a la plataforma tiene que identificarse y autenticarse antes de acceder a un recurso tecnológico a través de un usuario y una contraseña, y el usuario debe estar activo.
- ✓ Una vez se han identificado y autenticado, los usuarios sólo podrán acceder a los recursos sobre los cuales están autorizados.
- ✓ Debe quedar registro de los eventos de ingreso y autenticación de usuarios, para monitoreo de la Oficina TIC.

11.3. Responsabilidades de usuario

El usuario deberá realizar todas las medidas a su alcance para evitar el acceso de usuarios no autorizados, evitar poner en peligro la información y evitar el robo de información y de elementos tecnológicos de la Caja de la Vivienda Popular.

El compromiso de los usuarios autorizados es fundamental para una seguridad efectiva. Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario. Además, se debe implementar una política de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles, medios y equipos tecnológicos de la entidad.

11.3.1. Uso de contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, que constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios tecnológicos y de manejo de información de la entidad. Para esto se deben tener en cuenta los siguientes lineamientos:

- ✓ Mantener las contraseñas en secreto.
- ✓ Pedir el cambio de las contraseñas siempre que exista un posible indicio de amenaza que comprometa el sistema o la información.
- ✓ Seleccionar contraseñas de calidad, de acuerdo a los parámetros de seguridad y fortaleza establecidos en la presente Política, y que, además:
  - Sean fáciles de recordar.
  - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, como, por ejemplo, nombres, números de teléfono, fechas de nacimiento, etc.
  - No tengan caracteres idénticos consecutivos o grupos totalmente numeritos o totalmente alfabéticos.
- ✓ Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar
- ✓ o reciclar viejas contraseñas
- ✓ cambiar las contraseñas provisionales asignadas en el primer inicio de sesión ("log on").
- ✓ Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- ✓ Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de perdida de confidencialidad.
- ✓ Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se podrá utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

11.3.2. Equipo de usuario desatendido

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

La Oficina TIC debe coordinar las tareas de sensibilización a todos los usuarios charlas de capacitación, acerca de los requerimientos y procedimientos de seguridad, para la

protección de equipos desatendidos, así como de sus funciones en relación con la implementación de dicha protección.

11.3.3. Política de puesto de trabajo despejado y pantalla limpia

La entidad debe adoptar una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles, y una política de pantallas limpias, en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información, tanto durante el horario normal de trabajo como fuera de este.

Se deberán tener en cuenta las siguientes recomendaciones:

- ✓ Almacenar con el debido resguardo y cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes u otro tipo de mobiliario seguro, cuando no están siendo utilizados, especialmente fuera del horario de trabajo y teniendo en cuenta lo establecido en el procedimiento correspondiente a la gestión documental.
- ✓ Guardar bajo llave la información crítica de la entidad (preferiblemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina, y siguiendo los lineamientos establecidos en el procedimiento correspondiente a la gestión documental.
- ✓ Proteger los puntos de recepción y envío de correo postal, y las máquinas de fax no atendidas.
- ✓ Retirar inmediatamente la información confidencial una vez impresa o fotocopiada.

11.4. Control de acceso a la red

Las conexiones no seguras a los servicios de red pueden afectar a toda la entidad, por lo tanto, se debe controlar el acceso a los servicios de red tanto internos como externos, con el propósito de garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan su seguridad.

11.4.1. Política de uso de los servicios en red

La Oficina TIC tiene a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo con la solicitud formal del Director o Jefe de la dependencia que lo solicite para el personal.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad de la entidad.

Para ello, se cuenta con procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenden:

- ✓ Identificar las redes y los servicios de red a los cuales se permite el acceso.
- ✓ Definir lineamientos de autorización para determinar las personas, las redes y los servicios de red a los cuales se les otorgara el acceso.
- ✓ Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y los servicios de red.

11.5. Control de acceso al sistema operativo

La Oficina TIC deberá realizar una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo de los diferentes equipos de cómputo y servidores de la Caja de la Vivienda Popular.

11.5.1. Procedimientos seguros de inicio de sesión

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se deberá determinar un procedimiento que indique:

- ✓ El método de identificación automática de terminales utilizado.
- ✓ El detalle de transacciones permitidas por cada terminal.
- ✓ El acceso a los servicios de información solo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema debe ser diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado. Adicionalmente, el procedimiento de identificación deberá tener en cuenta los siguientes aspectos:

- ✓ Mantener en secreto los identificadores de sistemas o aplicaciones, hasta tanto se haya llevado a cabo exitosamente el proceso de conexión.
- ✓ Desplegar un aviso general advirtiendo que solo los usuarios autorizados pueden acceder al equipo de cómputo.

- ✓ Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
- ✓ Validar la información de la conexión solo al completarse la totalidad de los datos de entrada.
- ✓ Limitar el número de intentos de conexión no exitosos permitidos y registrar los intentos no exitosos.
- ✓ Impedir otros intentos de identificación, una vez superado el límite permitido.
- ✓ Desconectar conexiones de comunicaciones de datos.
- ✓ Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.
- ✓ El registro de conexiones deberá tener fecha y hora de la conexión, así como los detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

En caso de corresponder, la Oficina TIC junto con los Propietarios de la Información deberán definir cuales se consideran terminales de alto riesgo, por ejemplo, áreas públicas o externas fuera del alcance de la gestión de seguridad de la entidad, o que sirven a sistemas de alto riesgo.
Estas se apagarán después de un periodo definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para los equipos de cómputo, se debe implementar la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un usuario debe abandonar su puesto de trabajo momentáneamente, activara protectores de pantalla con contraseñas, con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

11.5.2. Sistema de gestión de contraseña

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad. El sistema de administración de contraseñas deberá:

- ✓ Exigir el uso de contraseñas individuales para determinar responsabilidades.

- ✓ Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de estas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- ✓ Imponer una selección de contraseñas de calidad, según lo establecido en la presente política.
- ✓ Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo establecido en la presente política.
- ✓ Mantener un registro de las ultimas contraseñas utilizadas por el usuario y evitar su reutilización.
- ✓ Evitar mostrar las contraseñas en pantalla cuando son ingresadas.
- ✓ Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- ✓ Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
- ✓ Modificar todas las contraseñas predeterminadas por el vendedor una vez instalado el software y el hardware (por ejemplo, claves de impresoras, hubs, routers, switches, etc.).
- ✓ Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal de forma no protegida.

11.6. Equipos tecnológicos portátiles y teletrabajo

Se deben establecer las directrices que permitan garantizar la seguridad de la información cuando se utilizan equipos tecnológicos móviles y para teletrabajo.

11.6.1. Dispositivos portátiles y comunicaciones móviles

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura de la Entidad. Para ello se debe tener en cuenta cualquier dispositivo móvil y/o removible incluyendo:

- ✓ Notebooks, Laptop o PDA (Asistente Personal Digital)
- ✓ Teléfonos Celulares y sus tarjetas de memoria
- ✓ Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, memorias, Discos Duros y cualquier dispositivo de almacenamiento de conexión USB
- ✓ Tarjetas de identificación personal (control de acceso)
- ✓ Dispositivos criptográficos, cámaras digitales, etc.

Esta lista no es taxativa ya que deben incluirse todos los dispositivos que pudieran contener información confidencial de la entidad y por lo tanto tengan la posibilidad de sufrir un incidente en el que se comprometa la seguridad del mismo.

La utilización, de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de perdida, roba o hurto. En consecuencia, debe entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles.

Por otra parte, se deben definir procedimientos que permitan al poseedor del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos la información y los sistemas de información de la entidad, los que deberán incluir:

- ✓ Revocación de las credenciales afectadas
- ✓ Notificación a grupos de trabajo donde potencialmente se pudieran haber comprometido recursos.

11.6.2. Teletrabajo

El teletrabajo utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo a las instalaciones de la entidad y sus diferentes sedes.

El trabajo remoto sólo podrá ser autorizado y definido por el Director o Jefe de Dependencia a la cual pertenezca el usuario solicitante, previa aprobación de la Subdirección Administrativa, y apoyado por la Oficina TIC, quien determinará las medidas que correspondan en materia de seguridad de la información, con el fin de garantizar el cumplimiento de esta Política, los lineamientos, normas y procedimientos existentes.

12. LINEAMIENTOS GENERALES PARA TODA LA ENTIDAD

- ✓ Toda adquisición de equipos de tecnología informática y de sistemas de información que se haga en la Caja de la Vivienda Popular debe contar con el concepto técnico de la Oficina TIC.
- ✓ La selección de hardware requerido debe ir de acuerdo con el plan estratégico de la Oficina TIC y sustentado por un estudio elaborado por la dependencia solicitante, en el cual se enfaticen las características técnicas y funcionales requeridas.
- ✓ La Oficina TIC debe realizarse un estudio y/o diagnóstico que determinen las necesidades y/o requerimientos de software y/o hardware, tomando como insumo la información entregada por las diferentes dependencias de la entidad

- ✓ Todos los desarrollos de software y las nuevas aplicaciones que se implementen en la entidad deben realizarse a través de la Oficina TIC.
- ✓ La plataforma tecnológica, las bases de datos y aplicaciones institucionales están bajo la responsabilidad de la Oficina TIC. Por lo tanto, las demás dependencias deben atender las políticas institucionales definidas para el uso, desarrollo y seguridad de las mismas.
- ✓ La Oficina TIC no realiza revisiones, manipulaciones, mantenimientos preventivos y/o correctivos, ni ningún tipo de intervenciones técnicas a equipos tecnológicos que no sean de propiedad de la entidad.
- ✓ Es responsabilidad de cada funcionario y contratista realizar un buen uso de los equipos, dispositivos y herramientas tecnológicas entregadas por la Caja de la Vivienda Popular para el desarrollo de sus funciones. Cualquier alteración, daño o inconsistencia presentada tanto en el hardware como en el software debe ser reportada a la Oficina TIC a través de correo a soporte@cajaviviendapopular.gov.co. Por lo anterior, 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.

13. MONITOREO Y SEGUIMIENTO

La Oficina TIC debe realizar el seguimiento y control a la implementación y/o mantenimiento de la Política de Seguridad de la Información.

14. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad (Statement of Applicability - SOA) referenciado en el numeral 6.1.3d de la norma ISO-27001, es un documento que lista los objetivos y controles que se van a implementar en la Entidad, así como las justificaciones de aquellos controles que no van a ser implementados.

Para el caso específico de la CVP, este tipo de análisis se hace evaluando el cumplimiento de la norma ISO-7002, para cada uno de los controles establecidos en los 14 dominios o temas relacionados con la gestión de la seguridad de la información que este estándar especifica; y una vez se complete este análisis se realizará la declaración de aplicabilidad de estos.

15. ACUERDO DE CONFIDENCIALIDAD

Todos los funcionarios, contratistas y terceros deben firmar la cláusula y/o acuerdo de confidencialidad que deberá ser parte integral de los contratos laborales y de prestación de servicios, 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 cuando se permita el acceso a información y/o a los recursos a personas o entidades externas.

16. CONTROL DE CAMBIOS

Versión	Fecha Aprobación (dd-mm-aaaa)		Revisó (Nombre y Apellido del líder del proceso)
1	25/09/2016	Elaboración primera versión Camilo Augusto Ramos Beltrán - Profesional Universitario Dirección Gestión Corporativa y CID - Sistemas	Aprobó Sandra Lorena Guacaneme Urueña – Directora DGC Richard Eduardo López - Jefe Oficina Asesora de Planeación Revisó Silenia Neira Torres – Contratista Revisó Claudia Marcela García – Profesional Oficina Asesora de Planeación
2	21/08/2019	Se inicia con el desarrollo de la actualización del documento de la política de seguridad informática. Oscar Javier Orduz Contratista – Oficina TIC Se cambió el nombre del documento (política de seguridad informática por política de seguridad de la información), se complementó y crearon directrices de los dominios de acuerdo a la NTC/ISO:27002, se ajustaron y crearon definiciones en el	Aprobó Andrés Orlando Briceño Díaz Jefe Oficina TIC

		documento y se diseñó el marco normativo. Maryury Forero Bohorquez Contratista – Oficina TIC	
		Se realizaron ajustes de forma de acuerdo al sistema de calidad, solicitados por la Oficina de Planeación. Maryury Forero Bohorquez Contratista – Oficina TIC	
		Se realizan ajustes al documento, se incluyeron controles específicos para prohibir la instalación de software no licenciado en los equipos de cómputo de la entidad, de acuerdo a observaciones realizadas por la Oficina Asesora de Control Interno. Maryury Forero Bohorquez Contratista – Oficina TIC	
		Se realizan ajustes de forma y fondo en el contenido del documento, de acuerdo a observaciones realizadas por la Oficina Asesora de Control Interno. Maryury Forero Bohorquez Contratista – Oficina TIC	

Elaboró	Revisó	Aprobó
Maryury Forero Bohorquez Contratista profesional-Oficina TIC	Ivonne Andrea Torres Cruz Jefe-Oficina Asesora de Control Interno.	Andrés Orlando Briceño Díaz Profesional Especializado Jefe Oficina TIC
Fecha: 16/08/2019	Fecha: 16/08/2019	Fecha: 21/08/2019