MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

OFICINA TIC

NOVIEMBRE - 2023

CAJA DE LA VIVIENDA POPULAR

BOGOTÁ

TABLA DE CONTENIDO

INTRODUCCIÓN

Con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información, la Caja de la Vivienda Popular - CVP ha generado e implementado las políticas de seguridad de la información las cuales se encuentras dispuestas en el documento: 208-TIC-Mn-07: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN CAJA DE LA VIVIENDA POPULAR, que se encuentra publicado en la página web de la Entidad. Este documento enmarca de una forma general los lineamientos y políticas en los que se basa el sistema de gestión de seguridad de la CVP cumpliendo con la normativa vigente, la política de gobierno digital y el modelo de seguridad y privacidad de la información – MSPI.

El presente documento buscar definir de una forma más específica estos lineamientos y actividades que llevan al cumplimiento de las políticas.

1. OBJETIVO

Establecer lineamientos y actividades complementarias a las políticas establecidas para la adecuada gestión de la seguridad y privacidad de la información en la Caja de la Vivienda Popular - CVP.

2. ALCANCE

El Manual de Políticas de Seguridad de la Información en conformidad a la política de seguridad de la información de la Entidad, aplica a los activos de información de 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.

3. RESPONSABLES

ALTA DIRECCIÓN

- Brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar la información.

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

- Aprobar y realizar el seguimiento a la estrategia de la implementación de las políticas de seguridad de la información.

- Verificar el cumplimiento de las políticas y lineamientos de seguridad de la información mencionados en el presente manual.

OFICINA TIC

- Elaborar, actualizar y hacer seguimiento al Manual de Políticas de Seguridad de la Información, asegurando así los recursos adecuados y promover una cultura activa de seguridad en la Entidad.

- Realizar la divulgación de las políticas de seguridad de la información en toda la entidad.

- 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 (cuartos de comunicación y centro de cómputo), lógicas y procedimentales para la protección de la información digital de la Entidad.

- Aplicar y hacer cumplir el Manual de Políticas de Seguridad de la Información y sus lineamientos.

- 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 del presente Manual de Políticas.

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 con 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 con 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

- Cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

- Reportar a la Oficina TIC las inconsistencias, anomalías y nuevos requerimientos.

- 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 se accede, 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 cumplir con los lineamientos descritos en el presente Manual de Políticas.

- 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.

4. DEFINICIONES Y SIGLAS

- **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), 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.

- **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.

- **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 la información de ser accesible y utilizable a demanda por una persona o entidad autorizada.

- **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 se tomen todas las medidas necesarias que posibilite prevenir una catástrofe cibernética, como el robo de información.

- **Hardware:** Conjunto de los componentes que integran la parte material de un equipo de cómputo o equipo informático.

- **Integridad:** Propiedad de salvaguardar la exactitud y completitud 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.

- **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 la ley 1712 de 2014.

- **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 la ley 1712 de 2014.

- **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.

- **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 usuarios7.

- **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.

- **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.

- **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 o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

- **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 con 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, 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 entre otros 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.

- **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.

- **Shareware:** Clase de software o programa, cuyo propósito es evaluar por un determinado lapso, 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.

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

- **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 autor13.

- **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.

- **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 servicios15.

- **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.

- **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.

- **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) Discos duros, servidores, discos o medios portables, cintas o medios de video yaudio (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 estos 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 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.

5. MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1 LINEAMIENTOS Y ACTIVIDADES PARA LA GESTIÓN DE ACTIVOS

- La oficina TIC es la responsable de coordinar la actualización del inventario de los activos de información para su control y administración, de acuerdo con el formato 208-TIC-Ft-21 INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION. 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 oficina TIC remitirá un comunicado a los directores de las áreas de la Entidad para que deleguen la tarea de levantar los activos, una vez se deleguen las personas, los colaboradores de la oficina TIC realizan una socialización donde se les explica cómo llenar la matriz de activos de información. Posteriormente las personas delegadas de cada área verifican, actualizan y clasifican la información de los activos de información correspondientes a su área. Las matrices diligenciadas y con la respectiva aprobación del jefe de área, deben ser reportadas a la oficina TIC.

- La oficina TIC recopilará la información y generará la matriz inventario de activos de información de la Entidad y el índice de información clasificada y reservada. Estas dos matrices deben ser remitidas a la Oficina Asesora de Comunicaciones para su publicación en la página web de la Entidad y a su vez, la Oficina TIC debe hacer la publicación en datos abiertos Bogotá.

- La información registrada en el formato es responsabilidad de cada propietario de información quienes verificarán su clasificación y valoración.

- 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 con sus roles y funciones.

- Los usuarios no deben mantener almacenados en los discos duros de las estaciones de trabajo o discos virtuales de red, archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter institucional o que no correspondan a las funciones laborales o contractuales asignadas.

- 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.

5.1.1 Lineamientos y Actividades para Equipos Servidores

- La oficina TIC deberá realizar copias de seguridad y ejecutar las pruebas de restauración respectivas, las cuales deben realizarse de manera periódica, con pruebas aleatorias de restauración sobre las copias de respaldo realizadas. Estas pruebas deben coordinarse en ambientes de pruebas controlados; no sobrescribiendo el medio original.

- En el caso de que los servidores estén en custodia de un tercero, la oficina TIC debe coordinar con el tercero para que éste como responsable de la infraestructura, realice las copias de seguridad y sus correspondientes pruebas de restauración tanto para las bases de datos como servidores que allí reposen.

5.1.2 Lineamientos y Actividades para Equipos de Cómputo de Usuarios

- Los usuarios son responsables por el equipo que la CVP les asigna y deben velar por el buen uso del dispositivo, 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.

- La oficina TIC entrega los equipos al usuario con el software autorizado en la Entidad, en caso de que el usuario necesite la instalación de software adicional, debe remitir por GLPI la solicitud que debe venir avalada por el jefe del área a Tecnología, donde se verificará la viabilidad de la instalación como tipo de licenciamiento, enlaces de descarga, requisitos de instalación y seguridad.

- Los usuarios deben reportar a la oficina TIC cualquier anomalía, fallo, desgaste o incidente del equipo para que se tomen las medidas correctivas pertinentes.

5.1.3 Lineamientos y Actividades para equipos Impresoras, scanner y plotter

- No se permite el uso de impresoras, scanner y plotter para uso personal.

- Los usuarios son responsables de recoger los documentos que se envían a imprimir con el fin de mantener su confidencialidad.

- La oficina TIC es la única área autorizada para la realización de mantenimientos, en caso de que un usuario encuentre fallos en estos dispositivos, debe reportar a la oficina TIC.

5.1.4 Lineamientos y Actividades para Bases de Datos

- La oficina TIC debe controlar el acceso de administradores de bases de datos y activar el log de auditoría.

- Los usuarios que utilizan aplicativos o sistemas de información institucionales como medio de registro de las actividades que tienen a su cargo, son responsables por la información que ingresan y su calidad, así como el debido uso de esa información conforme a la protección de datos personales y la información de la Entidad.

5.1.5 Lineamientos y Actividades para la Información Digital

- Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los computadores de usuario. Por lo tanto, es obligación de los usuarios almacenar la información institucional en la unidad compartida asociada a la cuenta de usuario del dominio de la Entidad. La Oficina TIC no garantiza la copia de información que se encuentre en los computadores en carpetas diferentes a la unidad compartida.

- No se permite almacenar información personal u otro tipo de información que no se encuentre relacionada con la Misión y Objetivos Estratégicos de la Entidad y la cual no hace parte del desarrollo de las funciones y/o

responsabilidades asignadas a cada colaborador en las unidades compartidas en la Entidad.

- La solicitud de carpetas compartidas debe de realizarse por GLPI a la oficina TIC, indicando los colaboradores que tendrán acceso y su respectivo permiso sobre ellas.

- Los directores o jefes de área son responsables de la información de cada dependencia y de los permisos asignados a las carpetas compartidas. Es deber informar a la oficina TIC sobre el cambio de rol o permiso que tengan los usuarios.

- En caso de un incidente de seguridad (daño, borrado, alteración) sobre la información dispuesta en las carpetas compartidas, debe ser informada a la Oficina TIC para su respectiva gestión.

- En caso de que se requiera, las solicitudes de restauración de backup de información deben realizarse a la Oficina TIC a través de la herramienta GLPI.

5.1.6 Lineamientos y Actividades para Red Wifi y Acceso a Internet

- Está prohibido la conexión a la red cableada de la Entidad o la red inalámbrica institucional de equipos personales o ajenos a la CVP, en caso de ser necesario el acceso a internet para este tipo de equipos la oficina TIC dispuso una red WiFi de uso de visitantes y ciudadanos.

- Solo se configurarán en la red computadores personales u otros dispositivos con la autorización de la Oficina TIC y previo análisis de seguridad de los equipos.

- La oficina TIC realizará monitoreo sobre los equipos conectados en la red institucional y podrá desconectar aquellos que no pertenezcan a la Entidad.

- Los usuarios son responsables por el uso que le den a las redes y navegación en la Entidad. La Oficina TIC no se hace responsable por conductas difamatorias, obscenas u ofensivas que los usuarios realicen a través de los servicios que proporciona, recayendo la responsabilidad directamente sobre el usuario.

- Es obligación del usuario informar a la Oficina TIC a través del GLPI, cualquier incidente que se presente durante el uso de los servicios de red, como la llegada de correos sospechosos, antivirus que no se actualiza, sitos de internet que se abren solos, etc.

- 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 que 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 información 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 esta, 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.

- La oficina TIC 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.

- Si un usuario requiere el acceso a un sitio web que está restringido por políticas de navegación, es necesario que remita una solicitud con la autorización del jefe del área, a la oficina TIC por medio de la herramienta GLPI, donde se evaluará y verificará la solicitud.

5.1.7 Lineamientos y Actividades de Soporte Técnico

- 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 en la jornada laboral establecida por la administración por medio del registro del caso en la plataforma de servicio (herramienta de Mesa de Ayuda) dispuesta por la Oficina TIC.

- La oficina TIC solo presta el soporte técnico a equipos institucionales.

- Los usuarios no tienen permitido la manipulación correctiva de los equipos de cómputo, escáner e impresoras. Sólo está autorizada la revisión por parte de personal de soporte técnico de la Oficina TIC.

- Cualquier movimiento de equipos o puntos de red debe ser solicitada a la oficina TIC por medio de la mesa de ayuda y debe contar con la aprobación del jefe del área y previa notificación a la subdirección Administrativa.

- 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, estos equipos no deben dejarse desatendidos y el usuario que lo solicita es el responsable del equipo. 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 incidentes y requerimientos de soporte técnico deben quedar registrados con un único número de caso que lo identifique, documentando sus avances y la solución dada, en la herramienta de Mesa de Ayuda de la Oficina TIC.

- 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.

- 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 a través de la herramienta de Mesa de Ayuda, para programar los recursos de la Oficina TIC. La atención estará enfocada a la instalación y desinstalación de los equipos en el sitio. La 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 la herramienta de Mesa de Ayuda, con mínimo 24 horas de anticipación.

- 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.

5.2 LINEAMIENTOS Y ACTIVIDADES PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Todos los colaboradores deben reportar a través de la mesa de servicios; los eventos o incidentes relacionados con la seguridad de la información o con los recursos tecnológicos con la mayor prontitud posible a través de los canales definidos.

- El reporte de incidentes de seguridad debe contener un mínimo de datos para poder dejar evidencia y soporte de las acciones realizadas, las cuales se deben registrar en el procedimiento definido y que debe estar alineado con la política de seguridad de la información.

- Los incidentes de seguridad de la información pueden ser detectados por alertas de sistemas de información o de plataformas de servicios TIC, colaboradores, proveedores o entidades externas que observen situaciones anormales o la existencia de vulnerabilidades, relacionadas con aspectos técnicos, físicos o procedimentales, que puedan afectar a la infraestructura tecnológica, información física, digital o electrónica, entre otros activos de información.

- La Oficina TIC debe asignar responsables para el tratamiento de los eventos e incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

- La Oficina TIC debe gestionar los incidentes de acuerdo con el procedimiento 208-TIC-Pr-13 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION, asegurando una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

5.3 LINEAMIENTOS Y ACTIVIDADES DE CONTROLES CRIPTOGRÁFICOS

- La Oficina TIC debe proporcionar los mecanismos de cifrado necesarios para asegurar que la transmisión de información confidencial de forma interna o externa se realice de forma segura. Los usuarios que van a transmitir información confidencial de la Entidad deben solicitar por medio de un GLPI a la oficina TIC los mecanismos adecuados de seguridad para su transmisión.

- La oficina TIC debe disponer de los mecanismos de cifrado para el aseguramiento de las conexiones de acceso remoto a la red CVP y recursos de la entidad.

- Todos los usuarios que trabajen de forma remota y que tengan necesidad de acceder a la red institucional, deben hacerlo por medio de la VPN que la oficina TIC dispone.

- La administración de llaves criptográficas y certificados digitales estará a cargo de la Oficina TIC, estableciendo mecanismos de control y gestión para la creación, activación, distribución, recuperación y revocación de las llaves criptográficas.

- Las llaves criptográficas serán deshabilitadas por la Oficina TIC, cuando estas se encuentren en riesgo de divulgación o cuando los Colaboradores de la Entidad autorizados culminen la relación laboral o contractual con la Entidad.

- Los tokens utilizados por los directivos para firmas de documentos son responsabilidad de cada usuario al que se le asigna.

5.4 LINEAMIENTOS Y ACTIVIDADES PARA EL DESARROLLO Y MANTENIMIENTO DE SOFTWARE

- Todos los desarrollos de software y las nuevas aplicaciones que se implementen en la entidad deben estar autorizados por la Oficina TIC.

- Se deben seguir los lineamientos de seguridad de la información dispuestos en el documento: 208-tic-in-02 lineamientos para la construcción de sistemas de información de la caja de la vivienda popular, en su capítulo 6: lineamientos de seguridad de la información para el desarrollo de aplicaciones.

- Para la puesta en producción de desarrollos realizados, de deben diligenciar los requisitos estipulados en el formato 208-tic-ft-15 paso a producción de software.

- Todo desarrollo que se realice debe generar los entregables establecidos en el procedimiento 208-tic-pr-11 desarrollo y mantenimiento de software.

- 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 y cumplimiento de la seguridad.

- La Oficina TIC sólo autoriza la realización de soporte técnico al software y aplicaciones definidas institucionalmente como herramientas de producción.

- 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 y deben seguir los mismos lineamientos y políticas para el desarrollo seguro de software dispuestos en el documento: 208-tic-in-02 lineamientos para la construcción de sistemas de información de la caja de la vivienda popular, en su capítulo 6: lineamientos de seguridad de la información para el desarrollo de aplicaciones.

5.5 LINEAMIENTOS Y ACTIVIDADES PARA CLASIFICACIÓN DE LA INFORMACIÓN

- 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.

- Los usuarios responsables de la información de la Caja de la Vivienda Popular deben identificar los activos de información y clasificarlos de acuerdo con los lineamientos descritos en el numeral 5.1 del presente manual.

5.6 LINEAMIENTOS Y ACTIVIDADES PARA LA GESTIÓN LIGADA A LOS RECURSOS HUMANOS

5.6.1 Antes del empleo o inicio de labores

- 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.

- Todo el personal de la Caja de la Vivienda Popular debe firmar la aceptación del Acuerdo de confidencialidad y hacer uso adecuado de los recursos informáticos y de información de la Caja de la Vivienda Popular.

5.6.2 Durante el empleo o desarrollo de labores

- 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 sensibilizaciones en seguridad de la información por medio de la oficina TIC.

- El usuario es responsable por la confidencialidad, integridad y disponibilidad de la información que se le entrega de la Entidad en calidad de su labor u obligación a realizar.

- Todo el personal debe acatar, aplicar y cumplir con las políticas de seguridad de la información de la Entidad.

5.6.3 Proceso Disciplinario

Todos los funcionarios y contratistas de la Entidad deben conocer y acatar las políticas de seguridad de la información, su incumplimiento puede generar acciones disciplinarias. Las investigaciones disciplinarias y las respectivas sanciones le corresponden a la Oficina de Control Interno y la Subdirección Administrativa.

5.7 LINEAMIENTOS Y ACTIVIDADES PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA Y DEL ENTORNO

5.7.1 Áreas de procesamiento y almacenamiento informático

- 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.

5.7.2 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.

- Todos los colaboradores deben portar el carné de identificación en un lugar visible dentro de las instalaciones de la Entidad.

- Está prohibido prestar el carné de identificación, se considera como suplantación de identidad por parte de la persona que lo usa sin ser la persona autorizada.

- El ingreso de equipos que no sean de propiedad de la Caja de la Vivienda Popular deben ser registrados de acuerdo al procedimiento que disponga la

empresa de vigilancia en concordancia con el supervisor del contrato, para tal fin la empresa de vigilancia deberá registrar como mínimo la siguiente información: fecha de ingreso, hora de entrada, hora de salida, nombre y apellido de la persona que ingresa el equipo, tipo de dispositivo, marca, serial y firma; de igual manera a la hora de salida y se debe verificar que el equipo que está saliendo sea el mismo número de serie del que entró con la persona responsable.

5.7.3 Trabajo en áreas seguras

- El área administrativa 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.

5.7.4 Política de puesto de trabajo despejado y pantalla limpia

Se establece los lineamientos de la 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 los siguientes lineamientos:

- 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.

- Los documentos que incluyan información Pública Reservada y Pública Clasificada que se envíe a las impresoras deben ser recogidos inmediatamente.

- Cada vez que un colaborador de la CVP se ausente de forma temporal o definitiva de su puesto de trabajo, debe bloquear la pantalla del computador a su cargo (ejemplo en Windows con las teclas Windows y L).

- No publicar o dejar a la vista, documentos o datos críticos como: nombres de usuario, contraseñas, direcciones IP, números de cuentas, archivos de propiedad intelectual, datos personales semiprivados, privados o sensibles y/o cualquier información pública clasificada o pública reservada.

- Los colaboradores que presten servicios de atención al público deberán ubicar el equipo de cómputo asignado para el desarrollo de las actividades, de tal forma que se evite el acceso o revisión de la información por parte de los usuarios que atienden, estos lugares deben estar protegidos por personal de seguridad y monitoreados por un circuito cerrado de televisión.

5.8 LINEAMIENTOS Y ACTIVIDADES PARA LOS EQUIPOS INFORMÁTICOS

- 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, y sin contar con el acompañamiento de personal de la Oficina TIC.

- 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.

- La Oficina de TI debe contar con un listado actualizado de los equipos tecnológicos y registro de los mantenimientos preventivos y/o correctivos realizados.

- Únicamente el personal calificado y autorizado por la Oficina TIC puede realizar actividades de mantenimiento y llevar a cabo reparaciones o modificaciones en los equipos tecnológicos.

- 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.

- Los colaboradores deberán informar a la Oficina TIC; la pérdida, robo o extravío del equipo tecnológico; de igual forma se deberá notificar cualquier comportamiento anómalo asociados con las funcionalidades de los dispositivos y/o activos de información almacenados.

- Es responsabilidad del usuario contar con las debidas aprobaciones para el retiro de los equipos de cómputo fuera de las instalaciones; también en el buen uso y adecuado transporte de los equipos en calidad de préstamo fuera de la entidad, preservando la confidencialidad e integridad de la información que se trabaje desde estos equipos.

- La Oficina TIC es la única autorizada para 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.

- Todos los usuarios deberán informar a la Oficina TIC a través de la herramienta de Mesa de Servicio, de cualquier conocimiento que tengan de violación al uso adecuado y legal del software o de los derechos respectivos del autor.
- 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.

- La Oficina TIC deberá Implementar un mecanismo de bloqueo automático cuando el equipo de cómputo esté inactivo después de tres (3) minutos.

5.9 LINEAMIENTOS Y ACTIVIDADES PARA LAGESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

5.9.1 Separación de los recursos de desarrollo, prueba y producción

- Para el desarrollo de sistemas de información, se contará con ambientes separados de desarrollo, pruebas y producción a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

- 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.

- Se prohíbe a los usuarios compartir contraseñas.

- Las interfaces de los sistemas identificaran claramente a que instancia se está realizando la conexión.

5.9.2 Gestión de cambios

- Todo cambio en ambiente productivo debe realizarse por medio del procedimiento 208-tic-pr-14 gestión de cambios de TI.

- 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.

- Informar a los propietarios de los activos de información los cambios que se realicen a los servicios, componentes, sistemas de información y/o infraestructura a su cargo.

5.9.3 Gestión de capacidad

- 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.

- La Oficina TIC debe supervisar continuamente el consumo, demanda y comportamiento de los recursos tecnológicos asignados, con el fin de realizar gestionar oportunamente los cambios y/o ajustes que se requieran y proyectar las futuras necesidades de capacidad.

- 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.

- El monitoreo de la capacidad de los servidores que se encuentran dentro de las instalaciones de la Entidad se realiza por configuraciones de políticas por directorio activo generando alertas que se remiten por correo electrónico.

- El monitoreo en servidores que se encuentran en custodia de un tercero se realiza con las herramientas de éste y será su responsabilidad proporcionar este monitoreo generando las alertas sobre la red y servidores y su capacidad para poder tomar decisiones.

5.9.4 Protección contra el código malicioso y descargable

- La Oficina TIC definirá e implementará controles de detección y prevención para la protección contra software malicioso.

- Está prohibido el uso de software no autorizado por la Oficina TIC.

- La Oficina TIC debe 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).

- Todo medio extraíble debe verificarse por antivirus antes de su uso.

5.9.5 Copias de seguridad

- Para el respaldo de la información se debe seguir el procedimiento 208-tic-pr-07 administración de copias de seguridad y restauración.

- Se deben realizar pruebas periódicas de restauración de la información para las copias de respaldo.

- En caso de ser necesario, la restauración de una copia de seguridad debe ser solicitada la Oficina TIC por medio de la mesa de ayuda.

5.9.6 Gestión de la seguridad de las redes

- Todos los usuarios que tengan acceso a la red se crean con los permisos básicos y de acceso mínimo (usuario y contraseña para acceso al computador y unidad z para guardar información y salida a internet por navegación). En caso de requerir accesos a otros sistemas y plataformas, los solicitarán a través de su jefe inmediato o supervisor de contrato por medio de requerimiento en la mesa de ayuda.

- La oficina TIC realizará monitoreo sobre las redes de la Entidad verificando posibles anomalías y actuando prontamente frente algún incidente.

- En la red inalámbrica solo está permitida la navegación con sus correspondientes restricciones. No se puede acceder a los servidores y/o servicios a través de ella.

- La red cableada se segmenta por piso y la red inalámbrica está segmentada en visitante, funcionario y directivo.

- Las impresoras se configuran en una Vlan distinta a la de los equipos.

5.9.7 Intercambio de información

- El uso del drive es exclusivo para funcionarios y contratistas que están en el dominio de la Entidad, su uso debe ser a través de la cuenta de correo electrónico institucional, el dueño de la información podrá dar acceso a otras cuentas institucionales en caso de ser requerido.

- Se deben establecer acuerdos de confidencialidad, acuerdos de intercambio o convenios con las entidades que por diferentes razones requieran conocer o

transferir información catalogada como Pública Clasificada y Pública Reservada y se debe solicitar el apoyo de la Oficina de TI para validar los controles tecnológicos para el intercambio seguro de información

- En los acuerdos deben estar especificadas las responsabilidades para la transferencia de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

- 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 etiquetado de información clasificada, garantizando que el significado de las etiquetas 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).

- Se deben establecer en los contratos que se constituyan con terceras partes, los acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la

divulgación no autorizada de información de la entidad que les ha sido entregada.

- Los propietarios y custodios de los activos de información deben proteger la confidencialidad e integridad de la información durante los procesos o actividades de transferencia de la información, estableciendo los riesgos y los canales de transferencia seguros que eviten la divulgación o modificación no autoriza de la información, los cuales permitan brindar los niveles de seguridad apropiados.

5.9.8 Mensajería electrónica

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

- Los usuarios son responsables por la información que remiten a través de los correos electrónicos.

- Los usuarios solo deben usar la cuenta institucional para el envió de información de la Entidad.

- No se permite usar la cuenta Institucional como cuenta personal ni se permite el uso para el envío de masivo de correos tipo spam. En caso de requerir envió de correos de forma masiva, es necesario contar con la aprobación de la Oficina de TI.

- Si se van a compartir archivos clasificados como información pública clasificada o pública reservada, es necesario que el usuario se comunique con la Oficina TIC para validar los controles necesarios para su transmisión.

- Cada usuario de la Entidad cuenta con su correo electrónico y está prohibido prestar los correos a otros usuarios, el usuario se hace responsable por su manejo y buen uso.

5.9.9 Control de Eventos

Para detectar las actividades de procesamiento de información no autorizadas, la Oficina de TI debe configurar los sistemas para que se haga registro de los eventos realizados por los usuarios.

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.

En conjunto con los responsables de los servicios TIC, definirán la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se operan los procesos de la entidad, determinando los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.

Se deberán implementar los controles necesarios para preservar la custodia, confidencialidad, integridad y disponibilidad de los registros de auditoría, producto de 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, entre otros, cumpliendo con los periodos de retención establecidos para dichos registros.

5.10 LINEAMIENTOS Y ACTIVIDADES PARA EL CONTROL DE ACCESOS

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 servicios TIC y 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.

5.10.1 Registro de cuentas de usuario

- Para el registro de usuarios, se debe seguir el procedimiento 208-tic-pr-06 procedimiento para la administración de cuentas de usuario en la CVP.

- El uso de identificadores de usuario son 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 o genéricos solo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas y debe ser autorizado por la Oficina TIC.

- Se prohíbe el préstamo de usuarios, el usuario se hace responsable por el buen uso que le dé a su cuenta.

- El jefe inmediato es quien solicita los usuarios de sus colaboradores y el perfil a los que el usuario tiene acceso, cumpliendo con el procedimiento para la administración de cuentas de usuario en la CVP.

- El jefe inmediato debe avisar a la Oficina TIC cuando haya cambios de rol en los colaboradores para así mismo hacer los ajustes necesarios en los sistemas de información que haya a lugar.

- En caso de existir excepciones, deberán ser debidamente justificadas y aprobadas. Las excepciones deberán ser solicitadas por director o jefe de área correspondiente.

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

- Todas las contraseñas de los sistemas (administrador de red, cuentas de administración de aplicaciones, cuentas de usuario etc.) deben cambiarse con una periodicidad mensual.

- Las contraseñas de acceso a los servicios TIC, deberán cumplir con las siguientes características:

    - 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 doce (12) caracteres.
    - La contraseña debe tener al menos una letra del alfabeto latino en mayúscula (A – Z).
    - La contraseña debe tener al menos una letra del alfabeto latino en minúscula (a – z).
    - La contraseña debe tener al menos un dígito numérico (0-9).
    - La contraseña debe tener al menos un carácter especial no alfanumérico.
    - La contraseña no deberá contener los nombres o apellidos del usuario.

- Las cuentas de usuario son personales e intransferibles. El usuario es responsable por el uso que se dé a su cuenta, por tal motivo, se prohíbe el préstamo de la cuenta o compartir la contraseña a otro usuario.

- Ningún usuario deberá intentar obtener contraseñas de otros usuarios para acceder a recursos tecnológicos o información institucional.

- En caso de que exista una prórroga para un contratista, debe ser reportado a la Mesa de servicio por 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 Talento Humano debe reportar por medio de correo electrónico o la herramienta de gestión de solicitudes 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.

- 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.

- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al servicio TIC.

- 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.

5.10.2 Responsabilidades de usuario

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.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar contraseñas usadas anteriormente.
- Cambiar las contraseñas provisionales asignadas en el primer inicio de sesión.

- Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de perdida de confidencialidad.

5.11 LINEAMIENTOS Y ACTIVIDADES PARA SEGURIDAD EN DISPOSITIVOS MÓVILES

5.11.1 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
- ✓ 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.

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 deben tener en cuenta los siguientes lineamientos:

- Para los dispositivos móviles tales como Tablet, celulares o computadores portátiles, se deberán implementar medidas de seguridad, para gestionar los riesgos introducidos por el uso de dispositivos móviles y así asegurar que no se comprometa la información de la Entidad.

- Garantizar las medidas de seguridad físicas de estos dispositivos cuando se dejan desatendidos; se deben resguardar en lugares bajo llave, y/o deben contar con guayas de seguridad para evitar su hurto o robo.

- Todos los equipos móviles deben implementar un esquema de autenticación a través de contraseñas, códigos, patrones o biométricos, los cuales no pueden ser compartidos con otras personas.

- Los dispositivos móviles de almacenamiento y procesamiento deben implementar una solución que permita la detección y eliminación de software malicioso.

- La Oficina TIC podrá implementar mecanismos necesarios para monitorear o restringir el uso de dispositivos de almacenamiento removibles en equipos de la entidad, estableciendo los procedimientos para las excepciones en caso de requerirse por las labores institucionales.

- Se debe concientizar a los colaboradores sobre las medidas de seguridad a tener en cuenta sobre los dispositivos móviles en lugares públicos; ejemplo “no se deben conectar estos dispositivos en computadores y/o puertos USB de uso público (Restaurantes, café internet, aeropuertos, etc.)”.

- Se debe llevar un registro de los dispositivos móviles de almacenamiento y/o procesamientos autorizados por la Entidad, para el uso dentro y fuera de la misma.

- Los usuarios que cuentan con equipos móviles asignados para el desarrollo de sus funciones no deberán tener los permisos para realizar cambios en la configuración, instalación/desinstalación de software posterior a su recibo.

- Los usuarios de dispositivos móviles asignados por la Entidad evitarán hacer uso de estos en lugares de alto riesgo de robo y/o pérdida, evitando de esta manera pérdidas y/o fugas de información de la Entidad.

- Los colaboradores deberán informar a la mesa de servicios la pérdida, robo o extravío del dispositivo móvil; de igual forma se deberá notificar cualquier comportamiento anómalo asociados con las funcionalidades de los dispositivos y/o activos de información almacenados.

- Los dispositivos móviles asignados por la Entidad a los colaboradores tendrán la configuración de seguridad base definida por la Oficina TIC.

- Los dispositivos deben contar con un borrado seguro antes de ser reasignados o dados de baja de la Entidad.

5.11.2 Medios Removibles

- Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD's,DVD's, memorias USB, discos duros externos, cámaras fotográficas, cámaras de video, entre otros, deben ser registrados y autorizados.

- Los medios removibles no deben almacenar información Pública Reservada y/o Información Pública Clasificada, sin la debida autorización del dueño del activo de información y sin la implementación de los controles de seguridad definidos para estos dispositivos.

- La Oficina TIC puede restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad de la CVP o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información a través de medios removibles.

5.12 LINEAMIENTOS Y ACTIVIDADES PARA LA SEGURIDAD EN 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.

Se debe garantizar la seguridad de toda la información y los recursos gestionados cuando se realiza el teletrabajo concientizando a los colaboradores de la importancia de cumplir las medidas de seguridad tanto dentro como fuera de la oficina para garantizar y preservar la confidencialidad, la integridad y la disponibilidad de los activos de información que es accedida, procesada o almacenada a través de la modalidad de Teletrabajo, basados en los lineamientos y medidas de soporte para proteger la información.

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.

5.13 LINEAMIENTOS Y ACTIVIDADES PARA LA CONTINUIDAD DE LOS SERVICIOS TIC

Garantizar que, ante un evento de contingencia o una situación de desastre, se debe mantener el estado actual de los controles que protegen la información crítica y sensible propia o en custodia de la Entidad; para ello se deben establecer un conjunto de procedimientos y estrategias que permitan contrarrestar las interrupciones de los servicios TIC que soportan las operaciones críticas de la Entidad.

La Oficina TIC deberá tener definido un plan de continuidad de los servicios TIC que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de TI, de acuerdo con su impacto en el cumplimiento de la misión de la Entidad.
- Identificar las amenazas que puedan ocasionar interrupciones
- Documentación de la estrategia de continuidad de los servicios TIC.

- Planes de recuperación de los servicios TIC, como los correspondientes procedimientos técnicos requeridos.
- Plan de pruebas de las acciones de recuperación de los servicios TIC.

La Oficina TIC deberá gestionar los recursos necesarios para mantener la continuidad operacional de la infraestructura TIC, así como el personal, proveedores y los planes requeridos que deben estar actualizados.

5.14 LINEAMIENTOS Y ACTIVIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

La seguridad de la información se debe integrar en la gestión de proyectos de la Caja de la Vivienda Popular, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Esto debe aplicar a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los líderes de proyectos, de los dueños de proceso, de los funcionarios y contratistas, asegurar que se sigan las siguientes directrices:

- Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto, para identificar los controles necesarios.

- Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.

- Los proyectos desarrollados en la caja de la vivienda popular deben tener en cuenta los lineamientos del presente manual de políticas

6. DOCUMENTOS RELACIONADOS

https://www.cajaviviendapopular.gov.co/sites/default/files/208-TIC-Mn-07%20POLITICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACIO%CC%81N%20-%20V2%20.pdf

6.1 Normograma

- Ver Normograma

6.2 Documentos Externos

Nombre del Documento	Fecha de publicación o versión del documento	Entidad que lo emite	Ubicación
Conpes 3701	Julio 2011	Departamento Nacional de Planeación	https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf
Conpes 3854	Abril 2016	Departamento Nacional de Planeación	https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
ISO-IEC 27001	2013	ISO - Icontec	https://ecollection.icontec.org/normavw.aspx?ID=6387
ISO-IEC 27002	2015	ISO - Icontec	https://ecollection.icontec.org/normavw.aspx?ID=308
MANUAL DE GOBIERNO DIGITAL	Diciembre de 2018	Ministerio de Tecnologías de la Información y las Comunicaciones	https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf
Guía para la Elaboración de la política general de seguridad y privacidad de la información.	Mayo de 2016	Ministerio de Tecnologías de la Información y las Comunicaciones	https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150520_G2_Politica_General.pdf

7. CONTROL DE CAMBIOS

Versión	Fecha Aprobación (dd-mm-aaaa)	Cambios	Revisó Nombre y Cargo Líder del Proceso
01	01-12/2023	Versión inicial del Manual de Políticas de Seguridad de la Información	LUZ YAMILE REYES BONILLA Jefe de Oficina de Tecnologías de la Información y Comunicaciones

8. APROBACIÓN

ELABORADO	REVISADO	APROBADO
Nombre: FABIO NELSON GONZALEZ ALVAREZ **Cargo:** Contratista Oficina de Tecnologías de la Información y Comunicaciones **Nombre:** GUSTAVO ADOLFO BELTRAN SABOGAL **Cargo:** Contratista Oficina de Tecnologías de la Información y Comunicaciones **Fecha:** 30/11/2023	**Nombre:** LUZ YAMILE REYES BONILLA **Cargo:** Jefe de Oficina de Tecnologías de la Información y Comunicaciones **Fecha:** 30/11/2023	**Nombre:** LUZ YAMILE REYES BONILLA **Cargo:** Jefe de Oficina de Tecnologías de la Información y Comunicaciones **Fecha:** 30/11/2023

"Este documento fue revisado por parte de la Oficina Asesora de Planeación frente a la estructura del documento y cumplimiento de los lineamientos del SIG conforme a lo establecido en el numeral 4 del procedimiento control de la información documentada: 01/12/2023"