POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA

VIGENCIA 2022-2023

TABLA DE CONTENIDO

1. INTRODUCCION

La información es un activo de alto valor para la Empresa de Vivienda de Antioquia - VIVA. A medida que los procesos de la entidad se hacen más dependientes de la información y de la tecnología que la soporta, se hace necesario contar con los lineamientos que permitan el control y administración de la seguridad y privacidad de la información.

El presente documento contiene las buenas prácticas que rigen la actuación de los funcionarios, contratistas y terceros relacionados con la Empresa de Vivienda e Antioquia - VIVA, en cumplimiento de las disposiciones legales vigentes, con el objeto de salvaguardar la información de la entidad.

La política de seguridad y privacidad de la información contiene los lineamientos y directrices de seguridad y privacidad de la información. Su adopción busca prevenir y afrontar integralmente las amenazas que pueden comprometer la información de la entidad.

2. PROPÓSITOS

Formalizar el compromiso de la Empresa de Vivienda de Antioquia - VIVA, frente a la seguridad y privacidad de la información, así como definir los lineamientos que deberán seguirse para proteger la información a través de la definición de procedimientos, protocolos y estándares de seguridad al interior de la Empresa de Vivienda de Antioquia – VIVA.

Los protocolos de seguridad son las reglas o normas diseñadas para garantizar la confidencialidad, la integridad y la disponibilidad de la información. Es decir, son las medidas de seguridad implementadas para evitar que personas no autorizadas puedan acceder a la información, manipularla o destruirla[1].

[1] https://protecciondatos-lopd.com/empresas/protocolos-seguridad-informatica/#:~:text=Los%20protocolos%20de%20seguridad%20inform%C3%A1tica%20son%20las%20reglas%20o%20normas,la%20informaci%C3%B3n%2C%20manipularla%20o%20destruirla.

3. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad y privacidad de la información en el presente documento se justifica y sustenta en los siguientes tres principios básicos de la seguridad de la información, los cuales se ilustran a continuación:

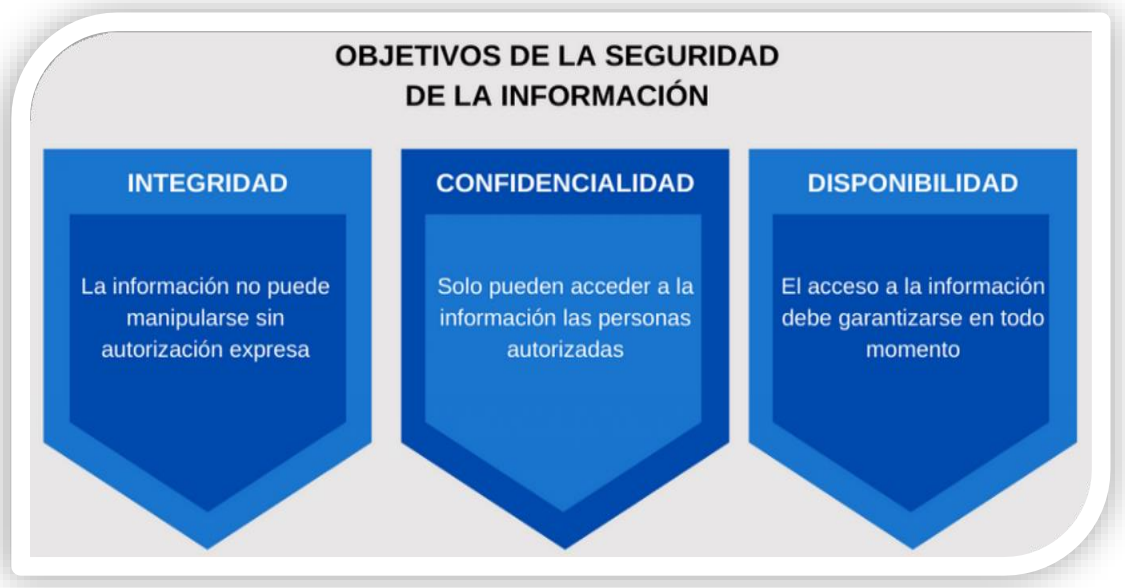

Imagen tomada de: https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/

4. OBJETIVO

Establecer la política de seguridad y privacidad de la información de la EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA con el fin de regular la gestión segura de la información al interior de la entidad.

5. ALCANCE

La política de seguridad y privacidad de la información cubre todos los aspectos administrativos, operativos y de control que deben ser cumplidos por los funcionarios, contratistas o terceros que laboren o tengan algún tipo de relación con la EMPRESA DE VIVIENDA DE ANTIOQUIA - VIVA, logrando un adecuado nivel de protección y calidad de la información.

6. RESPONSABILIDAD

Es responsabilidad de la Empresa de Vivienda de Antioquia – VIVA, la seguridad y privacidad de la información

7. MARCO LEGAL Y NORMATIVO

La Empresa de Vivienda de Antioquia - VIVA referencia las siguientes leyes y decretos que brindan las directrices para la gestión de la seguridad y privacidad de la información, en la Empresa de Vivienda de Antioquia - VIVA:

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por 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.
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones.
- Ley 1273 de 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.
- Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1474 de 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.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 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.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario

- Decreto 2609 de 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.
- Decreto 0884 del 2012. Por el cual se reglamenta parcialmente la Ley 1221del 2008.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo.

8. TÉRMINOS Y DEFINICIONES

- **Activo**: cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

- **Activo de Información**: recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso o que tiene relación directa o indirecta con las funciones de la entidad: software, hardware, personas (roles), físicos (instalaciones, áreas de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación).

- **Amenaza**: causa potencial de un incidente no deseado que pueda provocar daños a un sistema o a la organización.

- **Amenaza informática**: situación potencial o actual que tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

- **Antivirus**: programas cuyo objetivo es detectar y eliminar software malicioso.

- **Análisis de riesgos**: proceso para comprender la naturaleza del riesgo y determinar su nivel de riesgo.

- **Archivos PST**: son archivos electrónicos creados desde el software de mensajería Outlook con el fin de almacenar de forma local (computadores), copia de elementos de un buzón de correo electrónico

- **Autenticación**: mecanismo técnico que permite garantizar que una persona o entidad es la correcta.

- **Autenticidad**: Propiedad de que una entidad es lo que afirma ser.

- **Back up**: se refiere a una copia de respaldo de información.

- **Buzón**: espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros.

- **Canal de comunicación**: medio utilizado para la transmisión de información, por ejemplo: el cableado, fibra óptica y la atmósfera.

- **Centro de cómputo**: espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización llamado también data center por su término anglosajón.

- **Ciberseguridad**: capacidad para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- **Ciberespacio**: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética.

- **Confiabilidad**: persona o cosa en la que se puede confiar.

- **Confidencialidad**: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Control informático**: la política, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo reduciendo la probabilidad o impacto del evento.

- **Correo electrónico**: servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica.

- **Claves, contraseña o password**: forma de autentificación que utiliza información secreta o confidencial para controlar el acceso hacia algún recurso.

- **Criterios para adquisición de tecnología**: condiciones o requisitos mínimos para tener en cuenta al momento de implementar y/o adquirir tecnología

- **Compatibilidad**: el sistema a adquirir debe ser compatible con la tecnología e infraestructura que tiene la entidad.

- **Calidad**: se deben definir requisitos con los que se pueda evaluar la calidad, tales como reconocimiento de marca y tiempo de funcionamiento.

- **Garantía:** se deben tener en cuenta los plazos de vigencia de la garantía ofrecidos y los requeridos para el proceso de implementación, adaptación, pruebas, y puesta en funcionamiento. Acuerdos de servicio: se deben generar reglas para la prestación de los servicios para las diferentes tareas que surjan en las diferentes etapas para definir los tiempos de respuesta entre las dos partes.

- **Mantenimiento, actualizaciones y soporte**: se deben definir los tiempos o momentos para aplicar el mantenimiento, definir de qué manera se realizarán las actualizaciones, cada cuánto y cómo se realizarán. Además, se debe identificar el alcance del soporte que se realice.

- **Transacciones**: se deben identificar cuáles transacciones realiza el sistema, de qué manera las realiza y dónde se almacenan.

- **Reportes o salidas**: se deben identificar las salidas de información de los sistemas, reportes, consultas en pantalla o impresiones.

- **SGSI**: Sistema de Gestión de Seguridad de la Información.

- **SIG**: Sistema Integrado de Gestión.

- **MIPG**: Modelo Integrando de Planeación y Gestion

- **MSPI**: Modelo de Seguridad y Privacidad de la Información

DISPOSICIONES GENERALES

9. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA EMPRESA DE VIVIENDA DE ANTIOQUIA - VIVA

La Empresa de Vivienda de Antioquia - VIVA, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos de la organización, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales, previniendo eventos e incidentes de seguridad, dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación de las TIC a través de la política de seguridad y privacidad de la información, así como campañas de divulgación y sensibilización frente a la seguridad y privacidad de la información.

9.1 LINEAMIENTOS PARA LA GESTIÓN DE ACTIVOS DE INFORMACIÓN

La EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA es la dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por sus funcionarios o contratistas, derivadas del objeto del cumplimiento de funciones, tareas asignadas y actividades misionales, así como las necesarias para el cumplimiento del objeto del contrato.

La EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA es propietaria de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA (Denominados “usuarios”) que estén autorizados y sean responsables por la información generada en los procesos a su cargo, de los sistemas de información o aplicaciones informáticas.

La información y sistemas de información tendrán copias de respaldo conforme a lo establecido en el presente manual. Los propietarios de los activos de información deberán utilizar un almacenamiento estructurado y racional de carpetas, subcarpetas, y archivos electrónicos que tengan nombres cortos y no estén ubicados en más de 4 subniveles de almacenamiento (subcarpetas), conservando la ordenación de archivos definida en la Tablas de Retención Documental (TRD) que le corresponda. El nombre de un archivo incluirá: la ruta desde el directorio raíz, la carpeta y las subcarpetas, el nombre y extensión del archivo; la ruta no deberá superar los doscientos cincuenta y cinco (255) caracteres. Los medios que almacenan información electrónica se tendrán que organizar y etiquetar de acuerdo con el esquema de clasificación y de conformidad al código de identificación documental y sus respectivas TRD; cada administrador o propietario dispone o autoriza remover o transferir información evitando su mal uso.

9.2 LINEAMIENTOS DE CLASIFICACIÓN DE INFORMACIÓN

La EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA consiente de la necesidad de asegurar la información y que esta sea identificada con el fin de que reciba el nivel de protección apropiado de acuerdo con el tipo de clasificación establecido por la ley. De este modo, 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 EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA como, por ejemplo:

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

Los usuarios responsables de la información 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 EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA; independiente del tipo de activo, se deben considerar las siguientes características:

- El activo de información es reconocido como valioso para La EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA.
- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
- Forma parte de la identidad organizacional y sin el cual La EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA 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 EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA).
- Los niveles de clasificación de la información valiosa que se ha establecido son: Información pública reservada, información pública clasificada (privada y semiprivada) e información pública.

9.3 LINEAMIENTOS DE IDENTIFICACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

Los activos de información dentro del alcance del SGSI de la Empresa de Vivienda de Antioquia - VIVA deben ser identificados y clasificados. Sobre el inventario y la clasificación de los activos de información se determinará el nivel de protección; su estructura de almacenamiento e identificación de responsable para cada uno de ellos y se definen algunos lineamientos generales para la identificación y protección de la información dirigido a funcionarios y contratistas:

- Los activos de información deben ser identificados y registrados en un inventario.
- Los activos de información deben tener un propietario asignado.
- Las responsabilidades de los propietarios de los activos de información son:
  - ✓ Definir los roles y/o usuarios autorizados que pueden tener acceso al activo y sus privilegios de acceso.
  - ✓ Determinar las clasificaciones correspondientes según la sensibilidad de la información.
  - ✓ Asegurar que se gestionen los riesgos de seguridad de la información.
  - ✓ Establecer las reglas de uso de la información, cuando sea necesario.
  - ✓ Aplicar la política de seguridad y privacidad y controles para la protección de la información.
- Cada activo de información debe tener un custodio designado, quien ha de protegerlo mediante la aplicación y el mantenimiento de los controles de seguridad autorizados por el propietario.
- Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación.

- Al momento de finalizar cualquier relación laboral con la entidad, los funcionarios y contratistas deberán entregar al líder, coordinador y/o supervisor correspondiente, la información producida en el marco de su rol y funciones asignadas, previo a su retiro.

- El líder, coordinador y/o supervisor, deberán confirmar la veracidad y consistencia de la información entregada por su personal a cargo en el evento de terminación de contrato, para surtir el procedimiento de generación de documento de paz y salvo.

- El líder, coordinador y/o supervisor, deberán notificar vía correo al buzón de soporte@viva.gov.co, la pertinencia del respaldo de información que deberá ser realizado por el personal de TI.

9.4 LINEAMIENTOS PARA LA CLASIFICACIÓN Y LA GESTIÓN DE INFORMACIÓN

- **Información Pública**: Es toda información que la Empresa de Vivienda de Antioquia - VIVA genere, obtenga, adquiera, publique o controle en su calidad de obligado.

- **Información Clasificada**: Es aquella información que estando en poder o custodia de la Empresa de Vivienda de Antioquia - VIVA en su calidad de obligado, 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 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).

  https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

- **Transferencia de información Clasificada o Reservada:** sólo se permite cuando exista un acuerdo de confidencialidad o compromiso contractual que lo regule.

- **La Empresa de Vivienda de Antioquia – VIVA:** tiene control total sobre la información que se almacene, por lo tanto, la entidad se reserva el derecho de mover, borrar, monitorear o tomar custodia de dicha información.

- **Los funcionarios y contratistas son responsables de:** proteger y salvaguardar la información derivada de su trabajo mediante la sincronización OneDrive, nunca suspendiendo o cancelando la sincronización de este servicio en cada PC. también tiene su alcance solicitar al proceso de TI el almacenamiento seguro de la información en servidor o nube, cuya pérdida pueda causar incumplimientos legales y/o la interrupción de los procesos de la entidad.

- **Los funcionarios y contratistas deben:** acatar los lineamientos para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

- **La información física y digital de la Empresa de Vivienda de Antioquia - VIVA debe**: tener un periodo de almacenamiento y/o retención documental que puede ser determinado por requerimientos legales o en su defecto por el Archivo General de la Nación.

- **Los funcionarios y contratistas deben tener en cuenta al imprimir, fotocopiar y/o escanear**: Verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; así mismo, recoger inmediatamente de las impresoras, escáneres, fotocopiadoras y faxes, los documentos confidenciales para evitar su divulgación no autorizada.

- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y respaldo.

9.5 LINEAMIENTOS DE GESTIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN PARA FUNCIONARIOS Y CONTRATISTAS

- Los funcionarios y contratistas deben asegurarse de que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

- En la Empresa de Vivienda de Antioquia – VIVA, la gestión de los riesgos se debe enmarcar dentro del ciclo PHVA a través de la identificación de los mismos, su valoración y tratamiento a través de la implementación de controles y acciones de mejora que deberán ser parte de la operación y responsabilidad de los funcionarios, contratistas, en cada uno de los procesos organizacionales, quienes a su vez deben identificar y reportar las condiciones que podrían indicar la existencia de riesgos de seguridad y privacidad de la información. En la siguiente ruta del SIG se publica la matriz de riesgos del proceso de TI:

https://vivagov-my.sharepoint.com/:x:/r/personal/comunicaciones_viva_gov_co/_layouts/15/Doc.aspx?sourcedoc=%7BDD0686F9-D873-4864-9224-12487F440E7C%7D&file=DS-F07.V9%20Matriz%20de%20Riesgos%20Gesti%C3%B3n%20de%20TI.xlsx&action=default&mobileredirect=true

9.5.1 CONTROLES CRIPTOGRÁFICOS PARA FUNCIONARIOS Y CONTRATISTAS

La Empresa de Vivienda de Antioquia - VIVA velará porque la información clasificada de la entidad deberá ser cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

Los funcionarios, contratistas que sean responsables de llaves (o claves) de cifrado deben reportar al proceso de Gestión de TI las novedades acerca del manejo de dichas llaves, por ejemplo: cambio de dueños, cambio de custodia, pérdidas, acceso no autorizado.

Cada vez que se requiera utilizar el cifrado de una carpeta o archivos, los funcionarios, contratistas deben realizar una copia previa de la versión legible de los datos y realizar el cifrado sobre dicha copia y no sobre el original.

Se deben utilizar mecanismos de cifrado cuando se requiera el almacenamiento de información reservada o clasificada en medios removibles (como memorias USB, discos duros externos, CD y DVD), e incluso por correo electrónico.

9.6 LINEAMIENTOS PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Empresa de Vivienda de Antioquia - VIVA promoverá entre los funcionarios y contratistas, el reporte oportuno de actividades sospechosas (Eventos, amenazas e incidentes) que comprometan la seguridad y privacidad de la información y que pueden identificarse y detectarse a través de medios físicos y/o lógicos como: (Dispositivos USB, discos externos, internet, mensajes de correo maliciosos u otros). Por lo anterior se define:

- Los usuarios de los activos de información deben desconectar de la red corporativa el equipo de cómputo e informar al proceso de TI los incidentes de seguridad que identifiquen.

- Es responsabilidad de los funcionarios y contratistas reportar cualquier evento o incidente relacionado con la seguridad de la información con la mayor prontitud.

- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios y contratistas deben notificarlo al proceso de TI para que se revise y se le dé el trámite necesario. El personal de TI debe:

  - ✓ Seguir el plan de acción para la gestión de alertas, eventos e incidentes de seguridad de la información. Ver el documento: “Plan de atención de alertas, eventos e incidentes de seguridad”, publicado en la ruta correspondiente del SIG:

https://vivagov-my.sharepoint.com/personal/comunicaciones_viva_gov_co/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fcomunicaciones%5Fviva%5Fgov%5Fco%2FDocuments%2FSIG%2FSIG%2F03%20Procesos%20de%20Apoyo%2FGesti%C3%B3n%20de%20Informaci%C3%B3n%20y%20Tecnolog%C3%ADa%2F07%2DManuales%2FIT%2DM05%2Ev01%20Plan%20de%20Atenci%C3%B3n%20Alertas%2C%20Eventos%20e%20Incidentes%20de%20Seguridad%2Epdf&parent=%2Fpersonal%2Fcomunicaciones%5Fviva%5Fgov%5Fco%2FDocuments%2FSIG%2FSIG%2F03%20Procesos%20de%20Apoyo%2FGesti%C3%B3n%20de%20Informaci%C3%B3n%20y%20Tecnolog%C3%ADa%2F07%2DManuales

- ✓ Definir los canales para que los colaboradores de VIVA reporten los incidentes de Seguridad de la Información como: llamada telefónica, correo electrónico, contacto vía Teams, WhatsApp y/o conversación directa con el personal del proceso de gestión de TI.

- ✓ Encargarse de la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos siguiendo el instructivo para la gestión de incidentes de seguridad publicado en la ruta:

  https://vivagov-my.sharepoint.com/:w:/r/personal/comunicaciones_viva_gov_co/_layouts/15/Doc.aspx?sourcedoc=%7BF456D9E6-4BA5-4BFF-9887-BEF95121D871%7D&file=IT-I13.v04%20Gesti%C3%B3n%20de%20Incidentes%20de%20Seguridad.docx&action=default&mobileredirect=true

- ✓ Encargarse de la recolección de evidencias de los incidentes de seguridad de la información reportados e identificados mediante software, equipos de seguridad informática y reportes específicos enviados por la Gobernación de Antioquia.

- ✓ Dar a conocer a todos los funcionarios y contratistas de la entidad, los lineamientos establecidos para la Gestión de Incidentes de Seguridad de la Información.

9.7 LINEAMIENTOS SOBRE USO ADECUADO DE LOS RECURSOS DE LA PLATAFORMA DE TECNOLOGÍA DE LA INFORMACIÓN TI

Toda la información de la Empresa de Vivienda de Antioquia - VIVA, así como los recursos para su procesamiento, almacenamiento y transmisión, deben ser empleados únicamente para propósitos laborales, evitando su abuso, derroche, uso ilegal o desaprovechamiento, de esta forma se establece que:

- Se prohíbe el uso de los recursos de plataforma de T.I. de la Empresa de Vivienda de Antioquia - VIVA para la realización de cualquier actividad ilegal.

- Para verificar el cumplimiento de los lineamientos de seguridad y privacidad de la información, el proceso de TI en la Empresa de Vivienda de Antioquia - VIVA podrá monitorear y auditar el acceso y uso de las plataformas de TI de la entidad que son facilitadas a funcionarios y contratistas para el cumplimiento de sus deberes y actividades misionales.

- Los funcionarios y contratistas deben abstenerse de crear, acceder, almacenar o transmitir material ilegal, pornográfico, propaganda política que promueva la violación de los derechos humanos o que atente contra la integridad moral de las personas o de las instituciones.

- No deben almacenarse archivos personales en equipos de cómputo, carpetas y/o recursos compartidos de la red corporativa.

- Los funcionarios y contratistas deben abstenerse de enviar archivos e información de la entidad a cuentas de correo personales y/o gratuitas. Esto último, con excepción de la notificación de correo con las credenciales de acceso enviadas al personal que ingresa por primera y realizado sólo por personal del equipo de TI.

- No está permitida la instalación, ejecución y/o utilización de software diferente al autorizado en los equipos de cómputo e instalado por los integrantes del proceso de gestión de tecnología e información.

- Los parámetros de configuración del sistema operativo y la seguridad de Windows defender solo deben ser modificados por integrantes del área de tecnología a nivel local o política general de directorio activo.

9.8 LINEAMIENTOS DE CONTROL DE ACCESO

- El proceso de TI en la entidad define las reglas para asegurar un acceso controlado a la información y su plataforma informática en la Empresa de Vivienda de Antioquia – VIVA.

- El proceso de Talento Humano informará la contratación del nuevo personal al buzón de soporte@viva.gov.co, este comunicado debe contener el nombre completo, la cédula de ciudadanía, fechas de inicio y finalización, correo electrónico personal del nuevo colaborador y el proceso que apoyará en la entidad; el personal de TI notificará al correo

personal del nuevo funcionario o contratista las credenciales de red asignadas. Del mismo se debe notificar el retiro y/o desvinculación de personal.

- Los funcionarios y contratistas serán provistos con acceso al dominio, a los servicios de red y al equipo de cómputo que les sea asignado durante el tiempo que se encuentren activos en la Empresa de Vivienda de Antioquia - VIVA.

- Los directivos o coordinadores de procesos en la entidad, deben solicitar y justificar para sus funcionarios y contratistas los permisos y/o herramientas de tecnología hardware o software específicas y requeridas para el desarrollo de sus funciones, escribiendo al buzón de correo soporte@viva.gov.co, este comunicado debe contener nombre completo del funcionario o contratista, su correo electrónico, rutas de acceso, nivel de acceso, recursos compartidos: (carpetas, SharePoint de procesos, sitios web restringidos, conexiones vpn, otros), especificaciones de equipos (hardware), especificaciones de (software); el proceso de TI verificará el alcance de las solicitudes y gestionará su solución siempre y cuando se cumpla la política de seguridad y privacidad de la información.

- La conexión remota a la red corporativa en la entidad sólo debe realizarse a través de una conexión VPN Segura suministrada por el proceso de TI a funcionarios y contratistas.

- Todo sistema de información software o hardware que se requiera adquirir en la entidad, debe ser aprobado por el proceso de tecnologías y sistemas de información en concordancia con los lineamientos y procesos de adquisición de bienes y servicios en la Empresa de Vivienda de Antioquia - VIVA.

- Durante el tiempo de ausentismo laboral de funcionarios y/o contratistas, se restringirán los accesos a la red corporativa y sistemas de información para lo cual el proceso de Talento Humano reportará oportunamente al proceso de TI estas novedades, escribiendo al buzón soporte@viva.gov.co, este comunicado debe contener el nombre completo, correo electrónico del funcionario o contratista y las fechas de inicio y finalización del ausentismo.

- Los equipos de cómputo y periféricos y/asignados a funcionarios y contratistas que se ausentarán, o finalizarán sus actividades laborales deben ser entregados al proceso de gestión de TI para su custodia y cuidado.

- Los equipos de cómputo y periféricos y/asignados a funcionarios y contratistas que se desvinculan, o finalizarán sus actividades laborales deben ser entregados al proceso de gestión de TI para su custodia y des aprovisionamiento.

- En caso de que durante la ausencia de funcionarios o contratistas se requiera que los accesos a los sistemas de información en la entidad no sean restringidos, el director o coordinador debe solicitarlo al buzón de soporte@viva.gov.co, informando el nombre completo, correo electrónico y fechas de activación del acceso.

- Se controla el acceso a la red de datos y aplicaciones, mediante credenciales de acceso (usuario y contraseña).

- La identificación de cada usuario en los sistemas de información se define de manera individual para permitir el acceso controlado con determinado nivel de seguridad de acuerdo con sus funciones, actividades, roles y responsabilidades.

- Si algún funcionario o contratista dejara de prestar sus servicios a la Empresa de Vivienda de Antioquia - VIVA, el proceso de Talento Humano debe informar inmediatamente al proceso de TI, escribiendo al correo Electrónico soporte@viva.gov.co, este mensaje debe contener la fecha de finalización, nombre completo y cédula de ciudadanía.

9.9 LINEAMIENTOS PARA EL USO Y PROTECCIÓN DE CLAVES DE ACCESO

Los funcionarios y contratistas en la entidad accederán a la red de datos y servicios de tecnología con sus propias credenciales (usuario y contraseña), por ningún motivo podrá ingresar con credenciales ajenas, dado que estas son únicas e intransferibles. Las claves o contraseñas deben:

- Tener mínimo ocho (8) caracteres alfanuméricos.

- Cada vez que se cambian las contraseñas, estas deben ser distintas por lo menos de las últimas 4 anteriores.

- La contraseña debe incluir los siguientes cuatro requisitos:

  - ✓ Uno o varios caracteres en mayúsculas.
  - ✓ Uno o varios caracteres en minúsculas.
  - ✓ Un numero entre 0 y 9.
  - ✓ Uno o varios caracteres no alfabéticos (Ejemplo: ., ¡, $, %, &, /, *, +, ¿, ?, \).

9.9.1 LINEAMIENTOS PARA EL MANEJO DE CONTRASEÑAS ADMINISTRADORES DE TECNOLOGÍA

Se debe garantizar en las plataformas de tecnología, que el ingreso a la administración se realice con la vinculación directamente de las credenciales y cuentas de usuarios creadas a nivel del directorio activo.

Los usuarios de TI administradores y sus correspondientes contraseñas a las consolas administrables (Servidores, Bases de datos, Dispositivo Firewall, Consola Antivirus y demás componentes de infraestructura de TI) deben estar en custodia en sobre sellado en área segura indicada por el coordinador del proceso de TI; las credenciales allí contenidas deben ser modificadas de manera mensual o con la periodicidad definida acorde a las buenas prácticas de seguridad informática.

El personal del proceso de TI por ningún motivo debe dar a conocer sus claves.

Las contraseñas de los Administrador asignadas a personal de TI por ningún motivo serán divulgadas y se deberán cambiar con la frecuencia parametrizada a nivel de directorio activo o con una frecuencia menor.

El personal de TI debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y autenticación fuerte, que sean mayores a 11 caracteres alfanuméricos.

https://normaiso27001.es/a9-control-de-acceso/

Los administradores de TI deben seguir los lineamientos de cambio de claves y utilizar procedimientos para salvaguardar o custodiar las claves o contraseñas en un sitio seguro; a este lugar solo debe tener acceso el director del área, el coordinador de TI y el personal que sólo él autorice.

9.10 LINEAMIENTOS PARA LA SEGURIDAD DE LAS OPERACIONES DE TI

9.10.1.1 PROCEDIMIENTOS OPERACIONALES

Los procedimientos operacionales existentes se encuentran publicados en la herramienta del Sistema Integrado de Gestión (SIG) para su consulta y aplicación, estos documentos deberán ser actualizados en caso de cambios y de acuerdo con las necesidades de mejoramiento demandadas por el servicio y proceso de Gestión de TI. La ruta de publicación de documentos en el Sistema Integrado de Gestión es la siguiente:

https://vivagov-my.sharepoint.com/personal/comunicaciones_viva_gov_co/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fcomunicaciones%5Fviva%5Fgov%5Fco%2FDocuments%2FSIG%2FSIG%2F03%20Procesos%20de%20Apoyo%2FGesti%C3%B3n%20de%20Informaci%C3%B3n%20y%20Tecnolog%C3%ADa

9.10.2 COPIAS DE SEGURIDAD

Se debe realizar copia de seguridad de las aplicaciones, bases de datos y bodegas de archivos alojados en los equipos servidores. Estas se realizan desde el equipo de TI y para el caso del sistema de información ERP – SICOF es el proveedor ADA S.A quien lo realiza.

Se debe realizar copias de seguridad de los archivos e información almacenada en equipos de cómputo, la cual se encuentra sincronizada en cada uno de los equipos mediante OneDrive, por ningún motivo funcionarios o contratistas deben suspender la sincronización de este servicio ya que así se garantiza el respaldo de información constante; la capacidad de almacenamiento para cada funcionario es de 1 Terabyte equivalente a 1000 gigabytes.

9.10.3 INCIDENTES DE SEGURIDAD

Cuando se presenten alertas, eventos e incidentes que pongan en riesgo la integridad, disponibilidad y confidencialidad de la información, se deberán registrar y realizar las acciones tendientes a su solución de acuerdo con el documento: “Plan de atención de alertas, eventos e incidentes de seguridad”, publicado en la ruta correspondiente del SIG:

https://vivagov-my.sharepoint.com/personal/comunicaciones_viva_gov_co/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fcomunicaciones%5Fviva%5Fgov%5Fco%2FDocuments%2FSIG%2FSIG%2F03%20Procesos%20de%20Apoyo%2FGesti%C3%B3n%20de%20Informaci%C3%B3n%20y%20Tecnolog%C3%ADa%2F07%2DManuales%2FIT%2DM05%2Ev01%20Plan%20de%20Atenci%C3%B3n%20Alertas%2C%20Eventos%20e%20Incidentes%20de%20Seguridad%2Epdf&parent=%2Fpersonal%2Fcomunicaciones%5Fviva%5Fgov%5Fco%2FDocuments%2FSIG%2FSIG%2F03%20Procesos%20de%20Apoyo%2FGesti%C3%B3n%20de%20Informaci%C3%B3n%20y%20Tecnolog%C3%ADa%2F07%2DManuales

Para el registro de incidentes de seguridad, se tendrá en cuenta no solo el reporte de alertas de Riesgo Operativo del Estado, sino también el reporte del incidente que el funcionario público o contratista reporte al proceso de gestión de TI a través de correo soporte@viva.gov.co a la mesa de servicios de TI. El reporte deberá contener información completa y precisa indicando los datos personales y el detalle de los hechos. El proceso de Gestión de TI analizará cada reporte y de acuerdo a su gravedad se elaborará el concepto técnico, se realizarán las acciones tendientes a su solución, como sea procedente según sea el caso; se comunicará el incidente de seguridad a la todos los funcionarios y contratistas de la entidad, y en caso de máxima gravedad, se reportará el incidente a la oficina de Control

Interno Disciplinario y al organismo competente del Estado (Ej. Colcert, Policía Nacional, otros) en caso de ser necesario.

https://www.colcert.gov.co/800/w3-channel.html

https://www.policia.gov.co/ciberseguridad

En caso de requerirse, el proceso de TI deberá solicitar apoyo al equipo de Seguridad Informática de la Gobernación de Antioquia.

9.10.4 AUDITORÍA INTERNA DEL PROCESO DE GESTION TI

En la Entidad se realiza un ciclo de auditorías internas, en las cuales se contempla el proceso de Gestión de TI, y el cual debe de ser auditado mínimo una vez al año dentro del plan anual de auditorías de la Dirección de Control Interno.

10. LINEAMIENTOS PARA EL USO DEL CORREO ELECTRÓNICO

La Empresa de Vivienda de Antioquia - VIVA, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación y el trabajo colaborativo entre funcionarios y contratistas, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso de correo electrónico, para esto se deben tener en cuenta las siguientes directrices:

- Durante la ejecución de sus actividades en VIVA, los funcionarios deben siempre tener presente los principios de confidencialidad, integridad y disponibilidad.

  https://www.ontek.net/que-es-triada-cid/

- La cuenta de correo electrónico asignada es de carácter individual, por consiguiente, ningún funcionario de la entidad, en ninguna circunstancia debe utilizar cuentas de correo diferentes a la asignada; los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones para la entidad en apoyo al objetivo misional de la Empresa de Vivienda de Antioquia – VIVA.

- El correo institucional no debe ser utilizado para actividades personales.

- Los mensajes y la información contenida en los buzones de correo son propiedad de la Empresa de Vivienda de Antioquia - VIVA y cada usuario, como responsable de la administración de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- Está prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, de género, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana.

- No es permitido el envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por el proceso de Comunicaciones en la Empresa de Vivienda De Antioquia - VIVA y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad y sostenibilidad ambiental.

- Los nombres de buzones solo podrán ser modificados bajo necesidad justificada mediante requerimientos generado por Directivos o Coordinadores de proceso al buzón soporte@viva.gov.co.

- Las novedades reportadas por el proceso de Talento Humano, relacionadas con ausencias de los funcionarios o contratistas por: Retiros, vacaciones, licencias, permisos, calamidades, etc., derivan en bloqueos y si por necesidad del proceso, las cuentas no deben ser bloqueadas el Director o Coordinador del proceso envía correo al buzón soporte@viva.gov.co con los datos de correo, nombre de usuario, fecha de inicio y finalización, solicitando el no bloqueo.

- Las cuentas de correo asignadas a los funcionarios y contratistas cuentan con 50 GB de capacidad de almacenamiento. En casos específicos y debidamente justificados, los administradores de TI podrán ampliar la cuota de almacenamiento requerida.

- Los funcionarios y contratistas serán responsables de mantener depurado su buzón de correo para evitar bloqueo por insuficiencia de espacio de almacenamiento.

11. LINEAMIENTOS PARA EL USO DE DISPOSITIVOS MOVILES

La Empresa de Vivienda de Antioquia – VIVA establece los lineamientos de uso y manejo de dispositivos móviles (Teléfonos móviles, celulares Smartphone, tabletas, entre otros); suministrados por La Empresa de Vivienda de Antioquia – VIVA y personales que hagan uso de

los servicios de información de la Entidad; los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

Los funcionarios y contratistas se comprometen expresa y voluntariamente a mantener el dispositivo asignado bajo su custodia y cuidado, a darle un uso adecuado, conforme a las actividades que le fueron asignadas, propias de la labor que realiza al interior de la entidad, así mismo, a conservarlo(a) en buen estado, evitando su deterioro y, a usarlo(a) solo para fines laborales.

12. LINEAMIENTOS DE SEGURIDAD PARA LOS RECURSOS HUMANOS

Se debe asegurar que los funcionarios y contratistas de la Empresa de Vivienda de Antioquia – VIVA, adopten sus responsabilidades en relación con la política de seguridad y privacidad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones, fuga o uso inadecuado de la información y de los equipos de cómputo empleados para sus actividades.

En situaciones de incumplimiento y/o violaciones a la política de seguridad y privacidad de la información, se deberá tramitar el cumplimiento de la ley 734 de 2013, ley 200 de 1995 y demás normas que reglamenten los procesos disciplinarios para los empleados del estado.

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4589

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=318

Si el funcionario o contratista deja de prestar sus servicios a la entidad o se traslada a otra dependencia, debe entregar los equipos, accesorios y activos de información asignados para el ejercicio de sus funciones al proceso de Gestión de TI desde el cual se realiza el respectivo respaldo de información, de acuerdo al procedimiento de finalización de contrato o cambio de cargo establecido bajo el flujo de paz y salvo del sistema de gestión documental Mercurio. El supervisor del contrato o líder del proceso correspondiente (Director(a), Jefe, Coordinador(a)) es el encargado de confirmar la confiabilidad de la información entregada por el funcionario o contratista para su respaldo.

El equipo de Talento Humano es el encargado de notificar por medio de correo electrónico al buzón soorte@viva.gov.co la creación, actualización, bloqueo o eliminación de cuentas de usuario, así como la asignación de equipos de cómputo para el cumplimiento de las actividades que le sean asignadas.

Una vez se proceda con la vinculación o contratación de personal, se asignan los activos tecnológicos, confirmando aquellos que tendrá a cargo, se establece un acuerdo de buen uso,

confidencialidad y no divulgación de la información. Los funcionarios y contratistas deben aceptar dentro de sus obligaciones la cláusula de confidencialidad sobre la información a la que tengan acceso y aceptar el cumplimiento de la política de seguridad y privacidad de la información.

12.1 LINEAMIENTOS PARA LA CONTRATACIÓN DE FUNCIONARIOS Y CONTRATISTAS

La Empresa de Vivienda de Antioquia – VIVA reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos. De este modo, se establecen lineamientos generales relacionados con la vinculación de funcionarios y contratistas.

Cada supervisor de contrato, director, coordinador debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de aceptación de la política para el personal provisto por terceras partes o contratistas, antes de otorgar acceso a la información de la entidad.

Los funcionarios que realicen labores en o para la Empresa de Vivienda de Antioquia - VIVA, deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de la Política de Seguridad y Privacidad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

La cláusula de confidencialidad y buen manejo de la información dice:

El empleado se obliga durante toda la vigencia del contrato de trabajo suscrito a mantener en secreto y bajo estricta reserva todos los hechos, datos y demás información, que por razón de su trabajo o cualquier otro motivo llegue a conocer directa o indirectamente y que hagan parte del conocimiento científico y tecnológico de propiedad de la Compañía. Esto se refiere a cualquier tipo de información, técnica, financiera, comercial y de negocios, de mercado, estratégica o cualquiera otra relacionada con las operaciones de negocios de la misma. Esta información, calificada de tipo confidencial, puede ser conocida por medios escritos, orales o visuales y, estar contenida en medios magnéticos, o de cualquier otra forma que puede haber sido identificada como confidencial o no.

Así mismo se debe mantener en secreto cualquier idea, concepto, know-how, conocimiento o técnica relacionados con información respecto de la cual tenga acceso el TRABAJADOR,

proveniente de un cliente, un tercero o del mismo EMPLEADOR, en desarrollo de sus funciones.

NOTA: En virtud de lo anterior, se considera conocimiento científico y tecnológico, el conjunto de procedimientos, ilustraciones, habilidades, fórmulas técnicas y secretos industriales de la Compañía, que conozca o pueda llegar a conocer el TRABAJADOR, durante la vigencia del contrato de trabajo o en el desempeño de las funciones y labores propias de su cargo.

La violación de las obligaciones aquí pactadas, constituirá una justa causa para dar por terminado el contrato de trabajo por parte de la Empresa, sin perjuicio de las demás acciones legales a que haya lugar.

Así mismo, la violación antes descrita, se encuentra tipificada como delito en el Código Penal Colombiano, desarrollada en el Título VII, denominado “De la Protección de la Información y de los Datos”, artículo 269 A y siguientes y sancionada de acuerdo a la misma normatividad

En general, todo invento, desarrollo industrial, mejora en los procedimientos, tal como se describe en el artículo 536 del Código de Comercio, que por razón de su actividad llegase a desarrollar el TRABAJADOR, son propiedad de la Compañía, quien podrá patentarlos sin que haya lugar a reconocer compensación económica alguna.

12.2 LINEAMIENTOS PARA FUNCIONARIOS Y CONTRATISTAS SOBRE SEGRIDAD DE LA INFORMACIÓN

La Empresa de Vivienda de Antioquia - VIVA en su interés por proteger su información y los recursos de procesamiento de la misma, demostrará el compromiso de la Gerencia en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumpla la política de seguridad y privacidad de la información de la entidad.

Todos los funcionarios y contratistas de la entidad deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la entidad; de este modo, se establecen lineamientos generales durante la vinculación de funcionarios y contratistas

Los funcionarios y contratistas que por sus funciones hagan uso de la información de la Empresa de Vivienda de Antioquia - VIVA, deben dar cumplimiento a la política, los lineamientos y procedimientos de seguridad de la información.

13. LINEAMIENTOS SOBRE EL USO DE LOS ACTIVOS TECNOLÓGICOS (EQUIPOS DE CÓMPUTO)

La entidad implementa los lineamientos de protección adecuada y uso de los equipos de cómputo mediante reglas de directorio activo y dominio de red, esto permite controles de instalación, acceso y cuidado de los mismos de acuerdo con sus roles y funciones; para lo cual se establece las siguientes directrices:

- Los usuarios no deben mantener archivos de vídeo, música, fotos u otros tipos de archivos que no sea de carácter laboral, almacenados en los discos duros de los equipos de cómputo o unidades de red.
- Evite ingerir bebidas o alimentos cuando te encuentres realizando actividades con tu equipo de cómputo.
- Al momento de utilizar su equipo de cómputo tener las manos limpias y secas.
- Ubicar los equipos de cómputo sobre superficies amplias y firmes.
- No ingresar los equipos de cómputo a zonas húmedas como baños o cocinas.
- No apoyar los equipos sobre superficies acolchadas de tela u otro material, esto obstruye las rejillas de ventilación.
- Al momento de cerrar la tapa del equipo, revisar que no existan objetos que puedan fracturar la pantalla.
- Nunca limpiar los equipos con paños húmedos o telas mojadas.
- Nunca limpiar los equipos con disolventes, alcoholes, aceites, etc.
- Mantén limpio tu equipo de cómputo, siempre con trapo seco.
- No adherir calcomanías o material adhesivo en los equipos de cómputo asignados.
- No ejerza presión fuerte o golpee la pantalla del equipo, puede fracturarla.
- Nunca deje al sol su equipo de cómputo.
- Digite suavemente, no golpee o ejerza fuerza sobre las teclas.

- Realizar el apagado diario de los equipos al final de la jornada.

- Si va a dejar su equipo de cómputo sólo, recuerde bloquear siempre su sesión, oprimiendo la tecla "Windows" y la tecla "L" simultáneamente.

- No deje conectado el cable de energía todo el tiempo al su portátil, cuando la carga sea completa, desconecte el cargador y cuando el sistema le avise “batería baja", vuelva a conectarlo, esto mantiene la vida útil del cargador y de la batería.

- Evite el transporte de equipos portátiles con la pantalla abierta, se pueden presentar golpes o caídas, bloquee la sesión y cierre la tapa; de esta forma será más seguro su transporte.

- Cuando requiera desplazar su equipo de cómputo, no lo levante de la pantalla, recuerde cerrar la tapa y tome el equipo con firmeza.

- Nunca apoye o acerque imanes a los equipos de cómputo, pantallas, discos duros, celulares, tabletas, tarjetas electrónicas u otros.

14. LINEAMIENTOS SOBRE EL USO DE INTERNET Y NAVEGACIÓN SEGURA

La Entidad permite el acceso al servicio de Internet, estableciendo lineamientos y condiciones que garanticen la navegación segura y el uso adecuado de la red por parte de los funcionarios o contratistas, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información publicada en el sitio web www.viva.gov.co. El proceso de gestión de TI administrará la autorización de los cambios a nivel de los permisos generales de navegación de los funcionaros y contratistas en la Empresa de Vivienda de Antioquia – VIVA, y en caso de requerirse un permiso a sitios restringidos, el director o coordinador del funcionario o contratista que requiere el acceso hará el requerimiento al buzón de correo soporte@viva.gov.co . Desde el proceso de Gestión de TI se administra la autorización o rechazo de permisos de navegación a sus funcionarios y contratistas.

La infraestructura de la Empresa de Vivienda de Antioquia – VIVA, utiliza herramientas de Directorio Activo, Firewall y Antivirus, para la protección desde y hacia internet; además de proteger el correo electrónico también protege las estaciones de trabajo y los equipos servidores contra el software malicioso y el uso malintencionado de los mismos. Se han definido controles, reglas de seguridad, filtrado de contenidos, bloqueo de Url´s y direcciones IP sospechosas, segmentación de la red (VLANs), lineamientos de grupo y restricción en niveles de navegación, acorde con el alcance y funciones a realizar por parte del personal de la entidad.

Desde el proceso de Gestión de TI se implementa herramientas y/o directrices de grupo de Directorio Activo para evitar la descarga e instalación de software no autorizado y/o código malicioso en los equipos de cómputo asignados, así mismo se controla el acceso a la información contenida en portales a través del filtrado de contenidos.

Los usuarios de los activos de información de la Empresa de Vivienda de Antioquia – VIVA tienen restringido el acceso a redes sociales, plataformas de video y audio, sistemas de mensajería instantánea, aplicaciones tipo “Streaming”. En caso de ser requerido por las funciones del cargo, el director o coordinador debe remitir la solicitud al buzón soporte@viva.gov.co indicando el nombre, correo del funcionario o contratista y descripción de la razón del permiso.

14.1 LINEAMIENTOS DE PROTECCIÓN CONTRA SOFTWARE MALICIOSO

El antivirus instalado en los equipos protege en tiempo real contra virus informáticos, gusanos, troyanos, malware, spyware, phishing, ransomware y otras amenazas que provienen de la red.

Se utiliza una consola de administración para monitorear y actualizar los parámetros de la herramienta antivirus de la entidad:

- Kaspersky
  https://cloud.kaspersky.com/?logonContext=V8pQeRo0HrZXmGHrf2SAFx7jKgpNTPoQVZy3AlSqxPK4NnV2A8_epdLJczEIPG3JKef95Zm5Kfbf7JLvgWwot2C3hpwGLyH3qpawttiideJwocQHeOVggKZWSUmeK-Ob4LmTj6_ORIczQbNXMSWEefq5MY-tRdRIBKVTKCHM2HlwZrnbZiq4rJwuvhvbmCsQOk6WWEk9kc8axkQeLvHuyA#/companies/all

- Antivirus de Microsoft Defender
  https://www.microsoft.com/es-co/windows/comprehensive-security

Para controlar instalaciones de software, en los equipos cliente, estas se podrán realizar solo a través del usuario administrador controlado por las políticas del dominio; así mismo, se hará control de descargas de archivos de la red a través del dispositivo Firewall de seguridad Cisco Meraki MX84.

https://documentation.meraki.com/MX/MX_Overviews_and_Specifications/MX84_Datasheet

También se realiza análisis y control a partir de alertas y/o notificaciones emitidas por el área de TI de la Gobernación de Antioquia y otras entidades como el centro de Riesgo Operacional Y Ciberseguridad (COLCERT) y ciberseguridad de la Policía Nacional.

15. LINEAMIENTOS PARA EL USO Y CONECTIVIDAD A PUNTOS DE RED, UNIDADES DE RED O CARPETAS COMPARTIDAS

Asegurar la operación correcta y segura de los puntos de red, y el correcto y seguro acceso a los recursos de la plataforma informática de la Entidad.

Para ingresar a los recursos de red en la Empresa de Vivienda de Antioquia – VIVA se cuenta con protección de acceso, a través de configuraciones en el servidor DHCP, que solo asigna una dirección IP correspondiente a los equipos debidamente registrados, validados y matriculados en este servidor por personal del proceso de Gestión de TI.

16. LINEAMIENTOS PARA EL USO DEL SERVICIO DE IMPRESIÓN Y DIGITALIZACIÓN

Asegurar la operación correcta, segura y costo-eficiente del servicio de impresión, teniendo presente la Directiva Presidencial 04 de 2012" "Eficiencia administrativa y lineamientos de la política *"Cero Papel"* en la administración pública".

"De conformidad con las Bases del Plan Nacional de Desarrollo 2010-2014, es propósito del Gobierno Nacional tener una gestión pública efectiva, eficiente y eficaz. Dentro de las estrategias principales para la implementación de esta política, se encuentra la denominada "Cero Papel" que consiste en la sustitución de los flujos documentales en papel por soportes y medios electrónicos, sustentados en la utilización de Tecnologías de la Información y las Telecomunicaciones. Esta estrategia, además de los impactos en favor del ambiente, tiene por objeto incrementar la eficiencia administrativa".

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50155

El servicio de impresión para los funcionarios y contratistas se parametriza mediante el registro del usuario y contraseña con el fin de permitir la salida de impresiones controladas confidencialmente.

El servicio de impresión parametrizado mediante el uso de contraseña permite realizar un seguimiento y control en el consumo de papel por cada usuario registrado.

El funcionario y/o contratista no debe imprimir documentos de carácter personal.

El funcionario y/o contratista no debe realizar impresiones y digitalizaciones en Plotter sin contar con la autorización del coordinador del proceso de Vivienda y Hábitat.

El funcionario y/o contratista que requiera realizar impresiones y/o digitalizaciones, debe contar con el apoyo del personal del proceso de Gestion de TI y en su defecto enviar la solicitud al buzón de soporte@viva.gov.co. Previa autorización del coordinador de proceso.

17. LINEAMIENTOS SOBRE LEGALIDAD DE SOFTWARE

La Empresa De Vivienda De Antioquia – VIVA y su proceso de Gestion de TI velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información entre ella la referente a derechos de autor y propiedad intelectual razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales, contractuales, de licenciamiento aplicable y lineamientos generales de ley:

17.1 LINEAMIENTOS PARA EL CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

- Los funcionarios y contratistas no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.

- Los funcionarios y contratistas deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o sus códigos de activación, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada propiedad de la Empresa de Vivienda de Antioquia - VIVA y de uso exclusivo. Ejemplo: (Office 365).

- Se prohíbe el almacenamiento de archivos, multimedia (videos, música, imágenes o libros electrónicos) y cualquier otro tipo de contenido que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en los equipos y carpetas de red de la entidad.

- Se prohíbe el almacenamiento, uso, instalación y/o ejecución de software que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en la plataforma tecnológica de la Empresa de Vivienda de Antioquia - VIVA.

- Desde el proceso de gestión de TI, se debe reportar anualmente la información requerida sobre derechos de autor a la oficina de Control Interno para la rendición de dicho informe a Dirección Nacional de Derecho de Autor (DNDA).

18. POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES DE LA EMPRESA DE VIVIENDA DE ANTIOQUIA - VIVA

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA a través del Área Talento Humano, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y si además terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales la EMPRESA DE VIVIENDA DE ANTIOQUIA - VIVA, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la EMPRESA DE VIVIENDA DE ANTIOQUIA - VIVA exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Los funcionarios y contratistas deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

Es deber de los funcionarios y contratistas, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Los funcionarios y contratistas del portal de la EMPRESA DE VIVIENDA DE ANTIOQUIA - VIVA deben asumir la responsabilidad individual sobre la clave de acceso a dicho portal que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.

Los funcionarios y contratistas del portal de la EMPRESA DE VIVIENDA DE ANTIOQUIA - VIVA deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder al portal de la EMPRESA DE VIVIENDA DE ANTIOQUIA - VIVA.

Los funcionarios y contratistas del portal de la EMPRESA DE VIVIENDA DE ANTIOQUIA - VIVA deben aceptar el suministro de datos personales que pueda hacerla entidad a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoría interna o externa.

https://viva.gov.co/wp-content/uploads/2021/07/RESOLUCION-101-2020.pdf

19. LINEAMIENTOS DEL AREA DE TECNOLOGÍA

19.1 LINEAMIENTOS PARA FUNCIONARIOS Y CONTRATISTAS DEL PROCESO DE GESTIÓN DE TI.

Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso no autorizado.

Para el cambio o retiro de equipos asignados a funcionarios y contratistas, se deben seguir procesos de saneamiento, es decir, llevar a cabo mejores prácticas para la eliminación de la información de acuerdo con el software disponible en la entidad. Ejemplo: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos. El personal del equipo de TI será el único encargado de realizar la instalación o distribución de software, sólo instalarán productos con licencia propiedad de la entidad, también software de uso libre. El personal del equipo de TI no debe otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del jefe o coordinador del proceso de Gestión de TI.

El personal del equipo de TI se obliga a no revelar la información a la que tengan acceso en el ejercicio de sus funciones. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación. El personal del equipo de TI no utilizará la información para fines comerciales o diferentes al ejercicio de sus funciones. Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro. Las copias licenciadas y registradas del software adquirido deben ser únicamente instaladas en los equipos de cómputo (pcs, portátiles, workstations, servidores) propiedad de la Empresa de Vivienda de Antioquia - VIVA.

El acceso a información específica, en la nube o servidor, asignación de software especializado, asignación de hardware con características especiales, debe ser solicitado por directivos o coordinadores.

Todos los funcionaros y contratistas deben ser aprovisionados y configurados con el mínimo de servicios necesarios para desarrollar las funciones y labores misionales que lidera el proceso que pertenece:

- Cuenta de red
- Acceso a internet
- Acceso a intranet
- Correo electrónico
- Aplicaciones Office 365

- Acceso a impresión
- PC o portátil

En el caso del personal que ingresa bajo la modalidad contractual de “prestación de servicios”, la entidad no esta obligada en aprovisionar equipo de cómputo.

19.2 LINEAMIENTOS DE SEGURIDAD PARA LA RELACIÓN CON PROVEEDORES

- Documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información o sistemas de VIVA, todo esto con la solicitud previa de directivos o coordinadores de la Empresa de Vivienda de Antioquia - VIVA.

- Verificar y hacer seguimiento al cumplimiento de acuerdos de nivel de servicio establecidos con sus proveedores de tecnología en el caso que se tengan definiciones dentro de los respectivos contratos.

- En caso de requerirse, se deben establecer procedimientos que permitan asegurar la gestión de cambios a nivel de aplicativos y servicios tecnológicos que son soportados por proveedores, logrando estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir garantizando el éxito en la gestión de cambios. Lo anterior haciendo uso del documento “IT-I12.v04 Gestión de Cambios” publicado en:

  https://vivagov-my.sharepoint.com/:w:/r/personal/comunicaciones_viva_gov_co/_layouts/15/Doc.aspx?sourcedoc=%7B4A459346-A0CF-4AF6-852F-15DFE27179E0%7D&file=IT-I12.v04%20Gesti%C3%B3n%20de%20Cambios.docx&action=default&mobileredirect=true

19.3 LINEAMIENTOS PARA DEFINIR LA CONTINUIDAD DE LA OPERACIÓN

- Se debe aplicar la metodología establecida para la identificación y evaluación de riesgos en la continuidad de la operación de los servicios de VIVA publicada en:

  https://vivagov-my.sharepoint.com/:x:/r/personal/comunicaciones_viva_gov_co/_layouts/15/Doc.aspx?sourcedoc=%7BDD0686F9-D873-4864-9224-12487F440E7C%7D&file=DS-F07.V9%20Matriz%20de%20Riesgos%20Gesti%C3%B3n%20de%20TI.xlsx&action=default&mobileredirect=true

- Se debe desarrollar un análisis de impacto al negocio (BIA por sus siglas en ingles), para que se identifiquen los servicios críticos de VIVA.

- Se deben diseñar las estrategias y tiempos de recuperación de la operación de los servicios críticos de VIVA.

- Se debe realizar un plan de pruebas del plan de continuidad de la operación y deberá ser ejecutado mínimo 1 al año.

- Se debe revisar el plan de contingencia como minino una vez al año o cuando ocurra un cambio en el contexto interno o externos de VIVA.

- Se debe disponer de planes de contingencia de los servicios de TIC y un plan de recuperación ante desastres, enfocados a lograr el retorno a la operación normal.

- Se debe estructurar el plan de continuidad de la operación acorde al alcance del sistema de gestión de Seguridad de la Información en coordinación con los líderes de los procesos, conforme a la normativa interna vigente.

- En caso de incidente que conlleve una interrupción se deberá gestionar el manejo de la crisis y los mecanismos de comunicación apropiados tanto internos como externos durante el estado de contingencia.

19.4 LINEAMIENTOS DE GESTIÓN DE VULNERABILIDADES

- Se debe realizar el monitoreo de la seguridad (firewall, antivirus) y los recursos (espacio en discos) para asegurar la disponibilidad de los servicios.

- Se debe realizar pruebas técnicas de vulnerabilidad a intervalos planificados a los sistemas de información y comunicaciones de VIVA.

- Se debe implementar un procedimiento de gestión de vulnerabilidades técnicas que incluya el plan de tratamiento preventivo y/o correctivo de las mismas.

20. LINEAMIENTOS DE SEGURIDAD DE LAS COMUNICACIONES

- Se debe implementar medidas para asegurar la disponibilidad de los recursos y servicios de red en la Empresa de Vivienda de Antioquia - VIVA.

- Se debe aplicar los estándares técnicos de configuración y segmentación de red; monitoreo y configuración de seguridad.

- Interconectar los componentes tecnológicos bajo el cumplimiento de los estándares técnicos de configuración y de seguridad de las redes y servicios.

- Implementar sistemas de protección entre las redes y las redes externas no administradas por VIVA en el caso que aplique, en su defecto, implementar conexiones vía VPN. Ejemplo: (proveedor Thomas).

- Identificar y documentar los servicios, protocolos y puertos autorizados en las redes de datos e inhabilitar o eliminar los servicios, protocolos y puertos no utilizados.

- Segmentar la red (VLANS), de modo que permita separar los grupos de servicios de información.

21. LINEAMIENTOS DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- En caso de desarrollos propios, desde el proceso de Gestion de TI, se debe separar los ambientes de desarrollo, pruebas y producción, en diferentes servidores.

- Desde el proceso de Gestion TI, deberá realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación en ambiente de producción.

- Desde el proceso de Gestión TI desarrollará o adquirirá el software requerido por la Empresa de Vivienda de Antioquia – VIVA de manera coordinada con el área que reporte la necesidad.

- Desde el proceso de Gestión TI en compañía del proceso asociado y rol logístico del CTE, establecerán los requerimientos funcionales, proceso asociado, código, versión y demás especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de seguridad de la información.

- Todo nuevo hardware y/o software que se vaya a adquirir y conectar a la plataforma tecnológica de la Empresa de Vivienda de Antioquia – VIVA, deberá ser gestionado por el proceso de TI para su correcto funcionamiento.
- Toda aplicación y/o software debe ser adquirido con previa aprobación del proceso de Gestión TI en concordancia con la política de adquisición de bienes y servicios de la entidad.

- Cualquier copia de software o aplicaciones será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes en el marco de los derechos de autor.

- El proceso de Gestión TI será la única dependencia autorizada para realizar copia de seguridad del software original en caso de requerirse.
- La instalación del software en los equipos de cómputo propiedad de VIVA o que hagan parte del dominio y red corporativa, se realizará únicamente a través del proceso de Gestión TI.

- Desde el proceso de Gestión TI se implementará reglas, políticas de grupo (GPO) y/o herramientas que restrinjan la instalación de software en los equipos de cómputo propiedad de VIVA.

- Para la adquisición y actualización de software, es necesario efectuar la solicitud al proceso de Gestión de TI y rol logístico del CTE, quienes analizarán las propuestas presentadas y que las características requeridas cumplan con lo que necesita cada proceso.

- Es prohibido el uso e instalación de juegos en los computadores de VIVA.

ELABORÓ	REVISÓ	APROBÓ
Carlos Alberto Restrepo Buitrago - Coordinador TI Rafael Ruiz Uribe - Profesional de apoyo TI	Gloria Hernández Manrique – Gestión Organizacional	Carlos Alberto Restrepo Buitrago - Coordinador TI