TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Empresa de Vivienda de Antioquia - VIVA es una empresa industrial y comercial del orden Departamental, la cual tiene por objeto: "*Disminuir las brechas habitacionales a través de actuaciones integrales de vivienda social y hábitat en el contexto urbano y rural, en el departamento de Antioquia o del país. Para tal fin, podrá promover, impulsar y ejecutar actividades comerciales o industriales de suministro, consultorías, servicios de ingeniería, arquitectura, gestión comunitaria, social y cultural, habilitación de suelo para vivienda, legalización, gestión predial, titulación, relacionada con la infraestructura habitacional, construcción de vivienda nueva, mejoramientos de vivienda, mejoramientos integrales de barrio en el contexto de la vivienda social, gestión sostenible de proyectos y de territorios, desarrollo y ejecución de planes, programas y proyectos de infraestructura habitacional pública y/o privada y todas aquellas actividades que se requieran en aras de promover la vivienda digna y el hábitat sostenible, en situaciones normales o de calamidad que estén viviendo las familias o las comunidades, de acuerdo con las competencias que le asigne la ley*.

En desarrollo de su objeto podrá ejecutar proyectos, planes y programas con empresas públicas y/o privadas, nacionales y/o internacionales, a través de actos y/o contratos, convenios y alianzas, promoviendo a su vez, la integración habitacional con entornos saludables y sostenibles, fomentando la innovación social en todas sus actuaciones".

La Empresa de Vivienda de Antioquia - VIVA, tiene funciones de planeación estratégica para la formulación sobre los lineamientos de entornos habitacionales y elaboración de planes de menor escala que garanticen intervenciones integrales, dentro de las cuales, la vivienda es entendida como el principal de los componentes que configura a las comunidades sostenibles. Igualmente, tiene funciones de ejecución y supervisión de las viviendas, aportando a la calidad de vida de la población del Departamento.

Dentro de los programas misionales de la Empresa, se encuentran los proyectos municipales integrales para la construcción de vivienda nueva y mejoramientos de vivienda y hábitat. Dichos proyectos en el territorio, en un marco de planificación integral, articulan la vivienda, los equipamientos y el espacio público, apuntando a la cualificación de las condiciones habitacionales existentes en los municipios, y al incremento y calidad de las viviendas de acuerdo con el déficit cuantitativo y cualitativo, propendiendo por la conformación de comunidades sostenibles.

La Empresa de Vivienda de Antioquia - VIVA**,** como una empresa líder en los temas de vivienda y hábitat en la región y el país, debe contar con las herramientas tecnológicas que le permitan estar a la altura de las exigencias técnicas en cumplimiento de su misión. Para suplir ese

requerimiento y mejorar los procesos de sistematización de la información, es necesario contar con un plan de seguridad y privacidad que permita preservar la confidencialidad, integridad y disponibilidad, dando cumplimiento normativo a la legislación, políticas y lineamientos relacionados con la administración y protección de la información, las cuales aplican a las entidades estatales.

2. OBJETIVOS

a. Objetivo General

Establecer los lineamientos, controles y acciones necesarias para proteger la información de la Entidad, garantizando su confidencialidad, integridad y disponibilidad, mediante la identificación, evaluación y tratamiento de los riesgos asociados al uso, manejo, almacenamiento y transmisión de la información, en cumplimiento de la normativa vigente en materia de seguridad y privacidad de la información, y en coherencia con el Modelo Integrado de Planeación y Gestión – MIPG.

3. ALCANCE

Aplica a todos los procesos en VIVA que, debido al cumplimiento de sus funciones u obligaciones en VIVA, compartan, utilicen, recolecten, procesen, intercambien o consulten información; sus funcionarios, contratistas y aquellas personas o terceros información, así como a los entes de control, entidades relacionadas que acceden, ya sea interna o externamente a cualquier activo de información.

4. RESPONSABLE(S)

El líder del proceso de Gestión de Tecnología de la Información es el responsable de la elaboración, actualización, divulgación, ejecución y seguimiento del presente plan de seguridad y privacidad de la información con responsabilidad compartida entre los funcionarios, contratistas y aquellas personas o terceros que intervienen en calidad de participantes de la organización, sus áreas y procesos.

5. NORMATIVIDAD

- Decreto 612 de 4 de abril de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.”
- Decreto 1008 de 14 de junio de 2018, “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital”.

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- 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”
- Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- Resolución 0448 de 2022. Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 2256 de 2020.
- Actualización de la Política General de Seguridad y Privacidad de la Información 2024: Esta actualización, realizada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), alinea las actividades del MSPI con la NTC/IEC ISO 27001 y la política pública de seguridad digital.

6. TÉRMINOS Y DEFINICIONES

Activos: Todo aquello que es de valor para la organización.

Activos de información: Datos y conocimiento de valor para la organización.

Confidencialidad: proteger los activos de información contra accesos o divulgación no autorizada.

Integridad: garantiza la exactitud de los activos de información contra alteración, perdida o destrucción, ya sea de forma accidental o fraudulenta.

Disponibilidad: asegura que los recursos informáticos y los activos de información pueden ser utilizados en la forma y tiempo requeridos.

SGSI: Sistema de Gestión de Seguridad de la Información

CSIRT: Computer Security Incident Response Team, por sus siglas en inglés o equipo de respuesta a incidentes de seguridad de la información

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

Advertencia: Mensaje que comunica al usuario que una acción puede ocasionar u ocasionara la pérdida de datos del sistema del usuario.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación

de datos o negación de servicio.

Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

Gobierno digital: La Política de Gobierno Digital es la política del Gobierno Nacional que propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC. Hace parte del Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de Gestión y Desempeño Institucional. https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno- Digital/

Hardware: Equipos o elementos físicos que hacen parte de un computador o sistema informático.

Interoperabilidad: Habilidad de transferir y utilizar información de manera uniforme y eficiente entre varias organizaciones y sistemas de información. (Gobierno de Australia). Habilidad de dos o más sistemas (computadoras, medios de comunicación, redes, software y otros componentes de tecnología de la información) de interactuar y de intercambiar datos de acuerdo con un método definido, con el fin de obtener los resultados esperados. (ISO). El ejercicio de colaboración entre organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades. (Marco de Interoperabilidad para el Gobierno en línea, Versión 2010).

Sistemas de información: conjunto de componentes físicos y lógicos que interactúan entre sí con un fin común.

Software: conjunto de rutinas o programas creados con lenguajes de programación que permiten que las computadoras realicen determinadas tareas

Operador: Es la persona natural o jurídica, pública o privada, que es responsable de la gestión de un servicio de telecomunicaciones en virtud de autorización o concesión, o por ministerio de la ley.

7. ESTRATEGIAS(S)

- Definir, gestionar y difundir el Plan de Seguridad y Privacidad de la Información a todos los funcionarios de la Empresa de Vivienda de Antioquia - VIVA
- Asegurar el cumplimiento, la revisión y la actualización cuando sea pertinente de la Política General de Seguridad y Privacidad de la Información y sus políticas específicas.
- Implementar controles de seguridad de la información.

- Analizar periódicamente los niveles de riesgo y proponer soluciones para fortalecer la seguridad y privacidad de la información en la entidad.
- Gestionar los incidentes de seguridad y recomendar acciones preventivas y correctivas para evitar afectaciones dentro de la entidad.

8. POLITCA DE SEGURIIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación fue adoptada mediante la Resolución 486 de 2023, la cual establece los lineamientos para el uso y manejo adecuado de la información, así como su alcance y aplicabilidad en la Entidad.

Dicha política es de obligatorio cumplimiento para todo el personal de la Empresa de Vivienda de Antioquia – VIVA, incluidos funcionarios, contratistas, terceros y la ciudadanía en general que hagan uso de los servicios informáticos y manuales de la Entidad, traten datos o generen información. En este sentido, el presente Plan de Seguridad y Privacidad de la Información tiene como finalidad operativizar la política, mediante la definición de acciones, controles y responsables que permitan su adecuada implementación y seguimiento.

9. PROYECTOS

- Adquirir, desplegar y configurar nuevo licenciamiento de software antivirus.
- Adquirir e implementar nuevo dispositivo firewall de seguridad.
- Ampliar la cuota de almacenamiento de los dispositivos NAS para salvaguardar los respaldos de información.
- Asegurar la configuración IPv6 de comunicaciones para disponer la red de datos con mayor nivel de seguridad.

10. META(S)

Mejorar el nivel de protección de la información sensible de la organización, empleados y proveedores de la empresa, mediante la implementación de controles técnicos, administrativos y operativos, de acuerdo con las normas vigentes y las mejores prácticas en la materia.

11. ACCIONES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La etapa de implementación del plan se centra en la ejecución y cumplimiento de las acciones necesarias (Actividades y objetivos planteados), de la misma forma se tienen en cuenta los roles y responsabilidades y los tiempos de cumplimiento por parte del equipo

de trabajo involucrado en el Plan de Seguridad de la Información (Todos los procesos, actores clave, colaboradores, equipo directivo). El resultado esperado de esta fase es la adecuada implementación y cumplimiento de las actividades previstas en el presente plan.

El Plan de Seguridad y Privacidad de la Información comprende el siguiente cronograma de actividades con sus correspondientes responsables fecha de inicio y fecha de finalización:

Componente	Actividad	Evidencia	Responsable(s)
Inducción seguridad de la información y buenas prácticas TI	Ejecutar inducción corporativa, seguridad TI y buenas prácticas a nuevos usuarios.	Registro de asistencia y cumplimiento controlado por Talento Humano.	Proceso de Gestión de tecnologías de la información.
Gestión de incidentes de seguridad de la información	Publicar y mantener actualizada la guía de atención de eventos e incidentes de seguridad, cuando sea necesario. Socializar a todos los usuarios sobre las actividades fraudulentas.	Guía actualizada publicada cuando se requiera. Se envían correos permanentes a todos los usuarios sobre actividades fraudulentas.	Proceso de Gestión de tecnologías de la información.
Revisión y monitoreo Datacenter	Revisión y monitoreo del Datacenter y servicios tecnológicos asociados en aras de confirmar su correcto funcionamiento.	Actas de revisión firmadas por el ingeniero de infraestructura.	Proceso de Gestión de tecnologías de la información.
Revisión y monitoreo consola antivirus	Revisar e identificar posibles amenazas en consola antivirus.	Publicación de informes de amenazas y acciones correctivas en Documentos TI, cuenta de 365: Soporte@viva.gov.co	Proceso de Gestión de tecnologías de la información.

Cambio de contraseñas de red y correo	Configuración y seguimiento a política del directorio activo de dominio de red y/o AD de Azure (Office 365) para que exija el cambio de contraseñas tanto de red como correo	Política creada y activa en directorio activo y Azure (Doble factor de validación).	Proceso de Gestión de tecnologías de la información.
Gestión de riesgos	Identificación de riesgos. Aprobación mapa de riesgos. Tratamiento de los riesgos y acciones.	Publicación en intranet, sesión de gestión organizacional, mapa de riesgos aprobados. Matriz de riesgos consolidados del proceso Gestión de TI.	Proceso de Gestión de tecnologías de la información.
Ejecución de respaldos de información de cada usuario	Sincronización herramienta OneDrive en cada cuenta de usuario permitiendo el respaldo de la información corporativa.	Cuenta de Office 365 asignada a cada usuario con herramienta OneDrive.	Proceso de Gestión de tecnologías de la información.
Ejecución de respaldos de información de cada usuario al momento de presentar retiro	Respaldo de la información (Archivos y buzón de correo) gestionada por cada usuario durante sus labores misionales y/o de apoyo en la entidad.	Respaldo de la información y correos en carpeta respaldos en el servidor de la entidad.	Proceso de Gestión de tecnologías de la información.
Ejecución de respaldos de información de los sistemas de información y/o bases de datos)	Respaldo de la información (Sistemas de información y/o bases de datos) de aplicativos de la entidad.	Respaldo de la información (Sistemas de información y/o bases de datos) de aplicativos de la entidad (Mercurio, SICOF, Página web, File Server, otros). Indicador de respaldos (Ver caracterización proceso de Gestión de TI).	Proceso de Gestión de tecnologías de la información.

12. INDICADORES

Satisfacción:
(Suma de la cantidad de las calificaciones del nivel de satisfacción (Bueno y Muy bueno) / total de encuestas diligenciadas) *100

Obsolescencia:
(Se = Suma de los equipos tecnológicos con 60 meses o más de antigüedad /
Te = Total de equipos tecnológicos de la entidad) *100

Respaldos:
Eficacia en el Respaldo (ER) = (Respaldados ejecutados / respaldos programados) * 100

Virus:

Numero de equipos afectados por virus y/o amenazas / Número total de equipos conectados a la red *100

13. CONTROL DE DOCUMENTOS

ELABORÓ	*R*EVISÓ	APROBÓ
Willmar Agudelo Davila Profesional de TI	Tatiana Andrea Maya Gutiérrez Profesional Universitario Gestión Organizacional	Comité Institucional de Gestión y Desempeño