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

Definir las actividades a ejecutar registradas en el Plan de Seguridad y Privacidad de la Información en la Empresa de Vivienda de Antioquia VIVA, con base en los lineamientos del Modelo de Seguridad y Privacidad de la Información los cuales están alineados con la NTC/IEC ISO 27001, así como las políticas de Gobierno Digital y Seguridad Digital bajo la gestión y desempeño institucional del Modelo Integrado de Planeación y Gestión (MIPG).

b. Objetivos específicos

- ✓ Ejecutar las acciones para la implementación y apropiación de la política y Sistema de Gestión de Seguridad de la Información, con el objetivo de salvaguardar la seguridad y privacidad de la información.
- ✓ Incrementar el nivel de madurez del modelo de seguridad y privacidad de la información en VIVA.
- ✓ Proteger los activos de información.
- ✓ Identificar los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- ✓ Sensibilizar a los funcionarios y contratistas en VIVA sobre la política y Sistema de Gestión de la Seguridad de la Información (SGSI), fomentando la cultura institucional en materia de seguridad de la información, cuyo objetivo primordial será la preservación de la confidencialidad, integridad y disponibilidad de la información, a través de la socialización y divulgación de buenas prácticas; así como recomendaciones de seguridad.

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.

Roles: En la actualidad, la Empresa de Vivienda de Antioquia - VIVA, cuenta con una estructura organizacional de 5 personas en el equipo de Gestión de TI, adscritas a la Dirección Administrativa y Financiera; conformada por:

- ✓ Un profesional, cuyo perfil es de ingeniero de sistemas con especialización, encargado de coordinar el proceso de información y tecnología.
- ✓ Un profesional universitario, cuyo perfil es de ingeniero de sistemas o informática, encargado de la administración de la infraestructura entre otras funciones de analista y soporte de nivel 2 que estén a su alcance.
- ✓ Un auxiliar de apoyo técnico, cuyo perfil es de técnico en mantenimiento y reparación de computadores, encargado de prestar soporte de nivel 1 a los usuarios de la entidad, entre otras tareas asignadas que estén a su alcance.
- ✓ Un profesional de apoyo, con certificación en la norma ISO 27001 y cuyo perfil es de ingeniero de sistemas, encargado de todas las funciones propias del proceso de Gestión de TI que le sean asignadas.
- ✓ Un profesional de apoyo, cuyo perfil es de ingeniero de telecomunicaciones, encargado del análisis de los datos, diseño y construcción de tableros de información para facilitar la gestión de información propia de las áreas y procesos de la entidad.
- ✓ Un profesional de apoyo, cuyo perfil es de ingeniero de desarrollo de software, encargado del análisis, diseño y desarrollo de aplicaciones requeridas para resolver las necesidades particulares de VIVA y facilitar la gestión de información propia de las áreas y procesos de la entidad.

5. ESTRATEGIAS(S)

- Dar a conocer al personal de VIVA la Política de Seguridad y Privacidad de la Información aprobada mediante la resolución 486 del 05 de septiembre de 2023.

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

- Dar a conocer los protocolos de seguridad como las reglas o normas diseñadas para garantizar la confidencialidad, la integridad y la disponibilidad de la información; evitando que personas no autorizadas puedan acceder a la información, manipularla o destruirla.

- Realizar un monitoreo permanente de los componentes de infraestructura tecnológica y tomar las acciones que sean necesarias para mitigar los posibles riesgos de seguridad.

6. PROYECTO(S)

- 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.

7. 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.

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

Ver acciones bajo numeral de cronograma y/o plan de acción para su ejecución.

9. PRODUCTO(S)

- Manual de Política de Seguridad y Privacidad de la Información.
- Seguimiento a implementación de Política de Seguridad y Privacidad de la Información.
- Matriz de riesgos de TI y tratamiento eficaz de los riesgos de seguridad.
- Implementación y configuración de seguridad a nivel de la Infraestructura tecnológica (Hardware y Software).
- Indicador de seguridad (Virus y amenazas) e informes de consola.
- Guía de atención de eventos e incidentes de seguridad.

10. CRONOGRAMA Y/O PLAN DE ACCIÓN PARA SU EJECUCIÓN

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)	Inicio	Fin
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.	Enero	Diciembre
Gestión de incidentes de seguridad de la información	Publicar y mantener actualizada la guía de atención de eventos e incidentes de seguridad. Socializar a todos los usuarios sobre las actividades fraudulentas.	Se publica guía actualizada de atención de incidentes de seguridad en la Intranet, sesión de Gestión Organizacional. Se envían correos permanentes a todos los usuarios sobre actividades fraudulentas, así concientizamos a los usuarios sobre este tipo de hackeo.	Proceso de Gestión de tecnologías de la información.	Enero	Diciembre
Política de Seguridad y privacidad de la información	Creación y aprobación. Publicación y socialización. Seguimiento y ejecución.	Publicación en intranet, sesión de Gestión Organizacional. Lista de asistencia y envío de correo a todos los usuarios.	Proceso de Gestión de tecnologías de la información.	Enero	Diciembre
Revisión y monitoreo Datacenter	Revisión y monitoreo diario del Datacenter y servicios tecnológicos asociados en aras de	Actas de revisión firmadas por el ingeniero de infraestructura y coordinador de TI.	Proceso de Gestión de tecnologías de la información.	Enero (Diario)	Diciembre (Diario)

	confirmar su correcto funcionamiento.				
Revisión y monitoreo consola antivirus	Revisar e identificar posibles amenazas en consola antivirus.	Publicación de informen de amenazas y acciones correctivas en Documentos TI, cuenta de 365: Soporte@viva.gov.co	Proceso de Gestión de tecnologías de la información.	Enero (Diario)	Diciembre (Diario)
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.	Enero (Bimen sual)	Diciembre (Bimensual)
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.	Enero	Diciembre
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.	Enero (Diario)	Diciembre (Diario)
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.	Enero (Bajo deman da)	Diciembre (Bajo demanda)
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 tecnologías de la información.	Enero (Seman al)	Diciembre (Semanal)

		proceso de Gestión de TI).			

11. 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

12. RIESGOS DEL PROCESO

A continuación, se describe en los riesgos asociados al proceso, los cuales serán tratados en el plan de control de riesgos de seguridad:

RIESGO	DESCRIPCIÓN DEL RIESGO
Retraso en la ejecución de las actividades laborales de los funcionarios, por suspensión o falta de disponibilidad de los servicios tecnológicos del Proceso de TI	Suspensión y no disponibilidad de los servicios tecnológicos que son indispendables para la ejecución de las actividades de la empresa, tales como: Impresión, internet, almacenamiento, gestión documental (Mercurio), Xenco, dominio, control de acceso, antivirus, copias de seguridad, ERP (Sicof), correo y herramientas colaborativas (Office 365), red LAN, red inalámbrica; debido a fallas físicas, desconfiguraciones, desactualizaciones y pérdida de elementos por ausencia de controles y mantenimientos programados (Lógico, físico).
Pérdida de los activos de información de la empresa debido a la ausencia de respaldos y restauraciones	Inadecuado respaldo y restauración de los activos de información de la Empresa, debido a la falta de ejecución de actividades indispensables a nivel del Proceso y/o de un Sistema Especializado de Backups y restauraciones que permitan su aseguramiento Activo de información: Información indispensable en la que la empresa utilizó recursos para su construcción, modificación o ajuste, es decir todo proyecto, informe o producto que se tenga en formato digital y que esté almacenado en los servidores de la entidad
Posibilidad de vulnerar la seguridad de la información	Vulneración de la seguridad de la información, por falta de infraestructura, herramientas, políticas y procedimientos adecuados; debido a que no se ejecutan los controles necesarios y se desconocen las políticas de seguridad de la información.
Posibilidad de pérdida información de la página web de la entidad.	Pérdida de información de la página web de la entidad por fallas técnicas de infraestructura o manejo inadecuado de la información

13. DESARROLLO DE LA TEMATICA A TRATAR

Se pretende fortalecer la confidencialidad, la integridad y disponibilidad de la información en la entidad VIVA, mediante procedimientos, lineamientos y herramientas tecnológicas que generen cumplimiento y apoyo a los demás procesos de la entidad, enfocando los esfuerzos en la generación de cultura y cuidado de la seguridad informática a través del presente plan de seguridad y privacidad de la información.

14. MARCO NORMATIVO

TIPO NORMATIVA DOCUMENTO	No.	DIA	MES	AÑO	CONTENIDO (OBJETO OBLIGACIÓN)
Decreto	23	26	1	1982	Ley sobre Derechos de Autor: Consagra normas sobre los derechos de autor que recaen sobre la sobras científicas, literarias y artísticas y en fin toda producción del dominio científico, literario o artístico que pueda reproducirse, o definirse por cualquier forma de impresión o de reproducción,

					Pornografía, radiotelefonía o cualquier otro medio conocido o por conocer.
Directiva Presidencial	02	24	02	2022	“Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)”
Decreto	338	8	03	2022	"Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"
Ley	1915	12	7	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 en el entorno digital.
Resolución	746	11	03	2022	"Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021"
Directiva	02	12	2	2002	Se consagran disposiciones sobre el respeto a los derechos de autor y los derechos conexos, en lo referente a la utilización de programas de ordenador (software). Ley de Comercio Electrónico: Ley 527 de 1999 Por medio de la cual se define y reglamenta.
Ley	527	18	8	1999	Ley de Comercio Electrónico: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley	1341	30	7	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. **ARTÍCULO 1°. *Objeto.*** La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los

					habitantes del territorio nacional a la Sociedad de la Información.
Ley	1273	5	1	2009	Por medio de la cual se modifica el Código Penal, sé 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	1581	17	10	2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.
Decreto	1377	27	6	2013	Protección de datos Personales: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto	2693	21	12	2012	Por el cual se establecen los lineamientos generales de la estrategia de Gobierno Digital de la República de Colombia, se reglamentan parcialmente las leyes 1341 de 2009 y 1450 de 2011 y se dictan otras disposiciones.
Ley	44	5	2	1993	Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y decisión Andina 351 de 2015 (Derechos de autor).
Ley	603	27	7	2000	Por la cual se modifica el artículo 47 de la Ley 222 de 1995.
Decreto	1474	15	7	2002	Por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el (20) de diciembre de (1996).
Circular	1	15	12	2000	Orientación para el cumplimiento de la Ley 603 del año 2000, vinculada con el derecho de autor.
Decreto	1078	26	5	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto	415	7	3	2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Directiva	4	3	4	2012	Eficiencia administrativa y lineamientos de la política cero papel en la administración pública.
Ley	1712	6	3	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	1437	18	1	2011	Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo. Las normas de esta Parte Primera se aplican a todos los organismos y entidades que conforman las ramas del poder público en sus distintos órdenes, sectores y niveles.
Acuerdo	3	17	2	2015	Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.
Decreto	235	28	1	2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones publicas
Conpes	3854	11	4	2016	Política nacional de seguridad digital, ciberseguridad y ciberdefensa
Ley	594	14	7	2000	Por medio de la cual se expide la ley general de archivos
Ley	1221	16	7	2008	Por la cual se establecen las normas para promover y regular el teletrabajo y se dictan otras disposiciones
Decreto	886	13	5	2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Articulo	147			2019	Transformación Digital Pública: El Gobierno Nacional mediante la expedición de la Ley 1955 de 2019 definió el Plan Nacional de Desarrollo 2019-2022 “Pacto por Colombia, Pacto por la Equidad”

15. SIGLAS 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.

16. CONTROL DE DOCUMENTOS

ELABORÓ	APROBÓ	REVISÓ
Carlos Alberto Restrepo Buitrago Coordinador de TI	Luz Edilia López Vahos Directora Administrativa y Financiera	Gloria Estela Hernández Manrique Coordinadora de Gestión Organizacional