1. Introducción

En el marco de la Política de Gobierno Digital y del Modelo Integrado de Planeación y Gestión – MIPG, la Seguridad y Privacidad de la Información se constituye como un habilitador transversal que permite garantizar la confianza digital, la protección de los datos, la continuidad de la operación institucional y el cumplimiento de la normatividad vigente.

De conformidad con lo establecido en el Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, la Seguridad de la Información se reconoce como principio rector de la Política de Gobierno Digital y como habilitador transversal junto con la arquitectura y los servicios ciudadanos digitales.

En este contexto, el Fondo de Valorización de Medellín adopta el presente Plan de Seguridad y Privacidad de la Información, el cual define lineamientos, responsabilidades y acciones orientadas a la protección de los activos de información, en concordancia con el Modelo de Seguridad y Privacidad de la Información – MSPI y la misión institucional.

1.1 Objetivo

Garantizar la implementación, seguimiento y mejora continua de los controles de Seguridad y Privacidad de la Información, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información, gestionar adecuadamente los riesgos de seguridad digital y asegurar la continuidad de la operación tecnológica, en articulación con el Modelo de Operación por Procesos y el MIPG.

1.2 Alcance

El Plan de Seguridad y Privacidad de la Información está alineado con la misión, visión y objetivos estratégicos del Fondo de valorización de Medellín. Su alcance comprende todos los procesos y dependencias institucionales, así como a los servidores públicos, contratistas, terceros y ciudadanos que interactúan con ella.

Asimismo, el plan aplica a la totalidad de los activos de información, sistemas de información, servicios digitales, infraestructuras tecnológicas y medios físicos o electrónicos en los cuales se realicen actividades de recolección, procesamiento, almacenamiento, transmisión, consulta o eliminación de la información, garantizando su confidencialidad, integridad y disponibilidad.

2. Definiciones

- **Confidencialidad:** Propiedad que garantiza que la información no sea divulgada a personas, procesos o sistemas no autorizados.

- **Integridad:** Propiedad que asegura que la información no sea modificada de manera no autorizada.

- **Disponibilidad:** Característica que permite que la información esté accesible y utilizable por los usuarios autorizados cuando sea requerida.

- **Seguridad de la Información:** Conjunto de medidas orientadas a proteger los activos de información, garantizando su confidencialidad, integridad y disponibilidad, y asegurando que el acceso y modificación se realicen únicamente por personal autorizado.

- **Activos de Información:** Elementos que deben ser protegidos por la Seguridad de la Información, entre los cuales se incluyen:

    - **Información:** Datos y documentos con valor para la entidad.
    - **Equipos:** Infraestructura tecnológica, hardware, software y recursos organizacionales.
    - **Usuarios:** Personas que utilizan y gestionan la información y los sistemas de la entidad.

3. Glosario – MSPI

- **Activo de Información**: Elemento que tiene valor para la entidad y que debe ser protegido, incluyendo la información, los sistemas de información, los servicios digitales, la infraestructura tecnológica, los procesos, las personas y la documentación asociada, de conformidad con el Modelo de Seguridad y Privacidad de la Información.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede generar daño a un activo de información, afectando la confidencialidad, integridad o disponibilidad de la información.
- **Análisis de Riesgos de Seguridad y Privacidad de la Información:** Proceso sistemático y continuo mediante el cual se identifican, analizan, evalúan y priorizan los riesgos que puedan afectar la seguridad y privacidad de los activos de información, con el fin de definir y aplicar medidas de tratamiento acordes con el nivel de riesgo identificado.
- **Autenticación**: Mecanismo mediante el cual se verifica la identidad de un usuario, sistema o proceso que solicita acceso a los activos de información o a los servicios digitales.
- **Autorización**: Proceso mediante el cual se asignan y gestionan los permisos de acceso a los activos de información, de acuerdo con las funciones, responsabilidades y principios de necesidad de conocer y mínimo privilegio.
- **Confidencialidad**: Propiedad de la información que garantiza que esta solo sea accesible y divulgada a personas, procesos o sistemas debidamente autorizados.
- **Continuidad de la Operación**: Capacidad de la entidad para garantizar la disponibilidad de los procesos críticos y los servicios digitales, y para restablecerlos oportunamente ante la ocurrencia de incidentes de seguridad de la información.
- **Control de Seguridad y Privacidad de la Información**: Medida administrativa, técnica u organizacional implementada para prevenir, detectar, reducir o mitigar los riesgos que puedan afectar la seguridad y privacidad de la información.
- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una persona natural determinada o determinable, cuyo tratamiento debe realizarse conforme a la Ley 1581 de 2012 y las disposiciones que la reglamentan o modifiquen.
- **Disponibilidad**: Propiedad de la información que garantiza que los activos de información y los servicios digitales estén accesibles y utilizables por los usuarios autorizados, cuando sean requeridos.
- **Gestión de Incidentes de Seguridad Digital**: Conjunto de actividades orientadas a la identificación, reporte, análisis, atención, registro y cierre de los incidentes que afecten o puedan afectar la seguridad y privacidad de la información, de acuerdo con los lineamientos establecidos por el MinTIC.

- **Gestión de Riesgos de Seguridad y Privacidad de la Información**: Proceso permanente mediante el cual se identifican, evalúan, tratan y monitorean los riesgos asociados a los activos de información, con el fin de minimizar su impacto en la entidad y garantizar el cumplimiento normativo.
- **Gobierno Digital**: Política pública que orienta el uso estratégico de las tecnologías de la información y las comunicaciones en el Estado, con el propósito de fortalecer la gestión pública, la transparencia, la participación ciudadana y la prestación de servicios digitales.
- **Impacto**: Consecuencia o efecto que puede generar la materialización de un riesgo de seguridad y privacidad de la información sobre los procesos, los activos de información, los servicios digitales, la continuidad de la operación o la imagen institucional.
- **Incidente de Seguridad de la Información**: Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de los activos de información o de los servicios digitales de la entidad.
- **Información**: Conjunto de datos, documentos o registros, en cualquier formato o medio, que son generados, recibidos, administrados o custodiados por la entidad para el cumplimiento de su misión y objetivos institucionales.
- **Integridad**: Propiedad de la información que garantiza su exactitud, completitud y consistencia, evitando modificaciones no autorizadas.
- **Modelo de Seguridad y Privacidad de la Información – MSPI**: Conjunto de lineamientos, controles, prácticas y responsabilidades definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientados a fortalecer la seguridad y privacidad de la información en las entidades públicas.
- **Modelo Integrado de Planeación y Gestión – MIPG**: Marco de referencia que integra los sistemas de gestión y control de la administración pública, orientado a mejorar el desempeño institucional y la generación de valor público.
- **Riesgo de Seguridad y Privacidad de la Información**: Posibilidad de que una amenaza explote una vulnerabilidad de un activo de información y genere un impacto negativo en la entidad.
- **Seguridad y Privacidad de la Información**: Conjunto de políticas, procesos, procedimientos y controles orientados a proteger los activos de información, garantizando la confidencialidad, integridad, disponibilidad y el adecuado tratamiento de los datos personales.
- **Servicios Digitales**: Soluciones tecnológicas que permiten a la entidad ofrecer servicios, trámites y acceso a la información a través de medios electrónicos, en el marco de la Política de Gobierno Digital.
- **Sistema de Gestión de Seguridad de la Información – SGSI**: Parte del sistema de gestión institucional que permite establecer, implementar, operar, monitorear, revisar y mejorar la seguridad de la información, con base en la gestión de riesgos.

- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, tales como la recolección, almacenamiento, uso, circulación, actualización o supresión, conforme a la normatividad vigente.
- **Vulnerabilidad**: Debilidad de un activo de información, proceso, sistema o control, que puede ser explotada por una amenaza y generar un incidente de seguridad y privacidad de la información.

4. Marco normativo

El presente plan de Seguridad y Privacidad, las normas jerárquicas (leyes/decretos) se aplican antes que las técnicas (ISO/Estándares), y cronológicamente, las más recientes actualizan o complementan marcos más antiguos como la Ley 1581 de 2012 de Protección de Datos en Colombia, estableciendo directrices desde lo general a lo específico, priorizando la protección de datos y la ciberseguridad en la era digital.

- **Constitución Política:** Principios generales de protección de derechos fundamentales.
- **Leyes Estatutarias (Colombia):** Ley 1581 de 2012 (Protección de Datos Personales) y Ley 1712 de 2014 (Transparencia y Acceso a Información Pública).
- **Decretos y Regulaciones Nacionales:** Decreto 1078 de 2015, Decreto 338 de 2022 (Gobernanza de Seguridad Digital) y decretos que reglamentan leyes específicas.
- **Resoluciones y Directrices Ministeriales:** Resoluciones del MINTIC, sobre estrategia de seguridad digital que bajan las directrices a estándares específicos.
- **Estándares Internacionales y Marcos Técnicos:** Normas ISO/IEC 27000 (Sistemas de Gestión de Seguridad de la Información), que definen controles y mejores prácticas.
- **2022-2025:** Decretos de Seguridad Digital (D. 338/2022), Resoluciones MINTIC (500/2021, 1519/2020) y actualizaciones de planes que enfocan en digitalización, gobernanza y ciberseguridad.
- **2021:** Adopción de estrategias de seguridad digital y protección de datos (Resolución 500/2021)
- **2020:** Marco para la publicación de información y gestión de trámites digitales

(Resolución 1519/2020)

- **2014:** Ley 1712 de Transparencia y Acceso a la Información Pública.
- **2012:** Ley 1581 de Protección de Datos Personales (Habeas Data).

Estándares y marcos internacionales

- **ISO 27001 de 2013**. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la Información (SGSI). Requisitos.
- **ISO/IEC 27002:2013**. Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Guía vigente de administración del riesgo establecida por la Función Pública y con los lineamientos de la política de protección de datos ***"Por medio de la cual se adopta el manual de políticas y procedimientos para la protección de datos en el Fondo de valorización del distrito de Medellín –FONVALMED***

5. Responsabilidades

El responsable del área Administrativa y Financiera, en coordinación con el Proceso de Tecnologías de la Información, es responsable de asegurar el cumplimiento legal y la implementación de las medidas necesarias para mantener un nivel adecuado de seguridad y privacidad de la información.

- Definir, implementar, socializar y mantener actualizado el Plan de Seguridad y Privacidad de la Información.
- Velar por el cumplimiento de la normatividad vigente en materia de seguridad digital y protección de datos personales.
- Promover la implementación de controles técnicos, administrativos para la protección de los activos de información.
- Coordinar la gestión de riesgos de seguridad y privacidad de la información.
- Gestionar los incidentes de seguridad digital y activar los planes de contingencia cuando aplique.
- Asegurar la ejecución de estrategias de sensibilización y formación en seguridad y privacidad de la información.

Actividades

- Definir, actualizar y aprobar el Plan de Seguridad y Privacidad de la Información, en concordancia con los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI y el Modelo Integrado de Planeación y Gestión – MIPG.
- Articular el Modelo de Seguridad y Privacidad de la Información con los procesos y los instrumentos de planeación y gestión.
- Identificar, analizar, evaluar y priorizar los riesgos de seguridad y privacidad de la información asociados a los activos de información de la entidad.
- Definir e implementar los planes de tratamiento de los riesgos de seguridad y privacidad de la información, de acuerdo con el nivel de riesgo identificado.
- Identificar, clasificar y actualizar el inventario de activos de información, conforme a su criticidad y nivel de sensibilidad.
- Implementar controles técnicos, administrativos y organizacionales para proteger los activos de información, garantizando la confidencialidad, integridad y disponibilidad de la información.
- Administrar los accesos a los sistemas de información y servicios digitales de la entidad, de acuerdo con los principios de mínimo privilegio y necesidad de conocer.
- Reportar los incidentes de seguridad digital a las instancias definidas por el Ministerio de Tecnologías de la Información y las Comunicaciones, cuando aplique.
- Definir, documentar e implementar el procedimiento para la realización de copias de respaldo y restauración de la información.
- Realizar pruebas periódicas a las copias de respaldo para garantizar la disponibilidad de la información.
- Realizar análisis periódicos de vulnerabilidades sobre los activos de información y servicios digitales de la entidad.
- Desarrollar acciones de sensibilización y capacitación en seguridad y privacidad de la información dirigidas a servidores públicos y contratistas.
- Definir y hacer seguimiento a indicadores de seguridad y privacidad de la información, que permitan evaluar la efectividad de los controles implementados.

6. Política de seguridad y privacidad de la información.

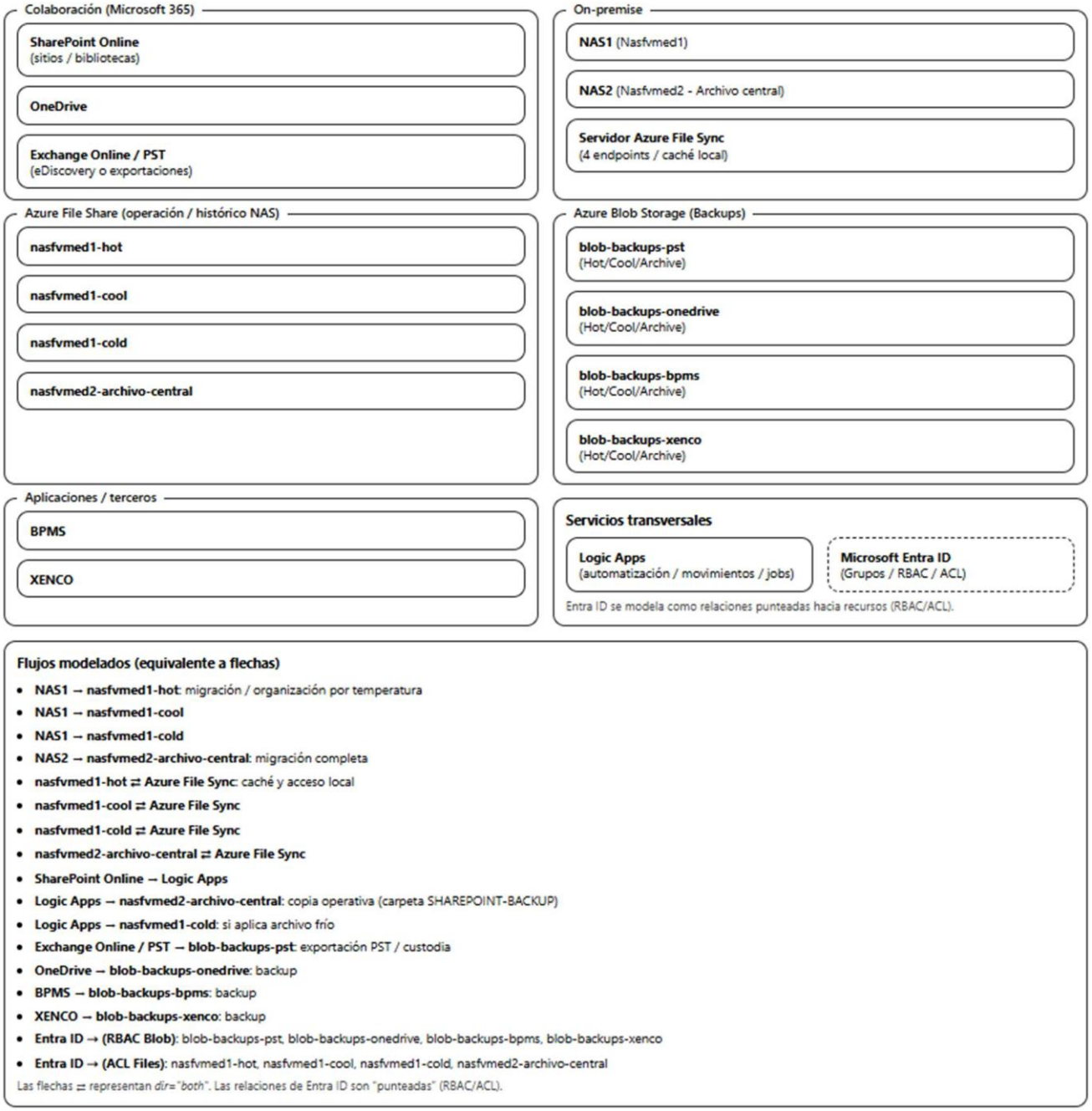
El Fondo de valorización adopta la Política de Seguridad y Privacidad de la Información como instrumento rector que establece los principios, lineamientos y compromisos institucionales para la protección de la información, la cual aplica a todos los servidores públicos, contratistas y terceros que accedan, usen o administren información institucional.

La política será revisada y actualizada periódicamente conforme a los cambios normativos, tecnológicos y organizacionales.

7. Operación del sistema de gestión de seguridad de la información – SGSI

El Sistema de Gestión de Seguridad de la Información – SGSI del Fondo de valorización opera bajo un enfoque de mejora continua basado en la gestión de riesgos de seguridad y privacidad de la información, garantizando la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar los activos de información y los servicios digitales de la entidad.

Diagrama respaldo fonvalmed (vista HTML)



Flujos modelados (equivalente a flechas)

- **NAS1 → nasfvmed1-hot**: migración / organización por temperatura
- **NAS1 → nasfvmed1-cool**
- **NAS1 → nasfvmed1-cold**
- **NAS2 → nasfvmed2-archivo-central**: migración completa
- **nasfvmed1-hot ⇄ Azure File Sync**: caché y acceso local
- **nasfvmed1-cool ⇄ Azure File Sync**
- **nasfvmed1-cold ⇄ Azure File Sync**
- **nasfvmed2-archivo-central ⇄ Azure File Sync**
- **SharePoint Online → Logic Apps**
- **Logic Apps → nasfvmed2-archivo-central**: copia operativa (carpeta SHAREPOINT-BACKUP)
- **Logic Apps → nasfvmed1-cold**: si aplica archivo frío
- **Exchange Online / PST → blob-backups-pst**: exportación PST / custodia
- **OneDrive → blob-backups-onedrive**: backup
- **BPMS → blob-backups-bpms**: backup
- **XENCO → blob-backups-xenco**: backup
- **Entra ID → (RBAC Blob)**: blob-backups-pst, blob-backups-onedrive, blob-backups-bpms, blob-backups-xenco
- **Entra ID → (ACL Files)**: nasfvmed1-hot, nasfvmed1-cool, nasfvmed1-cold, nasfvmed2-archivo-central

Las flechas ⇄ representan *dir="both"*. Las relaciones de Entra ID son "punteadas" (RBAC/ACL).

8. Organización del eje de seguridad de la información.

De conformidad con la Política de seguridad de la información del MIPG y dando cumplimiento al Modelo de seguridad y privacidad de la información en la entidad, el director(a) de la entidad, en cumplimiento de sus funciones y entendiendo la importancia de una adecuada gestión de la información, se compromete con el establecimiento, implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) como mecanismo para brindar a los ciudadanos y colaboradores confianza digital en torno al uso de los datos, al cumplimiento legal y mantener una actitud ética, transparente y en concordancia con la misión y la visión de la Entidad.

Siendo así este se encarga de articular procesos con el de Modelo de seguridad y privacidad de la Información (MSPI) y el Modelo integrado de Planeación y Gestión (MIPG).

9. Plan de sostenibilidad del modelo de seguridad y privacidad de la información

El Plan de sostenibilidad del Modelo de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento.

Subcomponente	Actividad	Producto	Responsable	Fecha aproximada
Gestión de incidentes de seguridad	Gestionar contingencias	Reporte y atención	Líder Proceso de Tecnologías de la Información	Mensual
Indicadores de seguridad de la información	Formular y hacer seguimiento a los indicadores que permitan monitorear trazabilidad de este componente	Indicador formalizado	Líder Proceso de Tecnologías de la Información	Trimestral
Respaldo de la información	Definir, documentar e implementar el procedimiento para la realización de copias de respaldo y restauración de la información.	Procedimiento para copias de respaldo y de	Líder Proceso de Tecnologías de la Información	Primer semestre
Respaldo de la información	Realizar pruebas periódicas a las copias de respaldo para garantizar la disponibilidad de la información	Evidencias de realización de pruebas	Líder Proceso de Tecnologías de la Información	Semestral

Subcomponente	Actividad	Producto	Responsable	Fecha aproximada
Respaldo de la información	Realizar sincronización compacta a los servicios de office 365 en donde se encuentra alojada la información (sharepoint, onedrive, Amazon sw3)	Información en tiempo real, respaldada en los servidores QNAS	Líder Proceso de Tecnologías de la Información	Primer Semestre
Análisis de vulnerabilidades	Realizar análisis de Identificación de vulnerabilidades de seguridad a los activos de información (hardware, software, aplicaciones, redes) y de servicios expuestos en internet	Informe de vulnerabilidades identificadas	Líder Proceso de Tecnologías de la Información	Mensual
Incidentes de Seguridad digital	Reportar los incidentes de seguridad digital acorde con lo establecido en la resolución 500 de 2022 del Ministerio de Tecnologías de la Información- MINTIC	Reporte de incidentes	Líder Proceso de Tecnologías de la Información	Cuando aplique

Subcomponente	Actividad	Producto	Responsable	Fecha aproximada
Gestión de seguridad y privacidad en los riegos	Realizar la identificación, clasificación, tratamiento y divulgación de incidentes seguridad de la información materializadas en atención a los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información	Reporte	Líder Proceso de Tecnologías de la Información	Cuando aplique
Capacitaciones	Desarrollar acciones de sensibilización y capacitación en seguridad y privacidad de la información dirigidas a servidores públicos y contratistas.	Videos, presentaciones, manuales	Líder Proceso de Tecnologías de la Información	Segundo semestre
Garantizar que el sitio web esté actualizado con las últimas versiones de Plataforma (WordPress),	- Verificar actualizaciones disponibles para WordPress, temas y plugins. - Realizar pruebas en un ambiente de desarrollo. - Implementar actualizaciones en el ambiente de producción.	Sitio web actualizado sin vulnerabilidades ni errores de compatibilidad	Líder Proceso de Tecnologías de la Información	Trimestral

Subcomponente	Actividad	Producto	Responsable	Fecha aproximada
Proteger la información y la configuración del sitio web mediante respaldos regulares.	- Realizar backups mensuales de dos niveles: Nivel 1 - Servidor Web completo / Nivel 2 - Sitio web Wordpress - Verificación de la integridad de los respaldos generados Almacenar los respaldos en una ubicación externa segura (nube) y en la NAS.	Copias de seguridad manuales y verificadas	Líder Proceso de Tecnologías de la Información	Mensual
Proteger el sitio web contra accesos no autorizados y ciberataques.	- Implementar medidas de seguridad a nivel de servidor y de plataforma web. Monitorear el tráfico web para identificar actividades sospechosas.	Informe de auditorías de seguridad y un sitio protegido.	Líder Proceso de Tecnologías de la Información	Trimestral
Mejorar la visibilidad del sitio web en motores de búsqueda para mayor acceso ciudadano.	- Realizar análisis de palabras clave relevantes. - Optimizar el contenido y las imágenes para SEO. - Monitorear métricas de rendimiento web con herramientas digitales.	Informes de posicionamiento SEO y aumento de tráfico web.	Líder Proceso de Tecnologías de la Información	Trimestral

Subcomponente	Actividad	Producto	Responsable	Fecha aproximada
Verificar el cumplimiento de las normativas colombianas (MINTIC, Matriz ITA, FURAG) para sitios web de entidades públicas.	- Realizar un diagnóstico de cumplimiento normativo. - Implementar ajustes en accesibilidad y seguridad según estándares MINTIC cada sea necesario. - Participar en el diligenciamiento de la matriz ITA y el FURAG para dar cumplimiento.	Informes de cumplimiento normativo y mejoras implementadas.	Líder Proceso de Tecnologías de la Información	Semestral

El presente plan de Seguridad y privacidad de la información será revisado anualmente o cuando se presenten cambios normativos, tecnológicos que así lo requieran, y será objeto de seguimiento en el marco del Comité institucional de Gestión y desempeño

Aprobado por el Comité de Institucional de Gestión y Desempeño
Medellín, 26 de enero de 2026

Alcaldía de Medellín Distrito de Ciencia, Tecnología e Innovación FONVALMED Fondo de Valorización de Medellín	**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** **Vigencia 2026**	Código: TI-PL04.V01 Versión: 01 Fecha de aprobación: enero 26 de 2026