

| | | |
|---|--|--|
|  | <p style="text-align: center;">PROGRAMA ESPECÍFICO</p> | <p>Código: asignado por quien emite el documento (F-ES-GM-024)</p> |
| <p style="text-align: center;">PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p> | | <p>Versión: consecutivo en que va el documento (01)</p> |
| <p style="text-align: center;">PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p> | | <p style="text-align: right;">Página 1 de 25</p> |



Alcaldía de Medellín
 Distrito de
Ciencia, Tecnología e Innovación

SAPIENCIA

Agencia de Educación
 Postsecundaria de Medellín

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión: **01**

Enero 2025

| | | |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 2 de 25 |

Tabla de contenido

Contenido

| | |
|--|-----------|
| 1. Introducción | 3 |
| 2. Objetivo..... | 4 |
| 3. Alcance | 4 |
| 4. Marco normativo | 5 |
| 5. Justificación | 8 |
| 6. Política General de Seguridad y Privacidad de la Información..... | 8 |
| <u>6.1. Objetivos Específicos Política General De Seguridad Y Privacidad de la Información</u> | <u>9</u> |
| 7. Alineación Estratégica..... | 10 |
| 8. Modelo Seguridad y Privacidad de la Información..... | 11 |
| <u>8.1. Plan De Implementación Del Modelo De Seguridad Y Privacidad De La Información.</u> | <u>11</u> |
| 9. Proyectos de Inversión | 24 |

| | | |
|---|---------------------|---|
|  <p>Alcaldía de Medellín Oficina de Ciencia, Tecnología e Innovación</p> <p>SAPIENCIA Agencia de Educación Postsecundaria de Medellín</p> | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 3 de 25 |

1. Introducción

En la actualidad la información es el activo más importante en todos los contextos, de igual manera es un recurso indispensable para el desarrollo, la toma de decisiones y el cumplimiento de la misionalidad de las organizaciones. Toda información puede llegar a ser sensible y por ello requiere de una valoración para establecer su nivel de criticidad y así mismo los controles a implementar para su protección con el fin de mitigar y/o evitar posible pérdida de su disponibilidad, integridad y confidencialidad.

La seguridad de la información debe ser un componente crítico y fundamental dentro de la estrategia de seguridad de las entidades a nivel nacional, por ello la **Agencia De Educación Postsecundaria de Medellín** reconoce su importancia para el sector educativo y ha identificado la información como uno de los activos más importantes y críticos para el desarrollo de sus funciones.

Debido a los múltiples riesgos y amenazas que hoy en día atentan contra la seguridad de la información, la protección y privacidad de los datos, es fundamental que las entidades del Estado, entre esas la Agencia De Educación Postsecundaria De La Alcaldía De Medellín implementen, conserven y optimicen de manera continua un sistema de gestión de seguridad de la información basado en los riesgos.

Con respecto a lo anterior desde la dirección de Planeación Estratégica y Gestión Sistemas De Información, el Agencia De Educación Postsecundaria De La Alcaldía De Medellín ve la necesidad de implementar y mantener un modelo de gestión de la seguridad de la información que permita alcanzar y mantener dentro de las

| | | |
|---|---------------------|---|
|  <p>Alcaldía de Medellín Oficina de Ciencia, Tecnología e Innovación</p> <p>SAPIENCIA Agencia de Educación Postsecundaria de Medellín</p> | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 4 de 25 |

diferentes áreas y colaboradores una cultura y conciencia en el acceso y uso adecuado de la información en la Entidad.

2. Objetivo

La finalidad de este documento es definir las actividades incluidas en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), así como su gestión mediante el SGSI, en conformidad con la norma NTC/IEC ISO 27001. Además, se alinea con la Política de Seguridad de la Información de la Agencia de Educación Postsecundaria de Medellín y el Plan Estratégico de Tecnologías de la Información.

Este enfoque sirve como marco para establecer y regular directrices y medidas que garanticen la protección y el uso responsable de la información, así como de los activos que la respaldan dentro de la Entidad.

3. Alcance

El Plan de Seguridad y Privacidad de la Información identifica e integra las alineaciones necesarias para gestionar el ciclo (PHVA) de operación del Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo se debe aplicar en todos los procesos de la Agencia de Educación Postsecundaria de la Alcaldía de Medellín y es de cumplimiento obligatorio para todos los colaboradores de la Entidad.

| | | |
|--|---------------------|---|
|  <p>Alcaldía de Medellín Centro de Ciencia, Tecnología e Innovación</p> <p>SAPIENCIA Agencia de Educación Postsecundaria de Medellín</p> | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 5 de 25 |

4. Relación de procesos y estructura organizacional

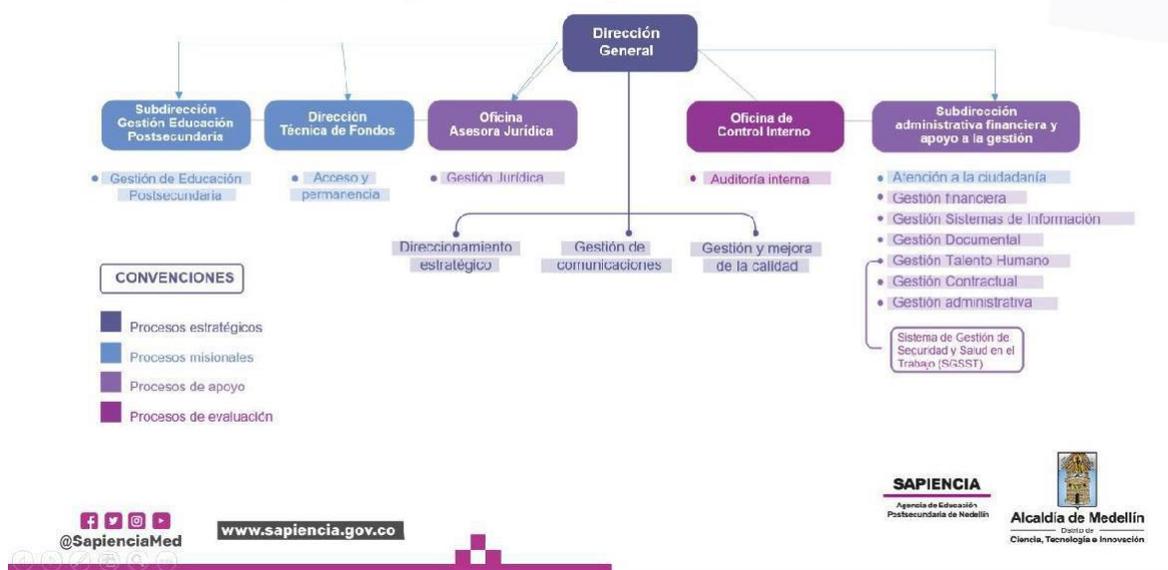


Ilustración 1 – Relación de Procesos del AGENCIA DE EDUCACION POSTSECUNDARIA DE MEDELLIN

4. Marco normativo

| NORMAS Y DOCUMENTOS DE REFERENCIA | | |
|------------------------------------|------|--|
| Norma | Año | Descripción |
| Constitución Política | 1991 | Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a |
| Plan Nacional de Desarrollo | | Ley 1712 de 2014 Decreto 1083 de 2015 Decreto 2482 de 2012 |
| MINTIC - Gobierno Digital | | Ley 1273 de 2009 Ley 1341 de 2009 Ley 1437 de 2011 Ley 1581 de 2012 Ley 1712 de 2014 Decreto Ley 019 de 2012 Decreto 415 de 2016 Ley 2080 de 2021 Decreto 2573 de 2014 Decreto 1078 de 2015 Decreto 1008 de 2018 |

| | | |
|---|---------------------|---|
|  <p>Alcaldía de Medellín Oficina de Ciencia, Tecnología e Innovación</p> <p>SAPIENCIA Agencia de Educación Postsecundaria de Medellín</p> | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 6 de 25 |

| | | |
|-------------------------------------|------|--|
| Ley 527 | 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”. |
| Decreto 1151 | 2008 | Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones |
| Ley 1341 | 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. |
| Ley 1273 | 2009 | Por 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. |
| Directiva Presidencial No.09 | 2010 | Directrices para la elaboración y articulación de los planes estratégicos sectoriales e institucionales e implementación del Sistema de Monitoreo de Gestión y Resultados |
| Directiva Presidencial No.04 | 2012 | Eficiencia administrativa y lineamientos de la Política de Cero papel en la Administración Pública. |
| Decreto 2693 | 2012 | Establece los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011. |
| Decreto Nacional 1377 | 2013 | Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales. |
| Ley 1712 | 2014 | Ley de transparencia y de acceso a la información pública nacional. |
| Decreto Nacional 2573 | 2014 | Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. |

| | | |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 7 de 25 |

| | | |
|-------------------------|------|--|
| Decreto 1078 | 2015 | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones |
| Decreto 103 | 2015 | Por el cual se reglamenta parcialmente la Ley 1712 de 2014 en lo relativo a la gestión de la información pública y se dictan otras disposiciones. |
| Resolución 3564 | 2015 | Reglamenta algunos artículos y párrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados). |
| Decreto 415 | 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 |
| Resolución 2405 | 2016 | Adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su comité |
| Decreto 728 | 2016 | Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico |
| Decreto 1413 | 2017 | Actualiza el Decreto Único Reglamentario del sector de las TIC, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales |
| Decreto 1008 | 2018 | Establece los lineamientos generales de la política de Gobierno Digital y actualizando el Decreto Único Reglamentario del sector de las TIC. |
| Doc. CONPES 3920 | 2018 | Política nacional de explotación de datos -BIG DATA. |
| Doc. CONPES 3975 | 2019 | Política Nacional para la transformación digital e Inteligencia Artificial. |
| Directiva 02 | 2019 | Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones |
| Ley 1955 | 2019 | Simplificación de interacción digital los ciudadanos y el Estado. |

| | | |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 8 de 25 |

| | | |
|--------------------|------|---|
| Ley 1978 | 2019 | Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones. |
| Decreto 620 | 2020 | Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales |

5. Justificación

El Plan de Seguridad y Privacidad tiene como objetivo convertir a la Agencia de Educación Postsecundaria de la Alcaldía de Medellín en un referente en la construcción de un Estado más eficiente, transparente y participativo. Esto se busca lograr mediante la implementación del MSPI, asegurando su alineación con lo estipulado en el Plan de Desarrollo, y contribuyendo a los pactos de legalidad, equidad y otros compromisos institucionales. Asimismo, se ajusta a los lineamientos del componente de seguridad y privacidad de la información establecidos en la estrategia de Gobierno Digital, además de incorporar las directrices propuestas en los Conpes de Ciberseguridad, Ciberdefensa, Seguridad Digital y Transformación Digital.

6. Política General de Seguridad y Privacidad de la Información.

“Mediante esta política la Agencia De Educación Postsecundaria de La Alcaldía de Medellín reconoce la información como un activo fundamental que se debe proteger adecuadamente para el desarrollo de las actividades de la Entidad, en donde la privacidad y seguridad de esta información y el conocimiento generado tiene una importancia primordial en el cumplimiento de su Plan estratégico Institucional vigente. La Dirección se compromete y es responsable de la gestión, ante el establecimiento, implementación, operación, seguimiento, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información – MSPI – de la AGENCIA DE EDUCACIÓN POSTSECUNDARIA DE MEDELLÍN, asignando y comunicando las funciones, responsabilidades y recursos necesarios para que la

| | | |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 9 de 25 |

Seguridad y Privacidad de la Información se integre a todos los procesos de la Entidad.”

6.1. Objetivos Específicos Política General De Seguridad Y Privacidad de la Información

Esta política establece una serie de objetivos que regulan las actividades relacionadas con la Seguridad y Privacidad de la Información en la Entidad, como son:

- Garantizar lineamientos y directrices formales para la actuación en temas de seguridad y privacidad de la información.
- Definir, gestionar y mantener roles y responsabilidades que respalden la gestión del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Asegurar la actualización continua de las políticas y procedimientos asociados a la seguridad y privacidad de la información.
- Proteger los datos y activos de información de la Agencia de Educación Postsecundaria de la Alcaldía de Medellín durante todo su ciclo de vida, mediante la aplicación de buenas prácticas y controles efectivos que garanticen la confidencialidad, integridad y disponibilidad.
- Cumplir con todas las obligaciones legales, regulatorias y contractuales relacionadas con la seguridad y privacidad de la información.
- Ofrecer una respuesta oportuna y efectiva ante eventos que puedan impactar los recursos esenciales para las actividades de la entidad, incluyendo personas, infraestructura, tecnología e información.
- Asegurar la continuidad de la seguridad de la información frente a situaciones adversas.
- Identificar, evaluar y gestionar los riesgos más críticos en materia de seguridad de la información, minimizando su impacto potencial.
- Implementar una gestión eficiente de incidentes y vulnerabilidades, mitigando su alcance, impacto y duración.
- Promover el fortalecimiento del conocimiento y la sensibilización sobre seguridad y privacidad de la información entre el personal de la entidad, incluyendo contratistas, aprendices y practicantes.

| | | |
|---|---------------------|---|
|  <p>Alcaldía de Medellín Oficina de Ciencia, Tecnología e Innovación</p> <p>SAPIENCIA Agencia de Educación Postsecundaria de Medellín</p> | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 10 de 25 |

- Garantizar la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), logrando el nivel de madurez necesario para satisfacer las demandas institucionales y regulatorias.

7. Alineación Estratégica

Es a partir de los Proyectos del PETI, que el Modelo de Seguridad y Privacidad de la Información que se enmarca y articula a la estrategia institucional con la estrategia de Seguridad y Privacidad.

| Código | Descripción |
|-------------|---|
| RI1 | Renovación Planta Telefónica |
| RI2 | Renovación y actualización de la infraestructura red de datos y nube Privada reduciendo los costos y aumentando la eficiencia en la nube |
| RA3 | Automatización de los procesos de la agencia como ERP |
| RI4 | Implementación de un sistema de código de barras para identificar y monitorear activos tangibles de la agencia |
| RA5 | Implementación de BI en los procesos de desarrollo |
| RN6 | Implementación de un sistema de gestión documental |
| RN7 | Implementación certificada de firmas digitales |
| RN8 | Programas de Continuidad de Negocio |
| RI9 | Renovación y actualización de los centros de computo |
| RI10 | Pruebas de seguridad aplicaciones para la implementación de protocolos de Seguridad de la Agencia (SSL) / Infraestructura Tecnológica y Base de Datos |
| RN11 | Diseño e implementación de metodologías para el análisis, valoración de Riesgos de TI e Implementación de herramientas para su gestión |
| RN12 | Implementar un sistema de gestión de calidad y un sistema de gestión de proyectos |
| RN13 | Implementación y adopción de herramienta Helpdesk |
| RI14 | Análisis de vulnerabilidad de la infraestructura informática y pruebas de intrusión |
| RI15 | Plan de mejoramiento de ISO/IEC 27001 |

| | | |
|---|---|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 11 de 25 |
| RN16 | Implementación Sistema de Gestión de la Seguridad de la Información | |
| RA17 | Implantación cultura DEVOPS para la línea de desarrollo de TI (Cadena de herramientas, automatización de lanzamientos, virtualización de servicios y gestión de rendimiento de aplicaciones, microservicios y contenedores) | |

8. Modelo Seguridad y Privacidad de la Información

El Modelo de Seguridad y Privacidad es un lineamiento publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, este es entregado a las entidades del Estado colombiano con el fin de que su adopción permita estar acorde con las buenas prácticas de seguridad y privacidad de la información, basado en norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para una correcta gestión de la información.

8.1. Plan de Implementación del Modelo de Seguridad Y Privacidad de La Información.

Esta fase dará paso a que la Agencia De Educación Postsecundaria de la Alcaldía de Medellín lleve a cabo la implementación de los requisitos base presentados del Modelo de Seguridad y privacidad de la información – MSPI y la norma ISO/IEC 27001, de la misma forma llegar a la implementación de los controles, que por normativa o por resultado de la identificación de riesgos deban ser implementados.

Dentro de la estrategia de la Entidad se encuentra la definición de los propósitos de seguridad y privacidad de la información, y por ende se definirán e implementarán políticas y directrices que guíen las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad.

Para esta fase de implementación la Agencia De Educación Postsecundaria de la Alcaldía de Medellín ha realizado contratos con diferentes entidades con el fin de iniciar varias actividades en torno a la implementación del MSPI, implementación de las políticas de Gobierno Digital y Transformación Digital.

| | | |
|---|---------------------|---|
|  <p>Alcaldía de Medellín Oficina de Ciencia, Tecnología e Innovación</p> <p>SAPIENCIA Agencia de Educación Postsecundaria de Medellín</p> | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 12 de 25 |

Estas actividades que se encuentran en desarrollo permiten que la Agencia De Educación Postsecundaria de la Alcaldía de Medellín empiece a tener análisis y gestión sobre los siguientes temas en el marco de seguridad: gestión de activos, gestión de comunicaciones y operaciones, gestión de recursos humanos, gestión de terceros, gestión de seguridad física, gestión de la continuidad de negocio, control de acceso lógico, cumplimiento regulatorio estrategia de seguridad en aplicaciones, estrategia de seguridad de datos y estrategia de seguridad tecnológica.

A continuación, se listan las actividades que la Agencia De Educación Postsecundaria de la Alcaldía de Medellín debe iniciar y documentar dentro de la esta fase.

| PRUEBA | ACTIVIDADES A DESARROLLAR | RESPONSABLE | FECHA INICIO | FECHA DE FIN |
|---|---|-------------------------------|--------------|--------------|
| a) utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios; | Elaborar y formalizar los procedimientos | Tecnologías de la información | 15/01/2025 | 30/12/2027 |
| b) separar los programas utilitarios del software de aplicaciones; | Generar directrices sobre el uso de programas utilitarios | Tecnologías de la información | 18/01/2025 | 30/12/2027 |

| | | | | |
|---|---|-------------------------------|------------|------------|
| c) limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados; | Generar directrices sobre el uso de programas utilitarios | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| d) autorizar el uso adhoc de programas utilitarios; | Generar directrices sobre el uso de programas utilitarios | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| e) limitar la disponibilidad de los programas utilitarios; | Generar directrices sobre el uso de programas utilitarios | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| f) registrar el uso de los programas utilitarios; | Generar directrices sobre el uso de programas utilitarios | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| g) definir y documentar los niveles de autorización para los programas utilitarios; | Generar directrices sobre el uso de programas utilitarios | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| h) retirar o deshabilitar todos los programas utilitarios innecesarios; | Generar directrices sobre el uso de programas utilitarios | Tecnologías de la información | 18/01/2025 | 30/12/2027 |

| | | | | |
|---|--|--------------------------------------|-------------------|-------------------|
| <p>i) No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.</p> | <p>Generar directrices sobre el uso de programas utilitarios</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>Revisar las siguientes directrices del proceso de borrado de discos y de encriptación del disco (para evitar la divulgación de la información confidencial cuando se dispone del equipo o se le da un destino diferente, siempre y cuando):</p> | <p>Generar directrices para la disposición o reutilización segura de los equipos</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>a) establecer que el proceso de encriptación sea suficientemente fuerte y abarque todo el disco (incluido el espacio perdido, archivos temporales de intercambio, etc.);</p> | <p>Generar directrices para el borrado de discos</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |

| | | | | |
|---|---|--------------------------------------|-------------------|-------------------|
| <p>b) definir que las llaves de encriptación sean lo suficientemente largas para resistir ataques de fuerza bruta;</p> | <p>Generar directrices de manejo del proceso de encriptación</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>c) establecer que las llaves de encriptación se mantengan confidenciales.</p> | <p>Publicar y Socializar directrices</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>Revisar se deberían sincronizar con una única fuente de referencia de tiempo Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.</p> | <p>Generar procedimiento para la sincronización de relojes con la hora legal colombiana</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |

Revisar se deberían sincronizar con una única fuente de referencia de tiempo. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se

Llevar a cabo la sincronización de todos los relojes

Tecnologías de la información

18/01/2025

30/12/2027

deberían sincronizar con una única fuente de referencia de tiempo.

Revisar se deberían sincronizar con una única fuente de referencia de tiempo. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.

Generar documentación soporte

Tecnologías de la información

18/01/2025

30/12/2027

| | | | | |
|---|--|--------------------------------------|-------------------|-------------------|
| <p>a) actualizar el software operacional, aplicaciones y bibliotecas de programas solo la debe llevar a cabo administradores entrenados, con autorización apropiada de la dirección;</p> | <p>Generar procedimiento para el control de la instalación de software en sistemas operativos.</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>b) definir que los sistemas operacionales sólo debe contener códigos ejecutables aprobados, no el código de desarrollo o compiladores;</p> | <p>Establecer controles para la instalación de software en sistemas operativos</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |

c) establecer que las aplicaciones y el software del sistema operativo solo se debe implementar después de pruebas extensas y exitosas; los ensayos deben abarcar la usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso, y se debe llevar a cabo en sistemas separados; se debe asegurar que todas las bibliotecas de fuentes de programas correspondientes hayan sido actualizadas;

Establecer que las aplicaciones y el software del sistema operativo solo se debe implementar después de pruebas extensas y exitosas

Tecnologías de la información

18/01/2025

30/12/2027

| | | | | |
|---|--|--------------------------------------|-------------------|-------------------|
| <p>d) usar un sistema de control de la configuración para mantener el control de todo el software implementado, al igual que la documentación del sistema;</p> | <p>Usar un sistema de control de la configuración para mantener el control de todo el software implementado</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>e) establecer una estrategia de retroceso (rollback) antes de implementar los cambios;</p> | <p>Establecer una estrategia de retroceso (rollback) antes de implementar los cambios;</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>f) mantener un log de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales;</p> | <p>Mantener un log de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales;</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>g) definir las versiones anteriores del software de aplicación se deben conservar como una medida de contingencia;</p> | <p>Definir las versiones anteriores del software de aplicación se deben conservar como una medida de contingencia;</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |

| | | | | |
|--|--|--------------------------------------|-------------------|-------------------|
| <p>h) establecer que las versiones de software anteriores se deben llevar al archivo permanente, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores, en tanto los datos permanezcan en el archivo permanente.</p> | <p>Establecer que las versiones de software anteriores se deben llevar al archivo permanente, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores, en tanto los datos permanezcan en el archivo permanente.</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>a) establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo;</p> | <p>Definir políticas de transferencia de información</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>b) definir los procedimientos para asegurar trazabilidad y no repudio;</p> | <p>Generar el procedimiento para la transferencia de información</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |
| <p>c) definir los estándares técnicos mínimos para</p> | <p>Definir los estándares técnicos mínimos para</p> | <p>Tecnologías de la información</p> | <p>18/01/2025</p> | <p>30/12/2027</p> |

| | | | | |
|--|--|-------------------------------|------------|------------|
| empaquetado y transmisión; | empaquetado y transmisión; | | | |
| d) tener certificados de depósito de títulos en garantía; | Tener certificados de depósito de títulos en garantía; | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| e) establecer los estándares de identificación de mensajería; | Establecer los estándares de identificación de mensajería; | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| f) definir las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos; | Definir las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| g) establecer el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entienda de inmediato, y que la información está protegida apropiadamente ; | Establecer el uso de un sistema de etiquetado acordado para información sensible o crítica | Tecnologías de la información | 18/01/2025 | 30/12/2027 |

| | | |
|---|---------------------|---|
|  <p>Alcaldía de Medellín Oficina de Ciencia, Tecnología e Innovación</p> <p>SAPIENCIA Agencia de Educación Postsecundaria de Medellín</p> | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 22 de 25 |

| | | | | |
|--|--|-------------------------------|------------|------------|
| h) definir las normas técnicas para registro y lectura de información y software; | Definir las normas técnicas para registro y lectura de información y software; | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| j) mantener una cadena de custodia para la información mientras está en tránsito; | Mantener una cadena de custodia para la información mientras está en tránsito; | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| k) definir los niveles aceptables de control de acceso. | Definir los niveles aceptables de control de acceso. | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| a) definir la cadena de custodia; b) establecer la seguridad de la evidencia; c) definir la seguridad del personal; d) definir los roles y responsabilidades del personal involucrado; e) establecer la competencia del personal; | Revisar y adecuar el procedimiento existente para incluir lo relacionado con recolección de evidencias | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| a) Restricciones de acceso que soportan los requisitos de protección para | Revisar y actualizar Soporte de entrega y devolución de | Tecnologías de la información | 18/01/2025 | 30/12/2027 |

| | | |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 23 de 25 |

| | | | | |
|--|--|-------------------------------|------------|------------|
| cada nivel de clasificación; | equipos de cómputo – F-AP-SI-014 para incluir los incisos indicados en la columna Prueba | | | |
| b) Registro formal de los receptores autorizados de los activos; | Registro formal de los receptores autorizados de los activos; | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| c) Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original; | Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original; | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| d) Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes; | Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes; | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
| e) Marcado claro de todas las copias de medios para la atención del receptor autorizado. | Marcado claro de todas las copias de medios para la atención del receptor autorizado. | Tecnologías de la información | 18/01/2025 | 30/12/2027 |

| | | |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
| | | Versión: consecutivo en que va el documento (01) |
| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | | Página 24 de 25 |

| | | | | |
|---|---|-------------------------------|------------|------------|
| f) De acuerdo a NIST la información almacenada (at rest) y en tránsito debe ser protegida. | De acuerdo a NIST la información almacenada (at rest) y en tránsito debe ser protegida. | Tecnologías de la información | 18/01/2025 | 30/12/2027 |
|---|---|-------------------------------|------------|------------|

9. Proyectos de Inversión

Actualmente la Agencia De Educación Postsecundaria De La Alcaldía De Medellín cuenta con su Plan Anual de adquisiciones:

<https://sapiencia.gov.co/plan-anual-de-adquisiciones/>

Adicionalmente para llevar a cabo las actividades descritas anteriormente y que están relacionadas con el cierre de brechas del MSPI, se han considerado los siguientes proyectos generales:

| Nombre Iniciativa | Descripción | Área Líder |
|---------------------|--|-------------------------|
| Proyecto TIC | El proyecto TIC es un proyecto nuclear y estratégico de la Entidad que pretende modernizar, sistematizar y automatizar las tecnologías y la operación del área de tecnologías de la información brindando un servicio, eficaz, eficiente y oportuno a sus usuarios. Este proyecto cubre necesidades y demandas para (entre otras): computación en la nube; renovación tecnológica; gestión de la mesa de ayuda; soporte y apoyo para la operación de TI. | Sistemas de información |

| | | |
|--|--|---------------------------------|
| <p>Desarrollo de la Política de Gobierno Digital Fase I</p> | <p>Este proyecto pretende favorecer el desarrollo de la Política de Gobierno Digital en la Entidad, teniendo en cuenta:</p> <p>Los habilitadores de arquitectura, seguridad y servicios ciudadanos digitales.</p> <p>La atención de los propósitos establecidos en la Política.</p> <p>El desarrollo del PETI 2024 – 2027 para la Entidad.</p> | <p>Sistemas de información</p> |
| <p>Gobierno de Datos</p> | <p>Buscar institucionalizar una política de gobernanza de datos AGENCIA DE EDUCACIÓN POSTSECUNDARIA DE MEDELLÍN, para la adecuada planeación y gobierno de los componentes de información: datos, información, servicios de información y flujos de información,</p> | <p>Sistemas de Información.</p> |
| <p>Gobernanza para la transformación Digital</p> | <p>Fortalecer la Gobernanza para la transformación Digital a fin de proveer la base arquitectónica que soporte aplicaciones de datos que permitan el uso y aprovechamiento de datos.</p> | <p>Sistemas de información</p> |
| <p>Big Data y ciencia de datos</p> | <p>Construir aplicaciones basadas en Big Data y Ciencias de datos que permitan avanzar en la transformación digital de la entidad y en el ofrecimiento de nuevos servicios a los grupos de interés</p> | <p>Sistemas de información</p> |