RESOLUCIÓN N° 3883
Diciembre 21 de 2023

"POR LA CUAL SE ADOPTA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL DE LA AGENCIA DE EDUCACIÓN POSTSECUNDARIA DE MEDELLÍN-SAPIENCIA"

La Directora General (E), de la Agencia de Educación Postsecundaria de Medellín-SAPIENCIA, mediante Resolución de encargo No. 202350097127, del 30/11/2023 y acta de posesión 400 de 6/12/2023, expedida por la Alcaldía de Medellín, en uso de sus facultades legales y en especial las que le confiere la Ley 80 de 1993, la Ley 1150 de 2007, la Ley 1882 de 2018, el Decreto Único Reglamentario 1082 de 2015 y demás decretos reglamentarios y normas estatutarias contenidas en el Decreto Municipal 1364 de 2012, modificado por el Acuerdo Municipal 019 de 2020 y el numeral 18 del artículo 18 del Acuerdo Directivo 003 del 2013, modificado por el artículo décimo primero del Acuerdo Directivo 29 de 2021, Estatuto General de Sapiencia, a partir del cual le corresponde a la Directora General (E) realizar las operaciones necesarias y celebrar los contratos, acuerdos y convenios que requieran para asegurar el cumplimiento de los objetivos y funciones de la Agencia de Educación Postsecundaria de Medellín - Sapiencia y,

CONSIDERANDO QUE:

1. El artículo 113 de la Constitución Política señala que los órganos del poder público deben colaborar armónicamente para el cumplimiento de los, fines del Estado.

2. El Decreto 1083 de 2015 reglamentó el Sistema de Gestión y actualizó el Modelo Integrado de Planeación y Gestión, permitiendo el fortalecimiento de los mecanismos, métodos y procedimientos de gestión y control al interior de los organismos y entidades del Estado.

3. El artículo 2.2.22.3.1 del Decreto 1083 de 2015 adoptó la versión actualizada del Modelo Integrado de Planeación y Gestión (MIPG) con el fin de lograr el funcionamiento del Sistema de Gestión y su articulación con el Sistema de Control Interno.

4. El Modelo Integrado de Planeación y Gestión (MIPG) es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y de los organismos públicos, dirigido a generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, en los términos del artículo 2.2.22.3.2. del Decreto 1083 de 2015.

5. El Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, modificado por el Decreto 1499 de 2017, desarrolló el Sistema de Gestión, creado en el artículo 133 de la Ley 1753 de 2015, el cual integró los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad.

6. El Decreto 1083 de 2015, modificado por el Decreto 1499 de 2017, creó el Consejo y/o comité para la Gestión y el Desempeño Institucional integrado por las entidades y organismos que, por su misión, tienen a cargo funciones transversales de gestión y desempeño a nivel nacional y territorial, instancia a la cual le corresponde, entre otras funciones, proponer políticas, normas, herramientas, métodos y procedimientos en materia de gestión y desempeño institucional, presentar al Gobierno Nacional recomendaciones para la adopción de políticas, estrategias o acciones para mejorar la gestión y el desempeño institucional de las entidades y organismos del Estado y proponer estrategias para la debida operación del Modelo Integrado de Planeación y Gestión (MIPG).

7. El Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), a través de la Dirección de Gobierno Digital, presentó la política de Gobierno Digital -expresada en el Decreto 1263 del 22 de julio de 2022-, cuyo objetivo es establecer lineamientos y estándares para la Transformación Digital de la Administración Pública en el marco de la Política Digital.

8. Tal política determinada como una estrategia, en virtud de un desarrollo de mejoras en la gestión de las entidades, en una calidad de servicios y tramites vinculados en un entorno digital, denotando la gran necesidad de que las organizaciones apropien y generen una transversalidad soportado en las TI como eje transformador de los procesos, procedimientos y actividades propias que buscan unos servicios innovadores que beneficien a la ciudadanía en términos de transparencia, confianza y calidad como valores agregados a la operatividad de las mismas a raíz de esta descripción, se puede determinar la fundamentación para la consolidación del proyecto, donde se logra evidenciar la necesidad y la importancia para el gobierno distrital en la implementación de la arquitectura empresarial donde se focaliza dominio de Gobierno de TI y que aportaría al cumplimiento de los indicadores y metas definidas.

9. El Decreto Presidencial 767 de 2022: “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”. Definió cinco elementos para la implementación de la política de gobierno digital como son: Gobernanza, innovación, política digital. Habilitadores, líneas de acción e iniciativas dinamizadoras.

10. La Resolución Ministerial 00500 de 2021: estableció 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.

11. El numeral 8° del artículo 2° de la Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC-, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones", establece como principio orientador la Masificación del Gobierno en Línea (hoy Gobierno Digital), según el cual las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las

Comunicaciones (TIC) en el desarrollo de sus funciones, para lo cual el Gobierno Nacional fijará los mecanismos y condiciones que garanticen el desarrollo de este principio. Asimismo, el artículo 4 ibídem establece que el Estado intervendrá en el sector TIC, entre otros, para promover su acceso, teniendo como fin último el servicio universal; así como para promover el desarrollo de contenidos y aplicaciones, la prestación de servicios que usen TIC y promover la seguridad informática y de redes para desarrollarlas.

12. El artículo 64 de la Ley 1437 de 2011 "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo", faculta al Gobierno Nacional para definir los estándares y protocolos que deberán cumplir las autoridades para incorporar en forma gradual los medios electrónicos en los procedimientos administrativos. Que, de conformidad con el artículo 230 de la Ley 1450 de 2011 "Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014", modificado por el artículo 148 de la Ley 1955 de 2019 "Por la cual se expide el Plan Nacional de Desarrollo, 2018-2022 "Pacto por Colombia, pacto por la equidad', y en concordancia con el numeral 11 del artículo 2.2.22.2.1 del Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", la Política de Gobierno Digital es una Política de Gestión y Desempeño Institucional, por lo cual todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional, a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) como líder de esta Política, para su implementación.

13. La Ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales, establece en el Art. 2° el ámbito de aplicación de la Ley, dentro del cual se encuentran las entidades de naturaleza pública, que realicen el tratamiento de datos personales en el territorio colombiano.

14. El literal a) del artículo 5° de la Ley Estatutaria 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", establece que son sujetos obligados a la aplicación de la misma toda entidad pública, incluyendo las pertenecientes a todas las Ramas del Poder Público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en los órdenes nacional, departamental, municipal y distrital.

15. Así mismo establece en el parágrafo tercero del artículo 9 que sus sujetos obligados deberán dar cumplimiento a la estrategia de Gobierno en Línea, o la que haga sus veces, en cuanto a la publicación y divulgación de la información.

16. El Decreto Presidencial 767 de 2022: “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”. Definió cinco elementos para la implementación de la política de gobierno digital como son: Gobernanza, innovación, política digital. Habilitadores, líneas de acción e iniciativas dinamizadoras.

17. La Resolución Ministerial 00500 de 2021: Estableció 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.

18. El artículo 143 de la Ley 2294 de 2023, Plan Nacional de Desarrollo 2022 - 2026, define las medidas que orientaran el diseño y la implementación de la estrategia integral para democratizar las TIC y desarrollar la sociedad del conocimiento y la tecnología del país.

19. El artículo 148 de la Ley 1955 de 2019, modificó el artículo 230 de la Ley 1450 de 2011, en el sentido de establecer que la Política de Gobierno Digital es una Política de Gestión y Desempeño Institucional, la cual es liderada por el MinTIC y, en este sentido, todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través de dicha Cartera para su cumplimiento.

20. MinTIC a través del Decreto 415 de 2016, estableció los lineamientos en materia de TIC para el fortalecimiento institucional de las entidades territoriales, por esto, existe la necesidad de la implementación de un modelo de gobierno corporativo de Tecnologías de la Información para la Agencia de Educación Postsecundaria de Medellín, que determine el cumplimiento de las políticas y estrategias de orden nacional (Modelo Integrado de Planeación y Gestión MIPG, Modelo de Seguridad y Privacidad de la Información MSPI, Gobierno Digital y Arquitectura AE), dentro de las cuales, se focaliza el dominio de Gobierno TI, que permite alinear los procesos estratégicos de la organización con las Tecnologías de la información. Donde el apoyo del nivel directivo, control interno de gestión y el líder de Gestión Tecnológica; comprendan, apoyen y respalden este modelo de tal forma que se generen cadenas de valor orientadas al servicio y calidad de la información que forja la entidad.

21. El Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), a través de la Dirección de Gobierno Digital, presentó la política de Gobierno Digital -expresada en el Decreto 1263 del 22 de julio de 2022-, cuyo objetivo es establecer lineamientos y estándares para la Transformación Digital de la Administración Pública en el marco de la Política Digital.

22. Tal política determinada como una estrategia, en virtud de un desarrollo de mejoras en la gestión de las entidades, en una calidad de servicios y tramites vinculados en un entorno digital, denotando la gran necesidad de que las organizaciones apropien y generen una transversalidad soportado en las TI como eje transformador de los procesos, procedimientos y actividades propias que buscan unos servicios innovadores que beneficien a la ciudadanía en términos de transparencia, confianza y calidad como valores agregados a la operatividad de las mismas a raíz de esta descripción, se puede determinar la fundamentación para la consolidación del proyecto, donde se logra evidenciar la necesidad y la importancia para el gobierno distrital en la implementación de la arquitectura empresarial donde se focaliza dominio de Gobierno de TI y que aportaría al cumplimiento de los indicadores y metas definidas en el plan de desarrollo Medellín Futuro.

23. El Distrito de Ciencia, Tecnología e Innovación de Medellín, con el plan de desarrollo "Medellín Futuro" vigencia 2020-2023, en el cual, focaliza nuevamente la importancia y necesidad de establecer una transformación que le permita dinamizar y optimizar los procesos y servicios que le den una calidad y eficiente gestión administrativa; dentro del plan en su "Propuesta estratégica 9. Industria, innovación e infraestructura" define lo siguiente: "La construcción de la Medellín Futuro requiere la transformación del sistema educativo, avanzando en el desarrollo de contenidos pertinentes y de calidad, modernizando los proyectos educativos institucionales, fortaleciendo la formación en nuevas tecnologías, la integración multidisciplinar e investigación dirigida hacia el Ser+ STEM y la Cuarta Revolución Industrial, liderando una transformación curricular que posibilite consolidar al municipio de Medellín como el Valle del Software." (Alcaldía de Medellín, 2020). Es decir, que vincula de una forma necesaria y estratégica un uso y apropiación de Tecnologías de la información, para brindar una mejor calidad de servicios y procesos propios de la organización, con un enfoque hacia la educación de la ciudad.

24. Por lo anterior, se hace necesario adoptar la política de Seguridad Digital en la Agencia de Educación Postsecundaria de Medellín.

En mérito de lo expuesto, la Directora General (E) de la Agencia de Educación Postsecundaria de Medellín – Sapiencia,

RESUELVE:

ARTÍCULO PRIMERO: Adoptar la Política de Seguridad Digital en la Agencia de Educación Postsecundaria de Medellín - Sapiencia.

ARTÍCULO SEGUNDO: DEFINICIONES DE LA POLÍTICA. Se adoptarán para efectos de la presente política las siguientes siglas y definiciones, aplicables a la política:

International Standard Organización (ISO), (Fuente: Wikipedia)

Ministerio de Tecnología de la Información y las Comunicaciones (**MINTIC)** (Fuente: colombiatic)

Modelo de Seguridad y Privacidad de la Información (MSPI), Fuente: MinTic.

Sistema de Gestión de Seguridad de la Información (SGSI), (Fuente: gobiernodigital)

Plan Estratégico de Tecnologías de la Información (PETI), (Fuente: MINTIC)

Recovery Point Objective (RPO), Punto de recuperación objetivo. (Fuente: acronis)

Sistema de Gestión de Seguridad de la Información (SGSI), (Fuente: MINTIC)

Tecnología de información y las Comunicaciones (TIC), (Fuente: elaboración propia de Sapiencia)

Tecnologías de la información y la comunicación (TIC), (Fuente: elaboración propia de Sapiencia)

Ciber-riesgo o riesgo cibernético: posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos. (Fuente: ciber-riesgo)

Ciberseguridad: es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad. (Fuente: kasperski)

Cifrado: es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. (Fuente: cifrado)

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. (Fuente: confidencialidad)

Contingencia: se define como el conjunto de acciones y recursos para responder de la manera más óptima y eficaz a las fallas e interrupciones específicas que se puedan presentar en algún proceso. (Fuente: elaboración propia de Sapiencia)

Control de acceso: el proceso que limita y controla el acceso a los recursos de un sistema computarizado; un control físico o lógico diseñado para proteger contra usos o entradas no autorizadas. El control de acceso puede ser definido por el sistema (mandatory access control – MAC), o definido por el usuario propietario del objeto (discretionary access control – DAC). (Fuente: control de acceso)

Criptografía: el objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad. (Fuente: criptografía)

Encriptación (Cifrado, codificación): la encriptación es el proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc. (Fuente: Encriptación)

Firewall (Muro de Fuego - Cortafuego): herramienta de seguridad que controla el tráfico de entrada/salida de una red. (Fuente: firewall)

Hacking - Hackear: es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar. (Fuente: hackear)

Incidente de Seguridad: evento único o serie de eventos de seguridad de la información inesperados o no deseado que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (Fuente: iso27001)

Disponibilidad: propiedad de ser accesible y utilizable sobre demanda por una Entidad autorizada. (Fuente: disponibilidad)

Hardware: es un término genérico para hacer referencia a todos los componentes de Tecnología físicos (Redes, servidores, computadores, Portátiles, etc.) (Fuente: elaboración propia de Sapiencia)

Seguridad de la Información: son todas aquellas medidas preventivas de los sistemas de información que permitan resguardar y proteger la información. (Fuente: elaboración propia de Sapiencia)

Requerimiento: es una solicitud ante una nueva necesidad que se requiere por algún solicitante de la Agencia. (Fuente: elaboración propia de Sapiencia)

Responsable de Seguridad de la Información: es la persona con la función de supervisar el cumplimiento de la presente Política (Fuente: elaboración propia de Sapiencia)

Sistema de Información: el sistema de información es el que se encarga de recopilar los datos necesarios para que el director del proyecto conozca si el proyecto lleva la dirección prevista. Sin embargo, esa información debe ser puntual, y uno de los problemas que tienen algunas organizaciones es que los datos sobre el proyecto son recogidos, introducidos en un ordenador central, procesados y distribuidos a intervalos tan largos de tiempo que la información resulta inútil a efectos de control. (Fuente: elaboración propia de Sapiencia)

Tecnología de la Información y Comunicación: se refiere al Hardware y Software que interviene en el procesamiento de la información. (Fuente: elaboración propia de Sapiencia)

Teletrabajo: es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo (Fuente: teletrabajo, Artículo 2, Ley 1221 de 2008).

Troyano: es un programa malicioso capaz de alojarse en un computador y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de apoderarse de la información (Fuente: Troyano)

Wireless: referido a las telecomunicaciones, se aplica el término inalámbrico (inglés Wireless - sin cables) al tipo de comunicación en la que no se utiliza un medio de propagación físico, sino que utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión. (Fuente: wireless)

ARTÍCULO TERCERO: OBJETIVO Y ALCANCE.

OBJETIVO: establecer los lineamientos necesarios para que se garantice la seguridad, integridad y disponibilidad de la información de la Agencia de Educación Postsecundaria de Medellín - Sapiencia, así como de las tecnologías empleadas en su procesamiento, es

esencial para protegerla contra amenazas tanto internas como externas, ya sean premeditadas o accidentales, cumpliendo así los estándares de la Seguridad de la Información.

ALCANCE: la Política Institucional de Seguridad Digital, se debe aplicar a los diferentes procesos y actividades que requieran la transferencia, uso o modificación de la información, estableciendo parámetros basados en los lineamientos definidos por MINTIC y la norma Internacional ISO 27001:2022, esta última, no es de obligatoria certificación, pero se acogen elementos como marco de referencia para la gestión de la Seguridad de la Información en la Agencia, cuya implementación será gradual, acorde con las condiciones y avances de la infraestructura tecnológica de la Agencia.

ARTÍCULO CUARTO: ROLES Y RESPONSABLES EN LA POLÍTICA. Con el objetivo de identificar claramente los roles para la implementación de la Política Institucional de Seguridad Digital, es de aplicación obligatoria para todo el personal de la Agencia como servidor(a) público y contratista, en el proceso al cual pertenezca y cualquiera sea el nivel de las funciones u obligaciones contractuales que desarrollen.

Todos los servidores públicos y contratistas, deben utilizar los activos de información institucionales para el desarrollo de las actividades, acogiendo lo establecido en el Manual de Política interna de Tratamiento y protección de datos personales, el aviso de privacidad y las Condiciones de Uso de la página web. De esta forma se preserva la confidencialidad de la información, que por razones de sus actividades o funciones estén bajo su custodia.

Rol o Cargo	Responsabilidad
Director(a) General	• Dar aprobación de la política de seguridad de la información. • Evaluar el proceso de gestión de la seguridad. • Facilitar los recursos requeridos para el proceso de Gestión de sistemas de información y poder dar cumplimiento a la política. • Definir que usuarios deberán de tener acceso a la información de acuerdo a sus funciones u obligaciones contractuales. • Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de estos. • Ejercer liderazgo y compromiso para la aplicación de la política de seguridad de la información.
Dirección General, Subdirecciones, Jefe de Oficina Asesora Jurídica, Jefe de Oficina de Control Interno. (Nivel Directivo)	• Tener a cargo el desarrollo inicial de la política de seguridad al interior de la entidad y velar por la aplicación de la misma. • Supervisar el monitoreo y avance general de la implementación de las estrategias de control y tratamiento de riesgo de información digital. • Gestionar con las otras dependencias de la Agencia para apoyar los objetivos de la seguridad.

	• Apoyar a diferentes procesos institucionales para la adopción del sistema de gestión de seguridad de la información. • Servir como enlace entre los responsables de seguridad de otras entidades y especialistas externos, con el fin de mantener actualizado en tendencias de normas y métodos de la seguridad de la información. • Mantener en contacto con los grupos especiales en materia de seguridad de la información para asegurar de que la información sea actualizada y este completa. Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas y vulnerabilidades. • Las demás que les competen como integrantes del Comité Institucional de Gestión y Desempeño de la Agencia.
Jefe de Oficina Asesora Jurídica	• Velar por el cumplimiento legal de la política de la seguridad de la información. • Asesorar en cuanto a lo legal, asociado a la seguridad de la información que permita cumplir con los requerimientos legales.
Visitantes, Proveedores, Grupos de valor y Partes interesadas.	• Cumplir con las políticas de seguridad de la información cuando se autorice el acceso a la información de la Agencia. • Utilizar únicamente los canales de acceso que se otorguen. • No interrumpir o deshabilitar los controles de seguridad dispuestos para la protección de los activos de la información.
Servidores públicos y Contratistas.	• Dar buen uso de los equipos de cómputo y periféricos que le sean asignados para el cumplimiento de sus funciones o actividades, la relación de los mismos debe estar registrada en el Sistema de Inventarios de la entidad. • Hacer entrega en buen estado de los equipos de cómputo y periféricos que le sean asignados, cuando se presente retiro de la entidad, cambio de funciones y/o actividades contractuales o culminación del contrato según sea el caso. • Custodiar la información alojada en el equipo de cómputo y periféricos asignados. • Cumplir las políticas de respaldo, custodia y recuperación de la información definidas por el proceso Gestión de Sistemas de Información. • Conectarse a la red con el usuario asignado y la respectiva clave de acceso. • Utilizar solamente software licenciado y autorizado por el proceso de Gestión de Sistemas de Información. En

	caso de requerir la instalación de software adicional, el director o jefe del área o dependencia debe realizar la solicitud por medio de la Sistema de mesa de servicio, con la debida justificación para revisión y a probación. • Facilitar, cuando lo requieran, la revisión del equipo de cómputo a nivel físico, software instalado e información alojada.
Proceso de Gestión de Sistemas de Información	• Administrar y custodiar los equipos de hardware y comunicaciones alojados en el centro de datos. • Gestionar los servicios de información y de tecnología alineados con los objetivos sectoriales e institucionales para el cumplimiento de su misión. • Custodiar la información almacenada en los sistemas de información, aplicaciones y bases de datos. • Disponer de las medidas de seguridad para proteger la información digital de Sapiencia. • Informar al Comité Institucional de Gestión y Desempeño de las novedades frente a la seguridad de la información que se presenten y la solución planteada; dejando registro de modo, tiempo y lugar de cada evento, considerando también que este comité tiene funciones de comité de gobierno digital. • Dar los lineamientos para la administración de los equipos de cómputo, dispositivos de almacenamiento externo, sistemas de información, aplicativos e infraestructura tecnológica física o lógica. • Realizar el monitoreo y control automático del software instalado en los equipos de cómputo de la Agencia. Si se encuentra instalado software no autorizado, se notificará al jefe inmediato y/o supervisor para que se informe el motivo de la irregularidad y se opte por la desinstalación del software garantizando con esto que se cumplen los lineamientos relacionados con el uso de software y derechos de autor.
Usuarios y/o productores de los activos de información.	• Deben propender por la seguridad y la calidad de la información en los criterios de confidencialidad, integridad, disponibilidad, efectividad, eficiencia, confiabilidad y cumplimiento • Deben aplicar las políticas y los controles de seguridad de la información definidos por la entidad para garantizar la preservación de la confidencialidad, integridad, disponibilidad de los activos de información institucionales. • Está prohibido utilizar los activos de información de la Agencia para fines diferentes al cumplimiento de las funciones asignadas u obligaciones contractuales. • Toda la información que genere, procese, almacene, transfiera o transmita la Agencia Postsecundaria de

	Medellín- Sapiencia ya sea en medios físicos o digitales, en su servicios tecnológicos, infraestructura tecnológica o activos de información es de su propiedad y solo puede ser utilizada para el cumplimiento de las funciones institucionales. • El responsable debe inventariar y actualizar de manera periódica dichos activos, custodiar la información y tener definidas y actualizadas las restricciones de acceso. • Los propietarios de los activos de información son responsables del uso y protección mientras estén en su custodia mediante archivo de gestión ya sea física o electrónica. Así mismo, son responsables de informar a los jefes inmediatos de cualquier incidente de seguridad que se pueda presentar, tales como: uso indebido, alteración y/o divulgación no autorizados. • Los activos de información digitales y físicos deben seguir los line amientos para la organización de documentos asociados al proceso de Gestión Documental de la Agencia, que tiene como fin orientar a los(as) funcionarios(as), aprendices y contratistas de la entidad, en todos los aspectos relacionados con la organización, manejo, control y servicios de los documentos que producen cada una de las dependencias en el cumplimiento de sus funciones. • Los propietarios de los activos de información son responsables de su uso y protección mientras estén en su custodia en archivo de gestión ya sea física o electrónica, de tal forma que se evite su modificación, pérdida y divulgación no autorizada, acorde a su valor, confidencialidad e importancia. • No está permitido que dependencias diferentes al proceso de Gestión de Sistemas de Información tengan a cargo equipos servidores o conecten a la red de la Agencia equipos de cómputo y servidores sin previa gestión ante el proceso con el fin de que se cumplan los lineamientos de seguridad y privacidad de la información.

ARTÍCULO QUINTO: LINEAMIENTOS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN. La política de seguridad de la información se articula con el Sistema de Gestión Documental Institucional para la identificación de los activos de información institucionales y la responsabilidad respecto la protección de la información y medidas de control para prevenir la materialización de riesgos de seguridad digital. Los activos de información están conformados por la información procesada por los sistemas de información, y se identifican acorde con los procesos definidos en el proceso Gestión Documental, la información se clasifica en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada, acorde con este, se establecen los niveles de protección.

Los inventarios de activos de información se actualizan periódicamente y se publican en la web institucional y en la página datos.gov.

La Agencia, basada en las guías proferidas por el MINTIC, acoge la implementación de la política, bajo dicho estándar, reconociendo que la misma debe hacerse de forma gradual, conforme avanzan las adecuaciones de la infraestructura tanto física, como lógica, que deben ser incorporados al Plan Estratégico de Tecnologías de la Información (PETI), conforme a la disponibilidad presupuestal, priorizada para fortalecer los sistemas de información. Entendiendo que se avanza en la trasformación tecnológica, que permitirá migrar a mejores condiciones, generando ambientes de control, cada vez más seguros.

ARTÍCULO SEXTO: POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Sapiencia, entiende la importancia de una adecuada gestión de la información, es por esto que, se compromete con la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y Agencia, todo enmarcado en el estricto cumplimiento de las normativas y en concordancia con la misión y visión de la entidad.

La Agencia de Educación Postsecundaria de Medellín - Sapiencia, busca la protección de la información, la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de valor identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, proveedores, terceros, y Agencia en general; teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones de la entidad.
- Cumplir con los principios de seguridad de la información (confidencialidad, integridad y disponibilidad).
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de Agencia, proveedores, funcionarios y contratistas.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, proveedores de Sapiencia.
- Garantizar la continuidad del negocio frente a incidentes.
- Sapiencia ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Para dar cumplimiento a los objetivos planteados dentro del marco de SGSI se desarrolló el Plan Estratégico de Tecnología de la Información (PETI), donde se establecen los lineamientos y desarrollo de las TIC, la política de gobierno digital donde se establece los

parámetros para la transformación digital con los principios de calidad de vida hacia Agencia, por medio de las ayudas de la transformación, la eficiencia, la transparencia y la sostenibilidad y demás políticas involucradas.

A continuación, se establecen los principios que soportan el SGSI de Sapiencia:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas, proveedores, o terceros.
- Sapiencia protegerá la información generada, procesada o resguardada por los procesos de la Agencia, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros.
- Sapiencia protegerá la información creada, procesada, transmitida o resguardada por sus procesos internos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Sapiencia protegerá la información de las amenazas originadas por parte del personal.
- Sapiencia protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Sapiencia controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Sapiencia implementará control de acceso a la información, sistemas y recursos de red.
- Sapiencia garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Sapiencia garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- Sapiencia garantizará la disponibilidad de sus procesos internos y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Sapiencia garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

ARTÍCULO SÉPTIMO: SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI. Sapiencia realizará revisiones periódicas al SGSI, dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por la Función Pública y evaluaciones del Índice de Desempeño Institucional (IDI) o la herramienta definida para tal fin.
- Aplicación de los autodiagnósticos que la Función Pública facilite en el marco del Modelo Integrado de Planeación y Gestión (MIPG).

ARTÍCULO OCTAVO: DESCRIPCIÓN DEL CICLO OPERACIONAL. A continuación, se habla sobre el ciclo operativo del modelo a través de una descripción detallada de cada una de las cinco (5) fases que componen el modelo. En este se contienen metas, objetivos y herramientas (pautas) para hacer de la seguridad y privacidad de la información un sistema sostenible en Sapiencia.

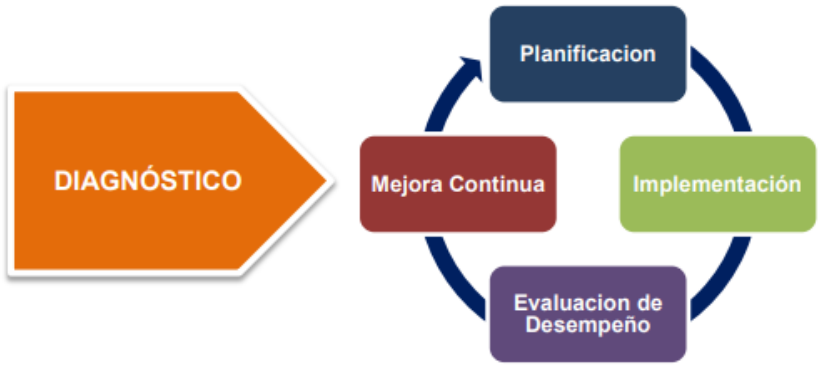

Imagen 1 – Ciclo de la operación del Modelo de seguridad y privacidad de la Información. MINTIC.[1]

FASE DE DIAGNÓSTICO: en esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad Digital.

Imagen 2. Diagnóstico

Durante la fase de diagnóstico del MSPI, se persiguen los siguientes objetivos:

- Determinar el estado actual de la gestión de la seguridad y privacidad de la información dentro de la entidad.

[1] Imagen extraída del portal: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- Identificar el nivel de madurez de los controles de seguridad de la información.
- Medir el avance de implementación del ciclo operativo dentro de la entidad.
- Determinar el nivel de cumplimiento de la legislación vigente en materia de protección de datos personales.
- Identificar el uso de buenas prácticas de ciberseguridad.

Para realizar esta fase, se debe recopilar información con la ayuda de herramientas de diagnóstico y métodos de prueba de validez, autodiagnósticos disponibles en plataforma MINTIC. Una vez obtenidos los resultados del diagnóstico inicial y determinado el nivel de madurez de la entidad, pasamos a la fase de planificación del desarrollo.

FASE DE PLANIFICACIÓN

Para desarrollar esta fase, la entidad deberá utilizar los resultados de la fase de diagnóstico y proceder a elaborar un plan de seguridad y privacidad de la información que sea consistente con los objetivos de la misión institucional, mediante un enfoque de gestión de riesgos en donde se establecen las acciones a implementar a nivel de seguridad y privacidad de la información.

El alcance de MSPI permite a las entidades definir restricciones que hagan cumplir la seguridad y la privacidad dentro de la entidad. Este enfoque se basa en gestión por procesos y debe extenderse a toda la entidad.

Para desarrollar el alcance y límites del modelo se deben establecer los siguientes parámetros: procesos, trámites y servicios, sistemas de información, ubicaciones físicas, partes interesadas relevantes e interrelaciones entre el modelo de privacidad y otros procesos que impactan directamente en el logro de la misión- objetivos.

A continuación, se ilustra el Modelo a seguir en la fase de planificación:

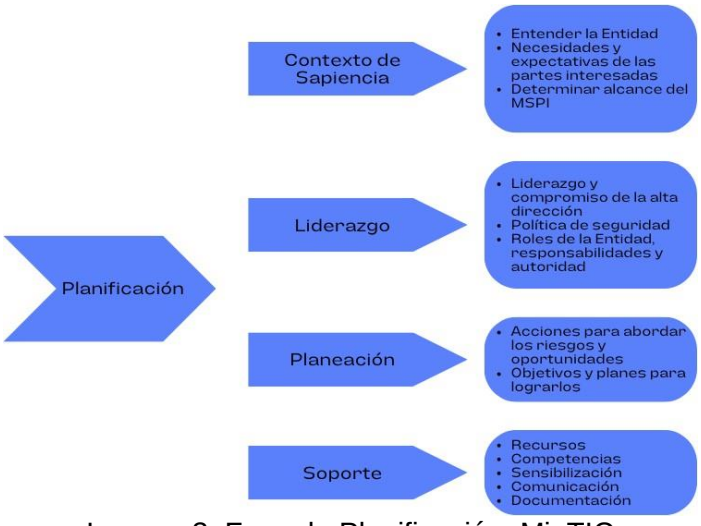

Imagen 3. Fase de Planificación. MinTIC

FASE DE IMPLEMENTACIÓN

La fase de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) es la etapa en la que ejecuta el plan definido, poniendo en práctica las medidas y controles a nivel de seguridad y privacidad que se definieron en la fase de planificación, las cuales se establecen considerando lo definido en las políticas vigentes relacionadas con el tratamiento y protección de datos, y las de privacidad y condiciones de uso de la página web. Esta fase integra las acciones definidas desde las diferentes políticas institucionales, dado que se debe tener una estrategia constante que permita y facilite el acceso transparente, el manejo responsable de la información y el cumplimiento normativo en materia de propiedad intelectual que se encuentre vigente, lo que es fundamental para garantizar que la entidad cumpla con sus objetivos de seguridad de la información.

A continuación, se ilustra el Modelo a seguir en la fase de implementación:

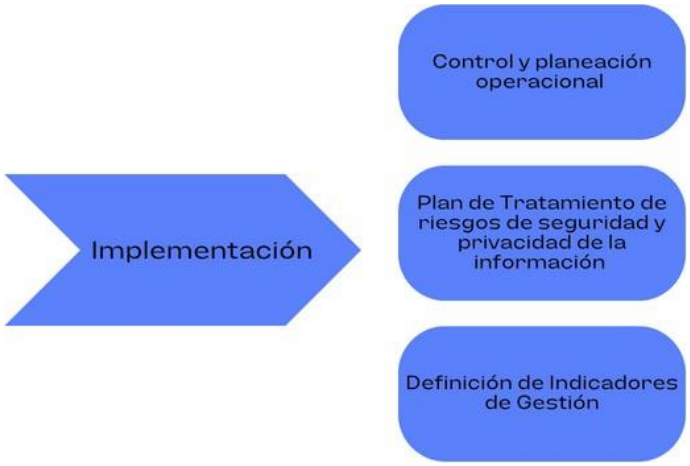

Imagen 4. Fase de Implementación. MinTIC

FASE DE EVALUACIÓN DE DESEMPEÑO

El seguimiento y monitoreo del MSPI, es clave para garantizar que el mismo modelo esté funcionando correctamente. Esta etapa se lleva a cabo a través de la conformación y medición de los indicadores de seguridad de la información. Los criterios de desempeño se determinan como actividad al interior del plan, los resultados del seguimiento y monitoreo se utilizan para tomar acciones correctivas o de mejora, bien sea inmediatas o para la siguiente anualidad.

A continuación, se ilustra el Modelo a seguir en la fase de evaluación del desempeño:

Imagen 5. Fase de Evaluación de Desempeño. (Fuente: MinTIC).

ARTÍCULO NOVENO: IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN. Siendo la política un lineamiento transversal, cada dependencia/proceso, debe elaborar y mantener un inventario de los activos de información que posean (procesada y producida), basado en el procedimiento definido desde el proceso Gestión Documental. La entidad ya cuenta con este instrumento, en el mismo se determina la clasificación, valoración, ubicación y acceso de la información. En este caso, el proceso de Gestión de Sistemas de Información brinda las herramientas necesarias que permitan la administración del inventario garantizando la disponibilidad, integridad y confidencialidad de los datos que la integran.

ARTÍCULO DÉCIMO: SEGURIDAD DE LA INFORMACIÓN EN EL TALENTO HUMANO. El talento humano que interviene en la gestión del proceso, cualquiera que sea su tipo de vinculación (empleados públicos y contratistas de apoyo), debe de tener un perfil de uso del recurso de la información, incluyendo el hardware y software. El proceso de Gestión de Sistemas de Información, debe definir el perfil que será asignado, con base a las funciones o actividades desarrolladas.

La responsabilidad de la custodia de la información usada, transformada o producida por el talento humano, antes del retiro o desvinculación de dicho personal, estará bajo la responsabilidad del(a) Jefe(a) de la dependencia, o supervisor(a) de contrato; quien debe efectuar la gestión pertinente ante los procesos de Gestión del Talento Humano y Gestión de Sistemas de la Información, efectuar el debido respaldo, cumpliendo los lineamientos documentados en ambos procesos, situación que debe ser corroborada al momento de trámite de paz y salvos. Este proceso de cambio en la cadena de custodia, es de suma importancia para la salvaguardia de la información institucional.

Tanto el Servidor público como el contratista de apoyo a la gestión debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de los recursos de tecnología, este documento puede estar inmerso en las obligaciones contractuales o estar expreso posteriormente, antes de identificarse como usuario de la información.

Para los empleados de planta de la Agencia, el proceso Gestión de Talento Humano debe adelantar la normalización del acuerdo consignado en este artículo, para facilitar la aplicación de la presente política, con apoyo de la oficina Asesora Jurídica, terminada la gestión debe reportar copia del insumo al proceso de Gestión de Sistemas de Información quien llevará un record solo por control, desvinculado(a) el(la) servidor(a) este récord solo quedará en el archivo de Gestión de Talento Humano.

ARTÍCULO DÉCIMO PRIMERO: SEGURIDAD FÍSICA Y DE ACCESO. La seguridad física de la Agencia, se encuentra documentada en procedimiento que hace parte del proceso de Gestión Administrativa, la seguridad es un servicio contratado por la Agencia, mediante el cual se ejerce el control del ingreso y debida salida en las diferentes sedes donde oferta los servicios la Agencia, los protocolos incluyen la identificación de cada persona y la inspección ocular y registro de los objetos que porta; si estos cumplen las características para ser registrados.

Al interior de la sede, el control al acceso a los cuartos técnicos de servidores principales y redes, se encuentra restringido y bajo llave y con limitación de ingreso de personal; control que ejerce el proceso de Gestión de Sistemas de Información y lo comparte con la Subdirección Administrativa, Financiera y de Apoyo a la Gestión, dado que el acceso para el archivo de custodia de títulos valores, se encuentra dentro del cuarto técnico de telecomunicaciones de la sede principal, separado por puerta con llave adicional, con un control único de registro de acceso, que ambas partes efectúan.

ARTÍCULO DÉCIMO SEGUNDO: SEGURIDAD EN LOS EQUIPOS. Los servidores y aplicaciones se mantienen en un ambiente seguro y protegido con lo siguiente:

- Control de acceso y seguridad física.
- Detección de incendios y sistemas de extinción de fuego.
- Control de humedad y temperatura.
- Control de riesgo de inundación.

Toda la información en formato digital, debe ser custodiada por los servidores del proceso de Gestión de Sistemas de Información, no se permite el alojamiento de información institucional en servidores externos; a excepción de las bases de datos e información institucional que se encuentre con la autorización para el uso y tratamiento de terceros que hayan suscrito con la Agencia, acuerdos de confidencialidad, licencias de usos de bases de datos o un contrato o convenio.

Los equipos de cómputo deben estar correctamente asegurados, mediante póliza todo riesgo daño material, para los equipos de cómputo portátiles, este debe tener adicionalmente guaya de seguridad.

Los préstamos de equipos, son controlados por el proceso de Gestión de Sistemas de Información, previa autorización del jefe de la dependencia; para este caso, el acceso se dará por medio de un usuario con rol local o visitante, bajo los controles parametrizados, que limitan el acceso a la información contenida en el mismo equipo.

Todas las dependencias y procesos deben tener la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad, el cual se encuentra documentado, a nivel de procedimientos o instructivos, como respaldo de la información.

ARTÍCULO DÉCIMO TERCERO: ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES.

Incidentes de Seguridad

El talento humano de la Agencia debe reportar de manera diligente, pronta y responsable las presuntas violaciones de seguridad a través del proceso de Gestión de Sistemas de Información con el fin de garantizar que la información no se vea afectada por cualquier índole de violación a la seguridad. El proceso de Gestión de Sistemas de Información debe garantizar las herramientas informáticas para que formalmente se realicen las denuncias.

Protección contra software malicioso o malware.

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque donde se involucren los controles humanos, físicos y técnicos. Se elaborarán manuales, procedimientos o guías que garanticen la mitigación de los riesgos a amenazas.

Como mínimo, todas las máquinas de Sapiencia deben estar protegidas por software antivirus con capacidad de actualización automática en lo relacionado a firmas.

Copias de Seguridad.

Toda información que pertenezca a los activos de información que sea de interés para un proceso operativo de la Agencia, debe ser respaldada por copias de seguridad tomadas de acuerdo a su criticidad para la Agencia.

Los registros de copias de seguridad deben ser salvaguardados en una base de datos creada para tal fin.

Administración de Configuraciones de Red

La configuración de los dispositivos de comunicaciones como lo son: switches, firewall, sistemas de detección de intrusos y demás, debe estar respaldada y documentada.

Intercambio de información con organizaciones externas

Las solicitudes por parte de entes externos o proveedores donde se requiere manipulación o intercambio de información, deben ser aprobadas por la Dirección Administrativa o la Dirección General.

Uso del correo electrónico

En la Agencia de Educación Postsecundaria de Medellín- Sapiencia se dispone de un servicio de correo electrónico que apoya las actividades de los funcionarios y contratistas de la entidad.

Los funcionarios y contratistas son responsables de todas las actividades realizadas con la cuenta de correo asignada por la Agencia. Toda la información transmitida a través de la cuenta de correo que no esté de acuerdo al uso y finalidades establecidas dentro de las políticas internas, así como las que vulnere el tratamiento de datos personales y confidencialidad de la información será única y exclusivamente responsabilidad del propietario de dicha cuenta.

El proceso de Gestión de Sistemas de Información, es responsable de la creación, modificación y eliminación de las cuentas de correo para los funcionarios y contratistas de la Agencia.

El uso de las cuentas de correo de la Agencia se utilizará única y exclusivamente para labores y actividades contractuales, por lo que no se permite el uso de este para fines personales.

Instalación de Software

Todas las instalaciones de software que se realicen deben ser aprobadas por El proceso de Gestión de Sistemas de Información, de acuerdo a las licencias adquiridas para las diferentes dependencias o procesos en su desempeño de funciones y que por esto se requieran.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y aquellas que la modifiquen, adicionen o deroguen.

Corresponde al proceso de Gestión de Sistemas de Información mantener una base de datos actualizada que contenga un inventario de software autorizado para el uso e instalación en los sistemas informáticos de la Agencia.

ARTÍCULO DECIMO CUARTO: SANCIONES. Le corresponde a la Superintendencia de Industria y Comercio como autoridad administrativa no solo garantizar el cumplimiento de la legislación en materia de datos personales e impartir instrucciones sobre los procedimientos a implementar para su adecuada operación, sino también, de adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data.

Por ese motivo, se podrá imponer multas y sanciones para quien efectúe el uso indebido de la información que en razón de sus funciones o actividades contractuales desarrolle. Así como las establecidas en la Ley 1273 de 2009 *por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.*

ARTÍCULO DÉCIMO QUINTO: CONTROL DE ACCESO. Los requerimientos orientados al riesgo, se entienden como aquellas necesidades de protección de activos de información involucrados, para preservar la disponibilidad, confidencialidad e integridad de la información, los cuales se identifican en el momento de la gestión del riesgo y se administran mediante mecanismos de control, en este caso frente al control de acceso tenemos:

Categorías de Acceso: los accesos a los recursos informáticos, deben estar restringidos según los perfiles de usuario definidos por el jefe de la dependencia y en armonía con las funciones o actividades contractuales que ostente el talento humano en la gestión de la Agencia.

Control de claves y nombres de usuario: el acceso a la información restringida debe estar controlado, mediante el uso de sistemas automatizados de autenticación que maneje las credenciales o firmas digitales. Las credenciales (usuarios y contraseñas) de administrador de los sistemas, deben ser alojadas y conservadas por el proceso de Gestión de Sistemas de Información, bajo la responsabilidad del líder y deben ser cambiadas de manera regular en el tiempo y cuando el personal adscrito al cargo o actividad contractual termine su periodo por retiro o terminación del contrato.

Acceso Remoto: el acceso de manera remota a los servicios y/o servidores de la Agencia, está sujeto a medidas de control definidas por el proceso de Gestión de Sistemas de Información, las cuales deben incluir acuerdos de confidencialidad y seguridad de la información, la Agencia cuenta actualmente con medidas que permiten la protección de la información como cláusulas contractuales, licencias de uso de bases de datos y acuerdos de confidencialidad que facilitan esta labor, los cuales pueden ser consultados dentro de los anexos del manual de política interna de tratamiento y protección de datos personales Resolución 2111 de 2023 por medio de la cual se actualiza la política interna de tratamiento y protección de datos personales de la Agencia de Educación Postsecundaria de Medellín-Sapiencia.

ARTÍCULO DÉCIMO SEXTO: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE SOFTWARE. La Agencia, adelanta los procesos de adquisiciones acogiendo los lineamientos, principios, pautas y procedimientos orientados para que en los procesos de contratación se garanticen los objetivos del sistema de compra pública, bajo estándares de eficacia, eficiencia, economía, promoción de la competencia, rendición de cuentas, manejo del riesgo, participación ciudadana, publicidad y transparencia, sirviendo de apoyo para el cumplimento de los propósitos misionales, el proceso que direcciona esta acción, la Oficina Asesora Jurídica desde el proceso de Gestión Contractual, el cual se encuentra debidamente documentado en el Sistema integrado de Gestión (SIG) de la Agencia.

Frente al desarrollo, se trata de una actividad inmersa en el alcance del proceso Gestión de Sistemas de Información, que consiste en la creación y/o modificación de soluciones a nivel informático, que acompañan la gestión de la Agencia, al respecto, el desarrollo puede ser contratado con terceros o se puede realizar desde el mismo proceso, para ambas alternativas se tienen consignados los protocolos requeridos frente a la seguridad; en este caso lo sugerido por el MINTIC y propiedad intelectual, bajo el marco normativo que cobija a la entidad.

En la actualidad, en cuanto a desarrollo, se efectúan los acuerdos de confidencialidad, que cada contratista suscribe con la aceptación de su contrato de prestación de servicios y que es previo a la actividad y cualquier acceso en servidor es supervisado por el proceso de Gestión de Sistemas de Información, el cual se deja consignado en acta como evidencia y control de lo desarrollado durante el acceso. Frente a los desarrollos in house, el repositorio donde está el código fuente es de carácter privado y su acceso es controlado por medio de permiso y rol de usuario.

Finalmente, la actividad de mantenimiento del software, se realiza con una periodicidad semestral, en el cual se deja registro por medio de log de eventualidades.

ARTÍCULO DÉCIMO SÉPTIMO: CONTINUIDAD DEL NEGOCIO (SERVICIO). La Agencia, a partir de la implementación de la presente política, debe efectuar una nueva valoración de riesgos, para identificar cuáles de estos podrían afectar las operaciones críticas de la Agencia, dicha identificación y tratamiento de riesgos, acoge los lineamientos del Sistema Integrado de Gestión y metodologías de la Función Pública que para tal efecto tiene definidas, de la cual se deriva un plan para prevenir y/o mitigar el riesgo, en base a estos, se tendrá documentada la acción para dar respuesta a incidentes y posterior a la implementación, se efectuará la recuperación con su respectivo protocolo de validación.

Para el caso en el que se presenten incidentes mayores, la Agencia, se acoge a lo definido en la guía para la implementación del MPSI, efectuando la respectiva denuncia, esto está consignado en el procedimiento de gestión de incidentes de seguridad de la información (disponible en el SIG y aplicativo Isolucion).

ARTÍCULO DÉCIMO OCTAVO: REFERENCIAS. Son referencias de la política de seguridad que se adopta las siguientes:

- ISO 27001:2022. Sistema de gestión de Seguridad de la Información - Requerimientos.
- ISO/IEC 13335-4:2000. Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección de salvaguardas
- MINTIC Modelo de Seguridad y Privacidad de la información (MinTIC).
- Gobierno Digital MINTIC – Modelo nacional de gestión de riesgo de la seguridad de la información en Entidades Públicas. (Gobierno Digital)
- ISO/IEC Guía 73:2002. Gestión de riesgo – Lineamientos para el uso en estándares.

PUBLÍQUESE Y CÚMPLASE

Narda Moreno.

NARDA CONSTANZA MORENO BENÍTEZ
Directora General (E)

Elaboró:	Revisó:	Aprobó:
Edison Salgar Marín -Contratista Seguridad de la Información	Yurany García Colorado- abogada contratista Oficina Asesora Jurídica. Diana Patricia Avendaño Lugo - Contratista Profesional Especializada transversal Subdirección Administrativa. Eliana Cristina Ríos Ortiz-Contratista Líder de Planeación. Eliana Rios Ortiz Ditter Alfonso López Ruiz - Contratista MIPG-SIG Luis Fernando Cifuentes Rojas-Contratista Líder de Gestión de Sistemas de Información. León David Quintero Restrepo- abogado contratista Asesor Subdirección Administrativa, Financiera y Apoyo a la Gestión	Mario Alfonso Álvarez Montoya - Jefe Oficina Asesora Jurídica.