



**ADMINISTRADORA DE LOS RECURSOS DEL SISTEMA
GENERAL DE SEGURIDAD SOCIAL EN SALUD**

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN


ADMINISTRADORA DE LOS RECURSOS DEL SISTEMA GENERAL DE SEGURIDAD SOCIAL EN SALUD

BOGOTÁ, 29 DE DICIEMBRE DE 2022

ADRES	PROCESO	ARQUITECTURA Y PROYECTOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-PL01
	POLÍTICA	GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión:	04
			Fecha:	29/12/2022

TABLA DE CONTENIDO

1.	INTRODUCCIÓN	3
2.	DECLARACIÓN	3
3.	OBJETIVOS	3
4.	ALCANCE	4
5.	NIVEL DE CUMPLIMIENTO	4
6.	LINEAMIENTOS GENERALES DE LA POLÍTICA	5
7.	TÉRMINOS Y DEFINICIONES.....	6
8.	MARCO NORMATIVO	7
9.	OPERATIVIZACIÓN.....	8
10.	VIGENCIA.....	8
11.	CONTROL DE CAMBIOS	8
12.	ELABORACIÓN, REVISIÓN Y APROBACIÓN.....	9

	PROCESO	ARQUITECTURA Y PROYECTOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-PL01
	POLÍTICA	GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión:	04
			Fecha:	29/12/2022

1. INTRODUCCIÓN

La Dirección General de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES reconoce que la información generada, almacenada y compartida en sus procesos es un activo esencial dentro de la Entidad. Por ello está comprometida con su Confidencialidad, vigilando que sólo quienes estén autorizados puedan acceder a ella; Integridad, propendiendo que la información y sus métodos de proceso sean exactos y completos; Disponibilidad, asegurando que los usuarios autorizados tengan acceso a ella cuando la requieran; y Privacidad, velando por tener los mecanismos apropiados para proteger la información de carácter sensible, clasificado o reservado. Esto lo logra, por medio de la aplicación de la legislación colombiana, así como las normas técnicas y mejores prácticas que aplican frente a la Seguridad y Privacidad de la Información, para así asegurar la continuidad de sus operaciones y establecer un marco de confianza en el ejercicio de sus deberes con los ciudadanos y por consiguiente con el Estado, para lo cual define la siguiente política.

2. DECLARACIÓN

“La ADRES que tiene como propósito administrar las fuentes y el uso de los recursos que financian el Sistema General de Seguridad Social en Salud en Colombia, bajo los principios de eficiencia, transparencia y calidad, con el fin de asegurar el adecuado flujo de recursos para la sostenibilidad del Sistema, se compromete a definir y establecer un Sistema de Gestión para la Seguridad de la Información garantizando los requerimientos de las partes interesadas, preservando la confidencialidad, disponibilidad e integridad de sus activos de información, con base en un enfoque de prevención de riesgos, mejora continua y autocontrol en los procesos y en la prestación de sus servicios, teniendo como apoyo de un equipo humano competente y comprometido para este fin.”

Como Entidad del orden nacional, la Dirección General de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES, a través de la presente Política, exhorta a reconocer que la información es uno de sus principales activos, por tanto, ha adoptado una posición consciente y comprometida frente al uso y limitaciones de los recursos, sistemas y servicios informáticos críticos de la Entidad.

Por su parte, los servidores públicos, contratistas, colaboradores y ciudadanía en general deben ser conscientes de la importancia y valor de la información, lo que hace necesario adoptar mecanismos de gestión de Seguridad y Privacidad de la Información, entre los que se pueden contar políticas, procedimientos, estructura organizacional y soluciones tecnológicas cuando aplique, sobre la base de estándares probados y reconocidos, tanto a nivel nacional como internacional.

3. OBJETIVOS

La Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES alineada con la Dirección Estratégica de la Entidad, establece la compatibilidad de la Política de Seguridad y Privacidad de la Información y define los siguientes objetivos de seguridad de la información:

- i. Minimizar los riesgos asociados a los activos de información de la ADRES, con el fin de asegurar su confidencialidad, disponibilidad e integridad a través de la gestión del sistema de gestión.

	PROCESO	ARQUITECTURA Y PROYECTOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-PL01
	POLÍTICA	GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión:	04
			Fecha:	29/12/2022

- ii. Definir controles y lineamientos de aseguramiento, con el fin de salvaguardar la información de la entidad utilizando procedimientos, instrumentos y mecanismos automatizados.
- iii. Concientizar a funcionarios y colaboradores de la Adres de la importancia de la protección de los activos de información para promover su uso seguro a través de programas y campañas de seguridad de la información.
- iv. Mantener la confianza de los ciudadanos respecto de la información de la ADRES mediante la adecuada gestión de las buenas prácticas en seguridad de la información

4. ALCANCE


La presente Política General de Seguridad y Privacidad de la Información aplica para todos los servidores públicos, contratistas y terceros quienes en pro de sus actividades tienen algún tipo de relación con la Dirección General de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES. Esto con el propósito de fomentar e incentivar de manera progresiva la cultura de Seguridad y Privacidad dentro de la Entidad buscando permear la cultura organizacional actual.

5. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento al 100% de la presente Política.

La Dirección General de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, el cual se encuentra soportado en lineamientos claros alineados a las necesidades de la Entidad, así como a los requerimientos regulatorios que le aplican a su naturaleza. A continuación, se establece el decálogo de políticas de seguridad específicas que soportan el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Entidad:

- i. **CLASIFICACIÓN DE LA INFORMACIÓN.** *La ADRES a través de la gestión de sus Direcciones, Subdirecciones, Oficinas Asesoras y Grupos Internos de Trabajo, vela por que la Seguridad y Privacidad sean parte integral del ciclo de vida de los Sistemas de Información y su contenido. Por tal razón, implementa mecanismos para propender por la clasificación de información de acuerdo con su grado de sensibilidad y que en sus procesos se recibe, genera, almacena, trasmite y puede llegar a eliminar.*
- ii. **GESTIÓN DEL RECURSO HUMANO.** *Como fruto de las directrices y acuerdos de confidencialidad que se definan por parte de la Dirección Administrativa y Financiera, las responsabilidades frente a la Seguridad y Privacidad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los servidores públicos y contratistas de la Entidad.*
- iii. **GESTIÓN DE ACTIVOS DE INFORMACIÓN.** *La ADRES conoce la importancia de sus activos de información, por tal razón, desde sus diferentes dependencias realiza la administración de manera adecuada de estos, con el firme propósito de asegurar la confidencialidad, integridad y disponibilidad de la información que en ellos se gestiona.*

	PROCESO	ARQUITECTURA Y PROYECTOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-PL01
			Versión:	04
	POLÍTICA	GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Fecha:	29/12/2022


- iv. **GESTIÓN DE LA SEGURIDAD Y CONTROL DE ACCESO FÍSICO Y LÓGICO.** La ADRES por intermedio de la Dirección de Gestión de Tecnologías de Información y Comunicaciones – DGTIC, controla y gestiona la operación de sus procesos de negocio mitigando los riesgos relacionados con la seguridad de los recursos tecnológicos, las redes de datos, las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- v. **GESTIÓN DE DESARROLLOS DE SISTEMAS DE INFORMACIÓN.** La ADRES mediante la Dirección de Gestión de Tecnologías de Información y Comunicaciones – DGTIC, controla y gestiona las actividades de desarrollo de los Sistemas de Información. Para esto, se basa en una metodología establecida para la mitigación de los riesgos de las soluciones que se implementen o mejoren para soportar tanto los procesos críticos y no críticos de la Entidad.
- vi. **GESTIÓN DE INTERCAMBIO DE INFORMACIÓN.** La ADRES a través de las definiciones y lineamientos de la Dirección de Gestión de Tecnologías de Información y Comunicaciones – DGTIC, propende que el intercambio de todo tipo de información por parte de los servidores públicos, contratistas y terceros que así lo requieran, se realice de manera confidencial tanto al interior como al exterior de la Entidad.
- vii. **GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD.** La ADRES gracias al oportuno reporte de sus servidores públicos, contratistas o terceros y el adecuado manejo de las debilidades asociadas con los activos de información por parte de sus Oficinas Asesoras, Direcciones y Subdirecciones en apoyo con la Dirección de Gestión de Tecnologías de Información y Comunicaciones – DGTIC, gestiona los eventos e incidentes de Seguridad y Privacidad con el fin de contenerlos y erradicarlos, donde adicionalmente, denuncia ante las instancias correspondientes a los infractores que se determinen.
- viii. **GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** La ADRES por medio de sus dependencias, vela por la disponibilidad de sus procesos misionales y la continuidad de su operación basada en la definición del Impacto del Negocio – BIA que puedan generar los eventos e incidentes de Seguridad y Privacidad de la Información.
- ix. **GESTIÓN DE LOS REQUERIMIENTOS LEGALES.** La ADRES a través de la gestión y direccionamiento por parte de la Oficina de Control Interno, cumple con las obligaciones legales, regulatorias y contractuales establecidas dentro del marco legal y contractual colombiano.
- x. **GESTIÓN DEL MEJORAMIENTO CONTINUO.** La ADRES mediante la planeación y ejecución de revisiones periódicas por parte de la Oficina de Control Interno, evalúa la madurez de su modelo de Seguridad y Privacidad de la Información – MSPI, con el fin que este se encuentre debidamente alineado con los requerimientos legales, normativos y del negocio.

El incumplimiento a la presente Política de Seguridad y Privacidad de la Información trae consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional en cuanto a la Seguridad y Privacidad de la Información.

6. LINEAMIENTOS GENERALES DE LA POLÍTICA

Se definen los siguientes lineamientos para el cumplimiento de esta política:

- Revisión periódica.
- Gestionar los riesgos de seguridad de la información y ciberseguridad.

	PROCESO	ARQUITECTURA Y PROYECTOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-PL01
	POLÍTICA	GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión:	04
			Fecha:	29/12/2022

- Medir y evaluar el sistema de gestión de la seguridad de la información – SGSI implementado.
- Aplicar buenas prácticas en el desarrollo de la gestión de seguridad de la información y ciberseguridad.
- Realizar ejercicios de investigación y análisis de las amenazas de ciberseguridad que enfrenta a la entidad.
- Aplicar los controles necesarios a los activos de información teniendo en cuenta las buenas prácticas.
- Garantizar el cumplimiento de las normas, definiciones y lineamientos que se establezcan en esta materia.
- Definir e implementar las políticas específicas requeridas para la adecuada protección de los activos de información.

7. TÉRMINOS Y DEFINICIONES

Activo de Información. Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (Datos, aplicaciones, personas, servicios, tecnología, instalaciones, equipo auxiliar) que tenga valor para la Entidad. Se clasifica de la siguiente manera: (i) Datos: Elementos básicos de información que cumplen con el ciclo de generación (recolección), almacenamiento, transmisión y eliminación. (ii) Aplicaciones: Es todo el Software que se utiliza para la gestión de la información. (iii) Personas: Todo tipo de persona involucrada con las actividades de la ADRES y que tengan acceso de una u otra manera a los activos de Información de la Entidad. (iv) Servicios: Actividades que se suministran tanto a nivel interno como externo con el propósito de cumplir una necesidad explícita para el usuario. (v) Tecnología: Hace referencia a todos los equipos que son utilizados para la gestión de la información y las comunicaciones dentro de la ADRES. (vi) Instalaciones: Ubicaciones en donde se alojan los sistemas de información. (vii) Equipamiento auxiliar: Son todos aquellos activos que dan soporte a los sistemas de información y que no se han referenciado en alguna otra categoría.


Confidencialidad: Según la norma ISO/IEC 27002:2013 es la propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Según la norma ISO/IEC 27002:2013 Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Información: De acuerdo con la Ley 1712 de 2014 “por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”, es un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Incidente de Seguridad: Según la norma ISO/IEC 27002:2013 es evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: En consideración a la norma ISO/IEC 27002:2013 es la propiedad de la información relativa a su exactitud y completitud.

	PROCESO	ARQUITECTURA Y PROYECTOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-PL01
	POLÍTICA	GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión:	04
			Fecha:	29/12/2022

Privacidad¹: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Riesgo: Según la norma ISO/IEC 27002:2013, es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Vulnerabilidad: De acuerdo con la ISO/IEC 27002:2013, es la debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.


8. MARCO NORMATIVO

- Constitución Política de Colombia de 1991. Artículo 15, mediante el cual se reconoce el Habeas Data como Derecho Fundamental. Artículo 20, Derecho a la Libertad de Expresión y de Prensa.
- Ley 734 de 2002 “Por la cual se expide el Código Disciplinario Único”, Artículo 95, acerca de la reserva de la actuación disciplinaria.
- 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”.
- 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.”
- Ley 1581 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Ley 1712 de 2014, “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- Decreto 2573 de 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”.
- Decreto 1078 de 2015, “por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Normas Técnicas

- NORMA IEC ESTÁNDAR 27000. (2013). 3rd ed. Ginebra: ISO INTERNACIONAL, pp.1-5.

¹ Modelo de Seguridad y Privacidad de la Información. (2017). 3rd ed. [ebook] Bogotá D.C.: MINTIC, p.15. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf [Accedido el 26 Dic. 2017].

	PROCESO	ARQUITECTURA Y PROYECTOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-PL01
			Versión:	04
	POLÍTICA	GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Fecha:	29/12/2022

9. OPERATIVIZACIÓN

Para la implementación de esta política, junto con el Manual de políticas específicas se define el siguiente plan:

- Socialización previa: Se realiza revisión de la Política y manual ajustados con la Dirección de Gestión de Tecnologías de la Información y las Comunicaciones – Seguridad Informática
- Comunicación a partes Interesadas: Se comunica a los miembros del comité institucional y se realiza la publicación respectiva a las partes interesadas en los mecanismos definidos para este fin.
- Aprobación: La política se aprueba por parte de la Dirección mediante resolución 73194 del 29 de diciembre de 2022.
- Socialización y sensibilización: Se desarrolla la socialización y sensibilización de la política y el respectivo manual de políticas específicas en el marco de la campaña “La clave eres tú”.
- Validación de cumplimiento y seguimiento: Se define indicador de gestión asociado al cumplimiento de esta política dentro del desarrollo de la gestión del plan de control operacional de la seguridad de la información.

10. VIGENCIA

La presente política entra en vigor el 29 de diciembre de 2022.

Cualquier cambio sustancial en la presente políticas será comunicado oportunamente a los titulares de los datos personales de una manera eficiente en los términos descritos en el artículo 5° del decreto 1377 de 2013.

11. CONTROL DE CAMBIOS			
Versión	Fecha	Descripción del cambio	Asesor del proceso
01	7 de marzo de 2018	Emisión y Publicación inicial	Gisela Rivera Gestor de Operaciones OAPCR
02	28 de marzo de 2019	Actualización política de seguridad y privacidad de información, marco normativo y definiciones	Marian Helen Batista Pérez Gestor de Operaciones OAPCR
03	18 de mayo de 2020	Actualización del responsable relacionado al nivel de cumplimiento Gestión de los Requisitos Legales, el cual es asociado a la Oficina Asesora Jurídica. Actualización de responsabilidades de la ADRES frente a la política de Seguridad y Privacidad de la información, las cuales se encuentran detalladas dentro del manual de Políticas de Seguridad de la Información. Cambio de codificación de la política conforme al mapa de procesos actual de la Entidad.	Olga Marcela Vargas Valenzuela Asesora OAPCR

ADRES	PROCESO	ARQUITECTURA Y PROYECTOS DE TECNOLOGÍA DE INFORMACIÓN	Código:	APTI-PL01
	POLÍTICA	GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión:	04
			Fecha:	29/12/2022

04	29 de diciembre de 2022	<p>Se ajusta redacción de la declaración de la política estableciendo como compromiso la implementación de un sistema de gestión para este fin, sustituyendo compromisos de la versión actual en donde la entidad no se puede comprometer a garantizar la confidencialidad, disponibilidad e integridad de la información.</p> <p>Se modifican los objetivos de la política con base en la declaración propuesta.</p>	Eliana Rodriguez Gomez Gestor de Operaciones OAPCR
----	-------------------------	---	---

12. ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Revisado por:	Aprobado por:
<p>Rodolfo Uribe Duarte OAPCR Seguridad de la información</p> <p>Fecha: 1 de noviembre de 2022</p>	<p>Luz Stella Hernández Ruiz Jefe OAPCR</p> <p>Fecha: 12 de diciembre de 2022</p>	<p>Juan Carlos Mendoza Pedraza Director General de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud- ADRES (E) Aprobado mediante resolución 73194 del 29 de diciembre de 2022. Fecha: 29 de diciembre de 2022</p>