POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

BOGOTÁ, 18 DE MAYO DE 2020

TABLA DE CONTENIDO

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. DECLARACIÓN

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.

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 y ciudadanía en general deben ser conscientes que la importancia de la información es proporcional al valor de sus procesos, 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.

2. 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 los objetivos de seguridad de la información, estos últimos correspondientes a:

i. Minimizar el riesgo de los procesos misionales de la Entidad.
ii. Cumplir con los principios de seguridad de la información.
iii. Cumplir con los principios de la función administrativa.
iv. Mantener la confianza de los servidores públicos, contratistas y terceros.
v. Apoyar la innovación tecnológica.
vi. Implementar el Sistema de Gestión de Seguridad de la Información.
vii. Proteger los diferentes activos de información.
viii. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

ix. Fortalecer la cultura de seguridad de la información en los servidores públicos, terceros, aprendices, practicantes y clientes de la ADRES.

x. Velar por la continuidad del negocio frente a eventos e incidentes de seguridad.

3. 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 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.

4. 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 específicas de seguridad y privacidad 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. **Obligaciones y Deberes del Recurso Humano***. Como fruto de las directrices y compromisos de confidencialidad que se definan por parte de la Dirección Administrativa y Financiera dentro del grupo interno de Talento Humano, 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.*

iv. ***Control de acceso****. 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. ***Adquisición o Desarrollo 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 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. ***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 el impacto que pueden generar los eventos e incidentes de Seguridad y Privacidad de la Información.*

ix. ***Gestión de los Requisitos Legales****. La ADRES a través de la gestión y direccionamiento por parte de la Oficina Asesora Jurídica, cumple con las obligaciones legales, regulatorias y contractuales establecidas dentro del marco legal y contractual colombiano.*

x. ***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.*

De igual manera, para dar cabal cumplimiento la Entidad ha adoptado una serie de políticas complementarias que apoyan directamente el desempeño de las políticas antes descritas, las cuales podrán ser consultadas dentro del Manual de Políticas Específicas de Seguridad y Privacidad de la Información.

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. En especial a las medidas administrativas, disciplinarias o legales a que haya lugar, acorde a la Ley 734 de 2002.

5. TERMINOS Y DEFINICIONES

Activo de Información. Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (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, trasmisión 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 explicita 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.

Amenaza. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos. Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo. Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo. Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

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.

Desastre. Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva o directriz. Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

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

Evaluación de riesgos. Proceso global de identificación, análisis y estimación de riesgos.

Gestión de incidentes de seguridad de la información. Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

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.

Inventario de activos. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de Seguridad de la Información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SSI a nivel mundial.

No repudio: Según CCN-STIC-405:2006 el no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según OSI ISO-7498-2 servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Plan de continuidad del negocio. Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos. Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Privacidad[1]: 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.

Seguridad de la información. Es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información

Seguridad informática. Se encarga de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que—articulados con prácticas de gobierno de tecnología de información—establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.

[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. 2018].

Trazabilidad. Según CESID:1997 es la cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

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

6. 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 23 de 1982 "Sobre derechos de autor".
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 734 de 2002 "Por la cual se expide el Código Disciplinario Único", Artículo 95, acerca de la reserva de la actuación disciplinaria.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- 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 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- Ley 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- 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".
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.
- Decreto 1008 de 2018, "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".

Normas Técnicas

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

7. VIGENCIA

La presente política entra en vigor el día 18 de mayo de 2020.

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

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Juan Carlos Escobar Baquero Gestor de Operaciones - Dirección de Gestión de Tecnologías de la Información y las Comunicaciones **Fecha:** *13 de mayo de 2020*	**Sergio Andrés Soler Rosas** Director de Gestión de Tecnologías de la Información y las Comunicaciones **Fecha:** *15 de mayo de 2020*	**Diana Cárdenas Gamboa.** Directora General de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud- ADRES **Comité Institucional de Gestión y Desempeño** **Fecha:** *18 de mayo de 2020*