REPUBLICA DE COLOMBIA

INSTITUTO NACIONAL DE SALUD

RESOLUCIÓN NÚMERO 186 DE 2019

(27 FEB 2019)

"Por la cual se actualiza la Política de Seguridad de la Información en el Instituto Nacional de Salud y se dictan otras disposiciones"

LA DIRECTORA GENERAL DEL INSTITUTO NACIONAL DE SALUD

En uso de sus facultades legales contempladas en el artículo 5 del Decreto 2774 de 2012 y

C O N S I D E R A N D O:

Que la Ley 1341 de 2009 *"por la cual se definen principios y conceptos sobre la seguridad 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"*, señala en su artículo 2º, como principios orientadores y aspectos fundamentales para la promoción de la libre competencia y el comercio electrónico, lo siguiente: la protección a los derechos de los usuarios de las TIC, el acceso y uso de las TIC, la garantía de los derechos de los ciudadanos y la masificación del Gobierno en Línea.

Que el Decreto 1078 de 2015 en el artículo 2.2.9.1.1.1. establece como objeto *"Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad".*

Que el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publicó el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Que el Ministerio de Tecnología de Información y Comunicaciones emitió la guía para la elaboración de la política de seguridad y privacidad de la Información el 11 de mayo de 2016, entre otros documentos, cuyo propósito es ofrecer un lineamiento de recomendaciones para la construcción e implementación de políticas de seguridad y privacidad de información para las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 2573 de 2014 recopilado a través del Decreto 1078 de 2015 y demás disposiciones concordantes.

Que mediante el Decreto 1081 de 2015 se expidió el Decreto Reglamentario Único del Sector Presidencia de la República, cuyas disposiciones son aplicables al INS.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones y el Gobierno Nacional, a través de la Resolución 451 del 8 de marzo de 2016 adoptó los siguientes instrumentos de la Gestión de Información Pública: el Registro de activos de información, el Índice de información clasificada y reservada, el Esquema de publicación de información y el Programa de Gestión Documental, bajo esos parámetros el Instituto Nacional de Salud mediante Resolución No. 1463 del 23 de octubre de 2017 adoptó la política de seguridad de la información, la cual debe ser revisada y actualizada según nuevos lineamientos y cambios exigidos en materia de seguridad y privacidad de la información.

Que, como consecuencia de lo anterior, este Despacho,

"Por la cual se actualiza la política de seguridad de la información en el Instituto Nacional de Salud y se dictan otras disposiciones"

R E S U E L V E:

ARTÍCULO PRIMERO. – Objeto: El Instituto Nacional de Salud (INS) es una entidad científico técnica, generadora de conocimiento del orden Nacional adscrita al Ministerio de Salud y Protección Social, el Instituto pertenece al Sistema General de Seguridad Social en Salud y al Sistema Nacional de Ciencia Tecnología e innovación, por lo tanto la Dirección General entendiendo la importancia de una adecuada gestión de la información, se ha comprometido a garantizar la confidencialidad, disponibilidad e integridad de los activos de información, a través del diseño, la implementación, operación y mejora continua del Sistema de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad, mediante un enfoque de revisión y mejora continua del sistema para asegurar el cumplimiento de los objetivos institucionales.

Para el Instituto Nacional de Salud (INS) la protección de la información busca la disminución del impacto generado sobre sus activos, empleando mecanismos para identificar y mitigar riesgos de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

PARÁGRAFO: El Instituto Nacional de Salud, mediante la Política de Seguridad de la Información da cumplimiento a los lineamientos de la Planeación Estratégica de la Entidad en concordancia con su misión, visión, objetivos estratégicos, que establecen la función de Seguridad de la Información en la Entidad, estos últimos correspondientes a:

a) Gestionar el riesgo de los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad.
b) Cumplir con los principios de seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

- ❖ CONFIDENCIALIDAD: la información debe ser accesible sólo a aquellas personas autorizadas.
- ❖ INTEGRIDAD: la información y sus métodos de procesamiento deben ser completos y exactos.
- ❖ DISPONIBILIDAD: la información y los servicios deben estar disponibles cuando se requiera.

c) Mantener la confianza de los funcionarios, contratistas y terceros.
d) Mantener y Mejorar el Sistema de seguridad de la información, cumpliendo con el ciclo PHVA
e) Proteger los activos de información.
f) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
g) Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del INS.
h) Proteger la información y los activos tecnológicos de la Institución.
i) Adquirir un compromiso de concientización para que todos los funcionarios, contratistas y practicantes del INS utilicen de manera adecuada los activos de información puestos a su disposición para la realización de las funciones y actividades.
j) Dar cumplimiento a los lineamientos de la Política de Gobierno Digital respecto a la Seguridad de la Información.
k) Garantizar la continuidad del negocio frente a incidentes.

ARTÍCULO SEGUNDO. – Alcance: El Sistema de Seguridad de la Información, Protección de Datos Personales abarca los activos de información , las bases de datos personales y los contenedores de información gestionados en el desarrollo de las funciones de todos los procesos definidos del Instituto Nacional de Salud (INS), así como todo el personal, es decir; funcionarios, contratistas y proveedores o partes interesadas que generen, acceden o utilicen información de la Entidad, con el fin de garantizar su confidencialidad, integridad y disponibilidad en el INS.

ARTÍCULO TERCERO. - Nivel de Cumplimiento: Todas las personas incluidas en artículo anterior deberán cumplir la política de manera obligatoria, en un cien por ciento (100%), sin perjuicio de las sanciones a que haya lugar.

ARTÍCULO CUARTO. - Justificación de Política General de la Seguridad de la Información: Para el Instituto Nacional de Salud (INS) como Autoridad Científico Técnica generadora de conocimiento, es de vital importancia salvaguardar la información obtenida de sus diversas actividades misionales, estratégicas y de evaluación, la cual es usada como herramienta para la toma de decisiones, la emisión de lineamientos, la ejecución de actividades y la prevención de riesgos relacionados con la salud pública, de acuerdo con nuestras funciones y competencias, en el marco del Sistema de Seguridad de la Información y las políticas de Estado.

"Por la cual se actualiza la política de seguridad de la información en el Instituto Nacional de Salud y se dictan otras disposiciones"

El Instituto Nacional de Salud (INS) reconoce la seguridad de la información como el conjunto de controles de protección que permiten resguardar y proteger la información, basados en el Estándar de ISO/IEC 27001 y el Modelo de Privacidad y Seguridad de la Información (MPSI) en lo que se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser: Electrónico, papel, audio y vídeo, entre otros.

ARTÍCULO QUINTO. - Objetivos de Seguridad de la Información:

El Instituto Nacional de Salud (INS), establece sus objetivos del Sistema de Gestión de Seguridad de la Información, realizando una alineación con la Planeación Estratégica de la Entidad apoyando el cumplimiento de los objetivos estratégicos, y de esta manera, expresar la intención articuladamente con el desempeño del resultado, el compromiso de la Dirección del INS.

- ✓ Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas.
- ✓ Aplicar un proceso de gestión de riesgos de seguridad de la información y bases de datos personales, mediante la ejecución de medidas apropiadas con el fin de identificar, analizar, evaluar, tratar y mitigar los riesgos y así reducir el impacto potencial a niveles aceptables sobre los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad.
- ✓ Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
- ✓ Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
- ✓ Reducir la probabilidad de violación de la privacidad de los datos personales en la Entidad.
- ✓ Establecer las acciones necesarias para asegurar la mejora continua del Sistema de Seguridad de la Información y Protección de Datos Personales.
- ✓ Fortalecer la cultura de seguridad de la información en la Entidad, a través de la gestión del conocimiento, las campañas de sensibilización, transferencias de conocimiento, capacitaciones y las necesarias definidas en el Plan de Comunicación de seguridad de la información

ARTÍCULO SEXTO. – Manual de Políticas Estratégicas de la Seguridad de la Información que soportan el SGSI:

Las Políticas Estratégicas de Seguridad de la Información establecidas por el Instituto Nacional de Salud (INS) son:

1. Política de Seguridad para el uso de dispositivos personales BYOD Dominio /Control A.6.2.1
2. Política de Capacitación y Sensibilización en Seguridad de Información Dominio /Control A.7.2.2
3. Política de Clasificación de la información Dominio /Control A.8.2
4. Política de Confidencialidad Dominio /Control A.7.1.2
5. Política de Contraseñas Dominio /Control A.7.4.2
6. Política de Control de acceso Dominio /Control A.9
7. Política de Controles Criptográficos Dominio /Control A.10.1.1
8. Política de Copias de seguridad Dominio /Control A.12.3
9. Política de Disponibilidad Dominio /Control A.17.2
10. Política de Dispositivo sobre dispositivos móviles Dominio /Control A.6.2.1
11. Política de Eliminación y destrucción Dominio /Control A.11.2.7
12. Política de Ética Empresarial Dominio /Control A.7.1.2
13. Política de Gestión de Activos Dominio /Control A.8
14. Política de Gestión de cambios Dominio /Control 12.1.2
15. Política de Gestión de Incidentes e Infraestructura critica de Seguridad de Información Dominio /Control A.16.1
16. Política de Integridad Dominio /Control A.12.1.6
17. Política de No Repudio Dominio /Control A.12.1.1
18. Política de Pantalla y escritorio limpios Dominio /Control A.11.2.9
19. Política de Registro y Auditoria Dominio /Control A.18.1.3
20. Política de Seguridad de la información y objetivos
21. Política de Seguridad Relación con los proveedores Dominio /Control A.15
22. Política de Transferencia de información Dominio /Control A.13.2
23. Política de Tratamiento de Datos Personales – Ley 1581 de 2018
24. Política de Uso Aceptable Dominio /Control A.5.1

"Por la cual se actualiza la política de seguridad de la información en el Instituto Nacional de Salud y se dictan otras disposiciones"

25. Política de Recurso Humano Dominio /Control A.7
26. Política de Estructura organizacional de seguridad de la información Dominio /Control A.6.1
27. Política para Uso de tokens de seguridad Dominio /Control A.9.4.2
28. Política de Uso de periféricos y medios de almacenamiento Dominio /Control A.8.3.1
29. Política de Registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información
30. Política de Gestión y aseguramiento de las redes de datos Dominio /Control A.13.1.2.
31. Política de Uso del correo electrónico Dominio /Control A.13.2.3.
32. Política de Uso adecuado de internet Dominio /Control A.9.13.2.1.
33. Política para el Establecimiento de requisitos de seguridad Dominio /Control A.5.1.1.
34. Política de Desarrollo seguro, realización de pruebas y soporte de los sistemas Dominio /Control A.14.2.1
35. Política para la Protección de los datos de prueba Dominio /Control A.12.1.4.
36. Política de Privacidad y protección de datos personales Dominio /Control A.18.1.4
37. Política de Seguridad en las operaciones Dominio /Control A.12
38. Política de Gestión de continuidad del negocio Dominio /Control A.17.1
39. Política de Cumplimiento Dominio /Control A.18.1
40. Revisión de las políticas de Seguridad de la Información Dominio /Control A.18.2
41. Política de Seguridad Fisica y del entorno Dominio /Control A.11
42. Política de Seguridad de Comunicaciones Dominio /Control A.13
43. Política de Seguridad adquisición, desarrollo y Mantenimiento de Sistemas de Información Dominio /Control A. 14

Para conocer el detalle de las políticas estratégicas, remitirse al "Manual de Políticas Específicas de Seguridad de la Información y Datos Personales".

ARTICULO SÉPTIMO. - Responsables del Sistema de Seguridad de la Información y Protección de Datos personales:

El Delegado como Responsable de Seguridad de la Información, encargado de establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información y demás actividades derivadas para la estandarización de la presente Política, es el Jefe de la Oficina de Tecnologías de Información y Comunicaciones, o quien haga sus veces.

El Delegado como Responsable de Protección de Datos Personales, encargado de implementar, mantener y mejorar continuamente, así como apoyar y coordinar con las demás áreas del Instituto Nacional de Salud (INS) el tratamiento de los datos personales, para asegurar una implementación transversal del cumplimiento de la Ley 1581 de 2012 es el Jefe de la Oficina Asesora Jurídica.

Los propietarios de la información, funcionarios, contratistas, practicantes, usuarios de la información, sin perjuicio de las funciones del Comité Institucional de Gestión y Desempeño y la Oficina de Control Interno, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos, buenas prácticas y responsabilidades asignadas en el Sistema de Gestión de Seguridad de la Información y protección de datos personales.

ARTÍCULO OCTAVO. - Responsabilidades Específicas frente a la Seguridad de la Información y al Sistema de Gestión de Seguridad de la Información y Protección de datos personales:

I. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN – JEFE DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

a) Planear, participar y realizar actividades de Seguridad de la Información que involucren a todo el personal.
b) Ejercer seguimiento y control del SGSI, aplicando los correctivos y ajustes necesarios para el logro de los objetivos, informando a la alta dirección sobre el desempeño del sistema.
c) Emplear la información, los procedimientos, el talento humano y los recursos materiales y financieros para el desarrollo de las actividades del SGSI adecuadamente.
d) Establecer y realizar la revisión y actualización de las políticas y los objetivos de Seguridad de la Información de la organización.
e) Analizar los datos arrojados por el SGSI y tomar las decisiones necesarias para garantizar el mantenimiento y mejoramiento del sistema.
f) Coordinar la realización de un análisis de riesgos de seguridad de la información en cada uno de los Procesos del Instituto Nacional de Salud (INS), y para cada una de las actividades subcontratadas, el cual debe llevarse a cabo como mínimo una vez al año, para determinar el grado de exposición a las amenazas relacionadas con los activos de información.

g) Definir y ejecutar los planes de entrenamiento y sensibilización y capacitación para los funcionarios y partes interesadas del Instituto Nacional de Salud (INS) en lo referente a seguridad de la información.
h) Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
i) Identificar todos los cambios significativos de amenazas y exposición de la información.
j) Evaluar la adecuación e implantación de los controles de Seguridad de la Información.
k) Evaluar la información de seguridad recibida a la hora de monitorear y revisar los incidentes de Seguridad de la Información, además de recomendar todas las acciones apropiadas en respuesta para identificar incidentes de Seguridad de la Información.
l) Aprobar las metodologías y los procesos para seguridad de la información.

II. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES – JEFE DE LA OFICINA ASESORA JURÍDICA

a) Asesorar y constatar que los responsables de la protección de los datos personales realicen el trámite a las solicitudes de los Titulares de los datos personales para el ejercicio de los derechos que se consagran en la Ley 1581 de 2012.
b) Realizar la revisión y actualización anual en conjunto con el Oficial de Seguridad de la Información, respecto de los riesgos jurídicos que se identifiquen frente a la protección de datos personales del INS.
c) Mantener un inventario de las bases de datos personales en poder del INS y clasificarlas según su contenido.
d) Coordinar con la Oficina de Tecnología de Información y comunicación la actualización anual de las Bases de Datos en la plataforma de la Superintendencia de Industria y Comercio - SIC
e) Realizar un Plan de Sensibilización anual, en conjunto con el área de Comunicaciones en materia de Protección de Datos Personales para el INS.
f) Servir de coordinador con las demás áreas de la organización para asegurar una implementación transversal del cumplimiento de la Ley 1581 de 2012.

III. RESPONSABILIDADES DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

a) Implantar, mantener y divulgar las políticas y procedimientos de tecnología, incluida esta política de seguridad de información, el uso de los servicios tecnológicos en toda la institución de acuerdo a las mejores prácticas y lineamientos de la Dirección General del Instituto y directrices del Gobierno.
b) Salvaguardar la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Institución.
c) Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Institución a la Dirección General, las diferentes Direcciones y Jefaturas del Instituto Nacional de Salud, así como a los entes de control e investigación que tienen injerencia sobre la Institución.
d) Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital del Instituto.
e) Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
f) Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio del Instituto Nacional de Salud.
g) Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.

IV. RESPONSABILIDADES DE LA OFICINA DE CONTROL INTERNO

a) Coordinar las auditorías internas para verificar el cumplimiento de las Políticas y Procedimientos en materia de Protección de Datos Personales y Seguridad de la Información, e informar el resultado de las mismas.
b) Realizar los planes de auditoria de los sistemas de Protección de Datos Personales, Seguridad de la Información.
c) La Oficina de Control Interno diseñará y ejecutará los programas de auditoria de Seguridad de Información y Protección de datos con el fin de verificar el cumplimiento de las políticas establecidas en el artículo 6º, de acuerdo con sus funciones, a partir de la firma y divulgación de este documento y realizará el seguimiento correspondiente al Sistema de Seguridad de la Información y Protección de datos.

"Por la cual se actualiza la política de seguridad de la información en el Instituto Nacional de Salud y se dictan otras disposiciones"

V. RESPONSABILIDADES DEL AREA DE SOPORTE TECNOLÓGICO DEL GRUPO DE GESTIÓN ADMINISTRATIVA DE LA SECRETARIA GENERAL

a) Atender las solicitudes de mantenimiento que puedan afectar la normal prestación de los servicios; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes Direcciones, Jefaturas o Coordinaciones siguiendo el procedimiento establecido, y así mismo programar e informar a todos los usuarios.
b) Determinar las estrategias para el mejoramiento de la prestación del soporte tecnológico y la optimización de los recursos tecnológicos.
c) Brindar el soporte necesario a los usuarios a través del apoyo del recurso humano y los diversos canales de ayuda que se han implementado en el INS.

VII. RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN

a) Son propietarios de la información cada uno de los directores, así como los jefes de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propio del desarrollo de sus actividades.
b) Valorar y clasificar la información que está bajo su administración y/o generación.
c) Autorizar, restringir y delimitar a los demás usuarios de la institución el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
d) Reportar a la Oficina Asesora Jurídica las Bases de Datos en el momento que surja una actualización para que se tenga actualizado el inventario de las Bases de Datos.
e) Determinar los tiempos de retención de la información en conjunto con el Grupo de Gestión Documental y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las políticas de la Entidad como de los entes externos y las normas vigentes.
f) Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de la misma.

VIII) RESPONSABILIDADES DE LOS FUNCIONARIOS, CONTRATISTAS, PRACTICANTES Y USUARIOS DE LA INFORMACIÓN

a) Conocer, divulgar, aplicar y cumplir la Política de Seguridad de la Información vigente.
b) Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones, Código Disciplinario Único o Contrato.
c) Manejar la Información del INS y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
d) Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
e) Evitar la divulgación no autorizada o el uso indebido de la información.
f) Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
g) Informar a directores, jefes de las oficinas y Supervisores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
h) Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
i) Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
j) Proteger los equipos de cómputo y demás dispositivos tecnológicos o técnico científico asignados para el desarrollo de sus funciones o actividades.
k) No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos al Instituto a la red Institucional ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones.
l) Usar software autorizado que haya sido adquirido legalmente por la Institución. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno de la Oficina de Tecnologías de la Información y las Comunicaciones.
m) Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección General del Instituto puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad del Instituto, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la Institución; lo anterior de llegar a ser el caso, con el acompañamiento del Grupo de

Gestión del Talento Humano o de la Oficina Asesora Jurídica.

n) Proteger y resguardar su información personal que no esté relacionada con sus funciones o actividades en el Institución. El Instituto Nacional de Salud no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito etc.

ARTÍCULO NOVENO. - Incorporación: Se entienden incorporadas al presente acto administrativo y por lo tanto hacen parte integral del mismo, la Resolución No. 1607 de 2014 "*Por la cual se adopta el Reglamento de Propiedad Intelectual del Instituto Nacional de Salud (INS), Ley estatutaria No 1581 de 2012 "por el cual se adopta el Régimen de Protección de Datos Personales y se dictan otras disposiciones"* la adopción de "el Decreto 1078 de 2015 con su componente de Modelo de Privacidad y Seguridad de la Información MPSI, adoptados en el Sistema Integrado de Gestión del INS, junto con sus respectivos anexos, o el acto administrativo que los sustituya modifique o adicione.

PARAGRAFO: De acuerdo con lo dispuesto en el presente artículo, la política de Seguridad de la Información se hace extensiva a los aspectos contenidos en los Anexos No 2° y 3° de lo Resolución 1607 de 2014 y demás disposiciones que la complementen, sustituyan o adicionen.

ARTÍCULO DÉCIMO. - Revisión y Actualización: La política deberá ser revisada mínimo una vez al año o cuando ocurran cambios significativos.

ARTÍCULO DÉCIMO PRIMERO. - Vigencia: La presente resolución rige a partir de la fecha de su expedición y deroga íntegramente la Resolución No. 1463 de 2017.

ARTÍCULO DÉCIMO SEGUNDO. – Divulgación: Se ordena la divulgación de esta política a todas las dependencias a través de la página web y demás medios de comunicación del Instituto Nacional de Salud-INS

Dada en Bogotá D.C., a los 27 FEB 2019

COMUNÍQUESE Y CÚMPLASE

LA DIRECTORA GENERAL

MARTHA LUCIA OSPINA MARTINEZ

Revisó: Esperanza Martínez Garzón, Secretaria General.
Luis Ernesto Flórez Simanca, Jefe Oficina Asesora Jurídica.
Luis Antonio Ayala Ramírez, Jefe Oficina Asesora de Planeación (E)
Diana Rocio Rojas Lasso, Coordinadora Grupo de Gestión Talento Humano
Luz Stella Pradilla Noreña, Coordinadora Grupo de Gestión Financiera
Edwin Alberto Melo Gonzalez, Coordinadora Grupo de Gestión Administrativa
Paula Camila Campos Abril, Coordinadora Grupo de Gestión Contractual
Andrea Carolina Boton Saenz, Coordinadora Grupo de Gestión Documental
Amanda Julieth Rivera Murcia, Coordinadora Grupo de Gestión Atención al Ciudadano
Proyectó: Elsa Marlen Baracaldo Huertas, Jefe Oficina Tecnología de la Información y comunicaciones