INSTITUTO NACIONAL DE SALUD

RESOLUCION NÚMERO 1463 DE 2017

(23 OCT 2017)

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

EL DIRECTOR GENERAL (E) DEL INSTITUTO NACIONAL DE SALUD

En uso de sus facultades legales y estatutarias 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 Instituto Nacional de Salud mediante Resolución No 1629 del 30 de diciembre de 2015 adoptó la política de seguridad de la información, la cual debe ser actualizada a los nuevos lineamientos dados por el Ministerio de Tecnología de Información y Comunicaciones y del Gobierno Nacional.

Que como consecuencia de lo anterior, este Despacho,

R E S U E L V E:

ARTÍCULO PRIMERO.- Objeto. La Dirección General del Instituto Nacional de Salud, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión 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.

Para el Instituto Nacional de Salud la protección de la información busca 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 interés identificados.

PARAGRAFO: El Instituto Nacional de Salud, mediante la Política de seguridad de 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 disponible cuando se le requiera.

c) Mantener la confianza de los funcionarios, contratistas y terceros.
d) Mantener y Mejorar el sistema de gestión 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 sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades.
j) o Dar cumplimiento a los lineamientos de la Estrategia de Gobierno en Línea respecto a la Seguridad de la Información.
k) Garantizar la continuidad del negocio frente a incidentes.

ARTÍCULO SEGUNDO.- Alcance. Esta política aplica a todo el Instituto Nacional de Salud, sus funcionarios, contratistas, terceros, colaboradores y ciudadanía en general, así como a todos los activos de información, servicios, procesos, las tecnologías de información incluida el hardware y el software, instalaciones imagen perceptual y demás herramientas utilizadas por la Organización en el ejercicio de sus funciones.

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

ARTÍCULO CUARTO.- Definiciones para la presente política: Son definiciones para la política de seguridad de la información en el INS:

a) **Política General de Seguridad de la Seguridad de la Información:** Para el Instituto Nacional de Salud 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 Sistema de Gestión de Seguridad de la Información y las políticas de Estado.

b) **Seguridad de la Información:** El Instituto Nacional de Salud reconoce la seguridad de la información como el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información, teniendo en cuenta la Norma ISO27001, 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: Electrónicos, En papel, Audio y vídeo, etc.

ARTÍCULO QUINTO.- Políticas específicas de la Seguridad de la Información que soportan el SGSI.

Las políticas específicas de la Seguridad de la Información establecidas por el INS son:

1. 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 que le aplican a su naturaleza. De igual manera las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
2. Proteger la información generada, procesada o resguardada por los procesos estratégicos, misionales, de apoyo y de evaluación, y garantizara su fiabilidad, integridad y disponibilidad por medio de la infraestructura tecnológica y los procesos y herramientas utilizadas, so pena de las sanciones que implican su incumplimiento.
3. Salvaguardar la información creada, procesada, transmitida o resguardada por sus procesos de negocio, 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.

4. Limitar el acceso a los activos de información dependiendo de su clasificación según lo establecido en el marco de la normatividad.
5. Proteger las instalaciones físicas para controlar el acceso de personas no autorizadas a las áreas restringidas, con el fin de resguardar la información que se encuentra en ellas.
6. Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. Garantizar el mantenimiento y seguridad de su infraestructura en donde se almacenen los Sistemas de Información para garantizar su ciclo de vida y los pilares de la seguridad de la información.
8. Evaluar a sus procedimientos, controles e infraestructura con el fin de detectar debilidades y riesgos asociados a la planta física en pro de una mejora efectiva en su modelo de seguridad.
9. Proteger los datos personales recolectados en ejercicio de sus actividades como Autoridad Científico y Técnica del orden nacional, en el marco de nuestras competencias y de acuerdo con la Ley 1581 de 2012 y la Ley 1755 de 2015 o las normas que la modifiquen o adicionen.
10. Preservar la información a la que tienen acceso los funcionaros, contratistas y colaboradores del Instituto Nacional de Salud y en consecuencia, incluirá cláusulas en los contratos o convenios, o suscribirá los actos jurídicos necesarios para la protección de la información de acuerdo con los lineamientos dados por la Oficina Asesora Juridica y el Comité de Propiedad Intelectual.
11. Velar por la concientización de los funcionarios, contratistas y terceros con respecto a la importancia y el cumplimiento de los lineamientos definidos a través del presente acto administrativo.
12. Informar a los terceros sobre la presente política de Seguridad de la Información y velar por su observancia en todos los actos jurídicos que suscriban con la Organización o en los trámites que realicen frente a la misma de acuerdo con nuestras funciones.
13. Implementar los controles necesarios para dar manejo a los riesgos detectados y proveerá un nivel de protección de la información apropiado y consistente.
14. Administrar controles físicos y lógicos para preservar y mantener seguras las áreas físicas y lógicas clasificadas como públicas y restringidas que sean utilizadas para la gestión, almacenamiento y procesamiento de la información.
15. Emitir mecanismos de control de acceso tales como puertas de seguridad donde se requieran, sistemas de alarmas, control biométricos, sistemas de detección y extinción de incendios, control de inundaciones, alarmas para detectar irregularidades en el desarrollo de las actividades, apartar líquidos inflamables y demás medidas que se deban tomar para la protección de la información de la Entidad. Las puertas de las oficinas y diferentes áreas de la entidad deben permanecer cerradas y aseguradas cuando las mismas se encuentren desatendidas o sin personal de la entidad dentro de ellas.
16. Otorgar claves de acceso los sistemas de información, equipos de cómputo, alarmas, cajas fuertes entre otros únicamente a personal autorizado, salvo las situaciones de emergencia que se puedan presentar.
17. Restringir el acceso a los funcionarios de la Entidad, contratistas, colaboradores o terceros, sólo a áreas a las cuales tengan la debida autorización.
18. Custodiar en todo momento y sin excepción a todos los visitantes que ingresen a la Entidad, durante su permanencia en las instalaciones del INS.
19. Velar por la seguridad de la información de los equipos de cómputo que salgan de la institución, lo cual se realizar únicamente con autorización del Jefe inmediato.
20. Utilizar la documentación física generada, recibida y en general, manipulada por los funcionarios, únicamente para el ejercicio de las responsabilidades de la Entidad de acuerdo con las funciones del servidor público o actividades que realice el contratista o tercero, so pena del inicio de las acciones a que haya lugar, en concordancia con la normatividad.
21. Tomar las medidas a que haya lugar, una vez se tenga conocimiento de incidentes de seguridad o violación a las medidas que han sido tomadas para garantizar la seguridad de la información.
22. Bloquear el acceso a las páginas de contenido para adultos, mensajería Instantánea y demás páginas que no sean de uso corporativo mediante el uso de servidor proxy, firewall o el software institucional.
23. Definir y Divulgar el procedimiento para la realización copias de seguridad de la Información y velará por su archivo y custodia de acuerdo con la normatividad.
24. Realizar de manera periódica pruebas de funcionamiento de las copias de seguridad para garantizar su correcta recuperación en el caso de ser necesario.
25. Instalar o desinstalar software o programas de cómputo los cuales en todo caso contarán con las licencias de uso respectivas. Los funcionarios de la entidad no podrá instalar ningún programa sin la autorización respectiva y de acuerdo con sus funciones. lo anterior se realiza a través de la Oficina TIC.
26. Tomar las demás medidas a que haya lugar, en desarrollo y estandarización de la presente política de Seguridad de la Información.

ARTICULO SEXTO. Responsables. El Responsable Institucional de la implementación, aplicación, seguimiento 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 grupo de soporte tecnológico de la secretaria general, propietarios de la información, funcionarios, contratistas y practicantes usuarios de la

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

información, sin perjuicio de las funciones del Comité Institucional de Desarrollo Administrativo y la Oficina de Control Interno.

ARTICULO SEPTIMO. Responsabilidades Específicas frente a la Seguridad de la Información y al Sistema de Gestión de Seguridad de la Información.

I. RESPONSABILIDADES DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

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 dalos 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) Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los dalos e información gestionados en la Institución.
h) Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior del Instituto.
i) Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Dirección General y las diferentes direcciones.
j) Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.

II) RESPONSABILIDADES DEL AREA DE SOPORTE TECNOLÓGICO DE LA SECRETARIA GENERAL

a) Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios.
b) Resolver cualquier problema o mantenimiento que pueda afectar la normal prestación de los mismos; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes Direcciones, Jefaturas o Coordinaciones siguiendo el procedimiento establecido.
c) Establecer, mantener y divulgar las políticas y procedimientos de los servicios de tecnología, incluidos todos los capítulos que hacen parte de esta Política, en toda la institución de acuerdo a las mejores prácticas y directrices de la Entidad y del Gobierno.
d) Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado.
e) Brindar el soporte necesario a los usuarios a través del apoyo del Recurso Humano y los diversos canales de apoyo y ayuda que se han implementados en el INS.

III) 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, propia 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) Determinar los tiempos de retención de la información en conjunto con él grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.
e) 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.
f) Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y practicantes en las diferentes dependencias del Instituto.

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

a) 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 – Ley 734 de 2002 o Contrato.

b) 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.
c) Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
d) Evitar la divulgación no autorizada o el uso indebido de la información.
e) Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
f) Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
g) Proteger los dalos 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.
h) Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
i) Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico científico designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos al Instituto al a 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.
j) 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.
k) Divulgar, aplicar y el cumplir con la presente Política.
l) 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 dalos 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 Talento Humano o de la Oficina Asesora Juridica.
m) Proteger y resguardar su información personal que no esté relacionada con sus funciones en la 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.

ARTICULO OCTAVO. 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, la política para la protección de datos personales establecida en la ley estatutaria No 1581 de 2012 y se dictan otras disposiciones*" 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 2º y 3º de lo Resolución 1607 de 2014 y demás disposiciones que la complementen, sustituyan o adicionen.

ARTICULO NOVENO. La Oficina de Control Interno verificará el cumplimiento de las estrategias establecidas en el artículo 5º, de acuerdo con sus funciones, a partir de la firma y divulgación de éste documento y realizará el seguimiento correspondiente al Sistema de Gestión de Seguridad de la Información.

ARTICULO DECIMO. La presente resolución rige a partir de la fecha de su expedición y deroga la Resolución No 1629 de 2015.

Dada en Bogotá D.C., a los 23 OCT 2017

COMUNÍQUESE Y CÚMPLASE

EL DIRECTOR GENERAL (E)

FRANKLYN EDWIN PRIETO ALVARADO

Revisó: Luis Ernesto Flórez Simanca, Jefe Oficina Asesora Jurídica - Jefe Oficina Asesora de Planeación (E).
Esperanza Martinez Garzon, Secretaria General
Adecuación Juridica: Anderson Alberto Lopez Pinilla.
Proyectó: Elsa Marlen Baracaldo Huertas, Jefe Oficina Techología de la Información y comunicaciones.