INSTITUTO NACIONAL DE SALUD

RESOLUCION NÚMERO 1629 DE 2015

(30 DIC.)

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

LA DIRECTORA 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 Modelo de Seguridad y Privacidad de la Información expedido por el Gobierno Nacional y revisado el 3 de marzo de 2015, tiene como objetivos "*a) Contribuir al incremento de la transparencia en la gestión pública. b) Dar lineamiento para la implementación de la gestión de la seguridad y privacidad de la información, en las entidades del estado. c) Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de ciberseguridad en la entidad. d) Alinear el marco de referencia de arquitectura empresarial con los principios de seguridad y privacidad de la información."*

Que el Ministerio de Tecnología de Información y Comunicaciones emitió la guía para la implementación de la política de seguridad y privacidad de la Información, 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.

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 teniendo en cuenta lo anterior, la Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del INSTITUTO NACIONAL DE SALUD con respecto a la protección de los activos de información según lo establecido en la "Guía de Clasificación de Activos de Información" relacionado en la versión 3 del "Modelo de Seguridad y privacidad de la Información" del 3 de Marzo de 2015 y que soportan los procesos de la Entidad y apoyan la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Que como consecuencia de lo anterior, este Despacho

R E S U E L V E:

ARTÍCULO PRIMERO.- Adopción y objeto. Adóptese la política de seguridad de la información para el Instituto Nacional de Salud establecida por el Gobierno Nacional, cuyo objeto es asegurar la información como activo fundamental para la prestación de sus servicios y la toma de decisiones; razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad, que hace parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 2573 del 12 de diciembre de 2014.

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

PARAGRAFO: El Instituto Nacional de Salud, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, 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) 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 su totalidad, sin perjuicio de las sanciones a que haya lugar.

ARTÍCULO CUARTO.- Definición Política General 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.

ARTÍCULO QUINTO.- Definición de las Políticas de la Seguridad de la Información que soportan el SGSI. Las políticas de Seguridad de la Información establecidas por el INS son:

1. La entidad ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios 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. La entidad protegerá 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. La entidad protegerá 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. La entidad limitará el acceso a los activos de información dependiendo de su clasificación según lo establecido en el marco de la normatividad.
5. La entidad protegerá 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. La entidad controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. La entidad garantizará 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. La entidad realizará evaluaciones 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. La entidad protegerá 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.

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

10. La entidad preservará 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. La entidad velará 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. La entidad informará a los terceros sobre la presente política de Seguridad de la Información y velará 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. La entidad implementará los controles necesarios para dar manejo a los riesgos detectados y proveerá un nivel de protección de la información apropiado y consistente.
14. La entidad administrará 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. Se garantizará que el INS cuente con 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.
16. 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.
17. La entidad otorgará 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.
18. Se restringirá el acceso a los funcionarios de la Entidad, contratistas, colaboradores o terceros, sólo a áreas a las cuales tengan la debida autorización.
19. Se deberán custodiar en todo momento y sin excepción a todos los visitantes que ingresen a la Entidad, durante su permanencia en las instalaciones del INS.
20. Los funcionarios, contratistas o colaboradores son responsables 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.
21. La documentación física generada, recibida y en general, manipulada por los funcionarios deberá ser utilizada 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.
22. La entidad tomará 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.
23. La entidad bloqueará 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.
24. La entidad definirá y divulgará el procedimiento para la realización copias de seguridad de la Información y velará por su archivo y custodia de acuerdo con la normatividad.
25. La entidad realizará de manera periódica pruebas de funcionamiento de las copias de seguridad para garantizar su correcta recuperación en el caso de ser necesario.
26. La oficina de TIC es la única Dependencia autorizada para 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.
27. La entidad tomará 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, sin perjuicio de las funciones del Comité Institucional de Desarrollo Administrativo.

ARTICULO SEPTIMO. 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.

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

ARTICULO OCTAVO. La Oficina de Control Interno verificará el cumplimiento de las políticas 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 NOVENO. La presente resolución rige a partir de la fecha de su expedición y deroga las disposiciones que le sean contrarias.

Dada en Bogotá D.C., a los

COMUNÍQUESE Y CÚMPLASE

LA DIRECTORA GENERAL (E)

MARTHA LUCIA OSPINA MARTINEZ

Revisó: Martha Gemma Gomez Lopez, Secretaria General (E)
Angela Liliana Albarracin Cardenas, Jefe (E) Oficina Asesora Juridica
Luis Antonio Ayala, Coordinador Grupo de Desarrollo Institucional.
Elsa Marlen Baracaldo, Jefe Oficina Tic.
Adecuación Juridica: Anderson Alberto Lopez Pinilla, Abogado
Proyectó: Isabel Martínez.