MINISTERIO DE CULTURA
INSTITUTO CARO Y CUERVO

RESOLUCIÓN NÚMERO 0272 **DE 2017**

(28 NOV. 2017)

"Por la cual se adopta la política de seguridad de activos de información y se definen lineamientos frente a su uso y manejo."

LA DIRECTORA GENERAL DEL INSTITUTO CARO Y CUERVO

En uso de sus facultades legales y estatutarias señaladas en los artículos 78 de la ley 489 de 1998 y 2.2.9.1.2.3 del Decreto 1078 de 2015, en especial las que confiere el Decreto 2712 de 2010,

CONSIDERANDO:

Que el título Sexto de la Ley 30 de 1992, respecto de la disposiciones generales, especiales y transitorias, en su Capítulo II, y en su artículo 137 dispone respecto al Instituto Caro y Cuervo lo siguiente:

Artículo 137. La Escuela Superior de Administración Pública –ESAP–, el Instituto Tecnológico de Electrónica y Comunicaciones –ITEC–, el Instituto Caro y Cuervo, la Universidad Militar Nueva Granada, las Escuelas de formación de las Fuerzas Militares y de la Policía Nacional que adelanten programas de educación superior, y el Servicio Nacional de Aprendizaje –SENA–, continuarán adscritas a las entidades respectivas. Funcionarán de acuerdo con su naturaleza jurídica y su régimen académico lo ajustarán conforme a lo dispuesto en la presente ley.

Que el Instituto Caro y Cuervo es una Institución de Educación Superior –IES–, que está en el rango de instituciones universitarias o escuelas tecnológicas y el SNIES del Instituto Caro y Cuervo aparece como Institución universitaria / Escuela tecnológica.

Que el artículo 2 del Acuerdo 0002 del 8 de julio de 2010 del Instituto Caro y Cuervo, señala que es un establecimiento público del orden nacional, adscrito al Ministerio de Cultura, de altos estudios y de investigación científica, dotado de personería jurídica, autonomía administrativa y financiera y patrimonio propio e independiente, creado por la Ley 5 de 1942 el cual se reorganiza conforme a las disposiciones establecidas por la ley 489 del 29 de diciembre de 998 y las contenidas en los presentes estatutos; y en su artículo 4 destaca que el objeto es promover y desarrollar la investigación, la docencia, el asesoramiento y la divulgación de las lenguas del territorio nacional y de sus literaturas, con miras a fortalecer su uso y reconocimiento con base en el prestigio social y valoración estética. Con este fin, el Instituto Caro y Cuervo asesora al Estado colombiano y contribuye en la elaboración de políticas para el fortalecimiento y conservación del patrimonio inmaterial de la Nación.

Que mediante el Decreto 1080 del 26 de mayo de 2015, denominado "Único reglamentario del sector cultura", en el artículo 1.1.4.1.1, ratifica al Instituto Caro y Cuervo en calidad de establecimiento público adscrito al Ministerio de Cultura.

En cumplimiento de la Ley 1341 de 2009 –Ley TIC (Tecnologías de la Información y las Comunicaciones)–, se requiere incrementar en las entidades del estado acciones de implementación y uso de las tecnologías de la información y la comunicación.

En lo referente a seguridad de la información, la anotada Ley 1341 de 2009, en su artículo 2 señala como principios orientadores y aspectos fundamentales para la promoción de la libre competencia y el comercio electrónico, los siguientes: 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 de Gobierno en línea.

En concordancia con sus funciones y en virtud de la iniciativa de Buen gobierno y de la estandarización, gestión y seguridad de la información del Estado, el Viceministerio de Tecnologías y sistemas de la información formula el proyecto de fortalecimiento de las tecnologías de la información en la gestión del estado y la información pública, desde el cual se pretende formular políticas públicas y estándares, desarrollar capacidades para la gestión efectiva, acompañar y facilitar procesos de adopción e implementación de buenas prácticas para la gestión de TI en el Estado; dichas pruebas quieren cumplir con el objetivo de fortalecer los mecanismos de seguimiento y medición de la gestión, la seguridad y privacidad de TI en las entidades del Estado y en la actividad de implementar mecanismos de seguimiento que permitan realizar las mediciones que conlleven a establecer los avances en la gestión, seguridad y privacidad de TI en los sectores y entidades del Estado.

Que mediante la Ley 1273 de 2009 se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos", tipificando penalmente las conductas contra la confidencialidad, la integridad, la disponibilidad de los datos y de los sistemas informáticos.

Que el artículo 45 de la Ley 1753 del 9 de junio de 2015, establece el Plan Nacional de Desarrollo 2014–2018, en el que señala que se deben establecer estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano y aplicarán los siguiente casos entre otros: d) Publicación de datos abierto, f) Implementación de la Estrategia de gobierno en línea, g) Marco de referencia de arquitectura empresarial para la gestión de las tecnologías de información en el Estado, j) Interoperabilidad de datos como base para la estructuración de la estrategia que sobre la captura, almacenamiento, procesamiento, análisis y publicación de grandes volúmenes de datos (*big data*) formule el Departamento Nacional de Planeación.

Que el decreto 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de gobierno en línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes el de la seguridad y privacidad de la información, comprendido por las acciones transversales a los componentes de TIC para servicios, TIC para Gobierno abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, acceso, divulgación, eliminación o destrucción no autorizada.

Que dada la función establecida en el artículo 2.2.9.1.2.3 del Decreto 1078 de 2015 para el representante legal de los sujetos obligados, respecto a la coordinación de la implementación de la Estrategia de gobierno en línea, se hace necesario adoptar la política de seguridad de activos de información alineándola con las normas de protección de datos personales contenidas en la Ley 1581 de 2012, las normas de transparencia y acceso a la información de la Ley 1712 de 2014, así como aquellas que las han reglamentado.

Que el Gobierno Nacional, a través del Documento CONPES 3854 del 11 de abril de 2016, establece la *política nacional de seguridad digital* que busca "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".

Para cumplir con este objetivo, la política nacional de seguridad digital, entre otras acciones propone "Establecer un marco institucional para la seguridad digital, consistente con un enfoque de

gestión de riesgos" esto a su vez impulsado por la estrategia de "Implementar en el Gobierno nacional un modelo de gestión de riesgos de seguridad digital".

Que por lo anterior se hace necesario adoptar la política de seguridad de tecnologías de la información y las comunicaciones para el Instituto Caro y Cuervo.

Que en mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO. Adoptar la política de seguridad de tecnologías de la información y las comunicaciones TIC, la cual se encuentra descrita en el anexo que hace parte integral del presente acto administrativo y consta de veintinueve (29) folios.

PARÁGRAFO PRIMERO: La política antes adoptada se refiere a los siguientes temas: a) Gestión de activos de información, b) Uso de los activos de información, c) Respaldo y restauración de la información, d) Seguridad dirigida a los recursos humanos, e) Uso de correo electrónico, f) Uso de internet, g) Gestión de claves de acceso a los sistemas de información, h) Escritorio y pantalla limpia, i) Uso de estaciones cliente, j) Gestión y adquisición de bienes y servicios tecnológicos, k) Desarrollo y mantenimiento de sistemas de información, l) Prestación de servicios por terceros, m) Gestión de contenidos de páginas web (web máster), n) Uso de mensajería instantánea y redes sociales, ñ) Control de acceso a la red de datos LAN, o) Uso de puntos de red de datos LAN, p) Uso de dispositivos periféricos y de almacenamiento, q) Uso de servicios de impresión, r) Retención y archivo de datos, s) Seguridad de los centros de procesamiento de datos, t) Seguridad para la telefonía IP y u) Gestión y uso de la red eléctrica regulada.

PARÁGRAFO SEGUNDO: La política de seguridad de activos de información del Instituto Caro y Cuervo contiene la información relacionada con: investigaciones, encuestas de seguridad, estratificación, autoevaluación, generalidades de la política, gestión de riesgos, clasificación de activos, controles, indicadores, implementación de políticas, procedimientos y correspondencia de estándares.

ARTÍCULO SEGUNDO. Es responsabilidad de la alta dirección prestar el apoyo necesario para la implementación de la política de seguridad de la información y la verificación de su cumplimiento está a cargo del Coordinador de TIC del Instituto Caro y Cuervo.

ARTÍCULO TERCERO: La política de seguridad de tecnologías de la información y las comunicaciones TIC del Instituto Caro y Cuervo protege, preserva y administra la integridad, confidencialidad y disponibilidad de la información digital en el marco de la operación de sus procesos, a través de la implementación de mecanismos de seguridad físicos y lógicos.

ARTÍCULO CUARTO. Ámbito de aplicación. La política de seguridad de tecnologías de la información y las comunicaciones TIC, aplica para todos los usuarios de la red de datos del Instituto Caro y Cuervo en todas sus sedes.

ATÍCULO QUINTO. Objetivos. La política tiene los siguientes objetivos:

- Brindar mecanismos que permitan asegurar la confidencialidad, la disponibilidad, la integridad y la confiabilidad de la información del Instituto Caro y Cuervo.

- Implementar planes de contingencia que permitan mitigar los incidentes de seguridad de la información del Instituto Caro y Cuervo.
- Establecer los lineamientos necesarios para la adquisición, gestión, parametrización y mantenimiento de los recursos tecnológicos del Instituto Caro y Cuervo.
- Gestionar los riesgos de seguridad de la información.

ARTÍCULO SEXTO. Actualizaciones. La política de seguridad de tecnologías de la información y las comunicaciones TIC será revisada semestralmente o cuando sea necesario, teniendo en cuenta la evolución de la tecnología, las amenazas de seguridad y los nuevos aportes legales en la materia, con el fin de garantizar su oportunidad, eficiencia y eficacia. Este proceso será gestionado y divulgado por el grupo de las TIC a los usuarios de la red de datos del Instituto Caro y Cuervo.

ARTÍCULO SÉPTIMO. De conformidad con lo preceptuado en el inciso primero del artículo 65 de la ley 1437 de 2011, publíquese el presente acto administrativo en el diario oficial y en la página web de la entidad

ARTÍCULO OCTAVO La presente Resolución rige a partir de la fecha de su publicación y deroga las demás disposiciones que le sean contrarias.

PUBLIQUESE, Y CÚMPLASE
Dada en Bogotá D.C., a los 28 NOV. 2017

CARMEN MILLÁN

Proyectó: Carlos Fredy Rey Camacho – Coordinador Grupo de las TIC
Revisó y ajustó: Oscar Fonseca, Abogado ICC
Revisó: Paola Gaitán – Subdirectora Administrativa y Financiera

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO