RESOLUCIÓN 184 DE 2014

(abril 24)

Diario Oficial No. 49.137 de 29 de abril de 2014

AGENCIA NACIONAL PARA LA SUPERACIÓN DE LA POBREZA EXTREMA

Por la cual se adopta la Política de Seguridad y se definen lineamientos frente al uso y manejo de la información de la Agencia Nacional para la Superación de la Pobreza Extrema (Anspe).

LA DIRECTORA GENERAL DE LA AGENCIA NACIONAL PARA LA SUPERACIÓN DE LA POBREZA EXTREMA (ANSPE),

en ejercicio de sus atribuciones legales y reglamentarias y en particular las establecidas en el Decreto 4160 de 2011, artículo 8o numeral 11, y

CONSIDERANDO:

Que mediante Decreto 4160 de 2011 se crea la Unidad Administrativa Especial Agencia Nacional para la Superación de la Pobreza Extrema, dotada de personería jurídica, autonomía administrativa y financiera y patrimonio propio, perteneciente al Sector Administrativo de Inclusión Social y Reconciliación con el objetivo de participar, con otras entidades competentes y los entes territoriales, en la formulación de política pública para la superación de la pobreza extrema y coordinar la implementación de la estrategia nacional de superación de la pobreza extrema a través de la articulación con actores públicos y privados y la promoción de la innovación social, entre otros.

Que el artículo 227 de la Ley 1450 de 2011, por la cual se expide el Plan Nacional de Desarrollo 20102014, señala que para el ejercicio de sus competencias, las entidades públicas y los particulares que cumplen con funciones públicas deberán poner a disposición de la Administración Pública, bases de datos de acceso permanente y gratuito con la información que producen y administran. De igual forma, el parágrafo 3o del mismo artículo señala que el Gobierno Nacional debe garantizar, mediante la implementación de sistemas de gestión para la seguridad de la información, que el acceso a las bases de datos y la utilización de la información sean seguros y confiables para no permitir su uso indebido.

Que la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, en su artículo 4o, literales g) y h), define como principios rectores para el tratamiento de los datos personales, la seguridad y confidencialidad, respectivamente.

Que el artículo 3o, literal d) del Decreto 2482 de 2012, por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión, adopta la política de eficiencia administrativa, incluyendo entre sus orientaciones, la gestión de tecnologías de información. Asimismo, se entiende que su modelo de gestión define la necesidad de contar con un Sistema de Seguridad de la Información.

Que el artículo 7o del Decreto 2693 de 2012, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011 y se dictan otras disposiciones, establece los componentes del Modelo de Gobierno en Línea, y a su vez el numeral 6 del mencionado artículo

dispone que la Entidad debe contar con una política de seguridad aplicada de forma transversal y mejorada constantemente.

Que la proliferación de amenazas en contra de la información hace necesaria la implementación de mecanismos de seguridad física y lógica, que permitan minimizar los riesgos de daños y pérdidas en la información y poder garantizar su integridad, disponibilidad y confidencialidad.

Que la Agencia Nacional para la Superación de la Pobreza Extrema (Anspe), reconoce abiertamente la importancia de sus activos de información, así como la necesidad de su protección para disminuir los riesgos inherentes asociados a su uso y manejo, por lo tanto ve conveniente la implementación de una política de seguridad y manejo de la información.

Que la política de seguridad de la información debe ser parte de la cultura organizacional y, apoyada por la alta dirección de la Agencia, deberá divulgarse a todos los servidores públicos y contratistas de prestación de servicios y de apoyo a la gestión, operadores y aliados, que de una u otra manera hacen parte de la gestión de la entidad.

Que en mérito de lo expuesto,

RESUELVE:

CAPÍTULO I.

DISPOSICIONES GENERALES.

ARTÍCULO 1o. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. En virtud del mandato constitucional la Agencia Nacional para la Superación de la Pobreza Extrema (Anspe), protege, preserva y administra la integridad, confidencialidad y disponibilidad de la información digital o física generada en el desarrollo de sus procesos misionales, estratégicos y de apoyo, a través de la implementación de mecanismos de seguridad como controles físicos y lógicos, que permitan prevenir fraudes y fuga de información que atente contra los derechos de los ciudadanos y la integridad de la Entidad.

ARTÍCULO 2o. ÁMBITO DE APLICACIÓN. Lo contenido en la presente Resolución aplica para toda la Entidad en el territorio nacional, donde la Agencia Nacional para la Superación de la Pobreza Extrema (Anspe) tenga presencia y desarrolle su acompañamiento a través de la recolección, procesamiento, almacenamiento, recuperación y consulta de información, para el desarrollo de la misión institucional y cumplimiento de los objetivos estratégicos. La Política de Seguridad de la Información, extiende su alcance a los funcionarios y contratistas de la Agencia, recursos tecnológicos, la totalidad de los procesos y procedimientos institucionales requeridos para su gestión, a sus operadores y aliados, sean estos de carácter público o privado, así como a sus contratistas y proveedores.

ARTÍCULO 3o. OBJETIVOS. Son objetivos de la Política de Seguridad de la Información de la Anspe, los siguientes:

– Proteger la información y la tecnología utilizada para su almacenamiento, procesamiento y análisis, frente a amenazas de cualquier tipo, deliberadas o accidentales, ya sea por el personal interno o externo con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información que hace parte de la gestión, y que sostiene la operación en la entidad.

– Asegurar la implementación y efectividad de los controles de seguridad en el marco de la presente política, asignando las responsabilidades inherentes a los funcionarios y contratistas de la Agencia, así como los recursos físicos, financieros y tecnológicos, necesarios para su ejecución y sostenimiento.

– Generar competencias organizacionales en materia de Seguridad de la Información.

– Prevenir los incidentes de seguridad de la información en la Agencia.

CAPÍTULO II.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 4o. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN. Las funciones que debían ser cumplidas por el Comité de Seguridad de la Información existente serán asumidas por el Comité de Gobierno en Línea, Antitrámites y Eficiencia Administrativa – Cero Papel.

PARÁGRAFO. Es responsabilidad de la alta dirección de la Agencia y de quien tenga personal a cargo, prestar el apoyo necesario para la implementación de la Política de Seguridad de la Información dentro de sus áreas, así como el cumplimiento de la política por parte de su equipo de trabajo.

CAPÍTULO III.

POLÍTICAS GENERALES DE MANEJO DE INFORMACIÓN.

ARTÍCULO 5o. ACUERDOS DE CONFIDENCIALIDAD. Como parte de sus términos y condiciones iniciales de trabajo, los funcionarios o contratistas, cualquiera sea su nivel jerárquico dentro de la entidad, firmarán un Acuerdo de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la entidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013 y la Sentencia de Unificación 458 de 2012 de la Corte Constitucional. Dicho acuerdo (documento original) deberá ser guardado y custodiado en forma segura por el Área de Talento Humano o el Grupo de Gestión Contractual, según el caso, si tal acuerdo de confidencialidad de la información no estuviere incluido como una cláusula del respectivo contrato de prestación de servicios o en el Acta de Posesión del funcionario. Así mismo, mediante el acuerdo de confidencialidad, el funcionario o el contratista declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos del funcionario o contratista.

ARTÍCULO 6o. TRATAMIENTO DE LA INFORMACIÓN. Para el tratamiento de la información de las familias a las cuales se presta el acompañamiento en el marco de la Estrategia Unidos, así como la información de los servidores públicos que participan en el desarrollo de las funciones de la Agencia, se cumplirá con lo dispuesto en la Ley 1581 de 2012, reglamentada por el Decreto 1377 de 2013, y las demás normas que los modifiquen, adicionen o complementen.

PARÁGRAFO. La Oficina de Tecnologías de la Información garantizará la generación de reportes y entrega de información concernientes a las familias vinculadas a la estrategia, siempre

que las diferentes áreas, oficinas o direcciones lo soliciten y estos no estén incluidos en el módulo de reportes del Sistema de Información SIUnidos. Esta solicitud deberá ser dirigida por medio formal al Jefe de Oficina, quien de acuerdo con la normatividad vigente y teniendo en cuenta el cumplimiento misional, determinará si es viable la entrega y dará respuesta mediante comunicado oficial.

ARTÍCULO 7o. POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN. La Agencia Nacional para la Superación de la Pobreza Extrema (Anspe), establecerá los lineamientos para la identificación, clasificación y buen uso de sus activos de información, con el objetivo de garantizar su protección.

a) Inventario de Activos: Los activos de la Anspe deben ser identificados y controlados para garantizar su uso adecuado, protección y la recuperación ante desastres. Por tal motivo, el Grupo de Gestión Administrativa debe llevar el inventario valorizado de los bienes de propiedad de la Anspe, discriminado por dependencias y según lo estipulado en el procedimiento de inventarios.

Con el objetivo de la implantación de controles de seguridad, las oficinas que tienen a su cargo la custodia de la información generada por los diferentes procesos de la Entidad, se encargarán de mantener y actualizar un inventario de activos de información relacionados con los servicios de cada dependencia, así como de los servicios, software, hardware y personas, relacionadas con ese proceso;

b) Tratamiento de Activos de Información: La clasificación de esta información debe estar alineada con las Tablas de Retención Documental;

c) Archivos de Gestión: Desde el Sistema de Gestión de Seguridad de la Información se impartirán lineamientos de Seguridad de la Información al Grupo de Gestión Administrativa para generar mecanismos de almacenamiento seguro a las oficinas para la custodia de su información;

d) Respaldo de la Información: La Oficina de Tecnologías de la Información debe realizar y mantener copias de seguridad de la información de la entidad en medio digital, siempre que esta sea reportada por el responsable de la misma, con el objetivo de recuperarla en caso de cualquier tipo de falla, ya sea de hardware, software, o de procedimientos operativos al interior de la entidad.

Se efectuará la copia respectiva de acuerdo con el esquema definido previamente en el documento “Plan de Backups” de la Entidad, el cual será diseñado por la Oficina de Tecnologías de la Información, en conjunto con los líderes de Proceso;

e) Clasificación de la Información: El método de clasificación de la información de la Anspe está basado en el método de separación recomendado por “Gobierno en Línea” en el documento “Guía para la apertura de datos en Colombia”, el cual permite filtrar la información no publicable de la que sí lo es, de conformidad con lo estipulado en la normatividad vigente. La Oficina de Tecnologías de la Información, en conjunto con la Secretaría General, la Oficina de Comunicaciones y la Oficina Asesora de Planeación, se encargarán de proponer los lineamientos de recolección y clasificación de la información, para la posterior aprobación por parte de la Dirección.

CAPÍTULO IV.

RESPONSABILIDADES DE LOS FUNCIONARIOS, CONTRATISTAS Y COLABORADORES EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 8o. Todos los funcionarios, contratistas y colaboradores que hagan uso de los activos de información de la Anspe, tienen la responsabilidad de seguir las políticas establecidas para el uso aceptable de los activos, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la continuidad de la misión institucional.

a) Del Uso del Correo Electrónico: El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios y contratistas de la Anspe.

-- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de orden institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad.

-- En cumplimiento de la Directiva Presidencial número 04 de 2012, Cero Papel y eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que las circunstancias lo permitan.

-- Está prohibido el uso de correos masivos tanto internos como externos, salvo a través de la Oficina de Comunicaciones, Dirección General o Secretaría General.

-- Todo mensaje SPAM o Cadena debe ser inmediatamente reportado a la mesa de servicios según procedimiento establecido, eliminado y nunca respondido. No está permitido el envío y/o reenvío de mensajes en cadena.

-- Todo mensaje sospechoso respecto de su remitente o contenido debe ser inmediatamente reportado a la mesa de servicios según procedimiento establecido y posteriormente eliminado, ya que puede ser contentivo de virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, tengan explícitas referencias eróticas, o alusiones a personajes famosos.

-- La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de compras, deportivos, agencias matrimoniales, casinos, o a cualquier otra ajena a los fines de la Anspe.

-- Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.

-- Está expresamente prohibido distribuir información de la Anspe, no pública, a otras entidades o ciudadanos sin la debida autorización.

-- El cifrado del correo electrónico no es necesario en la mayoría de casos, pero los mensajes confidenciales deben tener alguna forma de codificación.

-- Todos los correos electrónicos corporativos deben contener una sentencia de confidencialidad, que será diseñada por la Oficina de Tecnologías de la Información, y la Oficina de Comunicaciones

-- La divulgación de cifras o datos oficiales de la Entidad solo podrá ser emitida desde las

direcciones de correo electrónico de la Dirección General, la Oficina de Comunicaciones, Jefes de Oficina de Tecnologías de la Información y Oficina Asesora de Planeación.

-- El único servicio de correo electrónico autorizado para el manejo de la información institucional en la Entidad es el asignado por la Oficina de Tecnologías de la Información, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso. Además, este servicio tiene copia de respaldo (backup);

b) Del uso de Internet: Se establecerán políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, previa validación de la Oficina de Tecnologías de la Información.

-- El uso del Servicio de Internet está limitado exclusivamente para propósitos laborales.

-- Los servicios a los que un determinado usuario pueda acceder desde la Internet dependerán del rol o funciones que desempeña el usuario en la Anspe y para los cuales esté formal y expresamente autorizado.

-- Todo usuario es responsable de informar de contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones dentro de la Anspe.

-- Está expresamente prohibido el envío, y/o descarga, y/o visualización, de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.

-- Está expresamente prohibido el acceso a páginas web, portales, sitios web y/o aplicaciones web que no hayan sido autorizadas por la Anspe.

-- Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas, y/o de procedencia desconocida.

-- Está expresamente prohibida la propagación de virus o cualquier tipo de código malicioso.

-- Está expresamente prohibido acceder a páginas que agredan la ética y el buen comportamiento.

La Anspe se reserva el derecho de monitorear los accesos, y por tanto el uso del Servicio de Internet de todos sus funcionarios o contratistas, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines;

c) Del Uso de los Recursos Tecnológicos: Los recursos tecnológicos de la Anspe, son herramientas de apoyo a las labores y responsabilidades de los funcionarios y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

-- Los bienes de cómputo se emplearán de manera exclusiva y bajo su completa responsabilidad por el funcionario y contratista al cual han sido asignados y únicamente para el correcto desempeño de las funciones del cargo. Por lo tanto, no pueden ser utilizados con fines personales o por terceros no autorizados.

-- Solo está permitido el uso de software licenciado por la Entidad y/o aquel que sin requerir licencia sea expresamente autorizado por la Oficina de Tecnologías de la Información. Las aplicaciones generadas por la Anspe, en desarrollo de su Misión Institucional, deben ser

reportadas a la Oficina de Tecnologías de la Información, para su administración.

-- Es responsabilidad de los funcionarios y contratistas mantener copias de seguridad de la información contenida en sus estaciones de trabajo.

-- Los usuarios no deben mantener almacenados en los discos duros, de las estaciones cliente o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional.

-- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren estos elementos tecnológicos.

-- No está permitido realizar derivaciones eléctricas desde las fuentes de corriente regulada ni conectar multitomas a las mismas.

-- Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los funcionarios de la Oficina de Tecnologías de la Información o quienes sean designados por ellos para tal labor.

-- La Oficina de Tecnologías de la Información realizará monitoreo sobre los dispositivos de almacenamientos externos, con el fin de prevenir o detectar fuga de información.

-- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la mesa de ayuda vinculada a la Oficina de Tecnologías de la Información, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de dicho grupo de trabajo.

-- El retiro de recursos tecnológicos de la entidad solo está permitido, previa autorización del Grupo de Gestión Administrativa, y deberá ajustarse a los procedimientos y competencias de dicho grupo de trabajo.

-- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, debe ser informada de inmediato al Grupo de Gestión Administrativa por el funcionario o contratista a quien se le hubiere asignado.

-- Todo problema de orden técnico con los equipos tecnológicos debe ser reportado con el procedimiento establecido por la Oficina de Tecnologías de la Información a la mayor brevedad posible.

-- La Oficina de Tecnologías de la Información es la única dependencia autorizada para realizar copias del software licenciado por la Entidad, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.

-- Todo acceso a la red de la Entidad mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la Oficina de Tecnologías de la Información.

-- Los equipos deben quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina durante la noche, esto es, con el fin de proteger la seguridad y distribuir bien los recursos de la Entidad, siempre y cuando no vaya a realizar actividades vía VPN.

d) Del Uso de los Sistemas de Información: Todos los funcionarios y contratistas de la Anspe son

responsables de la protección de la información que acceden y/o procesan y de evitar su pérdida, alteración, destrucción y/o uso indebido.

-- Por ningún motivo se otorgará acceso a los orígenes de datos en ningún ambiente (desarrollo, pruebas o producción) a funcionarios o contratistas que no estén explícitamente asignados a la Oficina de Tecnologías de la Información.

-- Las credenciales de acceso a la red y/o recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y contratistas no deben revelar estas a terceros ni utilizar claves ajenas.

-- Todo funcionario y contratista es responsable de los registros y/o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.

-- En ausencia del funcionario y contratista, el acceso a la estación de trabajo debe ser bloqueado, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. La Oficina de Tecnologías de Información, aplicará políticas de bloqueo, correspondiente.

-- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato de la Anspe, todos los privilegios sobre los recursos informáticos otorgados deberán ser suspendidos inmediatamente; la información del empleado debe almacenarse en los servidores de la entidad y entregado al Jefe de la Oficina de Tecnologías de la Información.

-- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato de la Anspe, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información.

-- Todos los funcionarios y contratistas de la Entidad deben revisar, e investigar los derechos de propiedad intelectual para todo material como libros, artículos, informes, imágenes, software y/o sitios web encontrados en Internet antes de ser usados para cualquier propósito, haciendo referencia expresa de dichas fuentes, con el fin de asegurar el cumplimiento de las leyes que aplican para este tipo de información.

CAPÍTULO V.

POLÍTICAS ESPECÍFICAS.

ARTÍCULO 9o. El Sistema de Gestión de Seguridad de la Información, en conjunto con las áreas o procesos responsables, impartirán los lineamientos generales acordes con cada uno de los capítulos de la Política de Seguridad de la Información, estableciendo aquellos lineamientos específicos de Seguridad de la Información para la Agencia Nacional para la Superación de la Pobreza Extrema, los cuales contendrán:

a) Lineamientos de la Seguridad de los Recursos Humanos;

b) Lineamientos de Seguridad Física y del Entorno;

c) Lineamientos de Gestión de Comunicaciones y Operaciones;

d) Lineamientos de Control de Accesos;

e) Lineamientos de Adquisición, Desarrollo y Mantenimiento de Software;

f) Lineamientos de Continuidad de la Operación de la Entidad;

g) Lineamientos de Manejo de Incidentes y Requerimientos;

h) Lineamientos de Seguridad para la Gestión Documental;

i) Lineamientos de Protección de Datos Personales;

j) Demás lineamientos que son aplicables al SGSI y no se enmarcan en los ítems anteriores.

CAPÍTULO VI.

REVISIÓN Y VIGENCIA.

ARTÍCULO 10. REVISIÓN. La Política de Seguridad de la Información será revisada semestralmente, o antes si existiesen modificaciones que así lo requieran, para garantizar que sigue siendo oportuna, suficiente y eficaz. Este proceso de revisión será liderado por el encargado del SGSI y la Jefatura de la Oficina de Tecnologías de la Información, con aprobación de la Dirección General de la Anspe.

ARTÍCULO 12. <sic, es 11>. VIGENCIA. La presente resolución rige a partir de la fecha de su publicación.

Publíquese, comuníquese y cúmplase.

Dada en Bogotá, D. C., a 24 de abril de 2014.

La Directora General,

BEATRIZ LINARES CANTILLO.

Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.
Normograma del Ministerio de Relaciones Exteriores
ISSN 2256-1633
Última actualización: 31 de agosto de 2019