POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL

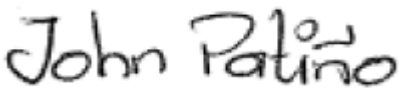
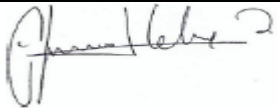
REVISÓ	APROBÓ
 Nombre: **JOHN EDILSON PATIÑO TENORIO** Coordinador Grupo Gobernabilidad de TI Fecha: 30-10-2020	 Nombre: **ALFONSO JAVIER CELEDÓN SIMÓN** Jefe Oficina Tecnologías de la Información y las Comunicaciones Fecha: 30-10-2020

TABLA DE CONTENIDO

1 INTRODUCCIÓN 4

2 OBJETIVO 5

3 DEFINICIONES 5

4 ALCANCE DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 10

5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 10

5.1 DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 10

5.1.1 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 5.1.2) 10

5.1.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 6) 11

5.1.3 POLÍTICA DE USO DE DISPOSITIVOS MÓVILES (ISO/IEC 27002:2013 NUMERAL 6.2.1) 13

5.1.4 POLÍTICA DE TRABAJO DESDE EL EXTERIOR (ISO/IEC 27002:2013 NUMERAL 6.2.2) 14

5.1.5 GESTIÓN DE RECURSO HUMANO (ISO/IEC 27002:2013 NUMERAL 7) . 16

5.1.6 GESTIÓN DE LOS ACTIVOS (ISO/IEC 27002:2013 NUMERAL 8) 18

5.1.7 POLÍTICA DE CONTROL DE ACCESO (ISO/IEC 27002:2013 NUMERAL 9) 22

5.1.8 POLÍTICAS SOBRE USO DE CONTROLES CRIPTOGRÁFICOS (ISO/IEC 27002:2013 NUMERAL 10) 26

5.1.9 SEGURIDAD FÍSICA Y DEL ENTORNO (ISO/IEC 27002:2013 NUMERAL 11) 27

5.1.10 POLÍTICA DE SEGURIDAD EN LAS OPERACIONES (ISO/IEC 27002:2013 NUMERAL 12) 33

5.1.11 POLÍTICA DE RESPALDO DE INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 12.3.1) 35

5.1.12 POLITICA DE SEGURIDAD EN LAS COMUNICACIONES (ISO/IEC 27002:2013 NUMERAL 13) 37

5.1.13 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 13.2) 38

5.1.14 POLÍTICA DE DESARROLLO DE SOFTWARE (ISO/IEC 27002:2013 NUMERAL 14) 40

5.1.15 POLÍTICA PARA RELACIONES CON PROVEEDORES (ISO/IEC 27002:2013 NUMERAL 15) 42

5.1.16 GESTIÓN DE INICIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 16) 43

5.1.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (ISO/IEC 27002:2013 NUMERAL 17) 45

5.1.18 POLÍTICA DE SERVICIOS DE COMPUTACIÓN EN LA NUBE 46

5.1.19 IDENTIFICACION DE LEGISLACION APLICABLE Y REQUISITOS CONTRACTURALES (ISO/IEC 27002:2013 NUMERAL 18.1.1 18.1.2) 47

5.1.20 POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES (ISO/IEC 27002:2013 NUMERAL 18.1.4) 48

1 INTRODUCCIÓN

Las políticas específicas de seguridad y privacidad de la información del Ministerio Agricultura y Desarrollo Rural (MinAgricultura en adelante) tienen como fin aportar en el cumplimiento del objetivo "*Definir e implementar medidas y mecanismos técnicos de seguridad de la información que protejan los activos de información (instalaciones de procesamiento, servicios tecnológicos, información, sistemas y recursos de red, entre otros), ante amenazas internas o externas*" de la Política de Seguridad y Privacidad de la Información del Ministerio de Agricultura y Desarrollo Rural.

Dichas políticas propenden por la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de procedimientos y controles debidamente alineados a las necesidades y objetivos estratégicos del MinAgricultura.

En lo esencial, las políticas aquí descritas brindan las herramientas necesarias para que funcionarios, contratistas, asesores, directivos, proveedores y en general la ciudadanía que tiene relación directa con los activos de información institucionales, de conformidad con el alcance de la Política de Seguridad y Privacidad de la Información puedan adoptar los controles exigidos para asegurarlos, gestionar adecuadamente los riesgos de seguridad y procurar la mejora continua del Sistema de Gestión de Seguridad de la Información.

Las políticas de seguridad de la información comprenden la integración de procesos, sistemas de información y controles orientados hacia un objetivo común: lograr una adecuada y eficiente gestión de los riesgos que genere un nivel de confianza óptimo a las partes interesadas. Entre otros fines, las políticas estarán orientadas a: generar controles para proteger los activos de información; generar conciencia en los usuarios frente al uso responsable de las tecnologías de la información y comunicaciones y realizar una gestión de riesgos adecuada que permita minimizar su impacto.

2 OBJETIVO

Establecer las políticas de seguridad de la información que permitan implementar controles aplicables para el aseguramiento de los activos de información del Ministerio de Agricultura y Desarrollo Rural.

3 DEFINICIONES

- **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Amenaza:** causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.
- **Amenaza informática:** la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).
- **Análisis de riesgos:** proceso para comprender la naturaleza del riesgo y determinar su nivel de riesgo.
- **Anonimización del dato:** eliminar o sustituir algunos nombres de personas (físicas o jurídicas). Direcciones y demás información de contacto. Números identificativos. Apodos o cargo.
- **Autenticación:** provisión de una garantía de que una característica afirmada por una entidad es correcta.
- **Autenticidad:** Propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).
- **Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- **Ciberespacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Control:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

- **Custodio de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

- **Datos abiertos:** son datos primarios o sin procesar. Los cuales son puestos a disposición de cualquier ciudadano. Con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

- **Datos biométricos:** parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (ej. huella digital o voz).

- **Datos personales sensibles:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

- **Dato privado**: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

- **Dato público:** es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

- **Dato semiprivado:** es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

- **Disco duro**: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y re-grabados como una cinta de audio.

- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **DVD:** Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

- **Evento de seguridad de la información:** ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

- **Gestión de claves:** son controles que realizan mediante la gestión de claves criptográficas.

- **Gestión de incidentes de seguridad de la información:** procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

- **Gestión de riesgos:** actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

- ***Habeas data*:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

- **Impacto:** el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.

- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)

- **No repudio**: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

- **Parte interesada (*Stakeholder*):** persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de continuidad del negocio**: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos**: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Proceso**: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000. es, 2012)

- **Propietario de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

- **Responsable del tratamiento:** persona natural o jurídica; Pública o privada; que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

- **Segregación de tareas:** reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Subsistema de Gestión de Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

- **Titular de la información:** es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

- **Teletrabajo:** actividad laboral que se desarrolla afuera de las instalaciones de la entidad, las cuales emplean tecnologías de la información y de la comunicación para su desarrollo.

- **Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

- **Vulnerabilidad:** debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

4 ALCANCE DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El alcance de las políticas descritas en el presente documento es el establecido en la Política General de Seguridad y Privacidad de la Información.

5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Este numeral contempla la descripción de las políticas de seguridad y privacidad de la información del MinAgricultura, a través de las cuales se da cumplimiento a la declaratoria de aplicabilidad de controles del SGSI, que buscan la protección de la confidencialidad, integridad y disponibilidad de los activos de información.

Periódicamente se deben realizar revisiones sobre el cumplimiento de las políticas, procedimientos y demás controles establecidos al interior del MinAgricultura. Se realizarán de igual manera auditorías externas para verificar el cumplimiento de las políticas de seguridad.

Las políticas de seguridad de la información serán revisadas cuando se presenten cambios en la tecnología, en los procesos o en la estructura organizacional en la Entidad.

A continuación, se describen las políticas de seguridad de la información que hacen parte del sistema de gestión de seguridad de la información, en adelante SGSI del Ministerio de Agricultura y Desarrollo Rural.

5.1 DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1.1 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 5.1.2)

OBJETIVO

Se deberá definir un conjunto de políticas para la seguridad y privacidad de la información que deberán ser presentadas para aprobación por los competentes, publicadas y socializadas a los actores responsables de su aplicabilidad.

ALCANCE ESPECÍFICO

Aplica para las políticas de seguridad y privacidad de la información presentes en este documento.

DETALLE

- Definir y mantener actualizadas las Políticas de Seguridad y Privacidad de la Información de conformidad con la declaratoria de aplicabilidad de controles de la Norma GTC-ISO/IEC 27002.
- Aprobar y formalizar las Políticas de Seguridad y Privacidad de la Información por quien corresponda.
- Dar a conocer a los funcionarios, contratistas, asesores, directivos, proveedores y en general la ciudadanía que tiene relación directa con los activos de información institucionales las Políticas de Seguridad y Privacidad de la Información.

5.1.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 6)

OBJETIVO

Establecer los lineamientos de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información.

ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACION (ISO/IEC 27002:2013 NUMERAL 6.1.1)

El Ministerio asigna las funciones relacionadas con la seguridad de la información al comité pertinente, el cual deberá asegurar que exista una dirección y apoyo para la administración y desarrollo de las iniciativas sobre seguridad de la información.

Se deberán asignar las funciones de seguridad de la información en el instrumento destinado para tal fin.

POLÍTICA – CONTACTO CON LAS AUTORIDADES (ISO/IEC 27002:2013 NUMERAL 6.1.3)

Elaborar una guía oficial de contactos apropiados de las autoridades pertinentes.

Designar un responsable que gestione los contactos apropiados con las autoridades pertinentes, en caso de la ocurrencia de incidentes de seguridad de la información.

POLÍTICA – CONTACTO CON LOS GRUPOS DE INTERESES ESPECIALES (ISO/IEC 27002:2013 NUMERAL 6.1.4)

El oficial de seguridad de la información deberá pertenecer a grupos de intereses especiales en seguridad de la información, a través de los cuales se tenga acceso a los foros, actualizaciones o novedades en temas de seguridad de la información.

POLÍTICA DE SEGURIDAD EN PROYECTOS (ISO/IEC 27002:2013 NUMERAL 6.1.5)

Dentro de la etapa de planeación del proyecto se deben incluir las actividades necesarias para identificar cualquier impacto en temas de seguridad de la información los cuales pueden ser entre otros:

- La creación o disposición final de activos de la información
- Cambio en los niveles de riesgos asociados a los activos de la información actuales.
- Impacto en los controles de los activos de la información actuales

Definir los responsables dentro del equipo del proyecto frente a las actividades de seguridad de la información.

Los objetivos y políticas de seguridad de la información son aplicables y deben ser conocidos y tenidos en cuenta por parte de todos los proyectos de la Entidad.

Gestionar el acompañamiento de los responsables de la seguridad de la información para la validación y aprobación de cualquier cambio o impacto que modifique el nivel de riesgo a los procesos o activos de información relevantes al proyecto y controles asociados.

La Entidad establece las directrices para que se incluya la seguridad de la información (identificación de activos, riesgos, controles) en los proyectos que se realicen al interior de la Entidad.

La Oficina de TIC, en coordinación con el Oficial de Seguridad serán los responsables de socializar los lineamientos de seguridad de la información en los proyectos de la Entidad.

El Oficial de Seguridad de la Información junto con los gerentes de proyectos, realizarán la identificación de los riesgos en seguridad de la información, así como el plan de acción respectivo.

5.1.3 POLÍTICA DE USO DE DISPOSITIVOS MÓVILES (ISO/IEC 27002:2013 NUMERAL 6.2.1)

OBJETIVO

Garantizar la seguridad, administración, transmisión o almacenamiento de los activos de información institucionales desde dispositivos móviles, y el uso de estos dentro de MinAgricultura.

ALCANCE ESPECÍFICO

La presente política aplica a todos los dispositivos y equipos móviles de los funcionarios, contratistas y terceros de MinAgricultura que tengan acceso a la red institucional a la información o a cualquier servicio de tecnologías de la información y las comunicaciones de MinAgricultura.

DETALLE

MinAgricultura implementará las directrices necesarias para la autorización de acceso a los recursos y activos de información a través de los dispositivos de tecnología móviles (computadores portátiles, *smartphone*, tabletas, o cualquier equipo de dispositivos electrónicos con capacidad de acceso a las redes), conforme a los riesgos asociados. Así mismo, establecerá mecanismos de control de seguridad de la información de estricto cumplimiento por parte de los funcionarios, contratistas y terceros para el acceso a la información, tecnologías de la información y comunicaciones o servicios y recursos de MinAgricultura desde dichos dispositivos.

CONDICIONES OBLIGATORIAS

- Los dispositivos móviles únicamente tendrán acceso a la información que se encuentra publicada en Internet.
- Se deberán proteger física y lógicamente los dispositivos móviles propiedad de MinAgricultura para evitar el hurto, acceso o la divulgación no autorizada de la información.
- Es responsabilidad de los usuarios velar por la confidencialidad de la información a la cual se accede desde los dispositivos móviles, por lo tanto, de acuerdo con los niveles de clasificación de la información, deberá si es necesario realizar el cifrado de la información, así como la ejecución de copias de respaldo.
- La Oficina de TICS, con la información suministrada del Área de Talento Humano o Grupo de Contratación, brindará o denegará el acceso a los funcionarios,

contratistas y terceros a la información o sistemas de información que son accedidos a través de dispositivos móviles.

- En caso de extravió o hurto de un dispositivo móvil asignado por MinAgricultura, el funcionario, contratista o tercero será el responsable de informar de manera inmediata a MinAgricultura a través de la mesa de servicio, con el propósito de establecer las medidas de seguridad adecuadas para la protección de la información contenida o acceso a los sistemas de información desde el dispositivo.
- Los funcionarios, contratistas y terceros de MinAgricultura que han sido dotados con dispositivos móviles de la entidad, no podrán instalar software sin previa autorización y coordinación por la Oficina de las TICS, así mismo, no se deberá realizar conexiones externas a redes públicas que no cuenten con protecciones de seguridad equivalentes a las definidas por el SGSI de MinAgricultura.
- Los dispositivos móviles de propiedad de MinAgricultura preferiblemente deberán tener la capacidad de determinar perfiles de usuario y negocio, para separar el uso personal del institucional para la protección de los datos de la entidad.
- El uso de servicios tecnológicos del Ministerio de Agricultura y Desarrollo Rural desde dispositivos móviles será administrado por la Oficina TIC, que tendrá la potestad de realizar la desactivación, borrado y retiro de los accesos a los servicios tecnológicos, cuando el dispositivo móvil haya sido extraviado o robado al funcionario o contratista responsable o cuando se incumplan las políticas de seguridad y privacidad.

RESPONSABILIDADES

- La Oficina TIC adaptará los mecanismos de seguridad adecuados para proteger los activos de información accedidos, contenidos o transmitidos desde los dispositivos móviles de los funcionarios, contratistas y terceros de MinAgricultura.
- Para hacer uso de los servicios tecnológicos del Ministerio, se aplicarán políticas técnicas de seguridad, las cuales son de obligatorio cumplimiento.

5.1.4 POLÍTICA DE TRABAJO DESDE EL EXTERIOR (ISO/IEC 27002:2013 NUMERAL 6.2.2)

OBJETIVO

Definir las pautas generales para asegurar los activos de información de MinAgricultura frente a riesgos asociados al trabajo desde el exterior.

DETALLE

El MinAgricultura autorizará el trabajo desde el exterior, conforme a las necesidades del trabajo. En todo caso, es responsabilidad de los colaboradores que acceden desde el exterior a activos de información institucionales disponibles en entorno local, garantizar el cumplimiento de las políticas de seguridad y privacidad de la información de MinAgricultura y frente al respectivo análisis del riesgo.

MinAgricultura dispondrá de los recursos tecnológicos y organizacionales para el acceso desde el exterior a activos de información institucionales disponibles en entorno local, que permita cumplir con los intereses y necesidades de la entidad, considerando los riesgos y su respectiva gestión.

MinAgricultura preverá mecanismos de seguridad física y lógica para el acceso desde el exterior a activos de información institucionales disponibles en entorno local, con el fin de conservar las características de integridad, disponibilidad y confidencialidad de la información.

Para el desarrollo de las actividades desde el exterior se deberá realizar un análisis de riesgos, a partir del cual se adopten los mecanismos de control para la protección de los activos de información accedidos durante las actividades.

En caso de pérdida o hurto de un equipo en el cual se lleven actividades desde el exterior o perdida de confidencialidad, será responsabilidad del funcionario, contratista o tercero informar de forma inmediata a través de la mesa de servicios de MinAgricultura el evento, con el fin de establecer las medidas de seguridad adecuadas para la protección de la información contenida.

RESPONSABILIDADES

- Referente a los componentes de tecnología, el jefe directo del área deberá notificar y justificar la necesidad de trabajo desde el exterior, detallando el nombre del usuario y los servicios que requiere.
- La Oficina de TIC, con la información remitida, brindará o denegará el acceso desde el exterior a servicios tecnológicos disponibles en entorno local.
- La Oficina de TIC será la responsable de implementar los controles de seguridad necesarios para llevar a cabo las actividades de trabajo desde el exterior.
- Los funcionarios, contratistas y terceros que se encuentren autorizados para el desarrollo de actividades desde el exterior, deberán cumplir con las responsabilidades aplicables en entorno local, así mismo reportar cualquier

situación que pueda afectar el desarrollo de las actividades o ponga en peligro los servicios tecnológicos de MinAgricultura.

- La Oficina de TIC, en coordinación con el Oficial de Seguridad, determinará los canales de comunicación y métodos de autenticación apropiados para controlar el acceso de usuarios remotos a los servicios tecnológicos de MinAgricultura.
- La Oficina de TIC, en coordinación con el Oficial de Seguridad, generarán protocolos que den respuesta a situaciones de alerta como una avería del ordenador causada por un virus, una configuración incorrecta o un fallo de hardware. Estableciendo controles de seguridad tales como copias de respaldo o equipos o dispositivos de reserva en caso de daño o pérdida de los equipos.

5.1.5 GESTIÓN DE RECURSO HUMANO (ISO/IEC 27002:2013 NUMERAL 7)

OBJETIVO

Establecer las directrices para la seguridad de la información en lo relacionado a la selección, contratación sensibilización, capacitación, retiro o cambio de cargo del recurso humano en la Entidad.

ALCANCE ESPECÍFICO

Esta política aplica para los funcionarios y contratistas que tengan una relación contractual con MinAgricultura. Se debe aplicar durante la contratación, vigencia y finalización de la relación laboral o contractual con la Entidad, así como durante cambios de cargo o rol.

DETALLE

Antes de asumir el empleo o el contrato.

- Previa a la vinculación al empleo para el caso de los funcionarios o la formalización del contrato para el caso de los contratistas, se deberá verificar el cumplimiento de los requisitos necesarios para el perfil. (Responsables: Talento Humano para el caso de los funcionarios, Grupo de Contratación para el caso de los contratistas).
- Se deberá realizar la verificación de antecedentes conforme lo establece la Ley. (Responsables: Talento Humano para el caso de los funcionarios, Grupo de Contratación para el caso de los contratistas).

Al iniciar un proceso de contratación o vinculación, el proceso responsable (gestión de talento humano y/o grupo de contratación) realiza las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo o vacante, antes de su vinculación definitiva.

Se deberán establecer mecanismos para establecer un Acuerdo de no divulgación o Cláusula de Confidencialidad, así como la aceptación y cumplimiento de Políticas de Seguridad de la Información.

Al momento de la vinculación, se deberá realizar la inducción a los empleados y contratistas en los siguientes temas:

- Políticas en Seguridad de la Información
- Objetivos de seguridad de la información

Durante la ejecución del empleo.

- Se deberá informar a los funcionarios, contratistas y partes interesadas las directrices sobre la seguridad de la información.
- Se deberá motivar a funcionarios y contratistas e interesados a cumplir las políticas de seguridad de la información de la Entidad.
- En cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información deberá establecer Planes de Sensibilización de Seguridad de la Información, alineado con las políticas y procedimientos pertinentes, con el fin de generar una cultura de seguridad de la información.
- Se deberá aplicar la sanción correspondiente a las faltas de segundo grado según sea el caso. Es de evaluar y calificar el desempeño actual de sus subalternos dentro de los plazos oficialmente establecidos (Art 83, Ley No 41-08 de la Función pública.)

Cuando en un incidente de seguridad de la información se determine un grado de culpabilidad o responsabilidad por parte de los servidores públicos o contratistas, la Entidad tomará las acciones pertinentes.

Los cambios de funciones en los servidores públicos deben estar guiados por procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, y la posterior entrega de estos (activos) de acuerdo con su nuevo rol.

El proceso de gestión de talento humano o quien corresponda para el caso de los contratistas notificará formalmente a la Oficina a través de los canales establecidos, los retiros del personal y las novedades administrativas, para el bloqueo o eliminación de datos de acceso y cuentas de correo.

RESPONSABILIDADES

- El Ministerio establece controles para asegurar que los servidores públicos se les aplique los controles de seguridad de la información definidos en el proceso de

ingreso y se les presente las responsabilidades en seguridad de la información durante el proceso de inducción.

- MinAgricultura diseña define y ejecuta de manera permanente un programa de sensibilización en seguridad de la información.
- MinAgricultura establece los controles para proteger los intereses de la entidad como parte del proceso de cambio de cargo, perfil o en la terminación laboral.

5.1.6 GESTIÓN DE LOS ACTIVOS (ISO/IEC 27002:2013 NUMERAL 8)

OBJETIVO

Establecer los requisitos para la identificación, clasificación, protección y buen uso de los activos de información en el MinAgricultura.

DETALLE

Identificar y mantener un inventario de los activos de información asociados a cada proceso de la Entidad. Cada activo debe ser claramente identificado, también su propietario y clasificación asociada a cada activo de información.

Cada activo de información de la Entidad debe tener asociado un responsable que debe velar por su seguridad. Los responsables identificados deben garantizar que sus activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.

Se debe promover el buen uso de los activos de Información, conservando el derecho a la intimidad, la privacidad, el habeas data si aplica, y la protección de los datos de sus propietarios o custodios.

Los servidores públicos y contratistas son los responsables del tratamiento de la información que se encuentra en los equipos de cómputo institucional, dispositivos móviles propios o de la Entidad, nube y documentación física para llevar a cabo sus funciones y deben abstenerse de realizar en ellos tratamiento de información no institucional.

Los dispositivos, equipos o servicios de almacenamiento de la Entidad no podrán ser usados para archivos personales: música, vídeos, fotografías o cualquier archivo en general que no sean para uso de institucional.

Los dispositivos de almacenamiento o equipos de cómputo, el servicio de acceso a servicios de red locales y externas a MinAgricultura, las aplicaciones, sistemas de

información, correo electrónico y usuarios de red son propiedad de la entidad y deben ser usados únicamente para el cumplimiento de actividades laborales o contractuales.

El Ministerio deberá asegurar que todos los funcionarios y contratistas devuelvan todos los activos de la entidad que se encuentren a su cargo al terminar su empleo o contrato

USO ADECUADO DEL SOFTWARE (ISO/IEC 27002:2013 NUMERAL 8.1.3)

El software licenciado de MinAgricultura debe ser usado únicamente en los equipos institucionales, toda copia, comercialización y/o sesiones no autorizadas, bien sea para uso propio o para proporcionarlo a personal externo a la Entidad no está permitido. Salvo previa autorización de la alta dirección.

Los servidores públicos y contratistas no deben efectuar ninguna de las siguientes actividades:

a. Copiar software licenciado del Ministerio para utilizar en sus computadores personales o en cualquier tipo de dispositivo diferente a los autorizados por el Ministerio, cualquiera sea su ubicación.
b. Intentar instalar software no autorizado por el Ministerio, en cualquier computador o servidor de la organización, sin autorización expresa de la Oficina TIC.
c. Introducir programas maliciosos en las redes o a los servidores (ejemplo: virus informáticos, gusanos, troyanos, spyware, adware, puertas traseras, spam, ataques DDOS, keyloggers o cualquier otro tipo de malware).

USO ADECUADO DE LOS RECURSOS TECNOLÓGICOS (ISO/IEC 27002:2013 NUMERAL 8.1.3)

Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, fondo de pantalla y protector de pantalla institucional.

Todos los escritorios físicos y virtuales de los servidores públicos o contratistas de la Entidad se deben mantener despejados y libres de información pública reservada o pública clasificada en ausencia de este.

Se debe velar por evitar accesos no autorizados, pérdida o daño de la información clasificada, almacenándola de forma segura, realizando el bloqueo del equipo de cómputo en el momento en que será requerido.

USO ADECUADO DEL CORREO ELECTRÓNICO (ISO/IEC 27002:2013 NUMERAL 8.1.3)

Ningún usuario debe permitir a otro usuario enviar correos electrónicos utilizando su cuenta. Las cuentas asignadas son únicas e intransferibles. Cada servidor público o contratista es responsable del alcance de las acciones y/o uso de cada una de ellas.

La cuenta de correo electrónico institucional asignada al usuario, sólo podrá ser utilizada para el desempeño de las funciones en la entidad en el marco del cumplimiento de los objetivos institucionales.

Los mensajes y la información contenida en los buzones de correo electrónico, así como los archivos adjuntos, son propiedad del Ministerio y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones laborales.

No se debe utilizar la dirección de correo electrónico de la institución, como punto de contacto en redes sociales, comerciales o cualquier otro sitio que no esté directamente relacionado con las actividades laborales.

No está permitido crear y/o enviar cadenas de correo electrónico, mensajes con contenido religioso, político, racista, pornográfico, publicitario no institucional, o que revelen el origen racial o étnico, la orientación política, convicciones religiosas, de derechos humanos o que promuevan cualquier partido político, así como los datos relativos a la salud, a la vida sexual y los datos biométricos, sin que los mismos estén autorizados a ser tratados, por los titulares de la información de conformidad con Ley 1581 de 2012, y demás normas que las adicionen, aclaren y modifiquen.

No está permitido el envío de archivos que contengan extensiones ejecutables.

No está permitido el envío de archivos de música y videos exceptuando la necesidad de suplir comunicaciones institucionales.

CLASIFICACIÓN DE LA INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 8.2)

Los niveles de clasificación de la información de MinAgricultura permiten identificar las características de protección, manejo y tratamiento de la información en cuanto a: niveles de acceso, métodos de distribución, restricciones en la distribución, almacenamiento, archivado, disposición y destrucción. Se establecen los siguientes niveles de clasificación en el Ministerio:

INFORMACIÓN PÚBLICA: Información que por sus características puede o debe estar a disposición de cualquier persona natural o jurídica en el Estado Colombiano, ha sido declarada de conocimiento público de acuerdo con alguna norma jurídica o por parte de la persona o grupo de personas con autoridad para hacerlo.

INFORMACIÓN PÚBLICA CLASIFICADA: Toda información que pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014.

INFORMACIÓN PÚBLICA RESERVADA: Toda información que estando en poder o custodia de la Entidad, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.

RESPONSABILIDADES

- Los líderes de proceso son los responsables de identificar, actualizar e informar al oficial o líder de seguridad o quién haga sus veces en la Entidad, sobre nuevos activos de información en el proceso o comunicar cambios (estado, responsable, valoración, etc) que se presenten en los actuales.
- Todos los servidores públicos serán responsables de proteger la información a la cual accedan o procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Los servidores públicos y contratistas deben hacer el respectivo proceso de devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.
- Cada usuario en la Entidad es responsable de dar uso adecuado y en ningún momento el activo puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros.
- Los usuarios deben cerrar la sesión activa en el equipo de cómputo al dejar el puesto de trabajo o bloquearla mediante la combinación de las teclas Windows + L para un bloqueo manual, el bloqueo se debe realizar incluso para periodos de ausencia cortos.
- El usuario debe realizar constantemente la depuración de su correo electrónico, tanto a los correos enviados como los recibidos.
- Los líderes de proceso deben realizar la clasificación y calificación en términos de seguridad de los activos de información a su cargo con la ayuda de Oficial de Seguridad o quien haga sus veces en la Entidad.

- Se deberá realizar el proceso de etiquetado a los activos de información tipo información, de acuerdo con la clasificación de la información asignada por cada propietario del activo.

GESTIÓN DE MEDIOS REMOVIBLES (ISO/IEC 27002:2013 NUMERAL 8.3.1)

- La información crítica de la Entidad no deberá ser almacenada ni transportada en medios removibles.
- Los medios removibles (cintas, discos, discos flash, discos duros, discos compactos, DVDs y medios impresos) propiedad de la Entidad que se dejen de utilizar, deben pasar por un proceso que haga irrecuperable la información allí almacenada.
- Los medios removibles deben almacenarse en sitios seguros.
- Los medios removibles que se conecten a equipos de la Entidad deben ser analizados en búsqueda de código malicioso.

TRANSITO DE MEDIOS (ISO/IEC 27002:2013 NUMERAL 8.3.3)

- El personal que transporte medios físicos de almacenamiento debe velar por la protección de estos durante su transporte.
- Los medios que contengan copias de seguridad de la información de la Entidad, y que requieran ser transportados a un destino final para su custodia, deben ser trasportados por personal de la Oficina TIC, y exclusivamente en los vehículos de la Entidad, o en su defecto por el proveedor contratado para tal fin.

5.1.7 POLÍTICA DE CONTROL DE ACCESO (ISO/IEC 27002:2013 NUMERAL 9)

OBJETIVO

Definir los lineamientos generales para controlar el acceso a la información, los activos y sistemas informáticos de MinAgricultura.

DETALLE

MinAgricultura, como se ha mencionado, tiene como fin preservar la confidencialidad, integridad y disponibilidad de los activos de información que son accedidos o se encuentran a cargo de los funcionarios o contratistas debido a su cargo y/o responsabilidades. Por tal motivo, ha establecido controles que permitan regular el acceso a las redes, datos e información, así como la implementación de perímetros de seguridad para la protección de las instalaciones, especialmente, aquellas clasificadas como áreas seguras, como los

centros de procesamiento de información, áreas de almacenamiento de información física, cuartos de suministro de energía eléctrica, aire acondicionado, entre otras.

MinAgricultura llevará a cabo un control de acceso a la información que tendrá en cuenta tanto los aspectos lógicos como físicos que permitan garantizar la trazabilidad de las acciones realizadas, identificando, entre otros datos relevantes, quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso, accesos denegados, etc.

Una vez se apruebe el acceso a la información, los funcionarios y contratistas no deben realizar modificaciones sobre la información sin la debida autorización, guardar confidencialidad de la información a la cual tiene acceso, no vulnerar los controles de seguridad establecidos por MinAgricultura, informar al Oficial de Seguridad de la Información sobre las debilidades o eventos de seguridad.

RESPONSABILIDADES

- La información de naturaleza pública de MinAgricultura debe de estar disponible al ciudadano siempre y cuando no esté sometida a reserva legal o existan restricciones para su acceso.
- El acceso a la información y sistemas de información será controlado conforme a los roles y responsabilidades de los funcionarios y contratistas de MinAgricultura. La autorización será otorgada por los responsables de los activos de información. Los registros de acceso y actividades desarrolladas podrán ser auditadas para propósitos de control e investigación a los que haya lugar dentro de la naturaleza de MinAgricultura, y así mismo para minimizar el riesgo de la pérdida de integridad o confidencialidad de la información.
- Como responsables de la información, los funcionarios, contratistas y terceros del Ministerio de Agricultura y Desarrollo Rural deberán administrar y hacer cumplir los lineamientos establecidos, con el fin de evitar accesos no autorizados, pérdidas o utilización indebida de los activos de información.
- Los funcionarios, contratistas y terceros del Ministerio de Agricultura y Desarrollo Rural tienen como responsabilidad velar por la integridad, confidencialidad y disponibilidad de la información, los activos y los sistemas informáticos para los cuales han sido designados y autorizados, asegurándose que estos solo sean utilizados para el desarrollo de las labores encomendadas dentro de MinAgricultura.
- Los accesos tanto físicos como lógicos, asignados a los funcionarios, contratistas y terceros deberán ser desactivados o modificados una vez terminados los vínculos contractuales con MinAgricultura.
- Todos los usuarios tendrán un usuario personal e intransferible, que permitirá los acceso y uso de la información. Todas las acciones realizadas con el usuario

asignado serán responsabilidad del funcionario o contratista o tercero a quien se le asignó el usuario.

- MinAgricultura establecerá controles para restringir accesos a áreas seguras, entre otros, deberá registrar los sistemas, datos de identificación de la persona que accede a la información, el motivo de ingreso, el tiempo empleado para el desarrollo de la actividad y, asimismo, cuidará que un responsable del activo de información acompañe a la persona durante su instancia en el área.
- El responsable o encargado del activo de información será el responsable de realizar revisiones periódicas de los derechos de acceso de los usuarios a intervalos regulares.
- Los propietarios de los activos de información periódicamente propenderán por la verificación de los niveles de acceso (o también llamados niveles de privilegios) asignados a los usuarios, para garantizar que sean apropiados de acuerdo con el propósito institucional y se conserve la separación de funciones. Para el caso de los contratistas, esta verificación se realizará anualmente o por cambio de contrato.
- El otorgamiento de un determinado nivel de acceso a un usuario o aplicativo en un sistema de información debe ser autorizado previamente por el líder del proceso o el dueño de la información del sistema de información, siempre partiendo del concepto de que se debe autorizar el mínimo nivel de privilegios necesarios para la realización de las funciones del usuario o el funcionamiento del aplicativo.
- Se debe verificar y retirar las cuentas redundantes de usuarios.
- En los casos en los que el otorgamiento de acceso se lleve a cabo por medio de una asignación de contraseña, se debe consultar la Política de Contraseñas, del presente documento.

CONTRASEÑAS SEGURAS (ISO/IEC 27002:2013 NUMERAL 9.4.3)

- Las contraseñas de usuario son de carácter confidencial, personal e intransferible.
- Por defecto debe existir una obligatoriedad para el cambio inmediato en el primer uso de contraseñas de usuario en las nuevas cuentas de la Entidad, o en proceso de restablecimiento de contraseñas.
- Las solicitudes de cambio de contraseña deben ser realizadas personalmente por el propietario de la cuenta.
- Las contraseñas se deben distribuir de forma segura, nunca mediante sistemas de transporte no cifrado (texto claro).
- Los usuarios no deben mantener registros de las contraseñas (hojas de papel, archivos de software, etc.), a menos de que sea un método de almacenamiento seguro para tal fin, que no represente riesgo ni exponga las contraseñas almacenadas.
- Los usuarios deben cambiar la contraseña siempre que haya indicio de puesta en peligro del sistema o a intervalos regulares, evitando la reutilización de contraseñas antiguas.

- Los usuarios deben seleccionar contraseñas con un mínimo de 8 caracteres con las siguientes características:

    a. Que contenga mayúsculas.
    b. Que contenga minúsculas.
    c. Que contenga números.
    d. Que contenga caracteres especiales (#$%@/).
    e. Que no tengan relación con el nombre propio, familiares, cargo de trabajo, etc
- No se deben compartir las contraseñas con ningún usuario ni personal de soporte.
- No se deben usar las mismas contraseñas para propósitos institucionales y para propósitos personales.
- Se debe permitir a los usuarios la selección y el cambio de sus contraseñas, en el momento que se requiera.
- La directiva de contraseñas implementada no deberá permitir que los usuarios reutilicen alguna de las cinco (5) contraseñas previas utilizadas por los mismos.
- No se deben mostrar contraseñas en pantalla en el momento del ingreso, se deben utilizar caracteres de ofuscación.

USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS (ISO/IEC 27002:2013 NUMERAL 9.4.4)

- El uso de programas privilegiados en la Entidad estará sujeto a la revisión y aprobación de la oficina TIC y del líder de seguridad de la información, previa solicitud del líder de proceso o jefe inmediato del solicitante.

CONTROL DE ACCESO A CODIGO FUENTE DE PROGRAMA (ISO/IEC 27002:2013 NUMERAL 9.4.5)

- El control de acceso al código fuente de los programas y/o aplicaciones, debe ser restringido solo al personal autorizado.
- Es responsabilidad de los administradores de sistemas de información, otorgar los accesos necesarios a los códigos fuente de cada uno de los proyectos.
- La Oficina TIC deberá tener acceso restringido a librerías de las fuentes de los programas.
- Se deberá mantener y copiar las librerías de fuentes de programa a través de procedimientos estrictos de control de cambios.

5.1.8 POLÍTICAS SOBRE USO DE CONTROLES CRIPTOGRÁFICOS (ISO/IEC 27002:2013 NUMERAL 10)

OBJETIVO

Proteger la confidencialidad, autenticidad o integridad de la información del Ministerio de Agricultura y Desarrollo Rural a través de medios criptográficos.

ALCANCE ESPECÍFICO

La presente política será aplicada para garantizar la confidencialidad, integridad y autenticidad en el tratamiento de la información de MinAgricultura, de acuerdo con los niveles de clasificación determinados y los sistemas electrónicos o de almacenamiento utilizados.

DETALLE

La Oficina TIC, con el apoyo del Oficial de Seguridad de la Información, serán los encargados de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de MinAgricultura, con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no repudio en las comunicaciones o en el tratamiento de la información. El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los funcionarios y contratistas de MinAgricultura.

Para establecer el sistema de cifrado, los responsables tendrán en cuenta la normatividad colombiana vigente frente a la protección de los datos, estándares aplicables y la tecnología existente, primando las necesidades institucionales. Así mismo, serán los encargados de realizar la respectiva creación, activación, distribución y revocación de las llaves criptográficas a los usuarios autorizados y velarán porque la llave se encuentre activa en el período de tiempo previsto.

RESPONSABILIDADES

- La solicitud de acceso o actualización al sistema o llaves de cifrado se debe efectuar de manera formal de acuerdo con los procedimientos establecidos para tal fin, en la medida en que las actividades laborales así lo demanden. Aquellas personas autorizadas deberán velar por la conservación de la disponibilidad, integridad y confidencialidad de las llaves, así como de la información a la cual se le haya aplicado algún proceso de cifrado. De igual modo, la información cifrada o

descifrada deberá ser tratada conforme a su nivel de clasificación y su eliminación deberá realizarse a través de borrado seguro.

- Los responsables del sistema de cifrado y de las llaves criptográficas serán los encargados de establecer los controles para asegurar el sistema y las llaves, así como gestionar el acceso sólo a los funcionarios, contratistas y terceros autorizados.
- MinAgricultura deberá establecer mecanismos de control y gestión para la creación, activación, distribución, recuperación y revocación de las llaves criptográficas.
- Las actividades relacionadas con la administración y eliminación de las llaves criptográficas deberán ser registradas por la persona encargada. Las llaves serán deshabilitadas cuando estas tengan riesgo de divulgación o cuando los funcionarios, contratistas y terceros autorizados culminen la relación laboral o contractual con MinAgricultura.
- Los funcionarios, contratistas y terceros tendrán la responsabilidad de reportar, mediante los canales autorizados, las fallas reales o potenciales y los posibles riesgos del sistema de cifrado.

GESTION DE CLAVES CRIPTOGRAFICAS (ISO/IEC 27002:2013 NUMERAL 10.1.2)

- En caso de que aplique, la Oficina TIC será la encargada de dar los lineamientos asociadas a los algoritmos de cifrado a utilizar.
- La contraseña de cifrado deberá cumplir con la Política de sistema de gestión de contraseña.

5.1.9 SEGURIDAD FÍSICA Y DEL ENTORNO (ISO/IEC 27002:2013 NUMERAL 11)

OBJETIVO

Establecer los lineamientos para la seguridad física y del entorno, en lo relacionado con el acceso físico, seguridad de los equipo y controles contra amenazas ambientales.

DETALLE

Seguridad General de las Instalaciones.

- En donde sea aplicable la Entidad deberá construir barreras físicas para impedir el acceso físico no autorizado.
- Se deberán implementar medidas de protección con vigilancia que permitan controlar el acceso a las instalaciones de la Entidad.

- Las instalaciones de procesamiento de información de la Entidad deberán estar debidamente separadas físicamente.

SEGURIDAD CENTRO DE DATOS (ISO/IEC 27002:2013 NUMERAL 11.1.5)

- El Centro de datos debe estar ubicado en un lugar alejado de áreas que contengan líquidos inflamables o presenten alto riesgo de incendio. No puede estar ubicado cerca de un sótano o en un último piso.
- Los gabinetes y puertas de los equipos que se encuentran en el Centro de datos deben permanecer cerrados, siempre y cuando se garanticen los niveles de temperatura y humedad requeridos por la infraestructura de cómputo allí instalada.
- No se debe enchufar, ni desenchufar ningún cable eléctrico, de datos o voz sin autorización y supervisión de algún responsable del Centro de datos.
- Los niveles de temperatura y humedad relativa en el Centro de datos deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo que en éste se resguardan.
- El responsable del Centro de datos debe realizar el control de la programación de los mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS, switches y servidores. Los mantenimientos deberán realizarse al menos una vez cada año.
- La asignación de espacio, ubicación, movimiento y demás requerimientos físicos para la infraestructura de cómputo instalada en el Centro de datos debe ser autorizada por el responsable del Centro.
- Debe existir un sistema de detección y prevención de incendios en el Centro de datos, que minimice el impacto que puede generar la ocurrencia de un evento o situación de incendio en el lugar. Así mismo, se debe contar con un sistema de control de acceso que permita registrar el ingreso del personal.
- El Centro de Datos deberá contar con el piso elevado, permitiendo la instalación de bandejas de cableado.

ACCESO FÍSICO A LAS INSTALACIONES (ISO/IEC 27002:2013 NUMERAL 11.1.2)

- El Ministerio deberá mantener un programa de seguridad física para el acceso a las instalaciones y verificación piso a piso que permita fortalecer la confidencialidad, disponibilidad e integridad de la información.
- El ingreso a las instalaciones de la Entidad debe estar restringido únicamente al personal autorizado.
- Todos los colaboradores de la Entidad deben portal el carné institucional en un lugar visible.

ACCESO FÍSICO DE VISITANTES A LAS INSTALACIONES (ISO/IEC 27002:2013 NUMERAL 11.1.2)

- Todos los visitantes deben llegar al sitio designado para el registro de visitantes (portería).
- El registro de visitante debe incluir el nombre e identificación del visitante, la fecha y hora.
- Todos los visitantes deben presentar un documento que los identifique al momento del registro.
- El ingreso de un visitante a las instalaciones de la Entidad debe ser autorizado por un colaborador del Ministerio.
- Los visitantes deberán ser acompañados por el colaborador de la Entidad que autorizó su ingreso, durante el tiempo que dure la visita, y específicamente cuando se accede a áreas restringidas.
- El colaborador de la Entidad que autorice el ingreso de un visitante es el encargado de hacerle conocer los requisitos de seguridad y los procedimientos de emergencia.
- En ningún caso un visitante puede autorizar el ingreso de otro visitante.
- Los dispositivos electrónicos ingresados por los visitantes, tales como portátiles, torres de computador o video beam, entre otros, deben ser incluidos en una tabla de registro donde se indique la marca del equipo, el modelo y el serial (o su equivalente). Este registro se realizará al ingreso y a la salida de las instalaciones de la Entidad, y es deber del personal de seguridad verificar que los datos suministrados correspondan con el dispositivo físico.
- Los distintivos de visitantes deben ser portados en un lugar visible durante todo el tiempo que dure la visita.
- Ningún visitante podrá ingresar a áreas que contengan información crítica del Ministerio, sin el acompañamiento del colaborador encargado, quien tendrá bajo su responsabilidad la permanencia del visitante en la Entidad durante el tiempo que dure la visita.
- Aquellos visitantes que requieren ingresar a las instalaciones de la Entidad con mayor frecuencia (p. ej. Proveedores), podrán hacerlo sin necesidad de registrarse diariamente en la recepción de las instalaciones, previo envío de comunicado por parte del colaboradore responsable, en el cual se autoriza el ingreso temporal indicando siempre el área o proceso del Ministerio, a la cual podrá acceder y la vigencia de la autorización.

ACCESO FÍSICO AL CENTRO DE DATOS (ISO/IEC 27002:2013 NUMERAL 11.1.2)

- Las puertas de acceso al Centro de datos deben permanecer cerradas y aseguradas, siempre y cuando se garanticen los niveles de temperatura y humedad requeridos por la infraestructura de cómputo allí instalada.

- Únicamente se permite el ingreso de manera regular al Centro de datos al personal autorizado, por lo que debe existir un mecanismo que registre y controle el ingreso y salida de personas, y cualquier tipo de material al Centro, conforme el esquema de niveles de acceso definido.
- De ser necesario el ingreso de algún visitante al Centro de datos, podrá realizarse siempre y cuando sea para actividades que no afecten o modifiquen el correcto funcionamiento de la infraestructura instalada. Durante la visita deberá estar siempre acompañado y bajo la supervisión del responsable del Centro de datos.
- Los registros de ingreso al Centro de datos deben ser auditados con frecuencia para identificar accesos no autorizados y confirmar que los controles de acceso definidos son efectivos.

ACCESO FÍSICO AL ÁREA DE ARCHIVO (ISO/IEC 27002:2013 NUMERAL 11.1.5)

- El área de Gestión Documental solo deberá tener el acceso al sitio de Archivo, donde se conserva la información de reserva de la Entidad.

SEGURIDAD EN OFICINAS, SALAS E INSTALACIONES (ISO/IEC 27002:2013 NUMERAL 11.1.3)

- Todas las áreas de la Entidad que tienen bajo su custodia activos de información sensibles o confidenciales deben identificar claramente los perímetros de seguridad para su protección, bien sea a través de elementos como paredes, puertas de acceso, escritorios atendidos, etc.
- En las áreas que contengan activos de información críticos para la Entidad se deben instalar mecanismos robustos físicamente (p.ej. cerraduras, alarmas, sistemas lectores de tarjeta, muros, puntos de acceso con vigilancia humana) de tal manera que sirvan para prevenir el acceso no autorizado a las mismas.
- Las puertas y ventanas de las oficinas de la Entidad, que tienen bajo su custodia activos de información con alta criticidad, deben permanecer cerradas con llave cuando no están atendidas, siempre y cuando las características del recurso físico lo permitan. Aquellas oficinas que no tengan puerta deben permanecer atendidas mientras se encuentren en ella personal externo a la Entidad.
- Los equipos y dispositivos que son utilizados para soportar las funciones críticas de la Entidad deben estar ubicados en áreas cuyo acceso sea restringido y esté supervisado por los responsables de estos.

PROTECCIÓN CONTRA AMENAZAS AMBIENTALES ARCHIVO (ISO/IEC 27002:2013 NUMERAL 11.1.4)

- Se deberán instalar sistemas adecuados para detección de intrusos e incendios.
- El papel y los combustibles deben ser almacenados en lugares aislados en contenedores y en pequeñas cantidades.

- Se debe asegurar que en las instalaciones de la Entidad se cuente con un equipamiento apropiado de seguridad: sistemas de extinción de incendios; salidas de emergencia, cableado, etc.
- El consumo de cigarrillo, o de sustancias que pueden afectar la integridad y correcto funcionamiento de los activos de información está restringido en las áreas internas.

TRABAJO EN ÁREAS SEGURAS (ISO/IEC 27002:2013 NUMERAL 11.1.5)

- Los visitantes no están autorizados para tomar fotografías dentro de las instalaciones de la Entidad, a menos que sean autorizados por un colaborador de la Entidad.
- El uso de equipos de grabación fotográfica, video o audio puede realizarse siempre y cuando su utilización esté autorizada.
- Se debe contar con un sistema CCTV, que permita monitorear y salvaguardar los diferentes activos de información de la Entidad.
- Se debe contar con un histórico del monitoreo de actividades registradas en el CCTV, por lo menos por 20 días.
- Se deberá evitar el trabajo en áreas no autorizadas

(ISO/IEC 27002:2013 NUMERAL 11.2.1)

EQUIPOS DE CÓMPUTO

- En horario laboral, cuando el usuario no esté haciendo uso del equipo de cómputo, el mismo deberá estar bloqueado, en horario no laboral deberá permanecer apagado siempre y cuando no se esté procesando información.
- Deben existir planos de ubicación física y de conectividad de los equipos de cómputo.
- Los equipos de cómputo deben ser usados apropiadamente, velando por el buen estado de cada uno de sus componentes.
- Para el uso de los equipos de cómputo debe existir un responsable de estos.

EQUIPOS DE IMPRESIÓN.

- Los equipos dispuestos para las tareas de impresión solamente deberán utilizados para imprimir documentos institucionales.
- Todas las actividades de mantenimiento y reparación de los equipos de impresión deberán ser realizadas directamente por los responsables de la gestión de estos.
- Los usuarios no deberán realizar acciones que afecten el normal funcionamiento de los equipos de impresión.

- Equipos como impresoras, fotocopiadoras deben estar en áreas definidas como seguras, esto aplica también para equipos de comunicaciones como Switches, enrutadores, firewalls entre otros.

SUMINISTRO ELÉCTRICO (ISO/IEC 27002:2013 NUMERAL 11.2.2)

- Se deberá propender porque todos los equipos de cómputo de la Entidad deberán estar conectados a la red de energía regulada, para evitar deterioros por posibles fallas eléctricas.
- Se deberá disponer de un Sistema de Energía interrumpible como UPS y/o plantas eléctricas, para asegurar el Apagado Regulado y Sistemático de los Equipos de TI de la Entidad, asegurando la continuidad de las operaciones mientras se restablece las fallas de suministro de energía eléctrica.
- Se deberá contar un sistema de respaldo eléctrico (planta eléctrica) que garantice la continuidad del fluido eléctrico cuando el servicio del proveedor no esté disponible.

CABLEADO ESTRUCTURADO (ISO/IEC 27002:2013 NUMERAL 11.2.3)

- Deben existir planos de ubicación física y de conectividad de los equipos de cómputo.
- Los canales de energía eléctrica deberán estar separadas de la estructura cableada de comunicaciones.
- Se deberá realizar el proceso de certificación del cableado, garantizando la calidad de sus componentes y su instalación.

POLÍTICA DE MANTENIMIENTO DE EQUIPOS DE TI (ISO/IEC 27002:2013 NUMERAL 11.2.4)

Se realizará el mantenimiento de los equipos de TI, conforme a los procesos y procedimientos establecidos para tal fin, esto para asegurar la confidencialidad, integridad y disponibilidad. Para ello se debe considerar:

POLÍTICA DE ESCRITORIO DESPEJADO Y PANTALLA LIMPIA OBJETIVO (ISO/IEC 27002:2013 NUMERAL 11.2.9)

Para lograr un adecuado aseguramiento de la información, los funcionarios, contratistas y terceros del Ministerio de Agricultura y Desarrollo Rural deberán adoptar buenas prácticas para el manejo y administración de la información física y electrónica que se encuentra a su cargo, conforme a su clasificación, con el fin de evitar que personas no autorizadas

accedan a dicha información. Para ello, los funcionarios, contratistas y terceros deberán tener presente:

- Almacenar de forma segura documentos y elementos de almacenamiento externos (CD, DVD, USB, etc.) conforme los niveles de clasificación de la información, para evitar accesos no autorizados, pérdida o daño de la información en la jornada laboral o fuera de ella.
- Durante los lapsos en los que se deja desatendidas las estaciones de trabajo, se tendrá cuidado con bloquear la sesión del equipo para evitar que terceros no autorizados accedan a la información contenida en el computador. Así mismo, se generarán los controles adecuados con la información que reposa sobre el lugar de trabajo.
- Al imprimir información reservada o pública clasificada, los documentos deberán ser retirados de forma inmediata para evitar divulgación no autorizada de la información.
- Los archivos que contengan información sensible o confidencial deberán ser almacenados en rutas que impidan el fácil acceso por terceros, evitando, por ejemplo, guardarlos en el área de escritorio de la pantalla del computador.
- Los funcionarios y contratistas deberán asegurar que sus escritorios se encuentren libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y que estos sean almacenados bajo las protecciones de seguridad adecuadas.

La Oficina TIC, con el apoyo del Oficial de Seguridad, será la encargada de establecer controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee en un lapso determinado.

Los funcionarios, contratistas y terceros que tengan dentro de sus funciones la atención al público, deberán almacenar los documentos y dispositivos de almacenamiento bajo llave y ubicar el equipo de cómputo de tal forma que se evite el acceso o revisión de la información por parte de los visitantes no autorizados.

5.1.10 POLÍTICA DE SEGURIDAD EN LAS OPERACIONES (ISO/IEC 27002:2013 NUMERAL 12)

OBJETIVO

Establecer las directrices para lograr la seguridad en las operaciones de las instalaciones de procesamiento de información.

ALCANCE ESPECÍFICO

Aplica para los sistemas de información que soportan los procesos de la Entidad**,** al igual que a los servidores públicos, contratistas y terceros.

DETALLE

Los procedimientos y responsabilidades de operación y administración de la plataforma tecnológica y de seguridad deben estar documentados, garantizando un adecuado control de cambios de conformidad con los procedimientos definidos para tal fin.

Todo cambio que se realice sobre la infraestructura tecnológica del Ministerio para el procesamiento de la información y comunicación debe ser controlado, gestionado y autorizado adecuadamente.

La Oficina TIC debe garantizar que los ambientes de desarrollo, pruebas y producción, siempre que sea posible, estarán separados (física o virtual), se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo. Así mismo se debe garantizar la independencia de los servidores públicos que ejecutan dichas labores.

Para ello, se tendrán en cuenta los siguientes controles:

a) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes, equipos, o directorios.
b) Separar las actividades de desarrollo y prueba, en entornos diferentes.
c) Impedir el acceso a los compiladores, editores y otros programas utilitarios en el ambiente operativo, cuando no sean indispensables para el funcionamiento de este.
d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
e) Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.

A efectos de proteger la integridad y confidencialidad de los activos de información es imprescindible que se cuente con protecciones como software de seguridad, mantenimiento de los equipos, administración de la red y bloqueo de puertos en la red de telecomunicaciones.

El Líder de seguridad de la información, definirá controles de detección y prevención para la protección contra software malicioso. El líder del proceso de gestión de servicios TIC, o el servidor público designado por éste, implementarán dichos controles.

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado.
b) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadores y medios informáticos, como medida de precaución y rutinaria.
c) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
d) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
e) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de estas, con inclusión de:

a) Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
b) Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
c) Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.
d) Ministerio de Agricultura y Desarrollo Rural, debe asegurar la protección de las instalaciones y de la información de registro de eventos protegiéndolas contra alteraciones.

RESPONSABILIDADES

- La Oficina TIC implementa controles para asegurar que las operaciones se ejecuten de manera correcta y segura en las instalaciones de procesamiento de información.
- Las actividades realizadas para la gestión de tecnología deben estar debidamente documentados y actualizados.
- Se deberá realizar monitoreo constante de la gestión de la capacidad de TI, a través del análisis y evaluación de rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información.

5.1.11 POLÍTICA DE RESPALDO DE INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 12.3.1)

OBJETIVO

Definir los lineamientos generales para la generación, administración, retención y custodia de las copias de respaldo, con el fin de preservar la disponibilidad e integridad de la información.

ALCANCE ESPECÍFICO

Esta política deberá ser cumplida por los funcionarios, contratistas y terceros que tengan a su cargo realizar, administrar y custodiar las copias de respaldo definidas por MinAgricultura, con el propósito de reducir el impacto frente a la pérdida de información o a incidentes que comprometan la continuidad del negocio.

DETALLE

La información requerida para el cumplimiento de las actividades misionales y los objetivos estratégicos del Ministerio de Agricultura y Desarrollo Rural deberá ser respaldada conforme a lo establecido en la Política Técnica de TIC, lineamientos legales, técnicos, requisitos de las tablas de retención documental, la gestión de riesgos, así como a los niveles de clasificación de la información. Los tiempos de preservación de las copias de respaldo serán definidos teniendo en cuenta los requerimientos anteriormente expuestos, así como también la tecnología requerida para la restauración de la información contenida.

Las copias de respaldo se almacenarán de forma segura para garantizar que no sea manipulada por personas no autorizadas. A su vez, se deberán registrar todas las actividades desarrolladas frente al tratamiento y manipulación de las copias de respaldo para asegurar la trazabilidad de estas.

El responsable de las copias de respaldo deberá realizar las respectivas pruebas de restauración conforme a los propósitos para las cuales han sido recaudadas.

Las copias de respaldo deberán ser almacenadas en lugares que tengan los debidos controles de seguridad físicos y tecnológicos, que permitan limitar el acceso sólo a las personas autorizadas y garanticen la disponibilidad de la información.

Al cumplir el ciclo de vida útil de los medios de almacenamiento de las copias de respaldo deberán ser destruidos o eliminados de forma segura, evitando la recuperación de la información contenida y acceso por personas no autorizadas.

RESPONSABILIDADES

- Los funcionarios, contratistas y terceros responsables de la infraestructura, sistemas de información y Bases de datos requeridos para la operación de MinAgricultura, deberán generar las respectivas copias de respaldo, estableciendo la periodicidad, tipo de almacenamiento y registrando la información según lo establecido dentro de la presente política.
- Los encargados de las copias de respaldo deben velar porque la información sea almacenada conforme a los lineamientos establecidos, de forma controlada y conforme a las necesidades de MinAgricultura. Así mismo deberán realizar una prueba periódica de las copias con el fin validar el correcto funcionamiento y la efectiva restauración.
- Los responsables de la información serán los encargados de velar porque las copias de respaldo se realicen de acuerdo con lo establecido y que las estrategias utilizadas se ajusten a las necesidades y requerimientos de MinAgricultura.
- Los funcionarios, contratistas y terceros de MinAgricultura deberán almacenar la información requerida para sus procesos operativos, en la ubicación establecida por la Oficina de TICS dentro del servidor de almacenamiento, con el fin de garantizar la disponibilidad y copias de respaldo de cada una de las áreas. Así mismo serán responsables de depurar la información para la optimización de los recursos de MinAgricultura.

5.1.12 POLITICA DE SEGURIDAD EN LAS COMUNICACIONES (ISO/IEC 27002:2013 NUMERAL 13)

OBJETIVO

Prevenir en gran medida que los equipos se vean expuestos a riesgos y carezcan de programas específicos para combatirlos como es el caso de los antivirus o los parches.

ALCANCE ESPECÍFICO

Esta política se aplica a los equipos servidores, servicios de red y en general equipo de TI conectados a la red de datos.

DETALLE

Se implementarán controles para garantizar la seguridad de los datos y los servicios conectados en las redes, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración de los equipos servidores, incluyendo los equipos en las áreas de usuarios.
b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de Internet, y para proteger los

sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.

c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.
d) Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la entidad.
e) La infraestructura del Ministerio estará separada por VLANs para garantizar la confidencialidad de los datos que se trasmitan.

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados y VLANs. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado.

RESPONSABILIDADES

- Se deberá bloquear el acceso a las páginas de contenido pornográfico, con contenido que vulnere la integridad de los colaboradores o represente riesgos a los activos de información institucionales.
- El acceso a internet debe hacerse desde una estación debidamente registrada o autorizada.
- Se deberá implementar y mantener la separación de las redes virtuales para garantizar la confidencialidad de la información en las redes de telecomunicaciones de MinAgricultura.
- El acceso a la red por parte de terceros deberá ser gestionado a través de los canales dispuestos para la mesa de ayuda, lo cual deberá ser solicitado por el competente.
- Los servidores públicos y/o contratistas directos de MinAgricultura son responsables de proteger la confidencialidad e integridad de la información y deben tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.
-

5.1.13 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 13.2)

OBJETIVO

Definir las pautas generales para la protección de la información durante su intercambio entre funcionarios, contratistas y terceros de MinAgricultura, y de la entidad con partes externas, preservando las características de disponibilidad, integridad y confidencialidad.

ALCANCE ESPECÍFICO

La presente política debe de ser adoptada por todos los funcionarios, contratistas y terceros de MinAgricultura que en cumplimiento de sus funciones realicen intercambio de información.

DETALLE

En la medida de lo posible, el intercambio de información entre entidades se deberá realizar a través de los protocolos de interoperabilidad adoptados, en todo caso, la transmisión de la información perteneciente a MinAgricultura se deberá controlar según los niveles de clasificación de la información establecidos y las políticas de seguridad de MinAgricultura. En caso de que se requiera intercambiar información sensible o confidencial, se deberán adoptar controles de cifrado de información de acuerdo con lo establecido en la política descrita en el presente documento.

Los intercambios de información sensible o confidencial, con otras entidades o partes interesadas externas deberán ser justificados cuando así se requiera. El uso de la información transmitida o intercambiada deberá realizarse exclusivamente para los fines pactados, en todo caso se deberá tratar como información confidencial y no podrá ser compartida con terceros no autorizados.

La transmisión de la información se desarrollará teniendo en cuenta la normatividad colombiana vigente, especialmente la relativa a la Ley de *Habeas Data* (Ley 1266 de 2008), la Ley de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios) y Ley de Transparencia (Ley 1712 de 2014) que se pueden observar más detalladamente en el **numeral 3** del presente documento.

RESPONSABILIDADES

- La información deberá protegerse de divulgación no autorizada conforme a los Procedimientos de Clasificación y Etiquetado de la Información definidos en el SGSI de MinAgricultura, así como a los mecanismos y controles establecidos para el tratamiento de la información. La información sólo podrá ser usada para las actividades autorizadas.
- Para el intercambio de información se deberán definir las responsabilidades y procedimientos para la transferencia segura de la información, el responsable y proceso a seguir en caso de presentarse un incidente de seguridad, los niveles de clasificación de la información a ser intercambiada.
- Para la transferencia de información se tendrán presentes los riesgos asociados y los canales a utilizar que permitan brindar los niveles de seguridad apropiados. En

cualquier medio que se lleve a cabo la transferencia de información (física o electrónica), esta se realizará a través de canales que preserven los niveles de confidencialidad e integridad de la información, conforme a su nivel de clasificación.

5.1.14 POLÍTICA DE DESARROLLO DE SOFTWARE (ISO/IEC 27002:2013 NUMERAL 14)

OBJETIVO

Definir los lineamientos generales para el desarrollo, mantenimiento y adquisición de *software* al interior del Ministerio de Agricultura y Desarrollo Rural, con el fin de determinar los controles de seguridad en el desarrollo de código fuente.

ALCANCE ESPECÍFICO

La presente política deberá ser cumplida por funcionarios, contratistas y terceros de MinAgricultura que realicen actividades correspondientes al desarrollo, mantenimiento y adquisición de *software* dentro de MinAgricultura.

DETALLE

Para el desarrollo de *software* dentro del Ministerio de Agricultura y Desarrollo Rural se deberá realizar un proceso de planeación en donde se determine la respectiva metodología a utilizar; las etapas de desarrollo; la estructura de desglose de trabajo, con sus respectivos responsables, criterios de aceptación y las pruebas de funcionalidad y seguridad teniendo en cuenta los requerimientos y el cumplimiento de los objetivos estratégicos de MinAgricultura. Las etapas deberán estar debidamente documentadas, con el objeto de generar registros de trazabilidad frente a los requerimientos, desarrollo y aceptación del *software*.

La identificación de las necesidades y requisitos de funcionalidad, calidad y seguridad se realizará entre el área solicitante y la Oficina TIC, y los mismos deberán ser validados durante el proceso de aprobación del desarrollo de *software*.

Para el desarrollo y puesta de producción del *software*, se deberán tener presente tres ambientes separados así: i) de desarrollo (puede ser en los equipos asignados a los colaboradores), ii) de pruebas y iii) de producción, evitando así las alteraciones o modificaciones no autorizadas del código fuente.

Los cambios requeridos sobre el *software* de MinAgricultura se llevarán a cabo a través del Procedimiento de Control de Cambios, el cual permite que se documenten y establezcan los requerimientos y los niveles de aceptación del cambio. Dentro de los requerimientos que se establezcan será necesario analizar los riesgos asociados a la seguridad de la información y la identificación de los controles a implementar para su aseguramiento.

Se establecerán acuerdos en procesos de desarrollo que establezcan con claridad la propiedad de las licencias y derechos intelectuales de los códigos fuentes, así como sus condiciones de usabilidad.

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

a) Acuerdos de licencias, propiedad de código y derechos conferidos (Derechos de Propiedad Intelectual).
b) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
d) Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto “Requerimientos de Seguridad en Contratos de Tercerización”.
e) Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte

RESPONSABILIDADES

- Antes de iniciar el desarrollo de *software*, la Oficina TIC y las áreas de MinAgricultura implicadas deberán acordar una metodología; una estructura de trabajo, con los respectivos responsables; así como el cronograma de desarrollo, determinando el alcance, los procesos afectados y los requerimientos.
- El área solicitante validará los criterios de aceptación correspondientes a la funcionalidad y calidad para dar la aceptación formal del desarrollo de *software*.
- La Oficina TIC en apoyo del Oficial de Seguridad validará los criterios de aceptación técnicos: interoperabilidad, buenas prácticas de programación y seguridad, para dar la aceptación formal del desarrollo de *software*. La aceptación de los criterios estará determinada por los resultados de las pruebas planteadas, las cuales tendrán dentro de sus objetivos detectar, entre otras vulnerabilidades, los códigos maliciosos, las puertas traseras, etc.

- Los datos de pruebas con los que se llevarán a cabo las pruebas del *software* no deben utilizar datos reales de producción.
- En el desarrollo de *software* es necesario establecer controles que permitan conservar la seguridad y privacidad de la información; por lo tanto, es importante tener en cuenta los mecanismos de acceso a la información, autenticación, detección de intrusos, cifrado de datos, salvaguarda de confidencialidad, integridad, disponibilidad y protección de los datos personales.
- La metodología de desarrollo de *software* debe contemplar una etapa de gestión de riesgos.
- La Oficina TIC deberá llevar a cabo revisiones periódicas a los desarrollos realizados, con el propósito de garantizar que se estén desplegando los controles conforme a lo establecido dentro de la fase de planeación.

En el desarrollo de software se llevará a cabo un control de versiones con los respectivos documentos de soporte, con el objeto de verificar el buen funcionamiento del *software* y el respectivo control de su ciclo de vida.

5.1.15 POLÍTICA PARA RELACIONES CON PROVEEDORES (ISO/IEC 27002:2013 NUMERAL 15)

OBJETIVO

Preservar los niveles de seguridad y privacidad de los activos de información del MinAgricultura que sean accedidos o administrados por proveedores, a través de la implementación de controles que minimicen los riesgos asociados.

DETALLE

Cuando se requiera otorgar acceso a los activos de información a los proveedores de MinAgricultura, el responsable del activo, con apoyo del Oficial de seguridad, deberá realizar un análisis de riesgos con el fin de determinar los controles de seguridad que preserven la confidencialidad, disponibilidad e integridad, así como la finalidad del uso de los datos y el respectivo consentimiento en los casos que aplique conforme a los procedimientos legales y administrativos.

Antes de conceder los permisos de acceso se determinarán por parte del responsable del activo: las necesidades del acceso, el acceso requerido (físico o lógico), el nivel de clasificación de la información a acceder, la finalidad de uso, los controles mínimos para

tener en cuenta frente al tratamiento de la información y el manejo de incidentes de seguridad de la información. En ningún caso se otorgará acceso a la información, sistemas de información o áreas seguras de MinAgricultura a proveedores, hasta no haber realizado la adecuada gestión de los riesgos, formalizado la relación contractual.

Dentro de los acuerdos, contratos o convenios formalmente firmados entre las partes se deberán definir claramente los requerimientos de seguridad y privacidad tales como: información a tratar; niveles de clasificación; finalidad; autorizados para el tratamiento; controles a tener en cuenta antes, durante y después del tratamiento de los datos por parte del proveedor, con el respectivo consentimiento por parte de los titulares en los casos que aplique; así como las responsabilidades de las partes conforme a los lineamientos de MinAgricultura y a la legislación vigente.

Siempre que se otorgue acceso a la información de MinAgricultura a terceros, se establecerán acuerdos de confidencialidad que tengan como principio el cumplimiento de las políticas de seguridad de la información de MinAgricultura y cláusulas requeridas para proteger la información a acceder.

RESPONSABILIDADES

- Todos los funcionarios, contratistas y proveedores que tengan acceso a la información deberán cumplir con las políticas de seguridad y privacidad de la información, así mismo, en caso de que identifiquen una amenaza que pueda llegar a vulnerar la información, deberán reportarla a la mesa de servicio a través de los conductos establecidos.
- El responsable del activo de información no permitirá el acceso a la información hasta no tener firmados y formalizados, por medio de un contrato o acuerdo con los proveedores, los fines de uso, condiciones de tratamiento, así como la debida implementación de los controles requeridos para preservar las características de confidencialidad, integridad y disponibilidad de la información.
- Antes de brindar acceso a los activos de información, los proveedores deben aceptar formalmente el cumplimiento de las políticas de seguridad y privacidad de la información del Ministerio de Agricultura y Desarrollo Rural.

5.1.16 GESTIÓN DE INICIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013 NUMERAL 16)

OBJETIVO

Asegurar un enfoque coherente y eficaz para la gestión de las situaciones de seguridad de la información, estableciendo las responsabilidades y procedimientos de gestión.

ALCANCE ESPECÍFICOS

Esta política se aplica para la gestión eficaz de las situaciones de seguridad de la información que se presenten en la entidad, y deben ser comunicadas a las partes interesadas.

DETALLE

La Oficina de TIC, aplica el procedimiento para gestionar el tratamiento de las situaciones de seguridad de la información “Procedimiento de Gestión de Incidentes de Seguridad de la Información”, con el fin de mitigar el impacto y disminuir la probabilidad de ocurrencia de incidentes futuros de seguridad de la información.

Se deberá designar un responsable para responder los incidentes de seguridad de la información, definiendo los tipos de responsabilidades.

Los funcionarios y contratistas de la Entidad deberán reportar los eventos y debilidades de seguridad de la información, tan pronto como sea posible a soporte y asistencia técnica.

Se deberá comunicar y advertir a funcionarios y contratistas que no intenten poner a prueba las debilidades de seguridad sospechosas, ya que podría ocasionar daño a los sistemas de información.

Una vez se reciba el incidente se deberá clasificar cada evento de seguridad de la información usando la escala de clasificación.

Se deberá priorizar el incidente, lo que puede ayudar a identificar el impacto del incidente y la urgencia.

Cuando el incidente se resuelva se deberá notificar al usuario sobre el incidente cerrado.

Se deberá definir y aplicar procedimientos para la identificación y recolección de información que pueda servir como evidencia; teniendo en cuenta:

a- Evidencia de la incidencia.
b- Análisis forense de seguridad de la Información.
c- Cadena de Custodia.
d- Escalar a las instancias superiores.

e- Tratar las debilidades que ocasionan el incidente de seguridad de la Información.
f- Competencia del personal.
g- Roles y Responsabilidades.
e- Registrar y cerrar formalmente el incidente se seguridad de la Información.

5.1.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (ISO/IEC 27002:2013 NUMERAL 17)

OBJETIVO

Establecer, implementar y evaluar las estrategias para mantener la seguridad de la información en la continuidad del negocio en la Entidad.

ALCANCE ESPECÍFICO

Esta política aplica para toda la gestión de continuidad de negocio que la Entidad establezca.

DETALLE

Documentar Políticas y procedimiento sobre la gestión de continuidad del negocio basado en las normas ISO/IEC 27031, ISO 22313 e ISO 22301, en las que se incluyen las fases de gestión de riesgos, análisis de impacto de negocio, desarrollo prueba y mantenimiento del plan.

Se define como requisito de seguridad de la Entidad, que en situaciones adversas o de interrupción no se debe disminuir el nivel de protección para los activos de información, para lo cual, la Entidad debe disponer los medios alternos necesarios que permitan cumplir los objetivos de recuperación de TI, sin afectar la confidencialidad o integridad de los activos de información.

El Ministerio definirá su estrategia de gestión de la continuidad de TI a partir de las necesidades operativas y misionales asociadas a la razón de ser de la Entidad.

Se deben definir las responsabilidades asociadas a la ejecución del Plan de Continuidad de la Entidad.

Se deberá proporcionar los recursos suficientes para dar una respuesta efectiva de funcionarios, contratistas y procesos en caso de contingencia o eventos catastróficos que se presenten en la Entidad, y afecten la continuidad de la operación.

La definición e implementación del Plan de Continuidad de TI, el cual debe hacer parte del Plan de Continuidad de Negocio (BCP) de la Entidad debe contemplar la creación de procedimientos y la implementación de controles, que mantengan el nivel de seguridad de los activos de información en situaciones adversas.

La estrategia de Continuidad de TI de la Entidad debe abordar las fases de prevención, respuesta y manejo de incidentes disruptivos, recuperación, y restauración de la operación.

El Plan de Continuidad de TI de la Entidad debe derivar en la implementación de los controles y medidas pertinentes, para gestionar incidentes de interrupción a la operación.

Se deberá mantener canales de comunicación adecuados hacia los funcionarios, contratistas, proveedores y partes interesadas, con el fin de responder de manera efectiva ante los eventos catastróficos.

Se debe monitorear la efectividad de los controles definidos en el Plan de Continuidad de TI establecido e implementado, con el fin de identificar oportunidades de mejora al desempeño, buscando siempre el cumplimiento de los objetivos de continuidad de la Entidad.

5.1.18 POLÍTICA DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

OBJETIVO

Mantener la seguridad de la información y de los servicios de procesamiento de información en plataformas de computación en la nube que son utilizados por la Entidad, garantizando su continuidad, cumpliendo los niveles de servicio requeridos por los procesos del Ministerio y reduciendo los riesgos legales y técnicos a niveles aceptables.

ALCANCE ESPECÍFICO

Esta política se aplica a los servicios de computación en nube que sean utilizados o contratados por la Entidad, así como a los procesos que hagan uso de dichos servicios.

DETALLE

Durante la implementación de servicios en plataforma en la Nube, se debe contemplar la implementación de mecanismos y medidas de seguridad.

En los contratos celebrados con proveedores de servicios de computación en la nube se debe incluir la necesidad de cumplir las políticas de seguridad de la información de la Entidad, el cumplimiento de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, leyes y regulaciones sobre la protección de la información de la Entidad e información de carácter personal.

En los casos que se requiera el almacenamiento de información en la nube clasificada como reservada, pública clasificada e información de carácter personal esta debe permanecer cifrada para evitar su divulgación o acceso no autorizados. El cifrado se debe realizar de acuerdo con las políticas de seguridad de la información definidas por el sistema de gestión de seguridad de la información de MinAgricultura.

RESPONSABILIDADES

- Los responsables de procesos de MinAgricultura son responsables de coordinar la ejecución de las actividades de análisis y gestión de riesgos para el uso de servicios de computación en la nube
- La OTIC es responsable de asistir a los diferentes procesos de la Entidad en la identificación, gestión y tratamiento de los riesgos asociados al uso de servicios de computación en la nube.
- Todos los usuarios de servicios TIC de MinAgricultura deben tramitar sus solicitudes de uso de servicios de computación o almacenamiento en la nube a través de la mesa de servicios de la Oficina TIC.

5.1.19 IDENTIFICACION DE LEGISLACION APLICABLE Y REQUISITOS CONTRACTURALES (ISO/IEC 27002:2013 NUMERAL 18.1.1 18.1.2)

OBJETIVO

Cumplir con las disposiciones normativas y contractuales en seguridad de la información, a fin de evitar sanciones administrativas a la Entidad y/o funcionarios y contratistas.

ALCANCE ESPECÍFICA

Aplica para toda la Entidad, en el conocimiento, entendimiento y aplicación de la legislación aplicable en lo referente a seguridad y privacidad de la información.

DETALLE

Se deberá identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la Entidad y relacionados con seguridad de la información.

Se debe certificar que todo el software que se ejecuta en la Entidad está protegido por derechos de autor y requiere licencia de uso o, en su lugar sea software de libre distribución y uso.

Los funcionarios y contratistas deberán cumplir con los acuerdos de licenciamiento de software.

Todo el software que se utilice en los equipos de cómputo de la Entidad debe ser autorizado y debe contar con su respectiva licencia. En ninguna circunstancia, se permite el uso de software que incumpla el tipo de licencia especificada por el fabricante.

Se deberá proteger las creaciones intelectuales de software cuando se realicen con terceros, incluyendo en los contratos la obligación de transferir a la Entidad los derechos patrimoniales sobre los productos desarrollados.

5.1.20 POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES (ISO/IEC 27002:2013 NUMERAL 18.1.4)

OBJETIVO

Establecer las medidas generales para garantizar los niveles de seguridad y privacidad adecuados para la protección de datos personales, con el fin de evitar posibles adulteraciones, pérdidas, consultas, usos o accesos no autorizados.

ALCANCE

La presente política será aplicable a los datos personales registrados en cualquier base de datos de MinAgricultura, cuyo titular sea una persona natural.

DETALLE

MinAgricultura implementará una política de Tratamiento de la información, en un lenguaje claro y sencillo, que deberá ser puesta en conocimiento de los Titulares y tendrá que incluir como mínimo:

1. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable.
2. El Tratamiento al cual serán sometidos los datos y la finalidad de este, si este no se ha informado por medio del aviso de privacidad.
3. Derechos que asisten a los Titulares de la información.
4. El área o persona responsable de la atención de las consultas, peticiones y reclamos ante la cual el Titular de la información puede ejercer sus derechos.

5. Procedimiento por medio del cual los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar, suprimir información y revocar la autorización.

Los mecanismos para la autorización del tratamiento de los datos personales podrán ser determinados a través de medios técnicos, de forma oral o por medio de conductas inequívocas que permitan determinar el otorgamiento de la autorización por parte del Titular. Los responsables del tratamiento de MinAgricultura deben conservar el registro de la autorización.

Así mismo, los funcionarios, contratistas o terceros sólo deberán recopilar la cantidad mínima de datos personales requerida para cumplir con los propósitos de MinAgricultura. Dicho recaudo sólo se realizará una vez se obtenga la respectiva autorización por parte del Titular de los datos.

Además, el responsable de las bases de datos deberá adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal y así evitar su destrucción, alteración, pérdida o tratamiento no autorizado. Estas medidas deberán incluir los mecanismos de seguridad físicos y lógicos más adecuados, de acuerdo con el desarrollo tecnológico, de tal forma que garanticen la protección de la información almacenada y el secreto profesional.

Las bases de datos que contengan datos personales deben ser administradas de tal modo que se garantice el respeto a derechos fundamentales como la intimidad, el buen nombre, y en especial, el *Habeas Data*.

Ningún funcionario o contratista de MinAgricultura deberá retirar o transmitir información que contenga datos personales sin la debida autorización expresa del responsable; y en caso de que se facilite información a terceros, se deberá garantizar el buen uso y contar con el debido consentimiento para el tratamiento de los datos conforme a su finalidad. Los mecanismos de transferencia se realizarán a través de las políticas y procedimientos de seguridad y privacidad descritas en el presente documento.

Los responsables y encargados del tratamiento de los datos personales sólo podrán recolectar, almacenar, usar o circular dichos datos durante el tiempo establecido para cumplir las finalidades que justificaron el tratamiento.

Los funcionarios, contratistas y terceros de MinAgricultura no podrán realizar el tratamiento de datos personales de niños, niñas y adolescentes, excepto cuando se trate de datos públicos. En este caso, MinAgricultura deberá respetar los intereses y los derechos fundamentales, conforme a una autorización previa del representante legal de cualquiera de ellos.

En el caso de que no sea posible poner a disposición del Titular de la información las políticas de tratamiento, los responsables deberán informar por medio de un Aviso de Privacidad al Titular sobre la existencia de las políticas y la forma en la cual puede acceder a las mismas, a más tardar en el momento en el que se vaya a realizar la recolección de datos personales.

RESPONSABILIDADES

- Los funcionarios, contratistas y terceros que tengan acceso a datos personales tratados y administrados por el MinAgricultura, deberán cumplir con la política anteriormente descrita, haciendo uso de los controles y medidas establecidas para la protección de la información conforme a su nivel de clasificación.
- El responsable de las bases de datos que contengan información personal deberá asegurar que antes de realizar cualquier tratamiento de los datos, el MinAgricultura cuente con las autorizaciones de los Titulares y los mecanismos de control para la protección de la información.
- Los funcionarios, contratistas y terceros deberán evitar el acceso a los datos personales para los cuales no se encuentren autorizados y en caso de que observen violación o fallas de los mecanismos de control de seguridad y privacidad, estos hechos deberán ser reportados a la mesa de servicios para determinar las acciones a desarrollar.
- En caso de que se requiera realizar transferencia de datos personales, se deberá efectuar de acuerdo con el Procedimiento de Recepción y/o Transferencia de Información del MinAgricultura.
- Se deberá realizar la actualización periódica de las listas de acceso de las personas y funcionarios autorizados para efectuar cualquier tipo de tratamiento frente a los datos personales. Así mismo, se identificarán, de acuerdo con los niveles de clasificación, los mecanismos apropiados para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.
- Una vez culmine el lapso del tratamiento de los datos personales, el responsable de los mismos deberá velar porque sean eliminados de forma segura, para evitar su recuperación

5. HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción
22-09-2016	1	Versión inicial.
18-12-2019	2	Se realizó la actualización del Logo de la Entidad. Así mismo, se cambió Gobierno en Línea por Gobierno Digital y se cambió el nombre del profesional y del jefe de la OTIC.
30-10-2020	3	Se realiza actualización en las políticas, incorporando políticas específicas de acuerdo con la declaratoria de aplicabilidad de controles de los dominios del anexo A de la norma ISO 27001:2013. Se realiza el cambio del nombre del documento.