TABLA DE CONTENIDO

1. OBJETIVO

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, con las cuales se busca la mejora continua en la Seguridad de la Información en la Agencia de Desarrollo Rural - ADR.

2. ALCANCE

Las políticas de seguridad y privacidad de la información están orientadas a toda la información almacenada, procesada y transmitida en medios electrónicos, estas políticas deben ser conocidas y cumplidas tanto por funcionarios y contratistas que apoyan la gestión y por los terceros o grupos de interés que utilicen la información generada y custodiada por la Agencia de Desarrollo Rural -ADR , y por quienes hagan uso de los servicios tecnológicos de la Entidad.

3. DESARROLLO

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN -MSPI

Teniendo en cuenta lo expresado en la resolución 1602 del 2017, "Por la cual crea el Comité Institucional de Desarrollo Administrativo de la Agencia de Desarrollo Rural, como instancia orientadora del Modelo Integrado de Planeación y Gestión y se establece su reglamentación" y en su lugar se integra el Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural." En su artículo Tercero. Funciones del comité institucional de gestión y desempeño de la Agencia de Desarrollo Rural, numeral 6 - "Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información".

Es por esto, que la Agencia de Desarrollo Rural (ADR), ha adelantado el posicionamiento de la Oficina de Tecnologías de la Información (OTI) como una oficina estratégica al interior de la entidad, en la definición de directrices relacionados con Transformación Digital y los avances en la implementación de las Políticas de Gobierno Digital y Seguridad Digital, por lo tanto, este documento tiene como fin reglamentar de manera detallada y clara en la declaración de aplicabilidad y de políticas de seguridad y privacidad de la Información en el establecimiento, implementación, operación, monitoreo, revisión y mejora continua de la Seguridad y Privacidad de la Información.

Dado lo anterior en el cumplimiento de la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la ADR, que está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo esto con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

En consecuencia, de los anteriormente mencionado se elabora el presnte Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los activos de información al interior de la ADR; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información, así como en detallar de manera general, las políticas, los principios de seguridad y la normatividad pertinente.Asi las cosas la ADR debe aprobar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

IDENTIFICACIÓN NECESIDADES Y EXPECTATIVAS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

• PRIVACIDAD DE LA INFORMACIÓN

Todo el equipo de la Agencia de Desarrollo Rural-ADR, es responsable de la seguridad de la información. Adicionalmente existen los siguientes roles y responsabilidades específicas dentro del Modelo de Seguridad y Privacidad de la Información al interior de la entidad, en conformidad con la Norma (NTC-ISO/IEC 27001:2013, 2013)

o Presidencia

Responsable por el direccionamiento estratégico de liderar la implementación del Modelo de Seguridad y Privacidad de la Información el cual requiere el compromiso, recursos y asignación de responsabilidades para la gestión de seguridad y privacidad de la información. a través de la aprobación del direccionamiento y los resultados por parte del Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural.

Como parte de la gestión de la presidencia para seguridad de la información se encuentran las siguientes responsabilidades:

- Asegurar que se establezcan la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la ADR. Por medio de la aprobación y verificación del cumplimiento de las políticas de seguridad de la información

- Dirigir y apoyar a funcionarios y contratistas, para contribuir a la eficacia en la gestión de la seguridad de la información.

- Apoyar otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad

o Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural.

Con la Resolución 1602 del 6 de diciembre de 2017 "Por la cual se deroga la Resolución No. 731 de 2017 "Por la cual crea el Comité Institucional de Desarrollo Administrativo de la Agencia de Desarrollo Rural, como instancia orientadora del Modelo Integrado de Planeación y Gestión y se establece su reglamentación" y en su lugar se integra el Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural.

El Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural, tendrá a su cargo las siguientes funciones:

- Aprobar y hacer seguimiento, por lo menos una vez cada tres meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión - MIPG de la Agencia de Desarrollo Rural.

- Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión - MIPG de la Agencia de Desarrollo Rural.

- Proponer al Comité Sectorial de Gestión y el Desempeño institucional, iniciativas que contribuyan al mejoramiento en la implementación y operación del Modelo Integrado de Planeación y Gestión - MIPG.

- Presentar los informes que el Comité Sectorial de Gestión y el Desempeño Institucional y los organismos de control requieran sobre la gestión y el desempeño de la entidad.

- Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión.

Las demás que tengan relación directa con la implementación, desarrollo y evaluación del Modelo.

Teniendo en cuenta el numeral 6 de la Resolución 1602 de 2017 ; "Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información" se tienen las siguientes responsabilidades:

* Definir la estrategia, el gobierno y la dirección de la gestión de la seguridad de la información.
* Aprobar la política de seguridad y privacidad de la información.
* Promover la gestión de la seguridad de la información mediante el compromiso de la dirección y la asignación de los recursos adecuados.
* Estudiar y aprobar las iniciativas de seguridad de la información que le sean propuestas.

o Responsable del funcionamiento del Modelo de Seguridad y Privacidad de la Información

El responsable del funcionamiento del Modelo de Seguridad y Privacidad de la Información en la Agencia de Desarrollo Rural-ADR, es del jefe de la Oficina de Tecnologías de la Información y sus principales responsabilidades son:

- Asegurar la disponibilidad de los recursos necesarios para la definición, la implementación y el mantenimiento del Modelo de Seguridad y Privacidad de la Información.

- Revisar periódicamente los documentos y controles del Modelo de Seguridad y Privacidad de la Información para asegurar que el que el Modelo de Seguridad y Privacidad de la Información logre los resultados previstos.

- Analizar la gestión de los incidentes de seguridad que le sean escalados y ponerse en contacto con las autoridades correspondientes.

- Definir lineamientos que den guía al profesional de seguridad de la información.

o Profesional de seguridad de la información

Las actividades del profesional de Seguridad Digital y Seguridad de la Información serán coordinadas y aprobadas por el jefe de la Oficina de las Tecnologías de Información. Por consiguiente, se encuentran las siguientes responsabilidades:

- Asesorar al Comité Institucional de Gestión y Desempeño en la planificación, diseño, implementación, operación, revisión y mejora continua del Modelo de seguridad de la información en la entidad, sus políticas, lineamientos y controles, conforme a los requerimientos legales y buenas prácticas de normas técnicas.

- Apoyar al Comité Institucional de Gestión y Desempeño en las actividades de implementación del Modelo de Privacidad y Seguridad de la Información de la estrategia de Gobierno Digital del Ministerio de Tecnología de la Información

- Apoyar el Comité Institucional de Gestión y Desempeño en las actividades de implementación de la estrategia de ciber seguridad definida por el Ministerio de Defensa Nacional.

- Apoyar al Comité Institucional de Gestión y Desempeño en las actividades de divulgación y promoción de la importancia de la política de seguridad digital, los beneficios de la seguridad de la información para la entidad y las implicaciones de la no conformidad con los requisitos de seguridad de la información de la Agencia de Desarrollo Rural-ADR, mediante la elaboración de propuestas de programas de toma de conciencia y formación en seguridad de la información.

- Velar por el cumplimiento de los requisitos del Modelo de seguridad de la información, base de datos y sistemas de comunicaciones informáticos.

- Apoyar en las acciones necesarias para identificar controlar, reducir y evaluar incidentes de seguridad de la información.

- Preparar los informes del estado de la seguridad de la información y la efectividad de los controles de la seguridad, para realizar la revisión periódica del estado del sistema y acompañar a la entidad en la evaluación de este para asegurar que el Modelo de seguridad de la información permanezca conforme a las necesidades de la entidad, y se identifiquen mejoras sobre el mismo.

- Proponer, diseñar y fomentar la implementación de mejoras a los controles y herramientas de seguridad de la información necesarias para el fortalecimiento de la seguridad de la información en la entidad, y el adecuado tratamiento de los incidentes de seguridad de la información detectados.

- Coordinar con los propietarios de los activos de información y los dueños de procesos las acciones para el cumplimiento del Modelo de Seguridad y Privacidad de la Información.

- Apoyar a los funcionarios y contratistas para que cumplan con las responsabilidades de su rol frente al Modelo de Seguridad y Privacidad de la Información

o Propietario de los activos de información

Es una parte designada de la Agencia de Desarrollo Rural-ADR, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso . Sus principales responsabilidades son:

- Cumplir con la política vigente de seguridad de la información adoptada por la entidad

- Identificar, establecer el alcance y el valor o criticidad de los activos de información de los cuales es propietario.

- Clasificar los activos de información siguiendo la metodología de identificación y clasificación de activos donde "Los líderes de los procesos, deberán identificar y asignar un custodio para uno de los activos de Información identificados; el custodio debe ser el Presidente, Vicepresidente o Jefe del área o dependencia en donde se realiza el levantamiento de los activos de información, para el caso de las UTT el custodio es el Director de la UTT", aprobada y verificada el responsable del funcionamiento del Modelo de Seguridad y Privacidad de la Información

- Identificar, definir y evaluar los riesgos a los que pudieran estar expuestos los activos de información de los cuales es propietario.

- Definir los requerimientos de seguridad de los activos de información en relación con su confidencialidad, integridad y disponibilidad.

- Informar los requerimientos y controles requeridos por los activos de información a los custodios y usuarios de los activos de información.

- Efectuar una verificación periódica de la correcta ejecución de los controles requeridos sobre los activos de información bajo su responsabilidad.

- Conocer la valoración actual del riesgo y verificar si se encuentra dentro del nivel de riesgo aceptable definido por la ADR.

- Gestión inmediata para el tratamiento definido en el Modelo de Seguridad y Privacidad de la Información cuando el riesgo se encuentre en una calificación por fuera del nivel de riesgo aceptable.

- Cumplir con el reporte formal del riesgo a la Oficina de Planeación, cuando se detecte que su valoración supera el nivel de riesgo aceptable.

- Seguimiento permanente a la aplicación de los controles requeridos para el tratamiento del riesgo hasta que se constate que el nivel se encuentra dentro del nivel de riesgo aceptable

o Custodio de los activos de información

Es el funcionario, contratista o área de la Agencia de Desarrollo Rural-ADR, responsable de administrar y hacer efectivos los controles que el propietario del activo de información haya definido. Sus principales responsabilidades son:

- Implementar y mantener los controles requeridos en los contenedores donde estén almacenados los activos de información que se encuentren a su cargo.

- Administrar los recursos donde residen los activos de información dando los permisos definidos por el propietario del activo a los usuarios interesados.

- Proteger los activos de información presentes en los contenedores a su cargo en la situación que corresponda: almacenamiento, transporte y procesamiento.

o Líder de procesos

Es el funcionario, contratista o área de la Agencia de Desarrollo Rural-ADR, al cual se le ha asignado la responsabilidad formal sobre un proceso de la entidad. Sus principales responsabilidades son:

- Apoyar la identificación de los activos de información que intervienen en el proceso correspondiente.

- Validar los activos de información identificados junto con las características básicas de cada uno de ellos.

- Apoyar y validar la identificación y designación de los propietarios de los activos de la información de su proceso.

o Usuario de la información

Es el funcionario o contratista de la Agencia de Desarrollo Rural-ADR, que utiliza la información para desempeñar sus funciones. Sus principales responsabilidades son:

- Utilizar los activos de información exclusivamente para el desempeño de sus funciones y obligaciones dentro y fuera de la Agencia de Desarrollo Rural-ADR.
- Conocer la clasificación de los activos de información que maneja.
- Preservar la seguridad de la información utilizada en el desempeño de sus funciones y obligaciones.
- No divulgar la información clasificada sin autorización del propietario del activo de información.
- Procurar el buen manejo de todos los activos, buscando protegerlos en relación con los principios de seguridad.

Todo lo anterior con el fin de: Identificar las necesidades y requerimientos la Agencia de Desarrollo Rural-ADR para tener en cuenta en la implantación del MSPI, definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información.

Establecer el estado actual y nivel de madurez de los procesos de seguridad y privacidad de la información, identificando vulnerabilidades, amenazas y riesgos.

Establecer y documentar el gobierno de gestión de seguridad de la información, alineado con el gobierno de TI
Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
Establecer lineamientos que permitan continuar con la gestión de la seguridad de la información al interior de la entidad. Evaluar y alinear el Modelo de seguridad y privacidad de la información con el fin de dar cumplimiento a los marcos regulatorios identificados. Planear programas y planes de auditoria para el monitoreo y mejora continua Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información como eje transversal.
Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

3. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN POLÍTICA DE TRATAMIENTO DE PROTECCIÓN DE DATOS

La Agencia de Desarrollo Rural - ADR, adopta en términos de la Resolución No. 04092 del 03-07-2019 “politica de seguridad y privacidad de la información”,asi como las actualizaciones de la misma, con el objetivo establecer mecanismos y procedimientos para la divulgación y socialización oportuna, eficaz y efectiva de las decisiones, comunicados, recomendaciones, politicas y en general toda actuación que adopte la Entidad en el marco de su misión, visión y funciones constitucionales y legales que deban ser de conocimiento al público en general o a sus servidores públicos y colaboradores.

Al cumplimiento del pacto por la transformación digital a partir de la ley 1955 de 2019 PND 2018 - 2022, armonizando los postulados y sus objetivos, como estrategia transversal establecida por el Plan Nacional de Desarrollo y con los objetivos del Ministerio de Ciencia, Tecnología e Innovación en relación con el desarrollo del conocimiento cientifico, tecnológico y de innovación, en aras de la modernización del Estado.

3.1 POLITICAS

3.1.1. Políticas dispositivas móviles y teletrabajo

La ADR a través de la Secretaria General establece las directrices de asignación desde la Dirección Administrativa y Financiera - Logística de Bienes y Servicios, los cuales son asignados a custodia del usuario quien es responsable del uso y manejo de dispositivos móviles (teléfonos móviles, La Entidad teléfonos inteligentes “smartphones”, tabletas, entre otros, suministrados por la ADR).

Los usuarios no están autorizados a cambiar la configuración, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo. Está permitido aceptar y aplicar las actualizaciones.

Los usuarios deben proteger el acceso a los dispositivos móviles, realizando la configuración el bloqueo (patrón, contraseña, huella o el que le aplique) de pantalla en el dispositivo móvil asignado, con el fin de evitar acceso a la información por un tercero.

Evitar hacer uso de redes inalámbricas de uso público inseguras para transmitir información institucional, así como conectar los dispositivos a equipos de uso compartido público como Centros comerciales, café internet entre otras.

Evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

Es responsabilidad de los funcionarios y contratistas mantener copias de seguridad de la información contenida en sus dispositivos móviles y entregarlas a la ADR en custodia al finalizar la vinculación con la Entidad

3.1.2. Política de seguridad de los Recursos Humanos.

La Agencia de Desarrollo Rural -ADR a través de la Dirección de Talento Humano debe asegurar que los funcionarios, contratista y demás colaboradores adopten sus responsabilidades en relación con la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación y actúen de manera consistente frente a las mismas, desplegar esfuerzos para generar conciencia y apropiación, con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información

En el cumplimiento de los lineamientos enmarcados en el MSPI, en relación con los contratistas, la Vicepresidencia de Gestión Contractual deberá incluir en los documentos contractuales, cualquiera que sea su naturaleza o modalidad, las obligaciones correspondientes al cumplimiento de la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación, las cuales deberán ser divulgadas a través de los supervisores de los contratos, a proveedores, a operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones, obligaciones y las de la Agencia de Desarrollo Rural -ADR, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.
Ingreso y retiro del personal

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013 y la legislación aplicable con relación a la contratación pública, la vinculación laboral, retiro laboral y el cambio de cargo se llevarán a cabo siguiendo las indicaciones del proceso de Gestión de Talento Humano y el procedimiento de Administración De Talento Humano

Para los contratistas, los lineamientos para la vinculación y el retiro laboral se encuentran en los contratos de prestación de servicios y acta de inicio

Capacitación y entrenamiento en seguridad digital y de la información
La ADR debe asegurar que todos los funcionarios, contratistas y todos aquellos con acceso a la información y que tengan definidas responsabilidades de seguridad digital y de la información sean competentes (en cuanto a capacitación formal y no formal) para desempeñar sus funciones. Para ello, la oficina de Tecnologías de la Información alineada con la Oficina de Comunicaciones y Talento Humano con el plan de capacitación institucional, elabora anualmente un plan de sensibilización e seguridad digital en el cual mediante, infografías informativas enviadas mensualmente por el correo de comunicaciones, capacitaciones presenciales y virtuales, dirigidas a los usuarios que les permitan adquirir un conocimiento adecuado del buen uso de las tecnologías en la seguridad de la información y su aplicación con las políticas que se tiene implementadas la ADR.

Procesos disciplinarios

La Agencia de Desarrollo Rural -ADR velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad y privacidad de la información, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional, para lo cual dispondrá una Matriz de Requisitos Legales para su control y seguimiento. La ADR llevará a cabo imposición de sanciones disciplinarias en los casos que lo ameriten de acuerdo con la normatividad vigente.

Intercambio de información

los funcionarios y contratistas deben conservar y tratar como confidencial toda la información suministrada o comunicada por la ADR que revista carácter confidencial, así como toda la información conocida en desarrollo de sus funciones y deben comprometerse a no utilizarla

para fines distintos a los previstos en la ejecución de sus contratos y no divulgar la información que conozca, ni los resultados del trabajo realizado conservando la confidencialidad del mismo, so pena de las acciones civiles, administrativas o penales a que haya lugar en favor de la Agencia de Desarrollo Rural-ADR.

Los funcionarios y contratista deben abstenerse de utilizar la información en beneficio directo o indirecto, propio o de terceros, de publicar, divulgar, difundir, ofrecer o hacer la información disponible a terceros total, o parcialmente. Así mismo, conservaré la información confidencial en condiciones seguras y tomaré todas las medidas que sean necesarias para evitar que sea hurtada, copiada, reproducida, distribuida, divulgada o difundida en forma no autorizada.

El intercambio de información con organismos de control y autoridades de supervisión se rige por el proceso de Participación y Servicio al Ciudadano en atención a entes externos de control y las directrices que impartan para el intercambio de información

3.1.3. Política de Gestión de Activos.
La Agencia de Desarrollo Rural -ADR a través de la Secretaria General con el apoyo de la Oficina de Tecnologías de la Información, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y buen uso de los activos de información con el objetivo de garantizar su protección, y estarán alineados a los procesos de la entidad. Dichos lineamientos se impartirán teniendo en cuenta los siguiente literales, que serán consolidados y publicados en el proceso de apoyo “Gestión Documental” por la Dirección Administrativa y Financiera - Gestión Documental.

a) Inventario de Activos: Los activos de la ADR deben ser identificados, clasificados, valorados y controlados para garantizar su uso adecuado, protección y recuperación ante desastres. Por tal motivo, se diseñará una metodología con los lineamientos necesarios para llevar el inventario de los activos de información de su propiedad, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la Entidad disponga.

b) Protección: Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la información, mantener y actualizar el inventario de activos de información relacionados con sus servicios (información física o digital, software, hardware y recurso humano), bajo los parámetros que establezca la Oficina de Tecnologías de la Información

c) Archivos de Gestión: La Secretaría General a través de la dependencia encargada de la Gestión Documental de la ADR, deben implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental, con el fin de proteger y conservar la confidencialidad, la integridad y la disponibilidad de la información de la ADR.

d) Clasificación de la Información: La clasificación de la información de la ADR tendrá en cuenta las previsiones contenidas en la Ley 1712 de 2014 reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, la Ley 594 de 2000 (Ley General de Archivos), y lo estipulado en la Guía para Desarrollo de Inventario y Clasificación de Activos de Información de la ADR.
Uso aceptable de los activos

La información, archivos físicos, sistemas, servicios, y los equipos (ej. Estaciones de trabajo, portátiles, impresoras, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad de la entidad, son activos de la entidad.

Recursos Tecnológicos: Los recursos tecnológicos de la Agencia de Desarrollo Rural -ADR, son Herramientas apoyo a las labores y responsabilidades de los servidores públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

a) Los bienes de cómputo de la ADR se emplearán de manera exclusiva y bajo la completa responsabilidad por el funcionario o contratista al cual han sido asignados, y únicamente para el correcto desempeño de las funciones del cargo o las obligaciones. Por tanto, no pueden ser utilizados con fines personales o por terceros, no autorizados ante la Oficina de Tecnologías de la Información mediante solicitud formal de la Presidencia, Vicepresidencias, Jefes de Oficina, Secretaría General, y Directores Técnicos Territoriales, a través de la Mesa de servicios.
b) Sólo está permitido el uso de software licenciado por la ADR o aquel que sin requerir licencia sea expresamente autorizado por la Oficina de Tecnologías de la Información. Las aplicaciones generadas o adquiridas por la Entidad, en desarrollo de su operación institucional, deben ser reportadas a la Oficina de Tecnologías de la Información para su administración.
c) En caso de que el servidor público o contratista deba hacer uso de equipos ajenos a la ADR, éstos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red de la ADR una vez esté avalado por la Oficina de Tecnologías de la Información.
d) Es responsabilidad de los funcionarios y contratistas mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas a la ADR en custodia al finalizar la vinculación con la Entidad.
e) Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional.
f) No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los elementos tecnológicos, en la medida que la exposición de los equipos a estos puede ocasionar daños en los mismos.
g) No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.
h) Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes, son los designados por la Oficina de Tecnologías de la Información para tal labor.
i) La Oficina de Tecnologías de la Información realizará monitoreo sobre los dispositivos de almacenamientos externos, con el fin de prevenir o detectar fuga de información, en la medida que la exposición de los equipos represente riesgos de daños en los mismos.
j) La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, el funcionario o contratista a quien se le hubiere asignado debe Informar la dependencia o sede donde se detecta la pérdida del bien a la Dirección Administrativa y Financiera de la ADR para realizar el procedimiento establecido para este tipo de siniestro, así como también a la oficina de tecnologías de la información con el fin de reportar evento o incidente se seguridad de la información.
k) La pérdida de información debe ser informada con el detalle de la información extraviada a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios para el diligenciamiento del reporte de gestión de incidente o evento de seguridad a la mayor brevedad posible para dar la solución.
l) Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información física o digital deberá ser reportado a la mayor brevedad a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios para el diligenciamiento del reporte de gestión de incidente o evento de seguridad a la mayor brevedad posible para dar la solución.
m) La Oficina de Tecnologías de la Información es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
n) Todo acceso a la red de la ADR, mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la Oficina de Tecnologías de la Información.
o) La conexión a la red wifi institucional para servidores públicos y contratistas deberá ser administrada desde la Oficina de Tecnologías de la Información quien implantará políticas para la seguridad de la información.
p) Los equipos deben quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina durante la noche, esto es, con el fin de proteger la seguridad y distribuir bien los recursos de la Entidad, siempre y cuando se programe actividades vía remota deben ser autorizadas por la Oficina

de Tecnologías de la Información

Uso del correo electrónico

El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los servidores públicos y contratistas de la Agencia de Desarrollo Rural -ADR, cuyo uso se facilitará en los siguientes términos:

a) El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la Entidad es el asignado por la Oficina de Tecnologías de la Información, que cuenta con el dominio @adr.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.
b) El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la Agencia.
c) En cumplimiento de la iniciativa del uso racional y eficiente del papel y del principio de la Eficiencia Administrativa, se debe preferir el uso del correo electrónico para el envío de documentos físicos, siempre que la Ley lo permita.
d) Los mensajes de correo electrónico tendrán en cuenta las previsiones contenidas en la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.), normativa que establece la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.
e) Está prohibido el envío de correos masivos (más de 30 destinatarios) a nivel nacional tanto internos como externos, con excepción de lo que se generen desde el correo electrónico asignado por los directores. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.
f) Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Oficina de Tecnologías de la Información a través de la herramienta de la mesa de Servicios como incidente de seguridad según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento; lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones ,exe, .bat, .prg, .bak, .pif, o explícitas referencias no relacionadas con la misión de la Entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos). Está expresamente prohibido el envío y reenvío de mensajes en cadena.
g) La Cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o a cualquier otra instancia ajena a los fines o a la misionalidad de la Agencia de Desarrollo Rural -ADR.
h) Esta expresamente prohibido el uso del correo institucional para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
i) Está expresamente prohibido distribuir información de la Agencia de Desarrollo Rural - ADR, que no tengan el carácter de datos abiertos, a otras entidades o ciudadanos sin la debida autorización de la Presidencia, Vicepresidencias, la Oficina de Planeación o la Oficina de Comunicaciones.
j) El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la Ley Colombiana vigente.
k) Todos los correos electrónicos institucionales en sus mensajes deben contener una nota de confidencialidad, que será diseñada por la Oficina de Tecnologías de la Información y debe reflejarse en todos los buzones con dominio @adr.gov.co.
l) Está expresamente prohibido distribuir, copiar, reenviar información de la Agencia de Desarrollo Rural -ADR a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.
m) Cuando un servidor público o contratista cesa en sus funciones o culmina la ejecución de contrato la Agencia de Desarrollo Rural -ADR, la oficina de tecnologías de la información deshabilitará el correo electrónico y no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa de la presidencia, Secretaria General, por orden judicial, por solicitud de la Oficina de Control Interno o de Control Disciplinario como parte de un proceso de investigación.

Uso de internet

La Oficina de Tecnologías de la Información, en conjunto con el Oficial de la Seguridad de la Información o quien haga sus veces, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones. Será responsabilidad de los colaboradores las siguientes, entre otras:

a) El uso del servicio de Internet está limitado exclusivamente para propósitos laborales y los servicios a los que un determinado usuario pueda acceder desde internet dependerán del rol o funciones que desempeña el usuario en la Agencia de Desarrollo Rural -ADR, y para los cuales esté formal y expresamente autorizado
b) Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
c) Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas.
d) Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
e) Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso

3.1.4. Políticas gestión de medios de almacenamiento

La Oficina de Tecnologías de la Información deberá realizar y mantener copias de seguridad de la información de la Entidad en medio digital, siempre que ésta sea reportada por el responsable de esta, con el objetivo de recuperarla en caso de cualquier tipo de falla.

Efectuará la copia respectiva de acuerdo con el esquema definido previamente en un procedimiento que enmarque la gestión, copias de seguridad de la información digital, sistemas de información, bases de datos y demás recursos tecnológicos de la Entidad; el diseño de este procedimiento se hará en conjunto con los líderes de proceso, con el fin de determinar la información a respaldar y la periodicidad del respaldo, los tiempos de recuperación y restauración, y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información.

Contar con un procedimiento de administración de copias de seguridad para respaldar, duplicar o restaurar activos de información almacenados en los servidores de la red de datos de la ADR, el acopio y custodia de las mismas, con el fin de garantizar la confidencialidad, integridad, disponibilidad y preservar y/o restaurar la información ante la posibilidad de pérdida de los datos.

3.1.5. Política de Control de Acceso.

Los propietarios de los activos de información y teniendo en cuenta el tipo de activo, deberán establecer medidas de control de acceso a nivel de estructura Física e instalaciones, hardware, información, personas, redes , software, intangibles, componentes de red y Servicio con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física de personal no autorizado, y así propender por salvaguardar la integridad, disponibilidad y confidencialidad de la información de la Agencia de Desarrollo Rural -ADR.

Acceso a redes y a servicios en red

La Agencia de Desarrollo Rural -ADR, se reserva el derecho de controlar los accesos a los sitios web, navegados desde la Red Interna hacia la Internet Pública, con el fin de evitar fuga de información y accesos a sitios que pongan en riesgo la integridad de la red institucional, así como, el parque computacional y demás infraestructura tecnológica, y por tanto el uso del servicio de internet de todos sus funcionarios o contratistas, puede limitar el acceso a determinadas páginas de Internet, los horarios de conexión, el acceso a los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad.

los funcionario o contratista podrá compartir archivos o carpetas con las herramientas colaborativas destinada para tal fin , si requieren apoyo se debe solicitar a la mesa de servicios.

El acceso a redes WiFi se controla desde la Oficina de Tecnologias de la Información, alineado con la Política de Navegación Web de la ADR, la cual es controlada mediante perfiles de navegación.

La conexión remota a la red de área local de la ADR debe ser realizada a través de una conexión VPN segura o mediante conexión con el uso de las herramientas colaborativas suministrada por el Oficina de Tecnologias de la Información, previa autorización del jefe de área y/o dependencia, quien es el encargado de realizar la solicitud formal, en el cumplimiento del procedimiento de Administración de Redes y documento de Aseguramiento de Servicios en la Red

Gestión de acceso de usuarios

El registro y cancelación de usuarios, el suministro de acceso a usuarios, la gestión de derechos de acceso privilegiado, la gestión de información de autenticación secreta, y la revisión, retiro o ajuste de los derechos de acceso se realizan de acuerdo con el documento de Administración de Usuarios y Sistemas de Información, para gestionar acceso a los medios de procesamiento de información.

Uso de los Sistemas o Herramientas de Información

Todos los funcionarios y contratistas de la Agencia de Desarrollo Rural -ADR, son responsables de la protección de la información a la que acceden o procesan y de evitar su pérdida, alteración, destrucción o uso indebido, para lo cual se dictan los siguientes lineamientos:

a) Las credenciales de acceso a la red o recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y contratistas no deben revelar éstas a terceros ni utilizar claves ajenas.
b) Todo funcionario y contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.
c) Las contraseñas se deben establecer teniendo en cuenta los siguientes parámetros; Deben contener mayúsculas, minúsculas, números, caracteres especiales y mínimo ocho (08) caracteres.
d) Las contraseñas deben ser cambiadas en conformidad con la regla aplicada. Para ello, las aplicaciones controladas mediante el directorio activo al igual que el correo
electrónico, exigirán el cambio automático de las contraseñas con la periodicidad configurada por el administrador del directorio activo .
e) Todo funcionario y contratista es responsable de los registros o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.
f) En el caso de terminación del vínculo laboral de un funcionario de planta permanente o temporal la Dirección de Talento Humano, debe informar la novedad a la mesa de servicio con la resolución, para la inactivación de los servicios tecnológicos correspondientes, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad.
g) En el caso de terminación de ejecución el contrato con la ADR para los contratistas se cuenta con la fecha de inactivación de la terminación de contrato relacionada en el acta de inicio y cuando se realice la paz y salvo la mesa de servicio hará la verificación de los servicios tecnológicos correspondientes, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad.
h) Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato de la ADR, la información generada por funcionario o contratista será respaldada y entregada a petición de este o del jefe o Supervisor del Contrato.
i) Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato de la ADR, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual de acuerdo con la normativa vigente.
j) Todos los funcionarios y contratistas de la Agencia deben respetar lo estipulado en la Ley 23 de 1982 "Sobre derechos de autor", la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

Control de acceso a sistemas y aplicaciones

a) El control de acceso a sistemas y aplicaciones se rige por la política de control de acceso del directorio activo y para aplicaciones que no se autentique por el directorio activo deberán contar con una administración donde se aplique la política de control de acceso, para gestionar acceso a los medios de procesamiento de información.
b) Con el fin de controlar el acceso no autorizado a sistemas y aplicaciones, las contraseñas de cuentas de administración genéricas deben ser cambiadas cada vez cada vez que expiren el tiempo de acceso concedido a un funcionario, exfuncionario, contratista y/o proveedor y diligenciar los registro para cambios de contraseñas de administrador destinado para esta actividad.
c) El uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones no está permitido para fines diferentes a las actividades propias de la Oficina de Tecnologias de la Información
d) La ADR controla el uso de programas utilitarios privilegiados mediante directorio activo.
e) Para acceder a los códigos fuente de programas y elementos asociados (tales como diseños, especificaciones, planes de verificación y planes de validación) se debe contar con autorización de la Oficina de Tecnologias de la Información Lo anterior, con el fin de evitar la introducción de funcionalidades no autorizadas, evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual valiosa.
f) Se debe contar con un procedimiento de Procedimiento Desarrollo Implementación y Mantenimiento de Sistemas de Información. Así com tambien el lineamiento establecido en el documennto Ingreso Seguro a los Sistemas de Información

3.1.6. Políticas seguridad física y del entorno

La Agencia de Desarrollo Rural -ADR debe adoptar medidas para la protección del perímetro de seguridad de sus instalaciones físicas; para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones), además para mitigar los riesgos y amenazas externas y ambientales, con el fin de evitar afectación a la confidencialidad, disponibilidad e integridad de la información de la Entidad.

Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones físicas de la Agencia de Desarrollo Rural -ADR, deben estar debidamente identificados, con un documento que acredite su tipo de vinculación y dicho documento se debe portar en un lugar visible.

Los visitantes de la Agencia de Desarrollo Rural -ADR, siempre deben estar autorizados por un servidor público o contratista y se le dará un soporte de imagen impresa con los datos del visitante y el área que visita

El personal de empresas contratistas, que desempeñen las funciones de forma permanente o transitoria en las instalaciones de la Agencia de Desarrollo Rural -ADR, deben estar identificados con distintivos del Contratista y portar el carné de la Administradora de Riesgos Laborales -ARL.

La ADR cuenta con un plan de emergencias con el fin de brindar protección contra amenazas externas.

Oficina de Tecnologías de la Información establece un procedimiento, para ejecutar (mantenimiento correctivo y preventivo) y hacer seguimiento a los planes anuales de mantenimiento de la infraestructura tecnológica de la entidad.

La única dependencia autorizada para trasladar los elementos y recursos tecnológicos al interior y exterior de la entidad es la Dirección Administrativa y Financiera de la ADR, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de dicha dependencia.

Cuando una estación de trabajo, equipo portátil o medio removible vaya a ser reasignado o dado de baja por la Dirección Administrativa y Financiera de la ADR, se debe solicitar un caso a la mesa de servicio OTI, para realizar concepto técnico, una copia de respaldo de la información de la entidad que allí se encuentre almacenada (en caso de ser necesario y se deja en custodia de la OTI). Posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobreescritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma y dejar a disposición del almacén.

3.1.7. Política de Criptografía.

La Oficina de Tecnologías de la Información brindará a solicitud herramientas que permitan el cifrado para proteger la confidencialidad, integridad y disponibilidad de la información clasificada y reservada, en sistemas de información, mecanismos de transferencia de información internas o externas.

La ADR a través de Oficina de Tecnologías de la Información brindará tecnología SSL estandarizada que permite cifrar el tráfico de datos entre un navegador web y un sitio web (o entre dos servidores web), protegiendo así la conexión. Con el fin de impedir que un hacker pueda ver o interceptar la información que se transmite de un punto a otro y que puede incluir datos personales o financieros.

Las aplicaciones críticas del ADR que este expuestas deben contar con certificado de seguridad HTTPS.

La administración de llaves criptográficas y certificados digitales para firma digital está a cargo de la Oficina de Tecnologías de la Información. Sin embargo, cada uno de los funcionarios o contratistas a quienes les fueron asignados los Token son responsables de la custodia del mismo para evitar su pérdida o robo en el desempeño de sus funciones y obligaciones.

La administración de llaves criptográficas y certificados digitales, tokens para acceso a sistemas de información de Entes de Control y firmas digitales (SIIF), estarán a cargo de la Gestión Financiera de la entidad y cada uno de los funcionarios o contratistas a quienes les fueron asignados los Token son responsables de la custodia del mismo para evitar su pérdida o robo en el desempeño de sus funciones y obligaciones.

3.1.8. Política de Seguridad de las Operaciones.

La Oficina de Tecnologías de la Información de la ADR será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación. Así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información, y para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de prueba y producción sean controlados y debidamente autorizados.

De igual manera, proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo al crecimiento de la Entidad, e implementará mecanismos de contingencias y continuidad del negocio con el fin de propender por la disponibilidad de los servicios de Tecnologías de la información en el marco de la operación de la ADR.

La Oficina de Tecnologías de la Información Gestiona los cambios sobre de los servicios y componentes tecnológicos que se encuentran en ambiente productivo y hacen parte de los elementos administrados por la OTI, garantizando su correcta aplicación y seguimiento según los acuerdos y prioridades que eviten interrupciones en la prestación de los servicios en conformidad con el procedimiento Gestión de Cambios Tecnológicos .

La Oficina de Tecnologías de la Información gestiona la capacidad de su plataforma tecnológica (hardware y software) de acuerdo con las indicaciones de documento para gestionar la capacidad de infraestructura tecnológica.

La Oficina de Tecnologías de la Información proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes y Definir un documento para realizar la separación independiente de los ambientes de desarrollo, prueba y producción con el fin de evitar problemas operacionales que puedan generar incidentes críticos y mitigar los errores en los sistemas de información.

La Oficina de Tecnologías de la Información proveer las medidas de detección, corrección y prevención de amenazas causadas por códigos maliciosos que se llegaran a amenazar la integridad, confidencialidad y disponibilidad de la información de la Agencia de Desarrollo Rural – ADR en conformidad con el documento Gestión De Código Malicioso.

3.1.9. Política de Seguridad de las Comunicaciones.

La Oficina de Tecnologías de la Información establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios que dependen de ellas; así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información de la Agencia de Desarrollo Rural -ADR.

La Oficina de Planeación establecerá mecanismos para que el intercambio de información con las partes interesadas internas o externas se realice asegurando su integridad. En el evento que los acuerdos de intercambio de información requieran del desarrollo de webservice o cualquier otro medio tecnológico, el intercambio deberá realizarse con los controles criptográficos.

Como parte de sus términos y condiciones iniciales del contrato de prestación de servicio, todos los servidores públicos o contratistas, sin importar su nivel jerárquico, firmarán cláusula de derechos de autor y confidencialidad con una cláusula de tratamiento de datos que será elaborado por la Vicepresidencia de Gestión Contractual de la Entidad, y la autorización de tratamiento de datos personales. Dichos documentos originales serán conservados y archivados en forma segura en la historia laboral de los servidores públicos y en la carpeta de los procesos contractuales para el caso de los contratistas.

La OTI debe definir e implementar los mecanismos de control que considere apropiados para proteger la confidencialidad, integridad y disponibilidad de las redes, los servicios en red y la información por allí transmitida.

La OTI define e implementa los mecanismos de separación de las redes de la ADR con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de equipos de escritorio, dominio de servidores), por áreas o dependencias (por ejemplo, Talento Humano, Gestión Financiera, OTI) o alguna combinación. (por ejemplo, un dominio de servidores que se conecta a múltiples dependencias).

La OTI debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación de información en alguna de las dos redes, cuando la capacidad de puntos de red lo permita.

El acceso remoto a los servicios internos de la entidad se controla mediante conexión VPN
La OTI debe mantener actualizado los equipos activos de red a la última versión permitida por el fabricante.

La conexión de terceros contra la ADR se debe realizar por VPN site to site o SSL, según el criterio del personal de la OTI.
Los funcionarios y contratistas deben seguir las indicaciones del Gestión Documental para la transferencia de información siguiendo los parámetros de la clasificación de la información de acuerdo con las tablas de retención documental de la ADR

3.1.10. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas.

La ADR asegura que el software adquirido y desarrollado tanto al interior de la agencia, como por terceras partes, cumpla con los requisitos de seguridad y calidad establecidos.

La Oficina de Tecnologías de la Información velará porque el desarrollo interno o externo de los sistemas de información de la Agencia de Desarrollo Rural -ADR cumpla con los requerimientos de seguridad adecuados para la protección de la información.

La Oficina de Tecnologías de la Información será la única dependencia de la Agencia con la capacidad de adquirir, desarrollar o avalar la adquisición y recepción de software de cualquier tipo, conforme a los requerimientos de las diferentes dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la ADR. En consecuencia, cualquier software que opere en la ADR y no haya sido entregado a la Oficina de Tecnologías de la Información, no serán responsabilidad de esta, no se le brindará soporte y no se le salvaguardará la información.

En el cumplimiento de esta política tener en cuenta:

La adquisición, desarrollo y mantenimiento de sistemas de información incluye buenas prácticas de seguridad digital durante todo el ciclo de vida, los requisitos relacionados con la seguridad digital son incorporados a los sistemas de información tanto nuevos como ya existentes. Los servicios asociados a transacciones electrónicas se protegen para evitar transmisión incompleta, alteración o divulgación no autorizada o enrutamiento errado.

La ADR asegura que el software adquirido y desarrollado tanto al interior de la entidad, como por terceras partes, cumpla con los requisitos de seguridad y calidad establecidos.

Las áreas propietarias de sistemas de información, la Oficina de tecnologías de la información en adelante (OTI) y la oficina de contractual deben incluir requisitos de seguridad en la definición de requerimientos y posteriormente se aseguran de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido y se debe tener para los sistemas de información o desarrollos de software un área propietaria dentro de la entidad formalmente asignada.

La ADR debe establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad digital.

La OTI lidera la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

La ADR vela porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad definidos basado en buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad .

La ADR se debe asegurar que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido y que sistema de información que capture información de los usuarios incorpora mecanismo de autorización de tratamiento de datos personales.

La ADR debe realizar las pruebas para asegurar que se cumplen con los requerimientos de seguridad establecidos en ambientes de pruebas y producción, utilizando metodologías establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a

producción, considerando nuevos sistemas, nuevas funcionalidades, mantenimientos en aplicaciones construidas internamente, construidas por proveedores, aprovisionadas en la nube o híbrido de las anteriores.

La ADR debe aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos, cambios, o nuevas funcionalidades.

La OTI debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de Gestión de Cambios Tecnológicos.

La OTI debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del ADR.

La OTI debe asegurar que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual incluidos en el contrato.

La OTI debe generar, adoptar o recomendar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

La OTI debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches o actualizaciones generadas para las versiones en uso y que estén ejecutando la última versión estable publicada por el fabricante.

La OTI debe asegurar que las aplicaciones y desarrollos se diseñen y construyan en versiones vigentes y estables emitidas por el fabricante respecto a las herramientas, componentes, lenguajes de programación.

La OTI debe almacenar las copias de seguridad del código fuente de manera segura previendo riesgos asociados a pérdida de disponibilidad, confidencialidad o integridad.

La OTI debe aplicar el procedimiento de Gestión de Cambios Tecnológicos a los cambios para el software aplicativo y los sistemas de información de la entidad.

Los desarrolladores deben Considerar y aplicar las buenas prácticas y lineamientos de desarrollo seguro durante todo el ciclo de vida de los mismos sistemas de información.
Los desarrolladores deben proporcionar un nivel adecuado y oportuno de soporte para solucionar los problemas que se presenten en el software aplicativo del ADR.

Los desarrolladores deben Construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

Los desarrolladores deben Asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla.

ADR protege los datos de prueba que se entregan a los desarrolladores, asegurando que no revelan información calificada como clasificada y reservada de los ambientes de producción.

La OTI debe certificar que la información a ser entregada a los desarrolladores (tanto internos como externos) para sus pruebas es enmascarada o que los datos sensibles son eliminados con el fin de no revelar información confidencial de los ambientes de producción y, por ende, dar cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

Las áreas interesadas en el desarrollo de sistemas de información deben exigir el suministro de evidencia que se realizaron pruebas de seguridad al software desarrollado interno y externo alinedas a la Guía de Metodología De Pruebas De Efectividad ADR

3.1.11. Política de seguridad para relación con proveedores.

La ADR a través de la Vicepresidencia de Gestión Contractual, establecerá mecanismos de control en la relación con sus proveedores, teniendo en cuenta que se debe asegurar la información a la que genere, custodie, procese o se tengan acceso, supervisando el cumplimiento de lo establecido de las políticas de seguridad y privacidad de la información. Los supervisores de los contratos o convenios tendrán la responsabilidad de divulgar y sensibilizar las políticas y procedimientos de seguridad y privacidad de la información.

3.1.12. Política de Gestión de Incidentes de Seguridad de la Información.

La Agencia de Desarrollo Rural -ADR promoverá entre los servidores públicos y contratistas el reporte y seguimiento de incidentes relacionados con la seguridad de la información y sus medios. Así mismo, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, de acuerdo con su criticidad.

La Oficina de tecnologías de la información conforme al rol serán los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, se debe tener en cuenta los canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía.

La Oficina de tecnologías de la información realiza el seguimiento a los incidentes de seguridad de la información de acuerdo con las directrices del procedimiento Gestión de Incidentes de Seguridad de la Información

3.1.13. Política de Cumplimiento.

La Agencia de Desarrollo Rural -ADR velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad y privacidad de la información, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional, para lo cual dispondrá una Matriz de Requisitos Legales para su control y seguimiento.

4. APOYO O SOPORTE

Las políticas de Seguridad y Privacidad de la Información se aplican para todos los procesos del ADR, a todos los funcionarios, contratista y demás colaboradores que debido al cumplimiento de sus funciones utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación.

Para esto, el modelo de seguridad y privacidad indica pautas específicas para guiar a la ADR a robustecer sus plataformas y mitigar amenazas que pueden llegar a traer consigo las tecnologías implementadas, sin embargo, un programa robusto de seguridad y privacidad de la información no se basa únicamente en el aseguramiento de plataformas y procesos, sino que también debe involucrar los factores humanos, que en muchos casos, son la principal causa de los incidentes de seguridad dentro de un sistema determinado, esto debido a que no conocen
sobre seguridad de la información y su rol dentro de la ADR. Es necesario sensibilizar o capacitar sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información

5. TOMA DE CONCIENCIA

Con el propósito de realizar la implementación de un Modelo de Seguridad y Privacidad de la Información, basados en la norma ISO27001 o en el MSPI dado como guía metodología del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia en adelante (MinTIC), se debe desarrollar un proceso de capacitación y sensibilización, con el fin motivar la participación, conseguir el compromiso de los funcionarios, contratistas y terceros de la ADR y tiene como objetivo final el hacer cumplir las medidas de seguridad de la información en controles (procedimentales, de comportamiento y tecnológicas) con que cuenta la ADR para promover un adecuado comportamiento en el manejo de la información y así disminuir la materialización de las situaciones de riesgo.

Es de aclarar que los ciberataques pueden generar una serie de efectos colaterales que incluyen reducir la productividad, causar daños reputacionales e incluso pueden llegar a generar demandas y otros retos de carácter legal por fuga de información privilegiada y datos sensibles. Conocer los riesgos asociados a la ciberdelincuencia e identificar las buenas prácticas para enfrentarlos, fortalece el avance de la cultura en la ADR de la seguridad de la información, además de elevar la confianza digital, para que el ecosistema pueda seguir creciendo sin contratiempos. Este propósito claramente demanda el esfuerzo integrado por parte de la Oficina de Tecnologías de la Información con el apoyo de la Dirección de Talento Humano y la Oficina de Comunicaciones para promover y participar activamente en campañas de sensibilización para dar cumplimiento a los procesos, políticas y reglas, de tal manera que tanto en cada puesto de trabajo como en toda la entidad se cumplan sus directrices y lineamientos para el buen uso de la tecnología, la seguridad y privacidad de la información. En este caso se elabora un plan anual de sensibilización de seguridad digital en el cual participan los actores anteriormente mencionados

5.1. COMUNICACIÓN

Con el plan de Sensibilización se pretende como alcance permitir llegar a todos los funcionarios, contratistas y colaboradores de la ADR que se verán beneficiados con el plan de sensibilización, al contextualizar la necesidad de la seguridad de la información de una manera estructurada, que permitan adquirir un conocimiento adecuado del buen uso de las tecnologías en la seguridad de la información y su aplicación con las políticas que se tiene implementadas la ADR.

Así mismo propiciar la transferencia del conocimiento en los funcionarios, contratistas y terceros de la ADR en la sensibilización de las tecnologías de la información y en el sistema de seguridad y privacidad de la información, Propiciar el fortalecer las capacidades en la entidad para prevenir y dar respuesta a eventos de seguridad y de telecomunicaciones, a través de los espacios y herramientas de capacitación en la ADR, por consiguiente dar a conocer que son y como reportar los incidentes de seguridad y la ciberseguridad.

6. EVALUACIÓN DEL DESEMPEÑO

En la definición del Modelo de Seguridad y Privacidad de la Información, la fase de evaluación del desempeño hace parte de la etapa de Verificar, donde se establecen los aspectos a ser desarrollados por los responsables de la gestión de seguridad y privacidad de la información en todos los niveles, para así, evaluar y en donde sea aplicable, medir el desempeño del sistema contra la política, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados para su revisión y toma de decisiones.

6.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

Para realizar el seguimiento, medición, análisis y evaluación la ADR con la responsabilidad de la Oficina de tecnologías de la información realizara las siguientes actividades:

- Realizar anualmente la autoevaluación con el Instrumento de Evaluación MSPI entregado por MinTIC
- Elaboración, modificación y actualización del plan de seguridad y privacidad de a información ADR.
- Realizar seguimiento al cumplimiento de plan de seguridad y privacidad vigente
- Informe de gestión de incidentes de seguridad de la información.
- Medición de controles aplicados de la Norma ISO 27001:2013
- Levantamiento y actualización de activos de seguridad Digital y gestión de riesgo ADR
- Medición de los indicadores de gestión del MSPI anual.
- Acompañamiento en realización de auditorías.
- Elaboración y ejecución de Acciones o Planes de Mejora

7. REVISIÓN de MSPI

En conformidad con las funciones del Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural de "Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información". Se presentarán para aprobación de comité la gestión del MSPI anualmente.

Referencias

Departamento Nacional de Planeación (DNP). (03 de mayo de 2019). Bases Del Plan Nacional de Desarrollo 2018-2022. Obtenido de https://colaboracion.dnp.gov.co/CDT/Prensa/BasesPND2018-2022n.pdf

Departamento Nacional de Planeación. (11 de Abril de 2016). CONPES 3854 Política Nacional de Seguridad Digital. Recuperado el 12 de Septiembre de 2019, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. (1 de Julio de 2020). CONPES 3995 POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL. Recuperado el 1 de 12 de 2017, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (29 de Julio de 2016). Modelo de Seguridad y Privacidad. Recuperado el 3 de 10 de 2017, de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Junio de 2018). Manual de Gobierno Digital. Recuperado el 2019, de https://www.gobiernodigital.gov.co/623/articles-81473_recurso_1.pdf

NTC-ISO/IEC 27001:2013. (11 de Diciembre de 2013). Norma Técnica Colombiana NTC-ISO/IEC 27001:2013. Recuperado el 1 de Septiembre de 2018, de 2013-12-11: https://www.academia.edu/40913480/NORMA_T%C3%89CNICA_NTC_ISO_IEC_COLOMBIANA_27001_TECNOLOG%C3%8DA_DE_LA_INFORMACI%C3%93N_T%C3%89CNICAS_DE_SEGURIDAD_SISTEMAS_DE_GESTI%C3%93N_DE_LA_SEGURIDAD_DE_LA_INFORMACI%C3%93N_REQUISITOS

rural, A. d. (06 de 12 de 2017). www.adr.gov.co. Obtenido de https://www.adr.gov.co/normograma/DocumentosJuridica/Resoluci%C3%B3n%201602%20de%202017.pdf

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN

ELABORÓ		REVISÓ		APROBÓ	
Nombre:	Catherine Suarez	**Nombre:**	Genny Paola Ambrosio Villegas	**Nombre:**	Victor Manuel Mondragon Maca
Cargo:		**Cargo:**	2.4. Oficina de Tecnologías de la Información	**Cargo:**	2.4. Oficina de Tecnologías de la Información
Fecha:	17/Dic/2020	**Fecha:**	18/Dic/2020	**Fecha:**	21/Dic/2020