MANUAL OPERATIVO POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Agencia de Desarrollo Rural

Bogotá D.C., Diciembre 2024

TABLA DE CONTENIDO

INTRODUCCIÓN

La Agencia de Desarrollo Rural, en adelante ADR, reconoce que la información es uno de los activos más importantes para su funcionamiento y desarrollo de la misionalidad, asi mismo, es consciente de las amenazas que enfrenta la información y las consecuencias a las que se expone cuando no se cuenta con los controles lógicos y físicos que permiten responder a la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información, con el fin evitar la vulneración de la información.

Teniendo en cuenta lo anterior, el presente Manual tiene como finalidad establecer las políticas orientadas a la seguridad y privacidad de la información con el fin de ser implementadas y aplicadas por los funcionarios, contratistas, practicantes y terceros que tengan vínculos laborales o contractuales con la ADR, con el fin de reducir la posibilidad de ocurrencia de diversos incidentes de seguridad.

1 OBJETIVO

Establecer las políticas para la administración de la gestión de la seguridad y privacidad de la información, con el fin de propender por la protección de la confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad, no repudio de los activos de la ADR.

2 ALCANCE

Este documento aplica a todos los procesos de la Agencia de Desarrollo Rural-ADR y es de obligatorio cumplimiento para los funcionarios, contratistas, practicantes y terceros que tengan vínculos laborales o contractuales con la ADR.

3. TERMINOS Y DEFINICIONES

- **Activo de Información:** se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
- **Clasificación y etiquetado de la Información**: es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación de la información (pública, clasificada, o reservada) para recibir el nivel de protección adecuado.
- **Centro de cableado:** es el lugar donde se ubican los recursos de comunicación de tecnologías de información, como (Switch, patch, panel, UPS, Reuter, Cableado de voz y de datos).
- **BYOD:** Del inglés Bring Your Own Device (Trae Tu Propio Dispositivo). Son los lineamientos mediante los cuales la Agencia de Desarrollo Rural permite el acceso a su información y plataforma tecnológica a través de los dispositivos personales de los colaboradores o terceros para ejecutar sus funciones u obligaciones.
- **Datacenter:** Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.
- **Dispositivos Personales:** Se entiende como dispositivo personal cualquier artefacto que tenga la capacidad de almacenar, transferir y/o procesar cualquier tipo de información. Entre estos dispositivos se incluye los equipos computo (portátiles o de escritorio), teléfonos inteligentes, tabletas, entre otros.
- **Extensiones de archivos:** La extensión de un archivo es la parte de su nombre que indica de qué tipo es, si es de música, ejecutable, video, imagen, etc.l nombre completo de cualquier archivo consta siempre de dos partes separadas por un punto (por ejemplo "Windows.exe"), donde Windows es el nombre del archivo y la palabra seguida del punto exe es el tipo de extensión en este caso ejecutable.
- **E-books:** libro electrónico, libro digital o ciberlibro.

- **File Server:** Es un servidor de archivos o un equipo responsable del almacenamiento y administración central de archivos de datos para que otros equipos de la misma red puedan acceder a los mismos, lo anterior con base en la configuración de sus políticas de acceso.
- **Listas negras:** Lista que se excluye del trato o de una asociación por considerarlas indeseables.
- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.
- **Información Pública**: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, 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...
- **Información Pública Reservada**: Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos…
- **Masivo:** Es aquello que se aplica en gran cantidad, por ejemplo, envió de correos electrónicos con propagandas.
- **Mensajes publicitarios corporativos:** Mensajes con contenido informativo la Agencia de Desarrollo Rural dirigido a personal externo.
- **Paper:** Artículo científico, trabajo de investigación o comunicación científica publicado en alguna revista especializada.
- **Páginas de Hacking:** Páginas donde se encuentra herramientas e información para vulnerar sistemas de información.
- **Quemador de CD:** Herramientas utilizadas para copia o convertir información a un dispositivo como CD, DVD entre otros.
-

- **Streaming:** también llamado retransmisión o transmisión por secuencias consiste en la distribución o descarga de datos desde un proveedor o servidor en internet mientras el usuario hace uso de los datos en cuanto estos son descargados. Ejemplo escuchar música directamente desde una página de internet, reproducción de videos.
- **Recursos TIC:** Elemento o servicio físico o digital directamente relacionado con tecnologías de la información y las comunicaciones, pueden ser equipos de cómputo, cuentas de correo, servidores, servicios en la nube, cuentas corporativas entre otros.
- **Red Corporativa:** Es una red que permite conectar todas las localizaciones y dispositivos de la entidad de forma privada, segura y fiable. Permite a la entidad cursar todas sus comunicaciones, ya sean datos, voz, vídeo, imágenes, etc.…, de un modo rápido, seguro y totalmente gestionado dando calidad de servicio. De esta forma se asegura el correcto tratamiento a los distintos tipos de tráfico
- **Red pública o de visitantes:** Es una red abierta independiente a la red corporativa la Agencia de Desarrollo Rural, es decir no tiene acceso a información procesada por los diferentes dispositivos la Agencia de Desarrollo Rural para prevenir posibles interceptaciones o uso malintencionado. Su objetivo es brindar conectividad hacia internet a los visitantes, dispositivos que no son la Agencia de Desarrollo Rural y ciudadanía en general.
- **Spam:** Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.
- **Streaming:** Servicios de transmisión de contenidos de audio o video en tiempo real o en diferido.
- **Tablas de Retención Documental (TRD):** constituyen un instrumento archivístico que permite la clasificación documental de la entidad.
- **URL:** También conocida como dirección web, es una secuencia de caracteres que se utiliza para nombrar y localizar recursos, documentos e imágenes en Internet. URL significa "Uniform Resource Locador", o bien, "Localizador Uniforme de Recursos", ejemplo de URL es www.google.com.

- **Usuarios Genéricos:** Usuarios que vienen de forma predeterminada o por defecto configurados en un software como por ejemplo root, superuser, admin, etc.…
- **VPN:** Del inglés Virtual Private Network (Red Privada Virtual) supone una tecnología de red que brinda la posibilidad de conectarse a una red pública generando una extensión a nivel de área local.
- **Web Proxy:** Página o servidor intermediario que se utiliza como túnel, permitiendo saltar reglas o políticas de navegación.

4. MARCO DE REFERENCIA

El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión adecuada del ciclo de vida de la seguridad de la información. La OTI realizara su mayor esfuerzo incorporando la seguridad de la información en los procesos, sistemas de información, infraestructura y, en general, en los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

5. REFERENCIAS NORMATIVAS

- Decreto 767 de 2022 - Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 500 de marzo 10 de 2021 Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC) Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- Resolución 529 de 2024 - Por medio de la cual se adopta el Sistema Integrado de Gestión, se actualiza el Comité de Gestión y Desempeño de la ADR y se dictan otras disposiciones”

6. ESTRUCTURA ORGANIZACIONAL DEL SUBSISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se define la estructura del equipo del Subsistema de Seguridad y Privacidad de la Información el cual hace parte de la Oficina de Tecnologías de la Información

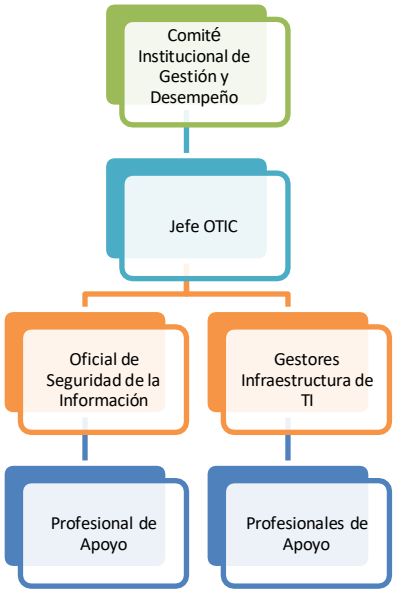

Imagen: Estructura organizacional del subsistema de seguridad y privacidad de la información

Fuente: elaboración propia

7. DESARROLLO DE LA TEMÁTICA

7.1. Política del Subsistema de Seguridad y Privacidad de la Información

La Agencia de Desarrollo Rural está comprometida en gestionar y promover el acceso a productos relacionados con la reforma agraria y el desarrollo rural integral, con un enfoque territorial diferencial e inclusivo. Nuestro objetivo es que los actores de la agricultura consoliden su modo de vida y producción sostenible.

Logramos esto a través del Sistema Integrado, el cual articula la planeación y gestión institucional. Cumplimos con la normativa vigente, aplicando principios preventivos basados en la administración integral de riesgos, gestión de documentos, datos e información, y preservando la integridad, disponibilidad, confidencialidad y autenticidad. Además, garantizamos la conservación de conocimientos clave en un entorno laboral responsable con la seguridad, salud y bienestar de las personas.

Mitigamos los impactos ambientales y contribuimos a la protección, ciudadano y conservación del medio ambiente para un desarrollo sostenible. Todo esto nos permite ser una entidad honesta y transparente, comprometida con el mejoramiento continuo de la gestión institucional y la satisfacción de nuestros grupos de valor en los diferentes frentes de servicio.

7.2. Objetivos del Subsistema de Seguridad y Privacidad de la Información

La política de seguridad y privacidad de la información se medirá a través de los siguientes objetivos:

- Velar y propender por el manejo seguro y clasificado de la información, con el compromiso de proteger estos activos frente a amenazas internas y externas, que puedan afectar la privacidad, confidencialidad, integridad y disponibilidad.
- Gestionar de manera oportuna y pertinente los eventos e incidentes de seguridad de la información que afecten o puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información reduciendo su impacto y propagación.
- Fortalecer la cultura, el conocimiento y las habilidades de los colaboradores en temas de seguridad y privacidad de la información.

7.3. Alcance del Subsistema de Seguridad y Privacidad de la Información

La política de seguridad y privacidad de la información las políticas definidas en este documento y las que se definan en el marco de la seguridad y privacidad de la información, aplican donde la ADR tenga presencia o desarrolle actividades de recolección, procesamiento,

almacenamiento, intercambio y consulta de información, asi mismo, aplica a todos los procesos descritos en el mapa de procesos de la ADR, funcionarios, contratistas, practicantes y terceros que tengan vínculos laborales o contractuales con la ADR.

8. POLITICAS DEL SUBSISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La declaración de aplicabilidad se encuentra documentada en el Anexo 1 “Declaración de Aplicabilidad”, donde se menciona como la entidad da cumplimiento a cada uno de los controles por la norma ISO 27001:2022; a continuación, se detallan las políticas asociadas a estos controles:

8.1. Políticas de Seguridad y Privacidad de la Información

a) Las políticas de seguridad de la información están descritas en este documento y en los documentos que hacen parte del Subsistema de Gestión de Seguridad y Privacidad de la Información ubicados en el aplicativo dispuesto por la entidad.
b) Las políticas son comunicadas a los colaboradores a través de los canales de comunicación disponibles por la entidad.
c) Las políticas se actualizan en el momento que se requiera y son aprobadas a través del Comité Institucional de Gestión y desempeño.

8.2. Roles y Responsabilidades en Seguridad de la información

Jefe OTI:

- Realizar la aprobación respecto a los cambios de infraestructura propuestos.
- Informar a la alta dirección sobre el avance, necesidades o aspectos que puedan ser relevantes del Subsistema de Gestión de Seguridad de la Información, con apoyo del Oficial de Seguridad de la Información.
- Socializar los incidentes de seguridad de la información de alto impacto a la alta dirección.
- Definir y asignar roles de seguridad de la información.

- Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.

Oficial Seguridad de la Información:

- Formular, documentar y gestionar el Plan Estratégico de Seguridad de la Información (PESI) y proponer planes de trabajo que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad.
- Identificar oportunidades para mejorar las políticas y los lineamientos de seguridad de la información en función de las necesidades de la entidad y de los riesgos identificados.
- Asesorar a los procesos en las actividades de identificación de activos y riesgos de seguridad de la información.
- Consolidar y entregar la información necesaria para la revisión por la alta dirección.
- Sensibilizar a los colaboradores en el cumplimiento de las Políticas de seguridad y privacidad de la información.
- Sugerir herramientas tecnológicas que faciliten y optimicen la protección de los activos de la entidad.
- Asesorar a la alta dirección en aspectos de seguridad de la información.

Gestores Técnicos:

- Implementar controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
- Desarrollar los procedimientos e instructivos necesarios para la correcta operación y administración de la seguridad informática de la entidad
- Evaluar y seleccionar herramientas tecnológicas que faciliten y aumenten la protección de los activos de la entidad.
- Gestionar los componentes de la infraestructura de TI desde rol asignado por el jefe de la OTI.

8.3. Segregación de Deberes:

a) La información deberá estar bajo la responsabilidad del Líder de Proceso para evitar conflicto y reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de información de la ADR.

b) El supervisor del contrato deberá hacer seguimiento al cumplimiento de las obligaciones generales de todos los contratos en materia de seguridad de la información, sin importar su naturaleza.

c) Una vez formalizado el proceso de vinculación, el supervisor de contrato o jefe inmediato solicitará la creación de la cuenta de usuario de acuerdo lo establecido en el procedimiento PR-GTI-004 Control de Acceso Lógico.

d) El supervisor de contrato o jefe inmediato, deberán informar a la Mesa de Ayuda las novedades del **colaborador** (ejemplo: terminación contrato, sesión de contrato, cambio de área, retiro de la entidad, entre otras). de acuerdo lo establecido en el procedimiento PR-GTI-004 Acceso Lógico.

8.4. Responsabilidades de la Dirección:

La alta dirección, con el fin de asegurar el liderazgo y apoyo en la implementación y mantenimiento al Subsistema de Seguridad y Privacidad de la Información define las responsabilidades a través de la Resolución *529 de 2024 "por medio de la cual se adopta el Sistema Integrado de Gestión, se actualiza el comité de Gestión y Desempeño de la ADR y se dictan otras disposiciones"* o la que la modifique o derogue.

8.5. Contacto con Autoridades y Grupos de Interés Especial

a) El equipo de Seguridad y Privacidad de la Información de la ADR tendrá contacto con las autoridades nacionales en materia de seguridad y privacidad de la información.

b) El equipo de Seguridad y Privacidad de la Información de la ADR tendrá contactos con los grupos de interés especial (Policía Nacional, INTERPOL, Bomberos, Defensa Civil, Grupos de atención de desastres, etc.), en el caso de que se presente un incidente de seguridad de la información, que requiera de asesoría externa.

8.6. Inteligencia de Amenazas:

La OTI analizara información sobre las amenazas existentes o emergentes de seguridad de la información a las que se encuentra expuesta la entidad y tomara las acciones respectivas para mitigarlas.

8.1.6. Seguridad de la Información en la Gestión de Proyectos:

La OTI aplicara la política “Relación con Proveedores” (descrita en este documento), para los proyectos que desarrolle en cumplimiento de sus funciones

8.7. Inventario de Información y Otros Activos Asociados

a) La gestión de activos de información se realiza de acuerdo con lo establecido en el documento MA-GTI-003 Manual de Gestión de Activos de Seguridad de la Información.
b) Los líderes de los procesos son los propietarios de los activos de información y deberán mantener un inventario de sus activos de información actualizado.
c) Los lideres de los procesos establecen y monitorean los controles definidos durante todo el ciclo de vida del activo de información, teniendo en cuenta la criticidad asignada, e informar al equipo de Seguridad y Privacidad de la Información de la OTI cualquier situación que ponga en riesgo la confidencialidad, integridad, disponibilidad y/o privacidad del activo de información.
d) Los lideres de los procesos definen, revisan y monitorean periódicamente los usuarios, permisos, restricciones, clasificaciones y perfiles de acceso a los activos de información, teniendo en cuenta las políticas de control de acceso aplicables.

8.8. Uso Aceptable de la Información y Otros Activos Asociados

La OTI establece los lineamientos para el uso aceptable de los activos que son propiedad de la entidad como la información, los sistemas, aplicaciones, servicios y los equipos (Desktops, laptops, impresoras, redes, internet, dispositivos móviles, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros), son activos de información que la entidad proporciona a los funcionarios y terceros autorizados, para cumplir con actividades específicas de la ADR , por lo tanto deben asegurar el buen uso de estos.

8.9. Uso de Internet

El Internet es un recurso que la ADR provee a sus colaboradores para apoyar el desarrollo de sus funciones u obligaciones, por tal motivo, se definen las medidas para hacer un buen uso y aprovechamiento de este recurso:

a) La Oficina de Tecnologías de la Información implementará políticas de navegación basadas en categorías y niveles de usuario, con el objetivo de proteger la entidad de riesgos como infecciones por programa maligno, fuga de información o navegación de contenido inapropiado.

NOTA: La alta dirección definirá las categorías mínimas autorizadas para toda la ADR. Los jefes de área o quien haga sus veces podrán solicitar la adición de categorías o URL que estén relacionadas con la función del proceso y no pongan en riesgo la entidad.

b) Está restringido el acceso a páginas relacionadas con pornografía, drogas, terrorismo, segregación racial, hacking y/o cualquier otra página que vaya en contra de la ética, la moral, las leyes vigentes o las políticas aquí establecidas.
c) La Oficina de Tecnologías de la Información al ser quien administra y gestiona los canales de internet, podrá verificar y monitorear la navegación en general de todos los funcionarios y contratistas, con el fin de velar por el adecuado uso de este recurso y el cumplimiento de las políticas de seguridad.
d) La ADR cuenta con servicios de almacenamiento en la nube para intercambio de información, por lo tanto, el acceso a portales de intercambio y almacenamiento de archivos gratuitos o abiertos en la nube como DropBOX, BOX, Mega, WeTransfer, entre otros estarán restringidos.
e) Se permitirán servicios de streaming de audio a través de sitios web que no pongan en riesgos las redes e infraestructura de la ADR.
f) Se permitirán servicios de streaming de video a través de sitios web que no pongan en riesgos las redes e infraestructura de la ADR, sin embargo, los portales permitidos

tendrán limitaciones en consumo de red, para optimizar el uso de los recursos disponibles.

g) Está prohibido el acceso a webproxies y/o cualquier página por la cual se intente violar las políticas definidas por la ADR.

h) Está prohibido el intercambio no autorizado de información de propiedad de la ADR, de sus clientes y/o de sus colaboradores, con terceros.

i) No está permitida la descarga y el uso de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.

j) No está permitido el acceso a servicios de mensajería, redes sociales o correo diferentes a los establecidos por la ADR como la suite Gmail, Outlook, Yahoo!, Messenger, Skype, Facebook, WhatsApp y páginas de chat no está permitida.

NOTA: Las áreas que, en cumplimiento de sus funciones, requieran el uso de redes sociales u otras páginas o categorías restringidas, la alta dirección o comité institucional de gestión y desempeño aprobara las excepciones para dichos casos, siempre y cuando se establezcan tratamientos o medidas compensatorias en cuanto a temas relacionados con seguridad de la información.

k) No está permitido el acceso, ni el uso de servicios interactivos, páginas de mensajería instantánea o que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias de la ADR.

l) La Oficina de Tecnologías de la Información, realiza monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, se podría inspeccionar, registrar e informar las actividades realizadas durante la navegación.

m) Es responsabilidad de los usuarios dar el uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten

contra terceros, legislación vigente y las políticas de seguridad y privacidad de la información, entre otros.

n) Los funcionarios, terceros y/o proveedores, al igual que los funcionarios o contratistas de éstos, no pueden asumir en nombre de la ADR, posiciones personales en encuestas de opinión, foros u otros medios similares.

o) El uso de internet no considerado dentro de las restricciones antes mencionadas es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad, ni la protección de la información de la ADR.

8.10. Uso Correo Electrónico

La Oficina de Tecnologías de la Información que presta servicios a la ADR, asigna una cuenta de correo electrónico (con dominio **@adr.gov.co**) como herramienta de trabajo para cada uno de los servidores públicos y/o contratistas que lo requieran para el desempeño de sus funciones, obligaciones y en algunos casos a terceros con previa autorización; su uso se encuentra sujeto a las siguientes políticas:

a) El único servicio de correo autorizado para el manejo o transmisión de la información institucional es el proporcionado por la Oficina de Tecnologías de la Información de la ADR.

b) La cuenta de correo electrónico debe ser usada únicamente para el desempeño de las funciones u obligaciones asignadas por la ADR.

c) Los mensajes y la información contenida en los buzones de correo son de propiedad de la ADR. Cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones u obligaciones.

d) Todo mensaje tipo SPAM o malicioso deberá reportarse a la Oficina de Tecnologías de la Información a través de la herramienta de mesa de servicios establecida. Está expresamente prohibido el reenvío de mensajes sospechosos a otros buzones, ya que se entenderá como propagación intencional de virus.

e) Todo mensaje de índole personal debe ser reenviado a un correo externo del colaborador y eliminado del buzón institucional.

f) El tamaño de los buzones de correo, de los mensajes enviados y recibidos, está determinado por la Oficina de Tecnologías de la Información, teniendo en cuenta que no se ponga en riesgo la instalación por extralimitación en la capacidad de almacenamiento.

g) No está permitido el envío de información clasificada como “Información Reservada” o “Información Clasificada” de la ADR sin previa autorización de la alta dirección o líder de proceso.

h) Todo correo electrónico que deba ser transmitido hacia Internet, deberá tener al final el mensaje de confidencialidad definido por la ADR.

i) No está permitido usar las cuentas corporativas para registrarse en servicios de terceros en internet como páginas publicitarias, comercio electrónico entre otros.

j) No está permitido el envío de correos masivos de más de 30 destinatarios tanto internos como externos, salvo los emitidos por el despacho de la Presidencia, Vicepresidencias, secretaria general, Directores de la Unidades Técnicas Territoriales (UTT), la Oficina de Comunicaciones y la Oficina de Tecnologías de la Información, todos los mensajes masivos deben cumplir con las características definidas por la Oficina de Comunicaciones.

k) Está prohibido enviar o recibir cadenas de correo, mensajes con contenidos religioso, juegos, políticos, racistas, sexistas, pornográficos, publicitarios no corporativos o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

l) No está permitido el envío de archivos que contengan extensiones como wav, .exe, .com, .dll, .bat. o cualquier otro archivo ejecutable; en caso de ser necesario deberá ser autorizado por el Oficial de Seguridad de la Información o Jefe de la oficina de Tecnologías de la Información.

m) Está prohibido distribuir, copiar o reenviar información de la ADR a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.

8.11. Dispositivos Personales- Trae Tu Propio Equipo-BYOD

Establecer los lineamientos mediante los cuales la Agencia de Desarrollo Rural permite el acceso a su información y plataforma tecnológica a través de los dispositivos personales de los colaboradores o terceros que utilizan para ejecutar sus funciones u obligaciones. Para lo anterior, se debe cumplir con las siguientes políticas:

a) Los colaboradores o terceros, que utilicen sus dispositivos personales al interior de la ADR para ejecutar sus funciones u obligaciones se conectaran a la red de “Funcionarios” de la ADR.
b) Al conectar el dispositivo personal a la red de “Funcionarios” de la ADR, el colaborador o tercero propietario del dispositivo acepta los controles establecidos en este documento.
c) Se debe registrar el ingreso de los dispositivos personales a las instalaciones de la ADR en la bitácora de ingreso de equipos la cual se encuentra ubicada en la recepción.
d) En caso de robo o pérdida del dispositivo personal, se debe reportar inmediatamente el incidente a través de los canales establecidos en el procedimiento “*PR-GTI-007 Gestión de incidentes, eventos y debilidades de Seguridad de la Información”*.
e) Toda la información relacionada con la ejecución de las funciones u obligaciones contractuales del colaborador o tercero contenida en los dispositivos personales, debe estar almacenada en el repositorio “File Server” o el que la entidad establezca.
f) Es responsabilidad del colaborador o tercero, la protección de la información de la ADR que tenga bajo su manejo en el dispositivo personal.
g) El colaborador o tercero propietario del dispositivo personal, deberá tener en cuenta las buenas prácticas de seguridad de la información incluyendo: contar con contraseña o pin para el inicio de sesión en el equipo y cerrar la sesión en aplicaciones cada vez que finalice su sesión o que se deba ausentar de su área o puesto de trabajo.

h) Cuando el colaborador o tercero utilice el dispositivo personal en lugares públicos, debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas, así mismo, evitar la conexión a redes públicas (aeropuertos, centros comerciales, entre otros), las cuales no cuentan con ningún tipo de monitoreo o seguridad y representan un riesgo para la seguridad de la información.

i) Una vez se autorice la conexión de un dispositivo a la red de dominio ADR (VPN, office 365, entre otros), la entidad tendrá acceso para visualizar y monitorear los datos de la ADR.

j) Aquellos colaboradores o terceros que utilicen las herramientas de la ADR en sus dispositivos personales, es importante considerar que su uso, gestión y protección estará bajo la responsabilidad del colaborador, por lo que la ADR podrá implementar herramientas de monitoreo a las aplicaciones de la ADR instaladas en los dispositivos personales.

k) La OTI no dará soporte técnico a los dispositivos personales, en caso de ser necesario a través de la mesa de servicio dará soporte a las aplicaciones que el colaborador tenga acceso.

8.12. Devolución de Activos:

Gestión Administrativa establecerá los lineamientos para la devolución de activos asignados a los colaboradores, teniendo en cuenta:

a) Cuando un colaborador termina o cambia la relación contractual o laboral con la ADR, el colaborador debe entregar al jefe de área, supervisor o área designada los recursos tecnológicos y los activos de información que le fueron entregados en el momento de su vinculación o durante la relación contractual o laboral.

8.13. Clasificado y Etiquetado de la Información:

a) Los niveles de clasificación y etiquetado de la información establecidos en la ADR son “Información Pública”, “Información Pública Clasificada” e “Información Pública Reservada”, lo cual aplica para la información física como para la información digital.

b) El etiquetado de la información (Pública, Clasificada, Reservada) se realiza de acuerdo con la criticidad de la información que esta contenga y a lo establecido en las Tablas de Retención Documental-TRD.

c) Todos los colaboradores de la ADR son responsables de clasificar y etiquetar la información que producen en cumplimiento de las funciones y obligaciones asignadas.

d) Los documentos digitales deben tener en el encabezado el espacio para marcar la clasificación (Pública, Clasificada, Reservada) de la información según corresponda.

e) Gestión Documental, definirá los lineamientos para el etiquetado de la información física, con el fin, que cuenten con el etiquetado correspondiente según la información contenida.

f) No se debe publicar en las carteleras o espacios de la ADR, información que contengan:

- Datos personales privados, semiprivados o sensibles,
- Documentos sin etiquetado
- Documentos con etiquetado “Clasificada o Reservada”

g) No debe permanecer en las impresoras, impresiones que contenga información “Clasificada o Reservada” estas se deben retirar inmediatamente.

h) Antes de depositar un documento en el contenedor de basura que contenga información “Clasificada o Reservada” se debe eliminar en su totalidad.

i) Toda información que contenga datos personales deberá estar sujeta a las disposiciones legales contenidas en la Ley 1581 de 2012 y las demás que la complementen, modifiquen o sustituyan y la Política de Tratamiento de Datos Personales de la Agencia (publicada en el portal web de la entidad).

8.14. Transferencia de Información:

a) La OTI aplicara los lineamientos descritos en el PR-GTI-013 Procedimiento de Intercambio, interoperabilidad o suministro de información.

b) El área Administrativa o su delegada dictará directrices sobre retención, disposición y transferencia de la información física de la ADR, de acuerdo con la normativa legal vigente.

8.15. Control de Acceso Lógico – Gestión de Identidades

La Oficina de Tecnologías de la Información que presta servicios a la ADR, asigna usuarios y contraseñas a todos los funcionarios y contratistas según sus roles y responsabilidades en los diferentes servicios tecnológicos disponibles en la ADR, por lo tanto, el uso adecuado de estas credenciales se encuentra sujeto a las siguientes políticas:

a) La gestión de accesos a los sistemas de información, aplicaciones institucionales, bases de datos entre otros, se realiza de acuerdo con el MA-GTI-004 Manual de Control de Acceso Lógico y el PR-GTI-004 Procedimiento de Control de Acceso Lógico.
b) Las acciones ejecutadas por los usuarios en los sistemas de información quedarán registradas en los sistemas nuevos que estarán acondicionadas para conservar esta trazabilidad, lo anterior para efectos de auditoría por parte de la Oficina de Tecnologías de la Información.
c) La creación y modificación de usuarios en la infraestructura tecnológica son responsabilidad de la persona designada por la Oficina de Tecnologías de la Información y debe seguir los procedimientos correspondientes.
d) La Oficina de Tecnología de la Información realizará monitoreo al uso, gestión y autenticación de las cuentas de usuario asignadas.
e) Los mecanismos de autenticación deben establecer periodos de vigencia y/o renovación, los cuales deben cumplir con las políticas definidas.
f) Los mecanismos de autenticación permitirán la trazabilidad de los accesos concedidos a los usuarios y las actividades realizadas (Adiciones, eliminaciones, modificaciones etc.…) en cada uno de los recursos informáticos.

8.16. Información de autenticación (Contraseñas)

Los colaboradores de la ADR deben asegurar la protección de las credenciales (contraseñas) de acceso a los sistemas de información, herramientas y servicios, cumpliendo las siguientes directrices:

a) Todas las contraseñas deberán son de uso personal e intransferible, no se deberán compartir con ninguna persona dentro o fuera de la ADR por ningún medio, por lo que los colaborades son responsables de la custodia, no divulgación y uso de estas.
b) Ningún usuario podrá acceder a un sistema de información o servicio tecnológico que requiera credenciales utilizando la cuenta o contraseña de otro usuario.
c) Los colaboradores son responsables de las acciones ejecutadas con sus usuarios en los sistemas de información de la ADR.
d) No está permitido almacenar en los navegadores de internet u otros sistemas las credenciales de acceso para ser recordada automáticamente por estos.
e) No escribir las contraseñas en post-it físicos, agendas, o en notas rápidas del sistema operativo donde personas no autorizadas puedan identificarlas.
f) Utilizar diferentes contraseñas para acceso a los sistemas de información y servicios institucionales, para los casos donde no están integrados con el directorio activo.
g) Para definir la contraseña no utilizar palabras comunes, nombres de fácil deducción por terceros, asi mismo, no vincular las contraseñas con datos personales o familiares como fechas de cumpleaños, números de teléfono, números de documento, nombres de familiares o de mascotas, entre otros.
h) En caso de ser divulgada la contraseña por error, esta debe ser cambiada de inmediato y reportar el incidente por los canales establecidos en el documento PR-GTI-007 Gestión de incidentes, eventos y debilidades de Seguridad de la Información.
i) La longitud mínima de la contraseña será igual o superior a ocho caracteres y estará constituida por combinación de caracteres alfabéticos, numéricos, mayúsculas, minúsculas y caracteres especiales.
j) No se debe utilizar usuarios genéricos como (root, superuser etc.…), en caso de requerirse será bajo la autorización expresa del Jefe de la Oficina de Tecnologías de la Información.
k) La contraseña de acceso se debe cambiar máximo cada noventa (90) días, o cuando considere que ha perdido la confidencialidad y se pueda comprometer la información.

8.17. Gestión de Proveedores

Asegurar una adecuada gestión con los proveedores de infraestructura de TI con el propósito dar cumplimiento a las políticas, procedimientos y lineamientos de seguridad y privacidad de la información, teniendo en cuenta lo siguiente:

a) La OTI dará cumplimiento a los lineamientos establecidos por Gestión Contractual para la contratación de proveedores.
b) Gestión Contractual establecerá el medio idóneo para verificar con proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
c) Gestión Contractual establecerá en los contratos con proveedores la cláusula de "Compromiso de Confidencialidad", con el fin de asegurar la información de la ADR.
d) La OTI, establecerá el mecanismo y permisos cuando un proveedor requiera tener acceso a la información por medio de la infraestructura tecnológica de la ADR.
e) La OTI realizara seguimiento al acceso a la información por parte de los proveedores a los recursos de almacenamiento o procesamiento, de acuerdo con las políticas y procedimientos de seguridad y privacidad de la información de la ADR.

f) La OTI verificara mensualmente el cumplimiento de los Acuerdos de Nivel de Servicio establecidos con los proveedores de tecnología (cuando aplique).
g) La OTI establecerá y monitoreará las condiciones de conexión para los equipos de cómputo y dispositivos móviles de los proveedores en la red de datos o recursos tecnológicos de la ADR.

h) La OTI gestionara los cambios de infraestructura, aplicativos y servicios tecnológicos que son soportados por proveedores, de acuerdo con lo establecido en el documento PR-GTI-002 Gestión de Cambios de Seguridad de la Información.
i) La OTI gestionara los incidentes de infraestructura, aplicativos y servicios tecnológicos que son soportados por proveedores de acuerdo con lo establecido en el documento P-GTI-003 Gestión de incidentes, eventos y debilidades de Seguridad de la Información.

Los proveedores deben:

e) Informar de manera inmediata y efectiva al supervisor del contrato los incidentes de seguridad y privacidad de la información que pongan en riesgo la confidencialidad, integridad, disponibilidad o privacidad de los activos de información de la ADR.

f) Divulgar al personal asignado para la ejecución de las actividades, las políticas y procedimientos de seguridad y privacidad de la información de la ADR.

g) Informar oportunamente a la ADR cualquier cambio que afecte el suministro de los servicios como: controles implementados previamente, mejoras, nuevas aplicaciones, modificación o actualizaciones de las políticas o procedimientos, nuevas tecnologías, ubicación física, contratación externa o interna, entre otros.

h) Si la ejecución del servicio contratado requiere la utilización de programas o software, estos deben estar debidamente licenciados.

i) Realizar la devolución de activos físicos y/o lógicos, generados, modificados, durante la ejecución contractual.

j) Dar cumplimiento a los requisitos legales y reglamentarios para la protección de datos, derechos de propiedad intelectual, derechos de autor y los que apliquen a razón del cumplimiento contractual.

k) Utilizar y/o emplear la información que reciban o conozcan de la ADR, exclusivamente para la ejecución contractual.

l) Definir un plan de recuperación y contingencia ante eventos que puedan afectar el cumplimiento contractual.

m) Propagar en la cadena de suministro las buenas prácticas, políticas y documentación relacionada con la seguridad de la información.

Los responsables de los activos de información y/o supervisores de los contratos deben:

n) Clasificar la información que se entregue o que tenga acceso el proveedor e informar los niveles de protección requeridos para esta, así como el tiempo de uso, conservación y disposición final de la información.
o) Definir y hacer seguimiento a la información que tendrá acceso los proveedores.
p) Divulgar las políticas y procedimientos de seguridad y privacidad de la información de la ADR a los proveedores.
q) Supervisar el cumplimiento de los requisitos acordados con el proveedor.

8.18. Seguridad de la Información para el Uso de Servicios en la Nube

La OTI definirá y establecerá la seguridad de la información para el uso del servicio en la nube, teniendo en cuenta:

a) Definir criterios para seleccionar los servicios en la nube existentes en el mercado y el alcance del uso del servicio.
b) Definir el control de acceso basado en roles (RBAC) y responsabilidades relacionadas con el uso y la gestión del servicio en la nube.
c) Los administradores de las plataformas de servicios en la nube tendrán habilitados en sus usuarios, como mínimo el múltiple factor de autenticación y los demás controles que la OTI identifique que sean necesarios.
d) Brindar lineamientos para la gestión de incidentes de seguridad de la información con el servicio en la nube.
e) Realizar monitoreo, revisión y evaluación del uso de los servicios en la nube.

8.19. Gestión de Incidentes

La OTI gestionara los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento PR-GTI-007Gestión de incidentes, eventos y debilidades de Seguridad de la Información.

8.20. Preparación de las TIC para la Continuidad del Negocio

a) La OTI definirá un plan de recuperación ante desastres tecnológicos, que consolide las actividades de los servicios críticos.

b) El plan de recuperación de desastres -DRP incluirá los requerimientos y controles de seguridad de la información que se deben cumplir en la situación de contingencia o interrupción de los servicios de la ADR.

c) La OTI definirá las estrategias de continuidad, realizará las pruebas y documentará el resultado.

d) Los productos y/o servicios que sean subcontratados por terceros deben disponer de planes de continuidad para no afectar el cumplimiento de la misionalidad de la ADR.

8.21. Requisitos Legales y Derechos de Propiedad Intelectual

a) La OTI identificara la normativa legal vigente que aplica a las tecnologías de información.

b) La OTI definirá controles con el objetivo de proteger adecuadamente la propiedad intelectual de la ADR, tanto propia como la de terceros, tales como derechos de autor de software, licencias y código fuente. El material registrado con derechos de autor no se deberá copiar sin la autorización del propietario.

c) La OTI a través del equipo de Seguridad y Privacidad de la Información generara conciencia a los colaboradores de la ADR sobre los derechos de propiedad intelectual.

8.22. Protección de Registros

Gestión documental dará lineamientos para cumplir con la protección de registros contra pérdida, destrucción y falsificación aplicando los requisitos legislativos, reglamentarios y los demás que apliquen, asi como:

a) Establecer directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información física y digital.

b) Establecer e implementar controles para proteger los registros en su confidencialidad, integridad y disponibilidad.

c) Establecer procedimientos de almacenamiento a largo plazo y manipulación de los registros físicos y digitales.

8.23. Privacidad y Protección de la Información Personal

La ADR cuenta con la política de tratamiento de datos personales la cual se encuentra publicada en la página web de la entidad.

8.24. Revisión Independiente de la seguridad de la información

a) Las Oficina de Control Interno de la ADR realizará de manera periódica auditorías internas para comprobar el cumplimiento de controles, políticas, procesos y procedimientos establecidos para el Subsistema de Seguridad y Privacidad de la Información.
b) Los líderes de los procesos deberán asegurar que la documentación (procedimientos, guías, manuales, entre otros), del Subsistema de Seguridad y Privacidad de la Información que son de responsabilidad del proceso se apliquen de manera oportuna y correctamente.
c) Es responsabilidad de todos los colaboradores aplicar la documentación (procedimientos, guías, manuales, entre otros) del Subsistema de Seguridad y Privacidad de la Información en la ejecución de sus actividades.

8.25. Cumplimiento de Políticas Reglas y Estándares de Seguridad de la Información:

Es responsabilidad de cada colaborador de la ADR dar cumplimiento a las políticas que se mencionan en este documento.

8.26. Procedimientos Operativos Documentados

Los documentos que definen los lineamientos para gestionar el Subsistema de Seguridad y Privacidad de la Información se encuentran disponibles en el aplicativo que la entidad establezca para tal fin.

8.27. Selección de Personal

Asegurar que el personal es adecuado para desempeñar las funciones y/o obligaciones para las que se considera y que sigue siendo elegible y adecuado durante su empleo, teniendo en cuenta:

a) Gestión del Talento Humano definirá un mecanismo de verificación del personal en el momento en que se postula al cargo. Dicho mecanismo deberá incluir los aspectos legales y procedimentales de vinculación a la ADR.
b) Vicepresidencia de Gestión Contractual definirá el mecanismo para la revisión de los antecedentes del personal a contratar por prestación de servicios, de acuerdo con lo que dicta la ley y la reglamentación vigente en atención al perfil solicitado en la contratación.
c) Los documentos de verificación deberán reposar en la historia laboral o carpeta contractual del colaborador.
d) Gestión del Talento Humano y la Vicepresidencia de Gestión Contractual deberán establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales

8.28. Términos y Condiciones de Empleo

Gestión del Talento Humano y la Vicepresidencia de Gestión Contractual definirán los lineamientos para que el personal que se vincula o se contrata cumpla con las políticas de la ADR en materia de seguridad y privacidad de la información

a) Vicepresidencia de Gestión Contractual definirá los términos y condiciones del contrato, en los cuales se establezca las obligaciones del contratista en materia de seguridad de la información.
b) Gestión del Talento Humano definirá dentro del proceso de vinculación de funcionarios las actividades y obligaciones en materia de seguridad de la información, que les aplique

8.29. Conciencia de Seguridad de la Información, Educación y Formación

Definir mecanismos para que los colaboradores de la ADR sean sensibilizados en temas de seguridad de la información, buenas prácticas y toma de conciencia, teniendo en cuenta:

a) Gestión del Talento Humano, incluirá los temas de seguridad y privacidad de la información en la inducción y reinducción de los colaboradores.

b) La OTI a través del equipo de Seguridad de la Información, diseñará un plan de sensibilización con temas relacionados a la seguridad y privacidad de la información para ser ejecutado al interior de la ADR.

8.30. Proceso Disciplinario

En lo pertinente al incumplimiento y desacato de las políticas de la seguridad de la información, se aplicará lo establecido en los procedimientos destinados para tal fin, por los entes de control disciplinario de la ADR.

8.31. Responsabilidades después de la terminación o cambio de empleo

Gestión del Talento Humano y la Vicepresidencia de Gestión Contractual definirá lineamientos para las responsabilidades y deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo, teniendo en cuenta:

a) En caso de retiro, investigación, inhabilidades, o cambio de funciones de un funcionario de planta, el jefe inmediato o a quien delegue deberá consolidar y custodiar la información de la ADR que se encontraba bajo su responsabilidad.
b) El supervisor del contrato o a quien delegue, deberá consolidar y custodiar la información de la ADR que se encontraba bajo la responsabilidad de los contratistas en caso de terminación anticipada, definitiva, suspensión o cesión del contrato.
c) El supervisor del contrato y/o jefe inmediato, informará de manera oportuna a la OTI las novedades de personal, con el fin de inhabilitar, suspender o modificar los accesos físicos y lógicos asignados en caso de que se requiera.
d) Una vez termine la relación contractual o laboral y en caso de requerirse, el supervisor del contrato y/o jefe inmediato podrá solicitar a la OTI una copia de la información que estaba a cargo del colaborador de acuerdo con la política de backup establecida en este documento.

e) Gestión del Talento Humano y la Vicepresidencia de Gestión Contractual establecerán la documentación y entregables requeridos para la desvinculación de los funcionarios de planta y contratistas de prestación de servicios.
f) El supervisor del contrato y/o jefe inmediato, informará a la OTI cualquier situación que sospeche o evidencie el incumplimiento de las políticas y procedimientos de seguridad y privacidad de la información establecidos en la ADR, por parte de sus funcionarios o contratistas.

8.32. Acuerdos de confidencialidad o no divulgación

Gestión del Talento Humano y Vicepresidencia de Gestión Contractual incluirán en dentro del clausulado del contrato o acto administrativo de posesión al cargo, el compromiso de confidencialidad de la Información y la autorización del tratamiento de datos personales, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.

8.33. Trabajo Remoto

Gestión de Talento Humano y la OTI, establecerán las medidas de seguridad de la información mientras se realiza teletrabajo, trabajo remoto o trabajo en casa, para proteger la información que se accede, procesa o almacenada en los lugares remotos, considerando los siguientes aspectos:

a) Es responsabilidad de los colaboradores almacenar la información institucional en los repositorios autorizados por la Agencia, en caso de ser almacenada en los equipos personales se traslada toda la responsabilidad al colaborador.
b) La OTI no realizara soporte ni licenciamiento a los equipos que son propiedad de los colaboradores de la ADR y son utilizados para gestionar actividades institucionales, por lo anterior es responsabilidad del colaborador garantizar que su equipo cuente con las mínimas condiciones de seguridad como un antivirus activo y actualizado. así como dar cumplimiento a las políticas "*Dispositivos Personales – Trae Tu Propio Equipo- BYOD"* del presente manual. Por lo que la ADR podrá realizar revisiones periódicas de dichas

condiciones, garantizando así la confidencialidad e integridad de la información de la entidad.

c) Realizar sensibilización sobre el uso adecuado de los dispositivos personales y concientizar sobre las amenazas y riesgos más comunes a los que se expone la entidad al permitir el acceso a sus recursos tecnológicos a través de este tipo de dispositivos personales.

8.34. Informe de Eventos de Seguridad de la Información

Los colaboradores de la ADR reportaran los eventos e incidentes de seguridad de la información a través de los canales establecidos en el procedimiento PR-GTI-007 Gestión de incidentes, eventos y debilidades de Seguridad de la Información.

8.35. Seguridad Física y del Entorno

Los servidores públicos, contratistas y visitantes de la ADR, deberán atender las siguientes indicaciones:

a) Todo servidor público, contratista o pasante sin carné, debe registrarse en la recepción de las sedes de la ADR, presentando su documento de identidad para validar el ingreso y, deberá proporcionar la información que sea solicitada por el personal de vigilancia, en concordancia a lo establecido en la Política de Protección de Datos de la ADR.
b) El ingreso de los visitantes (proveedores o terceras partes) debe estar autorizado por un colaborador de la ADR, este debe acompañarlo durante su estadía en la ADR, asi mismo, el visitante debe portar un elemento visible que lo identifique como visitantes.
c) El ingreso y salida de las instalaciones de la ADR está condicionado a la revisión obligatoria y sin excepción de bolsos y demás paquetes, así como la requisa mediante detector de metales o demás medios tecnológicos por parte del personal de vigilancia, destinados para este fin
d) Los servidores públicos, contratistas, terceros, usuarios y visitantes sin excepción, deben registrar los elementos tecnológicos en las bitácoras de vigilancia a la entrada y salida de

las sedes.

e) Está prohibido fumar y/o encender fósforos dentro de las instalaciones de la ADR excepto en las áreas que estén específicamente establecidas para tal fin.

f) Está prohibido el consumo de cualquier clase de bebidas alcohólicas, licor y/o sustancias psicoactivas dentro de las instalaciones de la ADR.

g) No está permitido a ningún servidor público, contratista, tercero, usuario o visitante el ingreso o porte de ningún tipo de arma, sea de fuego, arma blanca, arma letal o no letal, al interior de las instalaciones de la ADR a excepción de los servidores públicos que laboren con autoridades de policía, inteligencia o judicial, cuando la ley así lo disponga, y en desarrollo de sus funciones en las instalaciones de la ADR.

h) Los accesos físicos asignados a los colaboradores serán desactivados o modificados una vez terminado el vínculo contractual o laboral con la Entidad.

i) El perímetro de seguridad debe contar con vigilancia mediante cámaras de seguridad y debe ser monitoreado por el personal de vigilancia de la ADR.

j) Gestión Administrativa gestionara la adecuación y mantenimiento de la infraestructura física de la ADR.

k) Todo el personal de la ADR es responsable del cuidado y custodia de sus bienes personales.

8.36. Protección Contra Amenazas Fisicas y Ambientales

La OTI realizara seguimiento a las condiciones ambientales como la temperatura y humedad, identificando oportunamente las situaciones que puedan afectar negativamente las instalaciones del datacenter con el fin de tomar las acciones pertinentes.

8.37. Trabajo en Áreas Seguras

a) El personal que ingrese a los centros de cableado y datacenter deberá registrarse en la bitácora de ingreso.

b) Todo trabajo o mantenimiento de redes eléctricas, cableado de datos y voz, pruebas a los sistemas de UPS, aires acondicionados, plantas eléctricas y sistemas contra

incendios, entre otros, deben ser realizados por personal especializado, si lo realiza un externo debe estar identificado y acompañado por un colaborador de la OTI.

c) En los centros de cableado y datacenter no se deben almacenar elementos ajenos a los requeridos de acuerdo con la actividad que se realiza en esta área.
d) La OTI establecerá y monitoreará los controles preventivos y correctivos como sistemas de detección y extinción de incendios, control de inundación, alarmas entre otros.
e) Los centros de cableado y datacenter deben permanecer bajo llave.
f) No está permitido tomar fotos o realizar grabaciones de las áreas seguras sin la previa autorización del responsable de dicha área.
g) No se debe consumir alimentos ni bebidas.
h) No se deben ingresar elementos inflamables.
i) Toda persona ajena a la entidad que ingrese al área segura debe estar acompañada por un funcionario de la ADR durante el tiempo que dure su visita.

8.38. Escritorio y Pantalla Limpia

A continuación, se definen medidas preventivas para que los colaboradores las apliquen en los puestos de trabajo y así reducir los riesgos de acceso no autorizado a la información:

a) Cada vez que los colaboradores se retiren del lugar de trabajo deben bloquear los equipos de cómputo. La sesión de usuario se bloqueará automáticamente a los 3 minutos de inactividad.
b) El escritorio (digital) de las estaciones de trabajo, no debe tener ningún tipo de archivo, para evitar su fácil acceso, modificación o eliminación no autorizada.
c) No está permitido el consumo de alimentos y bebidas en los puestos de trabajo, ya que podrán verse afectado los activos de información (Computadores, Archivos Físicos entre otros).
d) Es recomendable, que los equipos de cómputo sean apagados al final de la jornada
e) Los puestos de trabajo deben permanecer limpios y ordenados y no debe existir información de tipo sensible (Clasificada o Reservada) sobre los puestos de trabajo, a menos que la misma se esté utilizando. Una vez el usuario se ausente de su puesto de

trabajo o no vaya a utilizar más la información, deberá almacenarla de manera segura en los cajones disponibles, para evitar robo o pérdida de esta.

f) Las llaves utilizadas para asegurar los cajones con información sensible no deben dejarse a la vista o a disposición de usuarios o visitantes.

g) Los computadores (portátiles) que son propiedad de la ADR deben asegurarse con una guaya o deben almacenarse dentro de los cajones del escritorio.

8.39. Ubicación y Protección de Equipos

a) Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y los posibles accesos no autorizado, adoptando controles contra robo, incendio, humo, agua, polvo, vibración e interferencia en el suministro eléctrico o de comunicaciones, entre otros.

b) Todo equipo de propiedad de la ADR que sea retirado de las instalaciones de la Agencia deberá ser autorizado a través del F-SAD-012 Formato solicitud salida y devolución de bienes e inmuebles.

8.40. Seguridad de los Activos Fuera de las Instalaciones de la ADR

a) La OTI establece los lineamientos para que los equipos y medios retirados de las instalaciones de la ADR se protejan adecuadamente.

b) Los colaboradores deben solicitar la autorización al Jefe Inmediato cuando vayan a retirar de las instalaciones de la ADR equipos de cómputo, asi mismo, deben diligenciar el F-SAD-012 Formato solicitud salida y devolución de bienes e inmuebles

8.41. Medios de Almacenamiento

La OTI establece lineamientos para la gestión de los medios de almacenamiento:

a) Todo medio removible deberá ser escaneado mediante antivirus cada vez que se conecte a un equipo de la red de la ADR.

a) En ninguna circunstancia se dejará desatendido los medios de almacenamiento y copias de seguridad de la información de la ADR como de los sistemas de información.

b) Los colaboradores que hagan uso del token para el desempeño de sus funciones u obligaciones velaran por la custodia y buen manejo de estos.

c) Es responsabilidad de cada colaborador tomar las medidas para la protección de la información contenida en medios removibles, con el fin de evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío de este.

8.42. Servicios Públicos de Apoyo

a) La ADR suministrará plantas eléctricas, UPS asi mismo garantizará su mantenimiento preventivo y correctivo.

b) La OTI con el acompañamiento de Secretaria general o dependencia designada deberán implementar mecanismos para regular el flujo de energía e interrupciones causadas por fallas en el soporte de los servicios públicos que puedan afectar los equipos de cómputo y procesamiento.

8.43. Seguridad del Cableado

a) El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debe estar protegido durante todo su recorrido contra interceptación, interferencia o daño.

b) Los equipos de cómputo que son propiedad de la ADR estarán conectados a la tomacorriente regulada.

8.44. Mantenimiento de Equipos

La OTIC dispondrá de un plan de mantenimiento para fortalecer la infraestructura tecnológica de la ADR y asegurar su ejecución.

8.45. Disposición o Reutilización Segura de Equipos

Por solicitud de Secretaria General o a quien esta delegue, la OTI verificara que cualquier dato sensible o software licenciado haya sido retirado o sobrescrito de forma segura, antes de la disposición o reúso del equipo de cómputo.

8.46. Dispositivos de Punto Final de Usuarios

Es responsabilidad de los colaboradores de la ADR dar cumplimiento a las políticas establecidas en este documento y las demás que entidad determine, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información de la entidad.

8.47. Derechos de Acceso Privilegiado

La OTI gestionara los accesos de usuarios privilegiados, considerando lo siguiente:

a) Identificar a los usuarios que necesitan derechos de acceso con privilegios para cada sistema (eje: sistemas operativos, sistemas de gestión de bases de datos, entre otros).
b) Gestionar los derechos de acceso privilegiado de acuerdo con lo establecido en el MA-GTI-004 Manual de Control de Acceso Lógico y el PR-GTI-004 Procedimiento de Control de Acceso Lógico.
c) Definir y establecer los requisitos para la expiración de los derechos de acceso privilegiado.
d) Los usuarios con derechos de acceso privilegiado tendrán habilitado el log de acceso y transacciones en el servicio tecnológico al que tenga acceso.
e) Los colaboradores deben custodiar las contraseñas y dar un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual se les ha permitido el acceso.

8.48. Restricción de Acceso a la Información

a) La OTI gestionara las solicitudes de acuerdo con lo establecido en el PR-GTI-001Procedimiento de Gestión de Requerimientos y Solicitudes TIC.
b) La OTI asignara a una cuenta de usuario (nombrada) permisos o privilegios de acuerdo con lo solicitado por el jefe inmediato o supervisor en el F-GTI-018 Formato solicitud de servicios TIC.

8.49. Acceso a Código Fuente

La OTI establecerá los lineamientos para controlar el acceso a los códigos fuentes de los programas con el fin de evitar la introducción de funciones no autorizadas, cambios intencionados o malintencionados y mantener la confidencialidad de la propiedad intelectual

valiosa.

8.50. Autenticación Segura

La OTI definirá e implementará los controles necesarios para que los usuarios o entidades se autentiquen de forma segura cuando se conceda el acceso a sistemas, aplicaciones, servicios e inicio de sesión, entre otras.

8.51. Gestión de la Capacidad de TI

La OTI realizara seguimiento al uso de recursos tecnológicos, con el fin de ajustar y proyectar los requisitos de capacidad futura de los servicios e infraestructura de tecnología de la ADR, teniendo en cuenta:

a) Los gestores de la OTI realizaran seguimiento trimestral a la infraestructura tecnológica con el fin de no sobrepasar la línea base del 60%.
b) Los gestores de la OTI en el último trimestre del año informaran por correo electrónico al jefe de la OTI los recursos de infraestructura tecnológica (obsolescencia, capacidad de usuario, almacenamiento, bases de datos y licenciamiento), que han llegado a un 60%, con el fin de incluirlos en el Plan Anual de Adquisiciones, el cual se ejecutara en la próxima vigencia.
c) La OTI dispondrá del personal idóneo y competente siempre y cuando, existan los recursos disponibles.

8.52. Protección Contra Malware

La OTI implementara controles para asegurar que la información y otros activos de información estén protegidos contra malware, teniendo en cuenta:

a) Instalar, monitorear y mantener actualizado en los equipos de cómputo y servidores que son propios de la ADR una herramienta de antivirus, que permita la gestión centralizada de las amenazas, eventos, estados de los equipos, entre otros.

b) Asegurar que la herramienta de antivirus brinde protección contra códigos maliciosos en todos los recursos informáticos de la ADR, garantizar que estas herramientas no puedan ser deshabilitadas, así como mantenerlas actualizadas.

8.53. Gestión de Vulnerabilidades

a) La OTI realizara la gestión de vulnerabilidades técnicas de acuerdo con lo establecido en el procedimiento de PR-GTI-010 Gestión de Vulnerabilidades Técnicas.
b) La OTI contara con una herramienta para identificar las vulnerabilidades de los principales sistemas de información con los que cuenta la entidad, asi mismo las dará a conocer a los gestores para que tomen la acciones pertinentes.

8.54. Gestión de la Configuración

La OTI a través del controlador de dominio del directorio activo gestiona las configuraciones de los equipos que son propiedad de la ADR.

8.55. Eliminación de información

a) Gestión documental realizara la eliminación de los documentos que hayan cumplido los tiempos de retención en el archivo.
b) Gestión documental conservara el registro de los resultados de la eliminación de la información

8.56. Enmascaramiento de Datos

La OTI establecerá los lineamientos para limitar la exposición de información sensible de la ADR, teniendo en cuenta:

a) Establecer técnicas que permitan ocultar información sensibles eje: pseudoanonimización o anonimización.
b) Identificar y establecer a que información se les debe aplicar estas técnicas
c) Establecer controles para restringir el acceso a la información sensible
d) Cumplir con la normatividad legal vigente que aplique a la entidad

8.57. Prevención Fuga de Datos

La OTI establecerá medidas de prevención contra la fuga de datos no autorizada, teniendo en cuenta:

a) Identificar, clasificar y proteger la información contra fugas (eje: información personal, misional, código fuente, entre otras)
b) Para los equipos propios de la ADR, establecer mecanismos que permitan controlar y supervisar la fuga de los datos al interior de la entidad (eje: información que se envía por correo, uso de USB, transferencia de archivos, dispositivos móviles, dispositivos de almacenamiento portátiles, entre otros).
c) Para los equipos que no son propiedad de la ADR, establecer mecanismos que permitan controlar y supervisar la fuga de los datos al interior de la entidad (eje: información que se envía por correo Y transferencia de archivos).
d) Sensibilizar y crear conciencia en los colaboradores (funcionarios de planta, contratistas, terceros, pasantes, entre otros) sobre la importancia de estos temas.

8.58. Copias de Seguridad de la Información (Backup)

La OTI garantizara el respaldo y restauración de la información importante para la ADR en función de su criticidad, bajo las siguientes premisas:

a) Ningún usuario debe realizar copias de la información “Reservada o Clasificada” en medios extraíbles personales, dado que la información es propiedad de la ADR.
b) La OTI realiza backup a la información que se aloja en el repositorio oficial de “File Server”, los usuarios deben solicitar el ingreso a este repositorio a través de la mesa de servicio.
c) Es responsabilidad de los colaboradores (funcionarios y contratistas) almacenar la información en el “File Server”.
d) Esta prohíbo alojar en el “File Server”, videos, archivos MP3, fotos y demás que no hagan parte de la ejecución de las funciones y obligaciones contractuales.
e) La OTI no realiza backup a la información que los usuarios almacenen en los discos duros de los equipos que son propiedad de la ADR.

f) Los medios de almacenamiento con información respaldada deben ser manipulados única y exclusivamente por el personal designado de la OTI.

g) La OTI no entrega backup de la información que los usuarios hayan almacenado en el "File Server" durante o al finalizar la ejecución de sus funciones o contrato, teniendo en cuenta que esta, es propiedad de la ADR.

8.58.1. Respaldo de las Cuentas de Correo Electrónico

a) En caso de que el colaborador requiera una copia del correo electrónico durante o al finalizar la ejecución de sus funciones o contrato, el líder de la dependencia lo solicita a través de la mesa de servicio, medio por el cual se le informara sobre la entrega del backup.

b) En el momento que se requiera reactivar el correo electrónico de un colaborador que ha finalizado su vínculo laboral o contractual con la ADR, el líder de la dependencia debe solicitarlo a través de la mesa de servicio. Cabe aclarar que deben haber transcurrido máximo 20 días hábiles una vez terminado su vínculo laboral o contractual, de lo contrario, no se reactivara y se entregara un backup del correo electrónico.

c) La reactivación de la cuenta de correo se realizará en días hábiles, máximo por 72 horas.

d) La OTI retiene la información de correos electrónicos por un periodo máximo de 3 años.

8.58.2. Buzón de Notificaciones (grupos de correos)

a) Cuando un área requiera un buzón de notificaciones (grupos de correos) debe solicitarlo a la OTIC a través de la mesa de servicio.

b) Es responsabilidad de cada área utilizar y hacer buen uso de los buzones oficiales

c) Las áreas serán las responsables de actualizar los miembros de los buzones de notificaciones (grupos de correos), en el momento que se presente una novedad (desvinculación contractual o laboral, entre otras)

d) La OTI no realiza backup a estos buzones de notificaciones (grupos de correos)

8.59. Redundancia de las instalaciones de procesamiento de información

a) Definir y documentar la estrategia de recuperación de desastres tecnológicos, que consolide las actividades de los servicios críticos que se apoyan en las TIC.
b) Definir las estrategias de contingencia, realizar las pruebas y documentar el resultado.
c) Los productos y/o servicios que sean subcontratados por la OTI deben disponer de planes de continuidad para no afectar la operación de la entidad.

8.60. Registro - Logs

a) La OTI realizara mensualmente la revisión aleatoria a los logs de accesos al AD (Active Directory) y a la red.
b) La OTI establecerá un espacio de almacenamiento (1 giga) donde alojará por 2 meses los logs de accesos AD (Active Directory) y a la red.
c) Después de realizar los backup (diario) de las bases de datos, se limpian los logs ya que en la entidad no se generan operaciones o procesos batch nocturnos.
d) Para los nuevos desarrollos, el desarrollador definirá las tablas principales de Logs dentro de las bases de datos para guardar las modificaciones realizadas a estas.
e) La OTI realizará revisiones periódicas de las configuraciones de monitoreo para garantizar que estén alineadas con las necesidades de la entidad.

8.61. Actividades de Seguimiento

La OTI implementara controles para detectar comportamientos anómalos y posibles incidentes de seguridad de la información, teniendo en cuenta:

a) Establecer mecanismos que realicen monitoreo al acceso a servidores, equipos de red, aplicaciones misionales, tráfico de red, sistemas y aplicaciones salientes y entrantes, acceso no autorizado, análisis no autorizado de aplicaciones, sistemas y redes de la entidad, intentos correctos e incorrectos de acceder a los recursos protegidos (servidores DNS, portales web recursos compartidos de archivos) entre otras.
b) Definir una línea base de comportamiento normal para vigilar sobre esa línea las actividades que realizan los usuarios con el fin de detectar anomalías frente la utilización

de los sistemas en periodos normales y fuera de lo normal, hora habitual de acceso, ubicación del acceso, frecuencia de acceso, a que paginas están ingresando, que información están descargando y/o almacenando en los equipos, entre otras.

8.62. Sincronización de Relojes

La OTI sincronizara los relojes de los servidores, sistemas de información, telefonía, estaciones de trabajo y demás (ítems de configuración) con una única fuente de referencia de tiempo, con el fin de garantizar la exactitud de los registros de auditoría.

8.63. Uso de Programas Utilidad Privilegiados

La OTI asegurara que el uso de programas de utilidad no perjudique los controles del sistema y de las aplicaciones, teniendo en cuenta:

a) Establecer controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información, no tengan instalados en sus equipos de cómputo utilitarios que permitan escalar privilegios o evadir controles de seguridad informáticos.
b) Monitorear a los administradores de los recursos tecnológicos y servicios de red, para que no hagan uso de utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para anular la seguridad de los sistemas de información alojados sobre la plataforma tecnológica.
c) Generar y actualizar programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información.
d) Retirar o deshabilitar los programas utilitarios privilegiados no autorizados de la plataforma tecnológica, los servicios de red y sistemas de información

8.64. Instalación de Software en Sistemas Operativos

La OTI aplicara controles para administrar de forma segura la instalación de software en sistemas operativos, teniendo en cuenta:

a) Controlar y documentar los cambios en las librerías de programas propios del ADR, software operacional y aplicaciones.
b) La instalación y actualización al software las realizara solo el personal autorizado

8.65. Seguridad de Redes, Servicios y Segregación

La OTI asegurara la protección de la información transmitida en las redes de comunicación, los servicios relacionados y las instalaciones de procesamiento de información contra acceso no autorizado, aplicando los controles necesarios que permitan tener un adecuado nivel de seguridad en la red y de la información, teniendo en cuenta:

a) Contar con segmentación a nivel de redes físicos y lógicos para el despliegue de políticas y acceso a los recursos de red requeridos para el desarrollo de las actividades de la ADR.
b) Realizar la gestión de acceso lógico a los servicios de red de la ADR de acuerdo con el MO-GTI-004 Manual acceso lógico y el PR-GTI-004 Procedimiento de acceso lógico.
c) Implementar mecanismos de control que permitan fortalecer la seguridad perimetral, minimizando la posibilidad de materialización de riesgos o reduciendo su impacto en caso de materialización.
d) Realizar monitoreo a los componentes de la infraestructura de red, de tal forma que se identifiquen de manera oportuna vulnerabilidades y fallas que puedan afectar la seguridad de la información.
e) Configurar y administrar el filtro de contenido que bloquee el acceso a sitios no productivos o clasificados dentro de listas negras por manejar temas tales como: pornografía, juegos, violencia, terrorismo, y demás páginas que no sean de uso laboral.
f) Realizar monitoreo a los servicios, protocolos y puertos permitidos en la red de datos de la entidad, inhabilitando o eliminando aquellos no identificados ni autorizados.
g) Establecer para los usuarios que utilizan las redes inalámbricas las mismas condiciones de seguridad de las redes cableadas en lo que respecta identificación, autenticación, control de contenido de internet y cifrado entre otros.
h) Proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet, bajo las restricciones de los perfiles de acceso establecidos; implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia.

i) Limitar o bloquear el acceso a sitios e impedir que se descarguen ciertos tipos de archivos que pueden afectar el servicio de internet y la información de la ADR.

j) Todas las conexiones para navegar en Internet desde la red corporativa se deben solicitar a través de la herramienta dispuesta por la entidad.

8.66. Filtrado Web

La OTI establecerá controles para proteger los sistemas de información contra malware y accesos no autorizados, teniendo en cuenta:

a) Identificar los sitios web a los que los usuarios deberían tener o no acceso.

b) Definir e implementar los controles para reducir el riesgo de que los colaboradores accedan a sitios web que contienen información ilegal, virus o material de Phishing.

c) Establecer perfiles de navegación de acuerdo con el rol, funciones del usuario o la dependencia, con el fin de asignar permisos para el ingreso a páginas.

8.66. Uso de la Criptografía

La OTI asegurara el uso adecuado y efectivo del cifrado para proteger la confidencialidad, autenticidad e integridad de la información de acuerdo con lo establecido en el PR-GTI-009 Gestión de Controles Criptográficos.

8.67. Ciclo de Vida de Desarrollo Seguro

La OTI son los responsables de planificar, documentar y ejecutar las actividades relacionadas con el ciclo de vida del software, teniendo en cuenta, como mínimo lo siguiente:

a) La OTI diseña, desarrolla y despliega aplicaciones y sistemas información de acuerdo con lo establecido en el MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software y el PR-GTI-012 Procedimiento Control de Versiones de Software.

b) Todo sistema de información adquirido o desarrollado debe utilizar herramientas de desarrollo licenciadas o libres reconocidas en el mercado.

c) La plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información deben estar actualizados con las versiones LST, las cuales deben estar en la última versión aprobada del sistema.

d) Todo desarrollo inhouse debe contar con mecanismos de seguridad (autenticación, autorización y auditoría) en todas las fases del desarrollo de software que utilice la ADR.
e) Los desarrollos nuevos o sistemas de información adquiridos deben contar con pistas de auditoría que permitan como mínimo revisar los accesos (Loguin) exitosos y fallidos, así como las creaciones y modificaciones de usuarios y permisos.
f) El uso de información catalogada como “Pública Clasificada” o “Pública Reservada” está restringido para propósito de desarrollo y pruebas, por lo que se deben utilizar métodos o estrategias para la anonimización, enmascaramiento u ofuscación de la información.
g) Definir y mantener actualizado los roles, perfiles y usuarios de los sistemas de información.
h) Cada sistema de información deberá contar con los manuales de uso, técnicos y administrativos disponibles de acuerdo con los niveles de protección de la información dados por la Entidad.
i) Para el desarrollo inhouse el código fuente debe reposar en el repositorio estableció establecido por la OTI.
j) La OTI debe asegurar que los sistemas de información adquiridos o desarrollados por contratistas cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
k) Todos los desarrolladores internos o externos, contratados por la ADR, deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, iniciando desde la fase de diseño hasta la puesta en producción.

8.68. Requisitos de Seguridad de las Aplicaciones

La OTI realizara la transferencia de información de acuerdo con el PR-GTI-013 Procedimiento de Intercambio, interoperabilidad o suministro de información.

a) La OTI establecerá los controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de información en las aplicaciones de la ADR, teniendo en cuenta los siguientes criterios: contar con información de autenticación secreta de usuario, mantener confidencialidad entre la ADR y las partes involucradas, usar cifrado

en las comunicaciones cuando sea necesario, los protocolos de comunicación estén asegurados y la información almacenada de las transacciones no se encuentre pública.

8.69. Arquitectura de Sistemas Seguros y Principios de Ingeniería

La OTI establecerá los principios para asegurar que los sistemas de información se diseñan, implementan y operan de forma segura dentro del ciclo de vida del desarrollo.

8.70. Codificación Segura

La OTI definirá, documentará y aplicará la metodología para la codificación segura tanto para los desarrollos inhouse como para los desarrollos subcontratados con el fin de mitigar posibles vulnerabilidades.

8.71. Pruebas de Seguridad en el Desarrollo y Aceptación

La OTI ejecutara las pruebas de seguridad y pruebas de aceptación a los cambios y nuevos sistemas de información de acuerdo con lo establecido en el MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software y el PR-GTI-012 Procedimiento Control de Versiones de Software.

8.72. Desarrollo Tercerizado

a) Aplicar lo establecido en el MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software y el PR-GTI-012 Procedimiento Control de Versiones de Software.

b) Cuando se adquieran soluciones ya desarrolladas, se deberán definir con el proveedor previo a la adquisición, los procesos de administración de parches de la aplicación para asegurar que la misma no sea vulnerable, considerando referentes como OWASP.

c) Establecer acuerdos de confidencialidad para respaldar el uso de la información de propiedad de la ADR que se requiere entregar al proveedor.

d) Los sistemas de información adquiridos o desarrollados por terceros deben contemplar la definición y entrega de acuerdos de licenciamiento, propiedad de códigos, los cuales

deben especificar las condiciones de uso del software y los derechos de propiedad intelectual.

e) Establecer en la documentación contractual y anexos técnicos los requisitos relacionados a prácticas seguras de diseño, codificación y pruebas.

f) Establecer acuerdos de niveles de servicio en cuanto a la calidad, oportunidad y seguridad de los entregables de los sistemas de información.

g) Solicitar al proveedor la generación y entrega de un informe de análisis y mitigación de vulnerabilidades realizado al sistema de información con un tiempo no mayor a seis (6) meses.

h) Documentar las características del ambiente de desarrollo usado para replicar ambientes similares.

i) Implementar o utilizar protocolos de comunicación cifrados para intercambiar datos o funcionalidad con los sistemas de información de la entidad.

j) Requerir en lo posible la integración del acceso a los sistemas de información a través de usuarios de dominio.

k) Para el caso de adquisición de software como servicios (SaaS) se deben contemplar requerimientos como: periodicidad y retención de las copias de respaldo de la información de la ADR, requerimientos de continuidad, redundancias, requisitos de seguridad a nivel de infraestructura, roles y privilegios, integración con el directorio activo, privacidad de la información, entre otros.

l) Para el caso de la información almacenada en SaaS cuando finalice la relación contractual entre la ADR y el proveedor, se debe solicitar el borrado seguro de dicha información previa entrega de una copia de respaldo completa de la información con corte a la finalización del contrato.

m) En caso de que se realicen cambios a un sistema de información adquirido, se debe conservar la versión original para ser restaurado en caso de requerirse.

n) Planear y ejecutar pruebas técnicas y funcionales que les permitan contar con la aceptación de los desarrollos y funcionalidades solicitados.

8.73. Adquisición de Software por áreas distintas a la OTIC

a) La OTI de acuerdo con sus funciones es la dependencia que cuenta con la capacidad técnica de adquirir, desarrollar o avalar la adquisición del software de cualquier tipo, conforme a los requerimientos de las dependencias con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad e integridad de la información de los sistemas con los que cuenta la entidad. Este aval lo emitirá el jefe de la OTI

b) En caso de que un área diferente a la OTI requiera la adquisición y/o desarrollo de un software o componentes de TI, debe contar con el concepto técnico y aval por parte del jefe de la Oficina de Tecnologías de la Información - OTI previo al proceso de contratación.

c) El área que adquiera un sistema de información y/o aplicación debe dar cumplimiento a las políticas de desarrollo tercerizado descritas en el numeral 8.72 de este documento.

d) Todo software que las áreas hayan adquirido y/o desarrollado y no cuentan con el concepto técnico y aval por parte del jefe de la Oficina de Tecnologías de la Información - OTI, deberá formalizar la entrega de la parte técnica del software, teniendo en cuenta:

- Documentación técnica (manual de usuario, manual técnico y manual de instalación, código fuente (cuando aplique))
- La administración funcional estará cargo del área correspondiente y la parte técnica de la OTI.
- El desarrollador o proveedor realizara a la OTI la transferencia de conocimiento sobre la parte técnica y funcional.

8.74. Solicitud Creación y/o Consulta de Bases de Datos

a) El líder de la dependencia debe solicitar a través de la mesa de servicio la creación y/o consulta de bases de datos, esta solicitud debe contener:

Crear: Cual es la necesidad de crear la base de datos, Tiempo de gestión de la base de datos y Roles y permisos de usuarios

Consulta: Cuál es la finalidad que se requiere para consultar la BD**,** Usuarios

autorizados para consultar la BD e Indicar por cada usuario el tiempo de acceso a la base de datos.

b) Cuando un área solicite la creación de una base de datos, la OTI la implementara en los motores licenciados de bases de datos con los que cuente la entidad.

8.75. Separación de entornos de desarrollo, pruebas y producción

La OTI realizara la separación de los ambientes de desarrollo, pruebas y producción teniendo en cuenta:

a) Realizar la separación física y lógica de los ambientes de desarrollo, pruebas, preproducción y producción, con el fin de reducir los riesgos de acceso o cambios no autorizados que puedan afectar la confidencialidad, integridad y disponibilidad de los entornos productivos.

b) Garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y no en los ambientes de pruebas o producción.

c) Utilizar nombres de dominios diferentes para los ambientes de prueba, desarrollo y producción para evitar confusiones y diferenciar de manera clara cada ambiente.

d) La OTI utilizara datos que no sean sensibles para la ADR en los ambientes de prueba, exceptuando aquellos casos en los que el usuario funcional solicita la restauración de datos de producción para verificar la correcta funcionalidad.

8.76. Gestión de Cambios de TI

La OTI gestionara los cambios que se presenten en la infraestructura tecnológica de acuerdo con lo establecido en el PR-GTI-002 Procedimiento de Gestión de Cambios de Seguridad de la Información.

8.77. Información de las Pruebas

a) Aplicar lo establecido en el MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software.

b) Garantizar que la información entregada para realizar las pruebas no revelará información Pública Clasificada y Pública Reservada en los ambientes de producción.
c) Establecer un periodo de retención de datos de pruebas, con el fin de evitar el uso no autorizado de la información de la prueba.

8.78. Protección de los sistemas de información durante las pruebas de auditoría

a) La OTI planificará actividades que involucren auditorías a los sistemas críticos en producción, limitando el acceso al sistema de información y a los datos de solo de lectura (en caso de acceso diferente al de solo lectura se deberá acordar previamente), determinando tareas, responsables y estas se deberán realizar fuera del horario laboral. Esta auditorias las realizara el Oficial del Seguridad de la Información.
b) La OTI definirá y gestionará los planes de mejoramiento que se generen de los resultados de las auditorías a los sistemas de Información de la ADR.

9. Gestión de Riesgos

La gestión de riesgos para el Subsistema de Seguridad y Privacidad de la Información se realiza de acuerdo con la metodología definida y establecida por la Oficina de Planeación de la ADR.

10. Inducción Capacitación y Desarrollo de Competencia

a) La OTI hará uso de la infraestructura tecnológica de la ADR para dar a conocer las buenas prácticas de seguridad y privacidad de la información con el propósito que cada colaborador las aplique en el desarrollo sus actividades.
b) El área de Talento Humano identificara las necesidades de aprendizaje de los servidores públicos, con el propósito de fortalecer los conocimientos y habilidades en temas de seguridad y privacidad de la información, necesidades que se planifican en el Plan Institucional de capacitación-PIC para ser ejecutados durante la vigencia.

11. Medición y Seguimiento

La política del Subsistema de Seguridad y Privacidad de la Información se medirá con base en

los siguientes indicadores:

Nombre Indicador	Formula Indicador	Frecuencia de Medición	Meta Acumulativa
Nivel de ejecución del plan de seguridad y privacidad de la información	No. de actividades ejecutadas / No. de actividades planeadas	Trimestral	95%
Efectividad Atención de Incidentes de Seguridad Digital	No. de incidentes de seguridad digital atendidos / No. total, de incidentes detectados o reportados) *100	Trimestral	95%
Nivel de ejecución del plan de concientización de SI	No. Actividades ejecutadas /No actividades programadas	Cuatrimestral	95%

12. Gestión de Cambios Estratégicos

La gestión de cambios del Sistema Integrado de Gestión del cual hace parte el Subsistema de Seguridad y Privacidad de la Información se realizarán de acuerdo con lo establecido en el PR-SIG-006 Procedimiento Gestión de Cambios.

13. Documentos Asociados

- Política Integral del Sistema Integrado de Gestión de la Agencia de Desarrollo Rural
- Política de Tratamiento de Datos Personales
- Resolución *529 de 2024 "por medio de la cual se adopta el Sistema Integrado de Gestión, se actualiza el comité de Gestión y Desempeño de la ADR y se dictan otras disposiciones"* o la que la modifique o derogue.
- Resolución 666 de 2024 – "*Por medio de la cual se aclara la Resolución 529 del 3 de septiembre de 2024"*, o la que la modifique o derogue.

14. Control de Cambios

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	02/10/2023	Aprobación del manual de políticas de seguridad de la información mediante la sesión 12 del comité institucional de gestión y desempeño del día 26 de septiembre de 2023.
2	12/12/2024	Se actualiza el manual de acuerdo con los controles del “Anexo A” de la norma ISO 27001:2022 se redefine los objetivos, alcance, marco de referencia, gestión de riesgos, gestión de cambios estratégicos, medición y seguimiento y la estructura organizacional del subsistema de SI.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Claudia Paola Andrade Murillo **Cargo:** Contratista Dependencia: Oficina de Tecnologías de la información	**Nombre:** Walter Silva Combita **Cargo:** Contratista Dependencia: Oficina de Planeación **Nombre:** Giovanny Andres Palacios Cuartas **Cargo:** Contratista Dependencia: Oficina de Tecnologías de la Información	**Nombre:** Fredy Ocampo Góngora **Cargo:** jefe Oficina de Tecnología de la Información (E) Dependencia: Oficina de Tecnología de la Información

Declarar la aplicabilidad o exclusión de los controles del "Anexo A" de la NTC-ISO 27001:2022 *"Seguridad de la información, Ciberseguridad y Protección de la Privacidad*", para la implementación del Subsistema de Seguridad y Privacidad de la Información en la ADR, con el fin de establecerlos y darlos a conocer a los funcionarios, contratistas, practicantes y terceros que tengan vínculos laborales o contractuales con la ADR para su respectivo cumplimiento.

No. CONTROL	CONTROL	DECLARACIÓN DE APLICABILIDAD SI/NO	
5	**Controles Organizacionales**		
5.1	Políticas de seguridad de la información	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.2	Roles y responsabilidades en la seguridad de la información	SI	Resolución 529 de 2024 - *Por medio de la cual se adopta el Sistema Integrado de Gestión, se actualiza el Comité de Gestión y Desempeño de la ADR y se dictan otras disposiciones, o la que la modifique o derogue.* Resolución 666 de 2024 – Por medio de la cual se aclara la Resolución 529 del 3 de septiembre de 2024, *o la que la modifique o derogue* MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.3	Segregación de deberes	SI	Resolución 529 de 2024 - *Por medio de la cual se adopta el Sistema Integrado de Gestión, se actualiza el Comité de Gestión y Desempeño de la ADR y se dictan otras disposiciones, o la que la modifique o derogue* Resolución 666 de 2024 – Por medio de la cual se aclara la Resolución 529 del 3 de septiembre de 2024, *o la que la modifique o derogue* MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-004 Manual de Control de Acceso Lógico PR-GTI-008 Procedimiento de Control de Acceso Lógico PR-GTI-001Gestión de Requerimientos y Solicitudes TIC
5.4	Responsabilidades de la dirección	SI	Resolución 529 de 2024 - *Por medio de la cual se adopta el Sistema Integrado de Gestión, se actualiza el Comité de Gestión y Desempeño de la ADR y se dictan otras disposiciones, o la que la modifique o derogue.* Resolución 666 de 2024 – Por medio de la cual se aclara la Resolución 529 del 3 de septiembre de 2024, *o la que la modifique o derogue* MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.5	Contacto con las autoridades	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información F-GTI-015 Contactos con autoridades y grupos de interés del sistema de gestión de seguridad de la información
5.6	Contacto con grupos de interés especial	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información

No. CONTROL	CONTROL	DECLARACIÓN DE APLICABILIDAD SI/NO	
			F-GTI-015 Contactos con autoridades y grupos de interés del sistema de gestión de seguridad de la información
5.7	Inteligencia de amenazas	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.8	Seguridad de la información en la gestión de proyectos	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.9	Inventario de información y otros activos asociados	SI	MA-GTI-003 Manual de Gestión de Activos de Seguridad de la Información MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.10	Uso aceptable de la información y otros activos asociados	SI	MA-GTI-003 Manual de Gestión de Activos de Seguridad de la Información MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información Política Uso de Internet Política Uso Correo Electrónico
5.11	Devolución de activos	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-003 Manual de Gestión de Activos de Seguridad de la Información F-GAD-010 Entrega y devolución de bienes asignados
5.12	Clasificación de la información	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.13	Etiquetado de la información	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.14	Transferencia de información	SI	PR-GTI-013 Procedimiento de Intercambio, interoperabilidad o suministro de información MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.15	Control de acceso	SI	MA-GTI-004 Manual de Control de Acceso Lógico PR-GTI-008 Procedimiento de Control de Acceso Lógico MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Control de Acceso Lógico – Gestión de Identidades
5.16	Gestión de identidades	SI	MA-GTI-004 Manual de Control de Acceso Lógico. PR-GTI-004 Procedimiento de Control de Acceso Lógico MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - política Control de Acceso Lógico – Gestión de Identidades
5.17	Información de autenticación	SI	MA-GTI-004 Manual de Control de Acceso Lógico. PR-GTI-004 Procedimiento de Control de Acceso Lógico MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.18	Derechos de acceso	SI	MA-GTI-004 Manual de Control de Acceso Lógico.

No. CONTROL	CONTROL	DECLARACIÓN DE APLICABILIDAD	
		SI/NO	
			PR-GTI-004 Procedimiento de Control de Acceso Lógico MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Control de Acceso Lógico – Gestión de Identidades
5.19	Seguridad de la información en las relaciones con proveedores	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Gestión de Proveedores
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información – Política Gestión de Proveedores MO-GCO-001 Manual de contratación, supervisión e interventoría Anexos Técnicos Acuerdos y Cláusulas Contractuales
5.21	Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Gestión de Proveedores
5.22	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política. Gestión de Proveedores PR-GTI-002 Procedimiento de Gestión de Cambios de Seguridad de la Información
5.23	Seguridad de la información para el uso de servicios en la nube	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.24	Planificación y preparación de la gestión de incidentes de la seguridad de la información	SI	PR-GTI-007 Gestión de incidentes, eventos y debilidades de Seguridad de la Información MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Gestión de Incidentes
5.25	Evaluación y decisión sobre eventos de seguridad de la información	SI	PR-GTI-007 Gestión de incidentes, eventos y debilidades de Seguridad de la Información
5.26	Respuesta a incidentes de seguridad de la información	SI	PR-GTI-007 Gestión de incidentes, eventos y debilidades de Seguridad de la Información
5.27	Aprender de los incidentes de seguridad de la información	SI	PR-GTI-007 Gestión de incidentes, eventos y debilidades de Seguridad de la Información Plan concientización en seguridad de la información
5.28	Recopilación de evidencias	SI	PR-GTI-007 Gestión de incidentes, eventos y debilidades de Seguridad de la Información

No. CONTROL	CONTROL	DECLARACIÓN DE APLICABILIDAD	
		SI/NO	
5.29	Seguridad de la información durante una interrupción	SI	Manual de recuperación de desastres de TI MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.30	Preparación de las TIC para la continuidad de negocio	SI	Manual de recuperación de desastres de TI MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Preparación de las TIC para la Continuidad del Negocio F-GTI-024 Formato Plan Backup
5.31	Requisitos legales, reglamentarios y contractuales	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información Normograma OTI
5.32	Derechos de propiedad intelectual	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Requisitos Legales y Derechos de Propiedad Intelectual Plan concientización en seguridad de la información
5.33	Protección de los registros	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información DE-DOC-002 Programa de gestión documental PR-DOC-003 Organización de archivo Tablas de Retención Documental - TRD.
5.34	Privacidad y protección de la información de identificación personal	SI	Política de tratamiento de datos personales, publicada en la página web de la ADR Clausula Tratamiento de Datos - Anexo clausulado general contrato de prestación de servicios profesionales y/o de apoyo a la gestión
5.35	Revisión independiente de la seguridad de la información	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información PR-SIG-005 Auditorias de sistema integrado de gestión F-EVI-002 Plan Anual de Auditorias
5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
5.37	Procedimientos operativos documentados	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información Los procedimientos operativos del Subsistema de Seguridad y Privacidad de la Información y demás se encuentran publicados en la herramienta dispuesta por la entidad.
6	**Controles Personas**		
6.1	Selección		MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información. Funcionarios de Planta: PR-GTH-001 Administración de Talento Humano F-GTH-001 Verificación requisitos mínimos y prueba de análisis de antecedentes

No. CONTROL	CONTROL	DECLARACIÓN DE APLICABILIDAD SI/NO	
			F-GTH-002 Lista de chequeo documentos requeridos para posesión Contratistas: F-GCO-021 Lista de chequeo contratación directa F-GCO-017 Tabla de análisis de experiencia e idoneidad Estudios previos
6.2	Términos y condiciones de empleo	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información. Funcionarios de Planta: Resolución asignación de cargos F-GTH-035 Acta de entrega del puesto de trabajo para transferencia del conocimiento Contratistas: F-GCO-026 Estudios previos contratos de prestación de servicios profesionales y de apoyo a la gestión Anexo clausulado general contrato de prestación de servicios profesionales y/o de apoyo a la gestión.
6.3	Conciencia de seguridad de la información, educación y formación	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información PR-GTH-003 Desarrollo del Talento Humano F-GTH-005 Ficha para el registro de necesidades de capacitación y formación Plan de concientización de seguridad de la información
6.4	Proceso disciplinario	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información PR-CDI-002 Control interno disciplinario ordinario PR-CDI-001 Control interno disciplinario verbal
6.5	Responsabilidades después de la terminación o cambio de empleo	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información PR-GTI-001 Gestión de Requerimientos y Solicitudes TIC F-GTI-018 Formato solicitud de servicios TIC
6.6	Acuerdos de confidencialidad o no divulgación	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información Resolución asignación de cargos Anexo clausulado general contrato de prestación de servicios profesionales y/o de apoyo a la gestión.
6.7	Trabajo remoto	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
6.8	Informe de eventos de seguridad de la información	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información PR-GTI-007 Gestión de incidentes, eventos y debilidades de Seguridad de la Información
7	**Controles Físicos**		

No. CONTROL	CONTROL	DECLARACIÓN DE APLICABILIDAD	
		SI/NO	
7.1	Perímetros de seguridad física	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información- Política Seguridad Física y del Entorno Contrato servicio de vigilancia PR-GAD-001 Adecuación y mantenimiento de la infraestructura física
7.2	Entrada física	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información- Política Seguridad Física y del Entorno Contrato servicio de vigilancia Bitácora ingreso a la entidad
7.3	Asegurar oficinas, e instalaciones	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información- Política Seguridad Física y del Entorno Contrato servicio de vigilancia Bitácora ingreso a la entidad
7.4	Monitoreo de la seguridad física	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Seguridad Física y del Entorno Contrato servicio de vigilancia Bitácora ingreso a la entidad
7.5	Protección contra amenazas físicas y ambientales	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
7.6	Trabajar en áreas seguras	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información Bitácora ingreso a centros de cableado
7.7	Escritorio y pantalla limpia	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información Plan concientización en seguridad de la información
7.8	Ubicación y protección de equipos	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información F-SAD-012 Formato solicitud salida y devolución de bienes e inmuebles
7.9	Seguridad de los activos fuera de las instalaciones	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información F-SAD-012 Formato solicitud salida y devolución de bienes e inmuebles
7.10	Medios de almacenamiento	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información (Política copias de respaldo)
7.11	Servicios públicos de apoyo	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información

No. CONTROL	CONTROL	DECLARACIÓN DE APLICABILIDAD	
		SI/NO	
7.12	Seguridad del cableado	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
7.13	Mantenimiento de equipos	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
7.14	Disposición o reutilización segura de equipos	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8	**Controles Tecnologicos**	SI	
8.1	Dispositivos de punto final de usuarios	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información Política Dispositivos Personales- Trae Tu Propio Equipo-BYOD MA-GTI-004 Manual de Control de Acceso Lógico y el PR-GTI-004 Procedimiento de Control de Acceso Lógico PR-GTI-007 Gestión de incidentes, eventos y debilidades de Seguridad de la Información Política Escritorio y Pantalla Limpia
8.2	Derechos de acceso privilegiado	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-004 Manual de Control de Acceso Lógico y el PR-GTI-004 Procedimiento de Control de Acceso Lógico
8.3	Restricción de acceso a la información	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-004 Manual de Control de Acceso Lógico y el PR-GTI-004 Procedimiento de Control de Acceso Lógico PR-GTI-001Procedimiento de Gestión de Requerimientos y Solicitudes TIC F-GTI-018 Formato solicitud de servicios TIC.
8.4	Acceso al código fuente	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.5	Autenticación segura	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-004 Manual de Control de Acceso Lógico y el PR-GTI-004 Procedimiento de Control de Acceso Lógico PR-GTI-001Procedimiento de Gestión de Requerimientos y Solicitudes TIC
8.6	Gestión de la capacidad	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.7	Protección contra malware	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información Herramienta tecnología que disponga la entidad para detectar y gestionar el malware

No. CONTROL	CONTROL	DECLARACION DE APLICABILIDAD	
		SI/NO	
8.8	Gestión de vulnerabilidades técnicas	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información PR-GTI-010 Gestión de Vulnerabilidades Técnicas Herramienta tecnología que disponga la entidad
8.9	Gestión de la configuración	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.10	Eliminación de información	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información Tablas de Retención Documental -TRD F-DOC-020 Acta de eliminación de documentos de archivo
8.11	Enmascaramiento de datos	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.12	Prevención de fuga de datos	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.13	Copias de seguridad de la información	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Respaldo de las Cuentas de Correo Electrónico - Política Buzón de Notificaciones (grupos de correos) F-GTI-024 Formato Plan Backup
8.14	Redundancia de las instalaciones de procesamiento de información	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.15	Registro	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.16	Actividades de seguimiento	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.17	Sincronización de relojes	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.18	Uso de programas de utilidad privilegiados	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.19	Instalación de software en sistemas operativos	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.20	Seguridad de redes	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Seguridad de Redes, Servicios y Segregación
8.21	Seguridad de los servicios de red	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Seguridad de Redes, Servicios y Segregación

No. CONTROL	CONTROL	DECLARACION DE APLICABILIDAD	
		SI/NO	
8.22	Segregación de redes	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Seguridad de Redes, Servicios y Segregación
8.23	Filtrado web	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información
8.24	Uso de la criptografía	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información PR-GTI-009 Gestión de Controles Criptográficos
8.25	Ciclo de vida de desarrollo seguro	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software PR-GTI-012 Procedimiento Control de Versiones de Software
8.26	Requisitos de seguridad de las aplicaciones	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software PR-GTI-012 Procedimiento Control de Versiones de Software PR-GTI-013 Procedimiento de Intercambio, interoperabilidad o suministro de información.
8.27	Arquitectura de sistemas seguros y principios de ingeniería	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software PR-GTI-012 Procedimiento Control de Versiones de Software
8.28	Codificación segura	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software PR-GTI-012 Procedimiento Control de Versiones de Software
8.29	Pruebas de seguridad en el desarrollo y aceptación	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software PR-GTI-012 Procedimiento Control de Versiones de Software
8.30	Desarrollo tercerizado	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información - Política Adquisión de Software por áreas distintas a la OTIC MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software

No. CONTROL	CONTROL	DECLARACION DE APLICABILIDAD	
		SI/NO	
			PR-GTI-012 Procedimiento Control de Versiones de Software
8.31	Separación de entornos de desarrollo, pruebas y producción	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software PR-GTI-012 Procedimiento Control de Versiones de Software
8.32	Gestión de cambios	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información PR-GTI-002 Procedimiento de Gestión de Cambios de Seguridad de la Información
8.33	Información de las pruebas	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información MA-GTI-005 Manual Metodología de Desarrollo Seguro de Software PR-GTI-012 Procedimiento Control de Versiones de Software
8.34	Protección de los sistemas de información durante las pruebas de auditoría	SI	MO-GTI-001 Manual Operativo Políticas de Seguridad y Privacidad de la Información

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	12/12/2024	Creación del documento de acuerdo con los controles del “Anexo A” de la norma ISO 27001:2022.