POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

CENTRO DE DIAGNOSTICO AUTOMOTOR DE RISARALDA

DIAGNOSTICENTRO S.A.S.

2025

Contenido

1. INTRODUCCIÓN:

Para la gerencia de Diagnosticentro SAS, comprendiendo la relevancia de una correcta administración de la información, se ha comprometido a instaurar un sistema de gestión de seguridad de la información con el objetivo de crear un ambiente de confianza en la realización de sus responsabilidades con el Estado y los ciudadanos, todo esto enmarcado en el cumplimiento de las leyes y en consonancia con la misión y visión de la empresa.

2. OBJETIVO:

Establecer los lineamientos en Políticas de Seguridad tecnológica de Información y de Comunicaciones, permitiendo aplicar las condiciones de uso de los equipos de cómputo (Hardware) y los programas utilizados (Software), además de la información digital que reposa en cada uno de los equipos y servidores pertenecientes al Diagnosticentro S.A.S. Es decir, que se tiene como objetivo la salvaguarda de la información y así reducir el efecto producido en sus activos debido a los riesgos detectados de forma sistemática, con el fin de preservar un nivel de exposición que posibilite actuar por la integridad, privacidad y disponibilidad de la información, de acuerdo con las demandas de los distintos grupos de interés.

3. ALCANCE:

Esta política es aplicable a toda la entidad, sus funcionarios, contratistas y terceros que utilicen equipos de cómputo o dispositivos con acceso a la red interna y/o acceso a internet del Diagnosticentro S.A.S.

4. DEFINICIONES:

- **SOFTWARE:** Equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen

posible la realización de tareas específicas.

- **HARDWARE:** Todas las partes físicas de un sistema informático.
- **COPIA DE SEGURIDAD:** Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos o CD`s), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto.
- **RECUPERACIÓN:** Hace referencia a las técnicas empleadas para recuperar archivos a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.
- **RESTAURACIÓN:** Volver a poner algo en el estado inicial. Una Base de Datos se restaura en otro dispositivo después de un desastre.
- **COPYRIGHT:** El Copyright o los derechos de autor son una forma de ley de propiedad intelectual que concede a los autores, artistas e inventores derechos exclusivos sobre sus obras originales. Abarca tanto las creaciones publicadas como las no publicadas, incluidos libros, música, obras de arte, programas informáticos, fotografías, vídeos y otras obras creativas. La protección de los derechos de autor otorga a su titular el derecho a controlar el uso que otros hacen de su obra.
- **PORTALES P2P:** P2P es una red de ordenadores que tienen los mismos privilegios y las mismas funciones. En un modelo clásico cliente-servidor, los clientes hacen peticiones y el servidor las responde**.**

5. GENERALIDADES:

Los usuarios y empelados del Diagnosticentro S.A.S. deben de seguir con exactitud las políticas emitidas en el presente documento por parte de la Dirección Financiera Administrativa y/o personal de apoyo que se encarga de administrarlas.

Cabe resaltar que los usuarios y/o visitantes que hacen uso de la red inalámbrica

(WI-FI) que se encuentra disponible y abierta dentro de las instalaciones del Diagnosticentro S.A.S., lo harán bajo su propia responsabilidad. El Diagnosticentro S.A.S., no se hace responsable por el contenido consumido, software descargado y utilizado, aplicaciones e información que sea descargada o compartida a través de esta red.

Con el fin de minimizar el riesgo en las funciones más importantes de la entidad, el documento integra las políticas que se relacionan a continuación:

- Políticas para el uso adecuado de las Tecnologías de la Información y las Comunicaciones.
- Políticas de contraseñas.
- políticas de uso de internet, correo electrónico y administración de la página web.
- Políticas para el uso de Software.
- Política Institucional.
- Políticas de administración de acceso de usuarios del servidor en el proceso diagnóstico automotor.
- Políticas para el respaldo de la información.
- Políticas de mantenimiento de hardware y software.

Estas políticas tienen como objetivo salvaguardar y garantizar la integridad de la información de empleados, contratistas y la organización en general. Además, buscan optimizar la seguridad informática y aprovechar al máximo la tecnología disponible, lo cual impulsará la eficiencia operativa y asegurará la continuidad de la misma.

6. POLÍTICA PARA EL USO ADECUADO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN.

6.1. Generales.

- Bajo ninguna circunstancia, los usuarios del Diagnosticentro S.A.S., están autorizados a utilizar los recursos tecnológicos para realizar actividades

que contravengan las normativas vigentes o las leyes nacionales e internacionales aplicables.

- En Diagnosticentro S.A.S., la Gerencia y la Dirección Financiera Administrativa en coordinación con los jefes de proceso están facultados para realizar y/o autorizar tareas de asistencia técnica y modificaciones en los equipos informáticos de la institución. Cualquier tarea de mantenimiento realizada por terceros deberá ser notificada y autorizada tanto por la Dirección Financiera Administrativa como por el supervisor.
- En el caso que Diagnosticentro S.A.S., tome en arrendamiento equipos informáticos, la compañía arrendadora será la única responsable y está autorizada para llevar a cabo actividades de mantenimiento, modificación o actualización de hardware y software, o bien, para otorgar la autorización correspondiente para dichas tareas.

6.2. Equipos de cómputo.

- Los dispositivos electrónicos y equipos de cómputo que sean de propiedad del Diagnosticentro S.A.S. o bien, estén en arrendamiento, únicamente deberán ser utilizados para las tareas y actividades relacionadas con los objetivos y metas de la empresa.
- La Dirección Financiera Administrativa es responsable de la asignación y distribución de los equipos tecnológicos y de cómputo.
- La adquisición de equipos, materiales y/o servicios relacionados con las Tecnologías de la Información y la Comunicación (TIC) se llevará a cabo en estricto cumplimiento de los principios legales de contratación, conforme a lo establecido en el Manual de Contratación del Diagnosticentro S.A.S., este proceso se regirá por normativas vigentes que aseguren la transparencia, la eficiencia y la legalidad en todas las etapas de la contratación, garantizando que los recursos sean utilizados de manera adecuada y que las decisiones de compra se realicen de acuerdo con los procedimientos y directrices internas de la entidad.

- La Dirección Financiera Administrativa implementará las acciones y actividades preventivas necesarias para el correcto funcionamiento de los equipos de cómputo.
- En caso de que ocurra cualquier incidente (robo, pérdida, daño físico o virtual, entre otros) que afecte directamente a un equipo relacionado con las tecnologías de la información y la comunicación del Diagnosticentro S.A.S., se deberá notificar de manera inmediata a la Dirección Financiera Administrativa, con el fin de tomar las acciones correctivas pertinentes en el menor tiempo posible.
- Solo el personal designado por la Dirección Financiera Administrativa tiene la autorización exclusiva para realizar la apertura de computadores portátiles o cualquier otro equipo de cómputo que sea propiedad del Diagnosticentro S.A.S. Esta medida asegura que todas las intervenciones en los equipos sean realizadas por personal capacitado y autorizado, garantizando la integridad de los dispositivos. En el caso de los equipos de cómputo en arrendamiento, la empresa arrendadora es la única entidad autorizada para llevar a cabo la apertura de dichos equipos o, en su defecto, otorgar la autorización correspondiente para que se realice dicha operación, siempre siguiendo los protocolos de seguridad y mantenimiento establecidos.
- Todos los equipos de cómputo del Diagnosticentro S.A.S. deben contar con un software antivirus actualizado y un firewall, con el objetivo de proteger el equipo y su contenido de programas maliciosos.
- Todos los dispositivos electrónicos y de cómputo que se encuentren en la planta baja del Diagnosticentro S.A.S. deben de ser instalados a una altura aproximada de 80 cm por encima del suelo, con el fin de evitar daños en posibles inundaciones.

6.3. Centro de cómputo.

- El Centro de procesamiento de datos del Diagnosticentro S.A.S., está

diseñado para alojar los servidores y equipos de comunicación fundamentales para el funcionamiento de las actividades informáticas de la empresa. Este espacio especializado asegura la infraestructura tecnológica necesaria para el procesamiento, almacenamiento y transmisión de datos, permitiendo la operación eficiente y continua de los sistemas críticos que soportan los procesos internos de la entidad. Además, se garantiza la disponibilidad, seguridad y rendimiento de los recursos tecnológicos mediante un control adecuado y el mantenimiento constante de los equipos alojados en este centro.

- El acceso al centro de procesamiento de datos (centro de cómputo) y los equipos contenidos en el, es restringido y solo el personal autorizado por el Director Técnico y el Director Financiero Administrativo puede tener accesos a este.
- El acceso a los servidores del Diagnosticentro S.A.S. tanto a través de la consola de administración local como remota, está estrictamente restringido al personal autorizado por La Dirección Financiera Administrativa con personal de apoyo. Cualquier intento de conexión o ingreso no autorizado a cualquiera de las consolas de administración de los servidores o a su punto físico, será considerado una violación de las políticas de seguridad, lo que puede traer consigo las sanciones correspondientes según la normatividad vigente.

6.4. Propiedad de la información.

- Los datos que los empleados, contratistas o usuarios creen y/o manipulen en los sistemas de información, aplicativos o cualquier medio de procesamiento electrónico, durante el desarrollo normal de las actividades laborales diarias son propiedad y responsabilidad del Diagnosticentro S.A.S.
- Los derechos patrimoniales sobre los programas de computación, hojas de cálculo (como Excel), archivos elaborados en procesadores de texto

(como Word), presentaciones (como PowerPoint), macros y otros documentos, tanto locales como en línea, que sean creados por uno o varios usuarios en el marco de sus actividades laborales, pertenecen exclusivamente al Diagnosticentro S.A.S., esto incluye todas las creaciones desarrolladas durante el ejercicio profesional dentro del ámbito de la institución, sin importar el medio o la plataforma utilizada para su elaboración. Dichos derechos son transferidos automáticamente al Diagnosticentro S.A.S. al momento de su creación, en virtud de las actividades profesionales realizadas por los empleados o contratista.

6.5. Actividades no permitidas.

- Vulnerar los derechos de cualquier individuo o entidad protegidos por derechos de autor, patentes u otros derechos de propiedad intelectual, así como el uso no autorizado de archivos multimedia de cualquier tipo (como música y video) que no sean de propiedad del autor original.
- Distribución o instalación de cualquier tipo de software el cual no posea ningún tipo de licenciamiento de uso adecuado previamente adquirido por el Diagnosticentro S.A.S.
- Divulgar o transmitir datos clasificados como privados o confidenciales mediante el uso de tecnologías de la información, incluyendo, pero no limitándose a, correo electrónico, dispositivos de almacenamiento redes movibles, unidades flash (USB), o cualquier otro medio digital que permita la transferencia o almacenamiento no autorizado de dicha información, comprometiendo así su integridad y confidencialidad.
- Introducir software malicioso en la red o en los servidores (virus, worms, ráfagas de correo electrónico no solicitado, entre otros).
- Emplear la infraestructura tecnológica del Diagnosticentro S.A.S., con el propósito de obtener, distribuir o difundir material con fines lucrativos, ya sea de manera directa o indirecta, en contravención de las normativas, políticas internas y objetivos establecidos por la organización, lo que podría

comprometer la integridad de los recursos tecnológicos y violar los principios éticos y legales aplicables.

- Se prohíbe el uso de las Tecnologías de la Información y la Comunicación (TIC) del Diagnosticentro S.A.S. si esta va a ser empleada con el fin de realizar cualquier tipo de acoso cibernético, difamación, calumnia o cualquier forma de actividad hostil.
- Fomentar o promover productos o servicios fraudulentos cuyo origen o desarrollo esté vinculado a los recursos, herramientas o servicios proporcionados por el Diagnosticentro S.A.S., contraviniendo así las políticas internas y los principios éticos establecidos.
- Realizar actividades que vulneren la seguridad de los sistemas o que generen interrupciones de la red de datos o de los servicios prestados por el Diagnosticentro S.A.S.
- Monitorear puertos o realizar análisis del tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad. El contratista de apoyo en el área sistemas es el responsable de la Seguridad Informática puede realizar estas actividades siempre y cuando tenga la autorización por parte del Director Técnico y el Director Financiero.
- Ejecutar o instalar cualquier herramienta o mecanismo de monitoreo de la red de datos del Diagnosticentro S.A.S., de manera no autorizada.
- Eludir o manipular de manera intencionada los mecanismos de seguridad, autenticación, autorización o auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario, con el fin de obtener acceso no autorizado, modificar configuraciones o comprometer la integridad de los sistemas y servicios gestionados del Diagnostiocentro S.A.S.
- Interferir o interrumpir el acceso de usuarios autorizados a los servicios, con la intención de causar daños a la calidad de la prestación del servicio o afectar la reputación e imagen del Centro de Diagnostico Automotor de Risaralda (CDAR). Esto incluye, pero no se limita a, la ejecución de

ataques de denegación de servicio (DoS) u otras técnicas similares que busquen perturbar la disponibilidad de los recursos.

- Ésta restringido el uso de comandos o programas para el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).
- Instalar cualquier tipo de software en los equipos de cómputo de Diagnosticentro S.A.S. sin la previa autorización de la Dirección Financiera Administrativa o Dirección Técnica, incluyendo software de dispositivos móviles y teléfonos celulares.
- Modificar la configuración del software antivirus, firewalls o las políticas de seguridad implementadas en los equipos de cómputo del Diagnosticentro S.A.S. sin haber obtenido previamente la autorización de la Dirección Financiera Administrativa o la Dirección Técnica, quienes deberán evaluar y analizar la viabilidad de los cambios propuestos, asegurando que estos no comprometan la seguridad ni el funcionamiento adecuado de los sistemas.
- Queda estrictamente restringido compartir una carpeta con derecho a todos los usuarios. El contratista de sistemas puede cambiar permisos de recursos compartidos por los usuarios si detecta que éstos no cumplen con las mejores prácticas definidas en los lineamientos internos de seguridad.
- Descargar archivos de multimedia desde Internet.
- Ver, reproducir, compartir, divulgar, promover o cualquier otra actividad o contenido explícito relacionada con niños, niñas y adolescentes, que vulneren cualquiera de sus derechos.

6.6. Excepciones.

Para propósitos de mantenimiento de la red y de seguridad, algunos usuarios del CDAR, pueden estar exentos de seguir algunas de las restricciones anteriores, debido a las necesidades y responsabilidades de su cargo o a eventos

programados.

Estas excepciones deben ser solicitadas al Contratista de Sistemas, previa autorización del Director Financiero Administrativo o Director Técnico.

7. POLÍTICA DE CONTRASEÑAS.

7.1. Generales.

- Todos los usuarios del CDAR están obligados a contar con un nombre de usuario y una contraseña únicos para acceder al equipo de cómputo que les ha sido asignado, así como a los diferentes servicios de red disponibles, tales como correo electrónico, impresión, unidades de red, dispositivos de almacenamiento físico, archivos compartidos y acceso a Internet. La solicitud para la creación o modificación de estos accesos deberá realizarse de manera formal, enviando un correo electrónico a la dirección sistemas@diagnosticentrorda.com, dirigido al área de Sistemas, Dirección Operativa y Financiera. Dicho correo debe incluir la información necesaria para gestionar la solicitud, la cual será evaluada y procesada conforme a los procedimientos internos establecidos por el área de sistemas.
- El software especializado o sistema de información de la revisión Técnico-mecánica y de emisiones contaminantes debe contar con protección para el acceso al mismo mediante el uso de contraseñas. Este sistema solicita automáticamente el cambio de contraseña cada 30 días para el personal de pista, en el caso de la Dirección Técnica e ingeniero/a suplente este cambio debe realizarse en un tiempo no mayor a 20 días, los usuarios autorizados deben realizar este cambio para poder seguir ejecutando tareas dentro de dicho sistema de información. Este control se debe llevar en el “Formato Control de Contraseñas” Para el uso de estas contraseñas se debe seguir el requerimiento consignado en el numeral 4.16.2.1 de la NTC 5385. ((ICONTEC), 2010)

- Todas las contraseñas de los usuarios deben cumplir con estrictos requisitos de seguridad para garantizar su robustez y evitar que los usuarios seleccionen contraseñas vulnerables. Los requisitos de seguridad establecidos para las contraseñas son los siguientes:
  - **a.** La contraseña debe de tener como mínimo seis (6) caracteres alfanuméricos y especial.
  - **b.** La contraseña no puede estar relacionada con los datos del usuario, por ejemplo, números de teléfono, nombres, fechas de nacimiento… etc.
  - **c.** La contraseña no puede contener caracteres que estén en secuencia, consecutivos repetidos o que solo contenga letras o números.
  - **d.** Las contraseñas son personales y conocidas únicamente por el propio usuario el cual será responsable de toda la actividad que se realice con ella.
  - **e.** El Director Financiero y Director Operativo se reservan el derecho de restablecer en cualquier momento la contraseña de cualquiera de los usuarios del CDAR, con previo aviso para no afectar de ninguna manera la continuidad de sus funciones, si se detecta que ha sido comprometida.
  - **f.** Contraseñas bancos (investigar y crear apartado).

8. POLÍTICAS DEL USO DE INTERNET, CORREO ELECTRÓNICO Y ADMINISTRACIÓN DE LA PÁGINA WEB.

8.1. Administración.

Los servicios de acceso a Internet y correo electrónico son autorizados por la Dirección Financiera Administrativa y gestionados por el personal de apoyo en el área de sistemas, quien se encarga de recibir los informes sobre problemas técnicos y fallas del sistema para su evaluación y posible atención inmediata. No obstante, el proveedor del enlace a Internet es responsable de garantizar la

disponibilidad continua de la conexión, así como de asegurar que se cumplan los anchos de banda contratados. El encargado del área de TI tiene la autorización para monitorear de manera periódica las actividades de los usuarios que acceden a Internet y utilizan la Red de Datos del Diagnosticentro S.A.S. con el fin de asegurar el cumplimiento de las políticas establecidas en este documento, garantizando en todo momento la confidencialidad de la información procesada.

8.2. Correo electrónico.

- La comunicación institucional efectuada por medio de email, únicamente se realizará mediante las cuentas corporativas asignadas (usuario@diagnosticentrorda.com), a excepción de nuevas cuentas que se deben crear a través del correo de Gmail (usuario@gmail.com).
- El correo electrónico se considera como correspondencia privada entre el emisor y el destinatario. En este sentido, no podrá ser transmitida a través de Internet ninguna información considerada confidencial o sensible hacia personal externo al Diagnosticentro S.A.S. salvo que exista una instrucción expresa por parte de la Gerencia, el director Financiero Administrativo, o cuando sea estrictamente necesario para el desempeño de las funciones inherentes al cargo del remitente. Cualquier transmisión de información confidencial fuera del Diagnosticentro S.A.S. deberá ser cuidadosamente evaluada y autorizada de acuerdo con los procedimientos establecidos.
- Cada usuario es responsable del contenido de los mensajes enviados, especialmente en lo que respecta a la inclusión de material prohibido o sensible. Esto incluye, entre otros, contenido ofensivo, obsceno, material relacionado con la explotación infantil, cualquier violación de derechos de propiedad intelectual, copyright, o cualquier otra información que sea ilegal o que contravenga las leyes vigentes. Los usuarios deben asegurarse de que el contenido de sus comunicaciones cumpla con las normativas legales y las políticas internas del Diagnosticentro S.A.S.
- No está permitida la transmisión de mensajes que puedan crear un medio

hostil sobre la raza, edad, sexo, religión, política, nacionalidad, origen, incapacidad u orientaciones personales; comentarios despectivos, noticias informales o mal intencionadas, cadenas de cartas, mensajes masivos de índole personal, y en general cualquier tipo de información que cause congestión en la red o interfiera con el trabajo de otros funcionarios y/o contratistas.

8.3. Internet.

- Los empleados y contratistas del Diagnosticentro S.A.S. son responsables de mantener su imagen profesional durante la navegación en internet, con el fin de proteger la imagen y reputación del Centro de Diagnostico Automotor de Risaralda.
- Ningún empleado o contratista tiene acceso automático a Internet al conectarse a la Red del Diagnosticentro S.A.S. Para poder acceder a Internet desde un dispositivo distinto al asignado inicialmente, el usuario deberá solicitarlo formalmente a la Dirección Financiera Administrativa o a la Dirección Técnica. En caso de que la solicitud sea aprobada, el contratista de sistemas será responsable de realizar la configuración necesaria en el equipo del usuario y de asignar los privilegios adecuados para el uso del servicio, de acuerdo con las actividades específicas que el usuario deberá desempeñar. Esta medida asegura que el acceso a Internet se otorgue de manera controlada y conforme a las necesidades laborales.

8.4. Seguridad.

- El Director Técnico con el apoyo del personal de sistemas, es el encargado de realizar la configuración correspondiente de los servicios asignados a cada usuario, asegurando que se cumplan los requisitos técnicos y de seguridad establecidos por la organización para un correcto acceso y funcionamiento de estos.

- Las cuentas y claves de acceso de los servicios de internet y correo electrónico son personales y confidenciales y se rigen por las políticas de contraseñas definidas en el presente documento**.**
- El usuario notificará inmediatamente al Director Técnico cualquier uso no autorizado de su cuenta o posible intrusión de seguridad desconocida o sospechosa.
- El usuario está estrictamente obligado a utilizar los servicios proporcionados exclusivamente para fines institucionales, en conformidad con las políticas y directrices establecidas por la organización, y no para fines personales o ajenos a las actividades relacionadas con su función.
- Se prohíbe el acceso, descarga o transmisión de datos e información cuyo origen no sea comprobado como seguro o del cual no se tenga conocimiento del origen y por ende de su confiabilidad.
- Cualquier programa, documento, archivo obtenido a través de internet o correo electrónico debe tener una revisión previa a su utilización, por el software antivirus adquirido por el Diagnosticentro S.A.S.
- No deberá utilizarse el correo electrónico en suscripciones a listas que saturen la capacidad de almacenamiento de la bandeja de entrada y/o no tengan ninguna relación con los procedimientos del Diagnosticentro S.A.S.

8.5. Almacenamiento.

- Todos los datos generados, adquiridos o descargados desde cualquier servicio, deberán ser almacenados de manera local en el equipo del usuario, específicamente en la carpeta 'Mis Documentos'. Se debe evitar la distribución o transmisión de estos datos a través de la red institucional o en otras carpetas compartidas, salvo que sea necesario. En tales casos, el almacenamiento se realizará en la carpeta 'Pública', designada para este propósito.
- El área de almacenamiento “Publica” en la red, específicamente en el servidor, será tratada como de almacenamientos temporales. La dirección

Financiero Administrativo revisará el óptimo aprovechamiento de los recursos compartidos para mantener la integridad y asegurar que los usuarios utilicen estos recursos de manera responsable.

8.6. Propiedad y derechos de contenido.

- La información disponible en internet, que incluye imágenes, textos, programas, música, sonidos, fotografías, videos, gráficos y otros contenidos, está protegida por la ley de derechos de autor, marcas registradas, patentes y otras normativas relacionadas con la propiedad intelectual. Su utilización está permitida únicamente con la autorización expresa del titular de los derechos, de lo contrario no es permitido hacer cualquier uso de estas.
- Los usuarios tienen prohibido descargar ni instalar cualquier tipo de software, ya sea comercial, de código abierto (opensource), shareware, freeware, aplicaciones de pago o gratuitas, así como controladores para dispositivos externos, en las unidades de disco, unidades externas o en cualquier otro medio de almacenamiento del equipo de cómputo, sin la debida autorización previa. Esta medida busca garantizar la seguridad y el cumplimiento de las políticas internas de la organización.

8.7. Conducta del usuario.

- El usuario (empelado y/o contratista) del Diagnosticentro S.A.S. es el único responsable del contenido de transmisiones a través de cualquier servicio.
- El usuario (empelado y/o contratista) del Diagnosticentro S.A.S. tiene la obligación de acatar las normativas de transmisión de información técnica desde los cuales y hacia los cuales se envían los mensajes de correo electrónico.
- El usuario (empelado y/o contratista) del Diagnosticentro S.A.S. no debe usar el servicio para propósitos ilegales o de entretenimiento.
- El usuario (empelado y/o contratista) del Diagnosticentro S.A.S. debe cumplir con todas las regulaciones, políticas y procedimientos de internet.

- La interacción con los usuarios (empelado y/o contratista) del Diagnosticentro S.A.S. debe realizarse de manera respetuosa y considerada, promoviendo un ambiente de cordialidad y colaboración, y evitando cualquier forma de abuso o el uso de un lenguaje inapropiado.
- Se prohíbe el acceso a cualquier fuente de información cuyo contenido no se encuentre relacionado con las actividades del Diagnosticentro S.A.S. o con las actividades del funcionario o contratista.

8.8. Administración y contenido de la página web.

La administración de la página web será ejercida por el personal de apoyo a la gestión bajo la supervisión del Director Financiero Administrativo y del Director Técnico.

8.8.1. Responsabilidades del administrador del sitio web.

- Administrar en contenido publicado en el sitio web.
- Actualizar los precios de los servicios o productos ofrecidos por el Diagnosticentro S.A.S.
- Publicar y actualizar en la página los contenidos solicitados por los jefes de proceso y representante legal.
- Verificar la disponibilidad de la página en el momento que sea solicitada.
- Verificar la veracidad del contenido publicado en el sitio web.

8.8.2. Actividades no permitidas.

- La promoción y/o publicidad de servicios que puedan afectar la imparcialidad del organismo de inspección del Diagnosticentro S.A.S.
- Publicar contenido sin autorización previa del supervisor del contrato.
- Publicar contenido que pueda afectar a terceros.
- Publicar contenido explícito o con lenguaje ofensivo.

9. POLÍTICAS DE USO DE SOFTWARE.

9.1. Política de administración.

El personal de apoyo a la gestión, en estrecha colaboración y bajo la supervisión directa del interventor del contrato, es el único con la autorización para llevar a cabo la administración de cualquier software que se necesite en el Diagnosticetro S.A.S. Esta responsabilidad exclusiva implica la gestión integral de todas las operaciones relacionadas con el software, asegurando su correcto funcionamiento, mantenimiento y actualización, conforme a las políticas y normativas establecidas. Dentro de sus responsabilidades se incluyen:

- Mantener bajo resguardo las licencias de uso de software.
- Llevar un control exacto de las licencias en operación y el equipo en el cual se encuentra en uso.
- Establecer políticas y lineamientos para el uso de software, previa aprobación por parte del Gerente y/o el director financiero Administrativo.
- Organizar la inspección de los equipos de cómputo en intervalos regulares.
- Difundir a los usuarios internos las Políticas de Uso de Software con el fin de que conozcan la normatividad.

9.2. Política de instalación.

El personal de apoyo a la gestión de Sistemas es la única persona autorizada y responsable de llevar a cabo la instalación del software, así como de proporcionar soporte técnico relacionado, en todos los equipos de cómputo del Diagnosticentro S.A.S. tanto aquellos de propiedad como los de arrendamiento. Esta responsabilidad incluye la correcta implementación, configuración y mantenimiento del software en los equipos mencionados, asegurando su adecuado funcionamiento y el cumplimiento de los estándares técnicos establecidos**.**

Esta responsabilidad abarca equipos de cómputo:

- De Escritorio (propiedad del CDAR y arrendados).
- Portátiles (propiedad del CDAR y arrendados).
- Ubicados en otras dependencias.
- De propiedad personal de los usuarios del CDAR.

El personal de apoyo a la gestión de Sistemas se compromete a instalar y proporcionar soporte técnico para el software, o, en su defecto, a orientar y supervisar el proceso de instalación, con el objetivo de asegurar que el sistema quede en pleno funcionamiento y en las mejores condiciones operativas posibles.

9.3. Software Institucional.

De acuerdo con las existencias actuales de software, se establecerá un estándar para su uso en las diversas áreas del Diagnosticentro SA.S. Cada equipo informático, antes de ser entregado al usuario final por parte del personal de apoyo a la gestión de Sistemas, contará con el software esencial para el desempeño adecuado de sus funciones. Adicionalmente, se dispone de software complementario que facilita la realización de las tareas específicas de los empleados y de los equipos dentro de la compañía.

9.3.1. Condiciones bajo las que puede utilizarse Software adicional:

- Software “preinstalado”
- Software proporcionado por el personal de apoyo a la gestión de sistemas con el fin de:
  - **a.** Realizar actualizaciones remotas.
  - **b.** Actualizar software preinstalado.
  - **c.** Sustituir software preinstalado.
  - **d.** Accesos o componentes de software instalados en los servidores de información.
  - **e.** Software de uso temporal (previo análisis de disponibilidad de licencia).
  - **f.** Software proporcionado por el personal de apoyo a la gestión de Sistemas a través de la intranet o por medios no directos (Instalaciones no asistidas).
- Software de Soporte o Complementario: Se entiende por este tipo de software aquel que es propiedad de entidades gubernamentales (como ministerios, organismos de control, entre otros) y que debe ser

instalado para garantizar la correcta ejecución, en tiempo y forma, de las actividades asignadas a los usuarios.

9.3.2. Software que no puede ser instalado:

- Copias ilegales de cualquier programa.
- Software descargado de Internet.
- Software que no se haya identificado como perteneciente al Diagnosticentro S.A.S.
- Instalaciones no autorizadas o no solicitadas al personal de apoyo a la gestión de sistemas.
- Software adquirido para uso personal del usuario (sin fines institucionales).
- Software de entrenamiento o esparcimiento.
- Software de dispositivos móviles de uso personal.

9.3.3. Licenciamiento:

El software institucional está debidamente protegido por las licencias de uso correspondientes, con la excepción de aquellas aplicaciones de código abierto que estén destinadas a fines institucionales. Estas licencias requieren un proceso formal de adquisición y registro para su correcta implementación y cumplimiento legal.

El Director Financiero Administrativo con el personal de apoyo a la gestión de sistemas tiene la responsabilidad de mantener actualizada toda la información relacionada con las licencias de software. Para cumplir con este objetivo, se compromete a garantizar la disponibilidad continua, la correcta posesión y la adecuada conservación de las licencias asociadas al software, asegurando que estén debidamente registradas y operativas.

9.3.4. Requerimientos del Software.

Todo usuario que necesite la instalación de un software específico en su equipo deberá presentar la solicitud al personal de apoyo a la gestión de sistemas. Este evaluará, en función de las características del software

gestionado, la disponibilidad de licencias para satisfacer la solicitud. En caso de no contar con licencias disponibles, procederá a realizar la solicitud correspondiente para su adquisición.

10. POLÍTICA INSTITUCIONAL.

La utilización de cualquier software sin licencia es ilegal y puede poner al Diagnosticentro S.A.S. en peligro civil y criminal bajo las normativas del Derecho de Autor. Por ende, el Diagnosticentro S.A.S. no autorizará el uso de software sin licencia o no autorizado por ningún usuario. De igual forma, cualquier usuario que sea detectado copiando software o información de forma ilegal o que copie software o información para suministrarlo a cualquier tercero fuera del Diagnosticentro S.A.S. incluyendo a los clientes, será penalizado conforme a las circunstancias y la normatividad vigente.

11. POLÍTICA PARA EL RESPALDO DE LA INFORMACIÓN ELECTRÓNICA.

11.1. Aspectos generales.

- El personal de apoyo a la gestión informara al responsable de cada equipo cómo funciona el programa que realiza las copias de respaldo, la ruta y el horario establecido en el documento itinerario copias de seguridad.
- Las copias de seguridad se realizarán diariamente, semanalmente o de forma mensual según cada caso en particular.
- La información de los archivos contenidos en las copias de seguridad debe ser única y exclusivamente de uso institucional y no personal.
- En caso de requerirse la inclusión o modificación de un servicio de copia de respaldo debe ser solicitada para su revisión, aprobación e implementación.
- Semanalmente se verificarán las copias comprimidas, para comprobar que se pueden restablecer cuando se necesiten.
- En caso de que algún funcionario necesite copias de sus archivos

almacenados en el servidor de copias, esta petición debe ser requerida al contratista de sistemas.

- Se deben realizar copias de respaldo de toda la información esencial del servidor de las pistas. Para asegurar que todo se pueda recuperar tras un desastre o un fallo de los soportes, se tendrán dispositivos de respaldo adecuados.

11.2. Copias de seguridad informática.

- El personal de apoyo a la gestión de sistemas creará una carpeta en los discos duros externos y en el equipo de publica (el computador) donde se almacenará dicha información.
- El personal de apoyo a la gestión de sistemas verificara que las copias de seguridad enviadas por cada uno de los funcionarios, sea generada correctamente por el programa.
- Para el registro de la realización de las copias de seguridad, y verificación de las respectivas pruebas de respaldo, El personal de apoyo a la gestión de sistemas debe diligenciar periódicamente el formato GA.24.7.2 **“Formato Control de Copias de Seguridad”.**
- Almacenar un nivel mínimo de información de respaldo, junto a los registros exactos y completos de las copias de seguridad y procedimientos documentados, en una unidad de disco en el mismo servidor.
- En caso de daños por un desastre en la locación del servidor; diariamente se respaldarán desde el servidor de pista, las copias de los días anteriores en un servidor externo en la nube.
- Se debe realizar pruebas a los respaldos periodicamente para asegurar que son fiables en caso de necesitar su uso en caso de emergencia este debe quedar registrado en el formato GA.24.7.1 **“Formato Control de Copias de Seguridad Servidores”.**
- Se puede verificar las copias de respaldo del servidor de pista siguiendo los pasos que se encuentran en el manual del Software de pista TECNI-

RTM en el ítem **"Instructivo para la realización y verificación de las copias de seguridad de tecni-rtm."**

11.3. Restauración de copias de seguridad.

En caso de que algún funcionario necesite la restauración de un archivo almacenado en el servidor como copia de respaldo, deberá presentar una solicitud, especificando la información o los archivos requeridos. Esta solicitud será evaluada y, en caso de ser procedente, se procederá con la restauración correspondiente, siempre y cuando se cumpla con los requisitos establecidos en el procedimiento. El personal de apoyo a la gestión de sistemas deberá seguir los pasos detallados en el "Plan de Contingencia Informática" asegurando que todo el proceso se realice de acuerdo con las normativas de seguridad y los lineamientos establecidos para garantizar la integridad y disponibilidad de la información.

12. POLÍTICAS DE MANTENIMIENTO DE HARDWARE Y SOFTWARE.

Todos los equipos de cómputo de la empresa deben ser incorporados en un programa de mantenimiento preventivo y correctivo, el cual debe ser cuidadosamente planificado y registrado en el formato "Cronograma de Mantenimiento".

Este cronograma debe contemplar las actividades necesarias para garantizar el correcto funcionamiento de los equipos, asegurar su disponibilidad continua y preservar su integridad a lo largo del tiempo. La implementación adecuada de este programa permitirá detectar y corregir posibles fallos antes de que afecten el rendimiento de los sistemas, minimizando así tiempos de inactividad y garantizando la eficiencia operativa del Diagnosticentro S.A.S.

- El mantenimiento preventivo de los equipos debe ser realizado al menos 2 veces al año y estar sometidos a un mantenimiento regular (limpieza general, verificación de estado de conexiones, verificación de actualizaciones) al menos una vez por mes.

- El mantenimiento será realizado en las instalaciones de la empresa (los equipos no deben ser retirados de las instalaciones físicas) a excepción de los equipos que requieran intervención externa, el cual deberá contar con la respectiva autorización de salida, y se llevara a cabo solo por el personal de mantenimiento contratado para tal fin.
- Los equipos deben de contar con una hoja de vida en la que El personal de apoyo a la gestión de sistemas debe registrar la información general del equipo, el software instalado con el registro de las respectivas licencias y el historial de labores desarrolladas durante los mantenimientos realizados.

13. DISPOSICIONES ADICIONALES PARA EL HARDWARE Y SOFTWARE DEL ORGANISMO DE INSPECCIÓN VEHICULAR.

13.1. Conexiones de red.

De acuerdo con lo estipulado en la Resolución 3768 del 26 de septiembre de 2013 del Ministerio de Transporte, que establece como requisito obligatorio la conectividad con el Registro Único Nacional de Tránsito (RUNT), y considerando que dicha conexión se realiza a través de un acceso a Internet, se prohíbe expresamente la navegación libre en Internet desde el equipo servidor Tecni-RTM. Esta medida tiene como objetivo principal evitar la descarga de información que pueda contener software malicioso, protegiendo así la seguridad y el correcto funcionamiento de los sistemas involucrados en el proceso.

13.2. Administrador de la Base de Datos.

Se prohíbe el uso de dispositivos de almacenamiento externo en los equipos de revisión y en el servidor. En caso de que sea necesario el uso de dichos dispositivos, recae sobre el usuario administrador la responsabilidad de ejecutar las acciones pertinentes para identificar la presencia de software malicioso. Asimismo, deberá tomar las medidas adecuadas para mitigar cualquier riesgo potencial y prevenir la pérdida de información, asegurando la integridad y seguridad de los sistemas.

14. OTRAS DISPOSICIONES.

- Diagnosticentro S.A.S. es responsable de la gestión de toda la información obtenida o generada durante las actividades de inspección, en el marco de los compromisos legales aplicables. El organismo de inspección deberá informar al cliente con antelación sobre cualquier información que tenga la intención de hacerse pública. Con excepción de la información de aquellos casos en los que se haya acordado previamente entre el organismo de inspección y el cliente (por ejemplo, para dar respuesta a quejas), toda otra información deberá ser considerada confidencial, de acuerdo con la ley 1581 del 2012, conocida como la norma colombiana que establece las disposiciones generales para la protección de datos personales.
- Cuando el organismo de inspección deba por ley divulgar información confidencial o cuando esté autorizado por compromisos contractuales, el cliente o la persona correspondiente debe ser notificado acerca de la información proporcionada, salvo que esté prohibido por ley.
- Los funcionarios de Diagnosticentro S.A.S. tienen estrictamente prohibido utilizar el nombre y/o la información del OEC en sus redes sociales con el objetivo de obtener beneficios económicos o realizar cualquier tipo de negociación con terceros. Esta medida tiene como finalidad preservar la integridad y la reputación de la empresa, así como evitar el uso indebido de información confidencial o sensible en plataformas públicas para fines personales o comerciales.

15. VIGENCIA DE LAS POLÍTICAS.

Estas políticas tendrán vigencia a partir de su divulgación y serán revisadas y aprobadas y modificadas por el Comité Institucional de Gestión y Planeación MIPG.

16. BIBLIOGRAFÍA

(ICONTEC), I. C. (2010). *NTC 5385.* Bogota DC. Obtenido de https://www.runt.gov.co/sites/default/files/normas/NTC%205385%20de%202010%2

0RTMyEC%20en%20CDA.pdf

17. REFERENCIAS.

- **Resolución 3768 del 26 de septiembre de 2013**: Por la cual se establecen las condiciones que deben cumplir los Centros de Diagnóstico Automotor para su habilitación, funcionamiento y se dictan otras disposiciones
- **ISO 27001**: Guía de implementación de sistemas de gestión de seguridad de la información.
- **Artículo 162623**: Modelo de Seguridad y Privacidad de la Información.
- **Artículo 150520**: Elaboración de la política general de seguridad y privacidad de la información.
- **Decreto 620 de 2020**: establecen lineamientos para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en las entidades públicas.
- **Constitución Política de Colombia (artículo 15):** Reconoce el derecho fundamental a la intimidad y al buen nombre, y obliga a las entidades públicas a garantizar la protección de la información personal.
- **Ley 1581 de 2012 – Protección de Datos Personales:** Establece disposiciones generales para el tratamiento de datos personales y exige a las entidades públicas implementar medidas de seguridad para proteger la información.
- **Ley 1712 de 2014 – Transparencia y Acceso a la Información Pública:** Obliga a las entidades a garantizar la seguridad, integridad y disponibilidad de la información pública que administran.

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
01	2025/11/25	Se adopta el documento mediante la resolución 069 de noviembre de 2025 y se incorpora al SG Con la adopción de la presente política, el **Procedimiento GA.24.7 "Procedimiento Seguridad Informática", revisión 05 de 2022 de febrero 21**, pierde vigencia y queda sin efecto dentro del Sistema de Gestión de la entidad.