1. OBJETIVO:

Establecer las actividades que se deben realizar por cambio o actualización del software de revisión técnico mecánica y análisis de emisiones contaminantes, para cumplir con los requisitos exigidos por la ISO/IEC 17020:2012, CEA 4.1-01V3 y Normas Técnicas Colombianas NTC 5375:2012, NTC 5385:2011, NTC 4983:2012, NTC 4231:2012, NTC 5365:2012 y Resoluciones emitidas por el Ministerio de Transporte para el manejo de la información recogida y generada en los procesos de inspección.

2. ALCANCE:

Este procedimiento aplica para el software que se utiliza en el CDA en la realización de la revisión técnico mecánica y análisis de emisiones contaminantes de los vehículos automotores.

3. DEFINICIONES Y ABREVIATURAS:

Cambio: acción o efecto de cambiar.

Actualizar: Se designa con el término actualizar a aquella tarea o actividad que supone la puesta al día de algo que por alguna razón se atrasó.

4. MARCO LEGAL:

- ISO 17020 de 2012.
- CEA 4.1 V3
- NTC 5375
- NTC 5385

5. RESPONSABILIDADES.

Supervisor Técnico:

- **Responsabilidad**: Asegurar que el software del equipo de diagnóstico sea validado de manera adecuada, garantizando que cumple con los requisitos de precisión, confiabilidad e imparcialidad.

- **Tareas**: Supervisar que los procedimientos de validación sigan las pautas establecidas, verificar que el software esté correctamente documentado y mantenga trazabilidad.

Jefe de pista /Jefe de pista suplente:

- **Responsabilidad**: Realizar las pruebas de validación del software, siguiendo los métodos y procedimientos aprobados.

- **Tareas**: Ejecutar las pruebas específicas del software, asegurando su correcto funcionamiento y actualización.

6. PROCEDIMIENTO POR CAMBIO O ACTUALIZACIÓN SOFTWARE DE INSPECCIÓN:

1. Los funcionarios encargados de la validación del software de inspección, por cambio o actualización serán el jefe de Pista y Coordinador de Calidad.

2. Para realizar la validación del software de inspección se utilizará el formato Validación software, donde se definen todas las actividades que se deben realizar.

3. Para la validación se realizarán videos, fotos e impresión de pruebas simuladas para verificación en FUR.

En general los pasos que en el formato se definen son:

- Validación recepción
- ISO IEC 17020:2012, CEA-3.0-01 V4
- Validación gases NTC 4983:2012, NTC 4231:2012, NTC 5365:2012
- Validación NTC 5385:2011 en lo referente al software de inspección.
- Validación Resolución 0762 de 2022
- Validación sensorial NTC 5375:2012
- Resolución 3625 de 2020

Para la validación de esta norma, se tendrán en cuenta las siguientes acciones:

- Validación suma de más de dos exploradoras: Con el software de inspección se realizarán pruebas simuladas realizando revisión a vehículos que cuenten con más de dos exploradoras, el software de inspección permite realizar suma hasta de seis exploradoras, se tomara un patrón con un valor especifico y en el FUR se verificara que este valor se sume según el número de exploradoras, más las luces bajas y altas según corresponda, si son independientes o simultaneas, se realizaran pruebas para dos exploradoras, cuatro exploradoras y seis exploradoras, verificando en el FUR los resultados.

- Validación de los cálculos del resultado final de emisiones contaminantes en motocicletas con doble tubo de escape, cumpliendo con la corrección de oxígeno solicitada por la NTC 5365:2012 y Resolución 910 de 2008: Se realizara un prueba simulada con una motocicleta con doble tubo de escape, verificando en el FUR que el software realice la corrección de oxigeno con los valores más altos registrados en las pruebas de los dos escapes, se anexa archivo buffer generado por el software y registro en FUR de los

resultados, se realiza la aplicación de la fórmula matemática según NTC 5365:2012 con los valores del archivo buffer y se verifica en FUR que sean los mismos valores que aparecen según análisis.

- Verificar que diferencia aritmética existe entre ciclos de aceleración en la prueba de opacidad de acuerdo a la corrección Beer Lambert aplicada: Se realizara una prueba simulada utilizando lentes de opacidad que nos den como resultado una diferencia aritmética entre prueba y prueba de más del 5%, más del 10% y entre el 5% y 10%, valores registrados en el FUR, para verificar que el software de inspección realiza una diferencia aritmética del 5% entre pruebas, por manejar un LTOE estándar de 215 mm, ya que no se han verificado diámetros de escapes mayores a este valor (215 mm).

- Verificar como el aplicativo realiza los cálculos entre los ciclos de aceleración de la prueba de opacidad, promedios últimos tres ciclos: Se realiza una prueba simulada de un vehículo Diesel y con los valores registrados en el FUR (últimos tres ciclos de aceleración) se verificará que el resultado final sea el promedio de estos valores, se aplica formula.

  - Validación luces NTC 5375:2012

- Teniendo en cuenta un patrón establecido, se realizarán pruebas simuladas para la verificación de las luces, datos que se verificaran en los FURES impresos, se realizaran pruebas para bajas, altas y exploradoras en forma independiente y simultánea, donde se verifica la suma de luces bajas, altas y exploradoras en forma independiente y simultánea.

- Validación FUR Resolución 3625 de 2020: verificar los códigos que emite el software al realizar las diferentes pruebas de análisis de emisiones contaminantes según lo exigido por la Resolución 3625 de 2020; realizando prueba simuladas se registraran todos los defectos que aparecen en esta resolución, revisando el código que aparecen en los FUR y comparándolos con los códigos de la Resolución 3625, para verificar que el software de inspección cumple con lo exigido en esta documento, se revisaran los defectos de las condiciones anormales para las pruebas de análisis de gases para vehículos accionados con gasolina, Diesel y motocicletas, que el software cumpla con lo definido en la Resolución.

También se realizarán las siguientes actividades:

- Capacitación manejo nuevo software de inspección a través del proveedor del software a todos los funcionarios involucrados en los procesos de inspección de vehículos; directores técnicos, Inspectores de Línea, Personal de Pre revisión, Auxiliar Operativo.
- Realización capacidad efectiva de revisión con el nuevo software de inspección.
- Calibración o verificación de los equipos definidos por la empresa como de influencia significativa en los procesos de inspección, con el nuevo software instalado.

En el formato se definen los requisitos que cada norma exige, y al frente de cada columna se especifica la evidencia de cómo se valida el software, con video, foto o mediante el registro en FUR.

El jefe de Pista en conjunto con el Coordinador de Calidad, verificaran punto por punto en cada tabla como el software de inspección por cambio o actualización cumple con todos los requisitos ahí exigidos, realizando videos de inspecciones simuladas, o fotos, o con registro de los resultados de las pruebas.

La revisión del software se debe realizar cada vez que se generen actualizaciones por parte del proveedor ya sea por actualizaciones internas o por disposiciones legales y cambios normativos aplicables a los CDA, se debe comprobar que los cambios realizados no afectan el funcionamiento del software y que dichos cambios normativos se aplican. Cada cuatro meses el Jefe de Pista en conjunto con el Coordinador de Calidad realizarán verificación del funcionamiento del software de inspección, realizaran a través de muestras aleatorias como el software cumple con las normas de inspección, tomarán puntos aleatorios de las normas o resoluciones y verificaran con pruebas simuladas, videos o fotos que el software de inspección sigue cumpliendo con lo exigido por estas normas; NTC 5375:2012, NTC 5385:2011, NTC 4983:2012, NTC 4231:2012, NTC 5365:2012, Resolución 3625 de 2020.

1. Documentos:

PR1-GS1-FT1_ Validación software

Elaborado:	Revisado:	Aprobado:
Firma en original	**Firma en original**	**Firma en original**
Supervisor Técnico	Control Interno	Gerente

Registro de Cambios:

FECHA	VERSION	DESCRIPCION
Octubre 16 de 2020	01	Creación
2024-05-14	02	Actualización: Validar software cada vez que se realiza una actualización o cambio normativo.
2025-07-10	03	Modificación de codificación documento

1. OBJETIVO.

Garantizar la continuidad de las operaciones de los elementos considerados críticos para el Centro de Diagnostico Automotor, definiendo acciones y procedimientos a ejecutar en caso de fallas en los servicios de la organización.

2. ALCANCE.

Este plan cubre los procesos que se ejecutan dentro del Centro de Diagnostico Automotor de Nariño, concentrándose en el personal administrativo, operativo y clientes, así mismo cubre los equipos tecnológicos (hardware y software).

3. DEFINICIONES Y ABREVIATURAS.

CDA: Centro de Diagnóstico Automotor.
SGC: Sistema de Gestión de Calidad.
Confidencialidad: Garantía de que la información solo es accesible por personal autorizado.
Integridad: Precisión y completitud de la información.
Disponibilidad: Acceso oportuno a la información cuando sea requerido.
Autenticación: Validación de identidad de un usuario antes de acceder a la información.
Backup: Copia de seguridad de datos
RIESGO: Proximidad de un daño
ERROR: Acción desacertada o equivocada
VIRUS: Programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, destruye total o parcialmente la información almacenada.

4. MARCO NORMATIVO.

NTC ISO/IEC 17020:2012 – Requisitos para el funcionamiento de diferentes tipos de organismos que realizan inspección.
NTC 5385:2017 – Centros de Diagnóstico Automotor.
NTC 5375:2012 – Inspección técnico-mecánica y de emisiones contaminantes.
Decreto 1079 de 2015 – Sector Transporte.
Ley 1581 de 2012 – Protección de datos personales.
Decreto 1377 de 2013 – Reglamenta la protección de datos.
Ley 1273 de 2009 – Delitos informáticos.

5. RESPONSABILIDADES

Cargo /Rol	Responsabilidades
GERENTE	- Aprobar la política y recursos de seguridad de la información.
SUPERVISOR TÉCNICO	- Implementar y mantener este procedimiento. - Monitorear incidentes y coordinar acciones correctivas.
TODO EL PERSONAL	- Cumplir con las políticas de seguridad de la información. - Reportar incidentes o anomalías.

6. PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN.

6.1 Control de la Información.

6.1.1 Identificación y Clasificación de la Información.

- Información confidencial: datos de clientes, certificados de inspección, reportes RUNT.
- Información de uso interno: procedimientos, registros de inspección, formatos.
- Información pública: avisos legales, material de divulgación.

6.1.2 Controles de Acceso.

- Cada usuario tendrá un usuario y contraseña individual para acceso a sistemas.
- Contraseñas deberán renovarse cada 90 días.
- Se aplicará el principio de mínimo privilegio: solo acceso a lo necesario para cumplir funciones.
- El acceso a servidores y equipos críticos será restringido al personal autorizado.

6.1.3 Seguridad Física

- Áreas de servidores y archivos físicos deben contar con acceso controlado y registros de ingreso.
- Documentos físicos confidenciales deberán almacenarse en archivadores con llave.
- Visitantes deben registrarse y estar acompañados en todo momento.

6.1.4 Seguridad Lógica e Informática

- Se implementarán firewalls, antivirus y software de seguridad actualizado.

- Respaldo automático de información mínimo 1 vez al día en servidores locales y nube segura.
- Cifrado de información sensible en tránsito y almacenamiento.
- Bloqueo automático de equipos tras 10 minutos de inactividad.

6.1.5 Protección de Datos Personales.

- Cumplimiento de la Ley 1581 de 2012.
- Consentimiento informado para uso de datos de clientes.
- Eliminación segura de información cuando ya no sea necesaria.

6.1.6 Reporte y Gestión de Incidentes.

- Todo el personal deberá reportar incidentes de seguridad (pérdida de datos, accesos indebidos, fallas de sistema) al Coordinador de Calidad.
- Se registrarán en el Formato bitácora de fallas de Seguridad de la Información (PR2-GSI-FT2).
- Se analizará la causa raíz y se implementarán acciones correctivas.

6.2 SITUACIONES PROBABLES QUE PUEDEN AFECTAR LOS EQUIPOS TECNOLÓGICOS E INFORMACIÓN Y ACCIONES CORRECTIVAS

6.2.1 Error físico de disco de un servidor.

Dado el caso crítico que el disco presenta fallas, tales que no puede ser reparada, se deben tomar las acciones siguientes:

a. Ubicar el disco malogrado.
b. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de cada proceso.
c. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
d. Bajar el sistema y apagar el equipo.
e. Restaurar el ultimo backup en el disco, seguidamente restaura las modificaciones efectuadas desde esa fecha a la actualidad.
f. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
g. Habilitar las entradas a los sistemas para los usuarios

6.2.2 Error en la memoria RAM.

Dado el caso se den los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de procesos o por no rendir ante el ingreso máximo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la empresa, a menos que la dificultad apremie cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

a. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y/o teléfono al jefe del proceso.
b. El servidor debe estar apagado, dando un correcto apagado del sistema.
c. Ubicar las memorias malogradas.
d. Retirar la conexión del servidor con el concentrador, esta se ubica detrás del servidor, ello evitara que, al encender el sistema, los usuarios ingresen.
e. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
f. Probar los sistemas que están en red en diferentes estaciones.
g. Finalmente, luego de los resultados, habilitar las entradas al sistema para los usuarios.

6.2.3 Error de tarjeta (s) controladora (s) de disco.
Al presentar esta falla se deben de ejecutar las siguientes acciones:

a. Avisar a los usuarios que deben de salir del sistema, utilizar mensajes por red y/o teléfono al jefe de proceso.
b. El servidor debe estar apagado, dando un correcto apagado del sistema.
c. Ubicar la posición de la tarjeta controladora.
d. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
e. Retirar la conexión del servidor con el concentrador, esta se ubica de tras del servidor, ello evitara que al encender el sistema los usuraos ingresen.
f. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
g. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

6.2.4 En caso de incendio.
En el momento que se de aviso de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información.

Se deberá tener en cuenta:

a. Ante todo, se recomienda conservar la serenidad. Es obvio que en una situación de este tipo impera el desorden, sin embargo, es muy recomendable tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
b. En ese momento cualquiera que sea (n) en (los) proceso (s) que se esté (n) ejecutando en el computador, se deberá enviar un mensaje (si el tiempo lo permite) de “salir de red y apagar el computador”, seguidamente digitar DOWN en el (los) servidor(es).
c. Se apagará (poner en OFF) la caja principal de corriente de la empresa.
d. Tomando en cuenta de que se trata de un incendio de mediana o mayor magnitud se debe tratar en lo posible de trasladar fuera del área el (los) servidor (es) y demás computadores de acuerdo a la importancia de su contenido, dependiendo de su señalización y etiquetado, se abandonara las instalaciones en forma ordenada, lo mas rápido posible, por las salidas destinadas para ello (vías de evacuación).

6.2.5 En caso de inundación.

En caso de inundaciones se deben ejecutar las siguientes acciones:

a. Si los equipos se encuentran instalados a una altura menor de 20cm se deberá colocar en una parte alta, de esta manera evitaremos inconvenientes con lo referido.
b. Proveer cubiertas protectoras para cuando el equipo este apagado dado el caso de que se obvio una conexión que esta a ras del piso se debe modificar su ubicación.
c. Se debe trata en lo posible de trasladar el servidor fuera del área inundada de acuerdo a la importancia de su contenido, dependiendo de su señalización y etiquetado

6.2.6 En caso de fallas de fluido eléctrico.

Se puede presentar lo siguiente:

a. Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.
b. Para el caso de apagón se mantendrá la autonomía que la UPS nos brinda hasta momento que la planta eléctrica sea activada.

6.2.7 En caso de un error lógico de datos.

La ocurrencia de errores en los sectores del disco duro del servidor puede verse a una de las siguientes causas:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.

- Fallas causadas usualmente por un error de cheque de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente, se deben realizar las siguientes acciones:

a. Verificar el suministro de energía eléctrica, en caso de estar conforme, proceder con el encendido del servidor de archivos.
b. Deshabilitar el ingreso de usuarios al sistema.
c. Descargar todos los volúmenes del servidor, a excepción del volumen raíz, reencontrarse este volumen con problemas, se deberá descargarlo también
d. Cargar un utilitario que nos permita verificar en forma global el contenido del (os) disco (s) duro (s) del servidor.
e. Al término de la operación de reparación se procederá a habilitar entradas a estaciones para el manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

6.2.8 En caso de virus.
Dado el caso crítico que se presente virus en las computadoras se procederá lo siguiente:

6.2.9 Virus en los servidores.
a. Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo aun directorio para su futura investigación.
b. El antivirus muestra el nombre del archivo infectado.
c. Estos archivos serán reemplazados del cd de instalación o del backup.
d. Si los archivos infectados son aislados y aun persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la causa de la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

6.2.10 Virus en computadores fuera de red.
De suceder que una computadora se haya infectado con uno o varios virus ya sean en la memoria o a nivel de disco duro se debe proceder a realizar los siguientes pasos:

a. Utilizar un cd que contenga sistema operativo igual o mayor en versión al instalado en computador infectado. Reiniciar el computador con dicho disquete.
b. Retirar el cd con el que arranco el computador e insertar el antivirus, luego activar el programa de tal forma que revise todos los archivos y no solo los ejecutables. De encontrar el virus, dar la opción de eliminar el virus; si es que no puede hacerlo el antivirus, se recomienda borrar el archivo, tomar nota de los archivos que se borren. Si estos son varios pertenecientes al mismo programa, reinstalar al término del escaneado. Finalizado el escaneado reconstruir el Master Boot del disco duro.

7. POLITICA USO DE SOFTWARE:

La empresa se compromete a utilizar en todos sus equipos de cómputo, solo software que cuente con su respectiva licencia de uso, además de instalar y actualizar antivirus como forma de protección contra riesgos asociados a la obtención de archivos y software por redes externas o cualquier otro medio, e instalar software de reparación como control preventivo.

8. FORMATOS.

- ✓ PR2-GSI-FT1-HOJA DE VIDA SOFWARE.
- ✓ PR2.GSI-FT2-BITACORA DE FALLAS

9. ELABORACIÓN Y APROBACIÓN DEL DOCUMENTO.

Tabla 1.
Elaboración y aprobación del documento.

Elaborado:	**Revisado:**	**Aprobado:**
Firma en original	**Firma en original**	**Firma en original**
Supervisor Técnico	**Control Interno**	**Gerente**

10. REGISTRO DE CAMBIOS

Tabla 2.
Registro de cambios.

Fecha	Versión	Descripción
2025-07-10	7	Se modifica codificación