INFORME SOFTWARE LEGAL

El presente informe tiene como objetivo verificar y evaluar el cumplimiento de la normatividad vigente en materia de Derechos de Autor y uso adecuado de los programas de computador (Software), dentro del **CENTRO DE DIAGNOSTICO AUTOMOTOR DE PALMIRA LIMITADA,** así como la efectividad de los controles implementados.

1. EQUIPOS DE COMPUTO

De acuerdo a lo anterior la entidad cuenta con los siguientes equipos de cómputo con corte a 31 de diciembre de 2023:

AREA	UBICACIÓN	EQUIPO	CODIGO INTERNO
Equipos Externos Alquilados			
OPERATIVO	OFICINA DT	CDAP-DT -	ALQUILADO
FINANCIERA	CAJA	CDAP-CAJA	ALQUILADO
FINANCIERA	INGRESO	CDAP-SERVICLIENTE	ALQUILADO
OPERATIVO	CERTIFICACIONES	CDAP-CERTMMBK	ALQUILADO
FINANCIERA	JEFE FINANCIERA	CDAP-CONT1	ALQUILADO
FINANCIERA	AUX ADMINISTRATIVA	CDAP-AUXCONT1	ALQUILADO
ADMINISTRATIVA	JEFE ADMINISTRATIVA	CDAP-JEFADM	ALQUILADO
ADMINISTRATIVA	ASISTENTE GERENCIA	CDAP-ASISGER	ALQUILADO
ADMINISTRATIVA	OFICINA DE SISTEMAS	CDAP-CONTINGENCIA	ALQUILADO

Equipos CDAP Ltda Funcionamiento.			
OPERATIVO	PISTA	GALAXY TAB A8 – TABLET	PROPIO
OPERATIVO	PISTA	GALAXY TAB A8 – TABLET	PROPIO
OPERATIVO	PISTA	GALAXY TAB A8 – TABLET	PROPIO
OPERATIVO	PISTA	GALAXY TAB A8 – TABLET	PROPIO
OPERATIVO	PISTA	GALAXY TAB A8 – TABLET	PROPIO
OPERATIVO	PISTA	GALAXY TAB A8 – TABLET	PROPIO
OPERATIVO	PISTA	GALAXY TAB A8 – TABLET	PROPIO
OPERATIVO	PISTA	GALAXY TAB A8 – TABLET	PROPIO
OPERATIVO	PISTA	GALAXY TAB A8 – TABLET	PROPIO
OPERATIVO	COMERCIAL	TELEFONO ULEFONE ARMOR 8	PROPIO
ADMINISTRATIVO	SISTEMAS	HP ML 350P GEN 08 -SERVIDOR	PROPIO

ADMINISTRATIVO	CONTABILID	AUX CONTABLE – EQUI ESCRITO	PROPIO

Equipos Sistemas Ltda (Almacén).			
OPERATIVO	SISTEMAS	TELEFONO ULEFONO ARMOR8X	PROPIO
OPERATIVO	SISTEMAS	GALAXY TAB A8	PROPIO
OPERATIVO	SISTEMAS	GALAXY TAB A8	PROPIO
OPERATIVO	SISTEMAS	TABLET LENOVO YOGA 1	PROPIO
OPERATIVO	SISETEMAS	TABLET LENOVO YOGA 2	PROPIO
OPERATIVO	SISTEMAS	TABLET LENOVO YOGA 3	PROPIO
OPERATIVO	SISETEMAS	TABLET LENOVO YOGA 4	PROPIO
OPERATIVO	SISTEMAS	TELEFONO ULEFONO ARMOR8X	PROPIO

Es importante resaltar que los equipos de cómputo externos son alquilados por medio de contrato de prestación de servicios profesionales y apoyo a la gestión No. 100.15.02.006.2023. Con la empresa ANDRÉS FERNANDO MUÑOZ LÓPEZ, identificado con número de ciudadanía 1'130.672304 de Cali, propietario del establecimiento de comercio NEWTEC INGENIERIA, Nit. 1130672304-1, teniendo como objeto **"CONTRATAR EL SERVICIO DE ALQUILER DE EQUIPOS DE COMPUTO DE ESCRITORIO QUE PERMITAN EL NORMAL FUNCIONAMIENTO DEL CENTRO DE DIAGNÓSTICO AUTOMOTOR DE PALMIRA LIMITADA."**

Además en el contrato en su **Clausula Segunda. Obligaciones Específicas del Contratista,** queda estipulado en el **PARÁGRAFO.** Se debe contemplar **licenciamiento de Office** actual en la cantidad de computadores suministrados, para lo cual el oferente presentará en el proceso como requisito habilitante un certificado suscrito por el representante legal en el que acredite la legalidad del software instalado en la máquina.

Además en el **numeral 5**. El contratista deberá cumplir con la normativa sobre **licenciamiento y derechos de autor para los equipos en arriendo**, y con ello, asumir la responsabilidad directa de los mismos (lo que incluye certificado de autenticidad correspondiente al Sistema Operativo instalado en la máquina).

El contratista emite certificación del licenciamiento de los equipos de cómputo dirigida al Centro de Diagnóstico Automotor de Palmira Limitada, con fecha de 04 de Mayo de 2023.

El software del **CENTRO DE DIAGNOSTICO AUTOMOR DE PALMIRA LIMITADA**, generalmente viene asociado a un computador de escritorio, portátil o servidor, es decir que teniendo en cuenta que la entidad adquiere licenciamiento tipo original Equipment Manufacturer (OEM) Fabricante original de equipo, para paquetes ofimáticos y sistemas operativos Windows. Este software está ligado a la vida útil del equipo, razón por la cual cuando los equipos son dados de baja igualmente se le da de baja al software adquirido con él.

2. SOFTWARE ADQUIRIDO

El Centro de Diagnóstico Automotor de Palmira Limitada, cuenta para su funcionamiento con dos aplicativos como son:

- ✓ El aplicativo contable MAX, donde la empresa comercializadora Interfase ltda. Emite un certificado de Licencia con fecha del 27 de marzo de 2.013, el cual está protegido por las leyes de propiedad intelectual y de los tratados internacionales correspondientes. Además el uso de este software está regido por los términos de la licencia de usos de software (licencia).

- ✓ El software de revisión técnico mecánica y emisiones contaminantes (TECNI-RTM). Se adquirió por medio de un contrato de suministro donde su **OBJETO. Adquisición del sistema de revisión técnico mecánica Teni-RTM**, para las Inspecciones Técnico Mecánicas y de Emisiones Contaminantes, realizadas por el Centro de Diagnóstico Automotor de Palmira Limitada, con la empresa **TECNIMAQ Ingeniería S.A.S NIT. 900.676.425-2.**

  La empresa Tecnimaq suministra el certificado de registro de soporte lógico emitido por el Ministerio del interior desde su oficina de Dirección Nacional de Derechos de Autor, Unidad Administrativa Especial – Oficina de registro. Libro – tomo – partida (13-48-414), de fecha de registro 06 de Agosto de 2015.

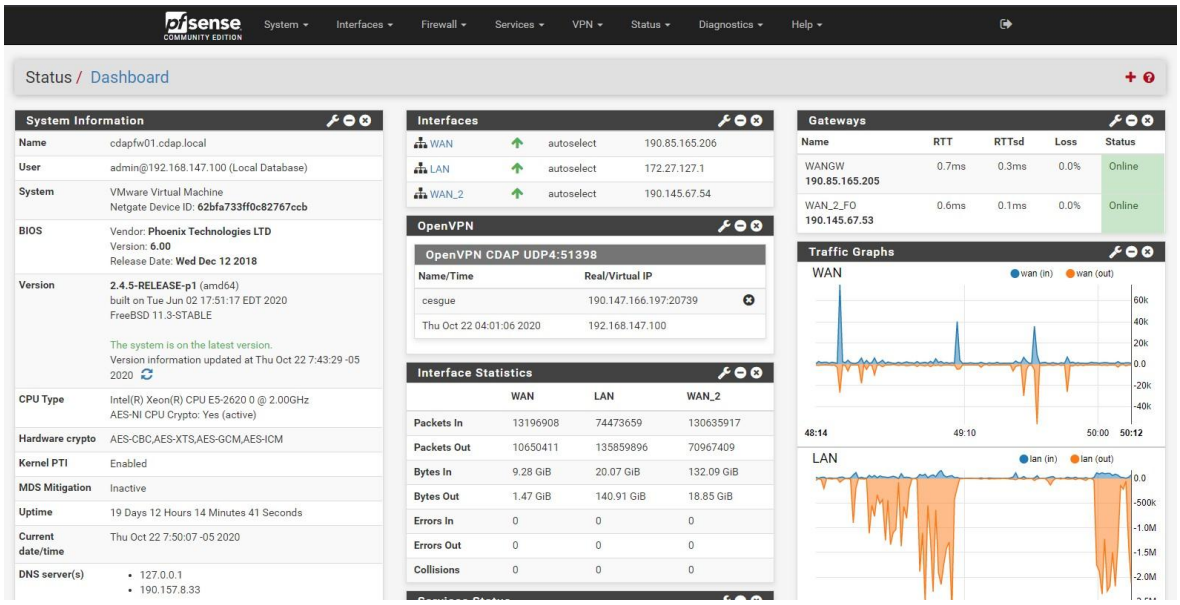
3. MECANISMOS DE CONTROL IMPLEMENTADOS

El centro de diagnóstico automotor de Palmira Limitada (CDAP), ha implementado tanto medidas administrativas (físicas) como técnicas (software), las cuales se relacionan a continuación:

- **Medidas de a nivel de software:**

✓ una instancia de FreeBSD 10 donde nos brinda una solución de **seguridad perimetral PfSense**, la cual permite Firewall: Filtrado (por IP, protocolo, puerto etc…), limitación de conexiones, enrutamientos por regla, creación de alias, Tabla de estado: informa del estado de los servicios y conexiones, NAT (Network Address Translation): con cuatro tipos de configuraciones, Multi-WAN: Se pueden agregar varias conexiones de Internet con diferentes proveedores para poder usar balanceo de carga, usándose para distribuir equitativamente el ancho de banda o utilizar otra conexión en caso de que un ISP falle, servidor VPN: con OpenVPN, IPsec o PPTP, PPPoE Server, Gráficos RDP, Soporte de DNS dinámico, Servidor DHCP, Portal cautivo, servidor Radius, Proxy Squid, IDS/IPS Snort.

Pfsense soporta la instalación de diversos Protección ante ataques de denegación de servicio (DoS), seguridad ante intrusión y sustracción de credenciales, accesos seguros desde equipos externos (SSL, iPSec), autenticación robusta con doble factor de autenticación y claves de un solo uso, filtrado Antivirus y antispam, detección de ataques e intrusiones. (IPS e IDS), filtrado de contenidos (Webfiltering), cortafuegos (físicos y VDOMS), cortafuegos de aplicaciones web (WAF), sistemas de Monitorización, en esta se configuran todos los roles de Router Requeridos para el correcto funcionamiento y protección de la red LAN y WAN, proporciona las direcciones IP Locales mediante DHCP y realizando los debidos rangos de exclusión DHCP para evitar conflictos de IP.

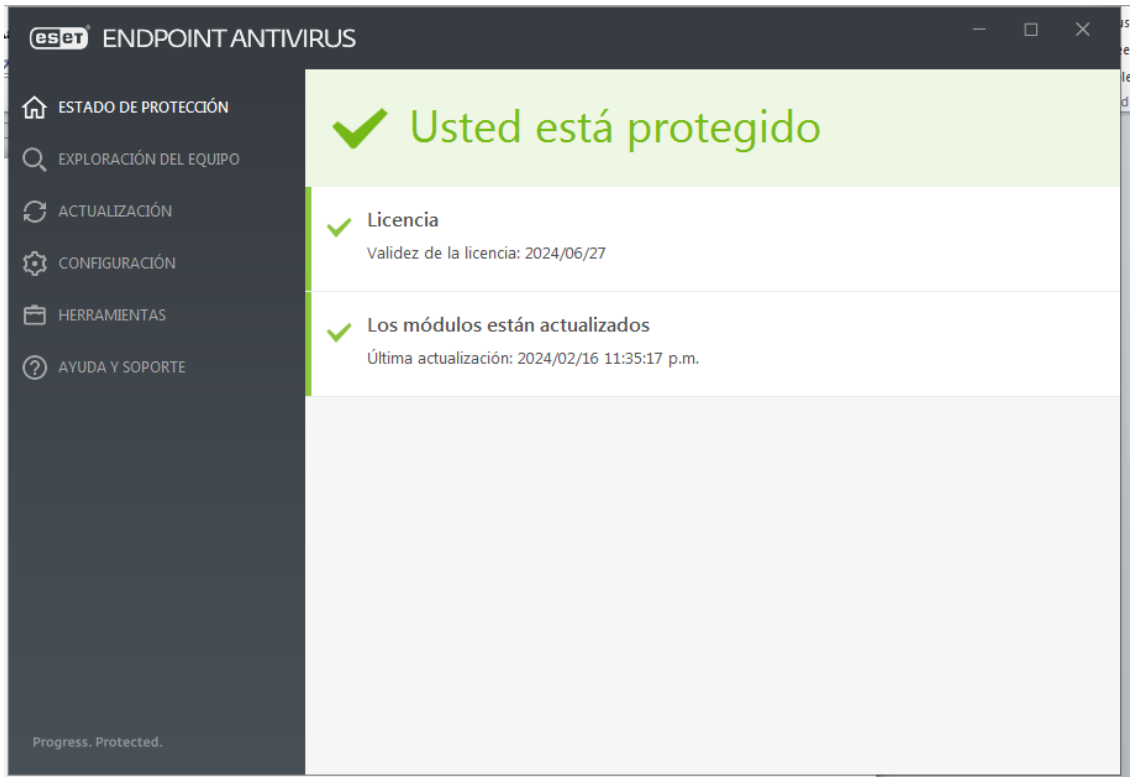


✓ **ANTIVIRUS:**

ESET HOME OFFICE SECURITY PACK, Seguridad completa para pequeñas y medianas empresas, Permite combinar la protección desde 5 a 25 equipos + 5 *smartphones* + 1 o 2 servidores de archivos; todas las opciones incluyen la herramienta de administración remota.

- Protección de identidad en línea
- Antivirus & Antispyware
- Antispam
- Protección ante redes públicas
- Control de Acceso Web
- Administración Remota
- Control de dispositivo USB
- Protección para servidores de archivos
- Gestión de móviles corporativos

Este software se renueva cada año donde se adquiere sus licencias y activación.



- **Controles Físicos:**

a) Dentro del marco del **Sistema de Gestión de Seguridad de la información** se han definido políticas de seguridad que pueden ser consultadas en el documento P-SI-08 Procedimientos de Protección de Software Malicioso, Ubicado en la carpeta del sistema de gestión.

Red\\CDAPFILES1\ssgt\SGC2017\5- SISTEMAS\PROCEDIMIENTOS\ Protección de Software Malicioso.

El objetivo de la política implementada es Proteger la plataforma informática de la entidad en sus componentes de servidores, equipos de escritorio y portátiles, para que estén libres de virus informáticos y software mal intencionado, para evitar la pérdida, daño o alteración de la información.

- **Condiciones Generales**

Para garantizar la confidencialidad, integridad y disponibilidad de la información de la red de datos, todo computador/servidor propiedad de la entidad o en su efecto alquilado debe tener instalado el antivirus debidamente licenciado, los computadores que no son propiedad de la entidad y van a Ser conectados a la red de datos, deben contar con un software antivirus que este actualizado o, de lo contrario, se restringirá el acceso. Los usuarios deben cumplir con todas las restricciones que la plataforma antivirus tiene configurada para evitar la propagación de virus informático.

El software instalado en las estaciones de trabajo, está debidamente licenciado, en consecuencia está prohibido usar software que no cumpla con las normas legales existentes al respecto. El Área de Sistemas, es la única autorizada para la instalación, de software en las estaciones de trabajo (computadores, portátiles, entre otros), así como la configuración y Administración del mismo. Está prohibida la instalación de software para uso exclusivo del funcionario adquirido por él. Todos los funcionarios son responsables de la integridad de los elementos tecnológicos asignados. Cada funcionario es responsable de la organización e integridad de la información almacenada en las estaciones de trabajo asignadas y/o en el ambiente de red utilizado, ya sea localmente (red interna) o en la nube (internet).

Se debe realizar una inspección con el antivirus antes de utilizar medios de almacenamiento extraíbles utilizados en los equipos de cómputo de la entidad con el fin de evitar la propagación de virus informáticos. Tener licenciamiento de software antivirus vigente.

b) PROTECCION Y MANTENIMIENTO DE DATOS

- **Protección de Datos**:
  Se basa en varios puntos entre ellos es el cumplimiento del plan de mantenimiento de los equipos de cómputo (P-SI-02), la autenticidad de licencias de software, la verificación o control de mecanismos de prevención de software malicioso mediante firewall y antivirus, , la verificación del almacenamiento de datos tal como lo establece el procedimiento P-SI-01 y la verificación de los mismos.

4. Destino Final del Software dado de Baja

El software del **CENTRO DE DIAGNOSTICO AUTOMOR DE PALMIRA LIMITADA**, generalmente viene asociado a un computador de escritorio, portátil o servidor, es decir que teniendo en cuenta que la entidad adquiere licenciamiento tipo original Equipment Manufacturer (OEM) Fabricante original de equipo, para paquetes ofimáticos y sistemas operativos Windows. Este software está ligado a la vida útil del equipo, razón por la cual cuando los equipos son dados de baja con el formato (F-FI-15)**,** igualmente se le da de baja al software adquirido con él.

MIYER RAMIRO QUEVEDO CAMACHO
Coordinador de Sistemas Integrados de Gestión
ENERO 2024

CONFIRMACIÓN PRESENTACIÓN INFORME SOFTWARE LEGAL VIGENCIA 2023

Respetado(a) Usuario(a):
Miyer Ramiro Quevedo Camacho
Centro de Diagnostico Automotor de Palmira
Palmira (Valle del Cauca)

Le informamos que luego de verificar en nuestros archivos, se encontró que efectivamente el 19-02-2024 usted remitió ante la Dirección Nacional de Derecho de Autor, con éxito el informe de software legal, con los siguientes datos:

Orden	Local
Sector	Tránsito y Transporte
Departamento	Valle del Cauca
Municipio	Palmira
Entidad	Centro de Diagnostico Automotor de Palmira
Nit	800123366-0
Nombre funcionario	Miyer Ramiro Quevedo Camacho
Dependencia	Sistemas
Cargo	Coordinador de Sistemas Integrados de Gestión
1.Con cuantos equipos cuenta la entidad	11
2. El software se encuentra debidamente licenciado?	Si

3. ¿Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?	3. MECANISMOS DE CONTROL IMPLEMENTADOS El centro de diagnóstico automotor de Palmira Limitada (CDAP), ha implementado tanto medidas administrativas (físicas) como técnicas (software), las cuales se relacionan a continuación: • Medidas de a nivel de software: una instancia de FreeBSD 10 donde nos brinda una solución de seguridad perimetral PfSense, la cual permite Firewall: Filtrado (por IP, protocolo, puerto etc…), limitación de conexiones, enrutamientos por regla, creación de alias, Tabla de estado: informa del estado de los servicios y conexiones, NAT (Network Address Translation): con cuatro tipos de configuraciones, Multi-WAN: Se pueden agregar varias conexiones de Internet con diferentes proveedores para poder usar balanceo de carga, usándose para distribuir equitativamente el ancho de banda o utilizar otra conexión en caso de que un ISP falle, servidor VPN: con OpenVPN, IPsec o PPTP, PPPoE Server, Gráficos RDP, Soporte de DNS dinámico, Servidor DHCP, Portal cautivo, servidor Radius, Proxy Squid, IDS/IPS Snort. Pfsense soporta la instalación de diversos Protección ante ataques de denegación de servicio (DoS), seguridad ante intrusión y sustracción de credenciales, accesos seguros desde equipos externos (SSL, iPSec), autenticación robusta con doble factor de autenticación y claves de un solo uso, filtrado Antivirus y antispam, detección de ataques e intrusiones. (IPS e IDS), filtrado de contenidos (Webfiltering), cortafuegos (físicos y VDOMS), cortafuegos de aplicaciones web (WAF), sistemas de Monitorización, en esta se configuran todos los roles de Router Requeridos para el correcto funcionamiento y protección de la red LAN y WAN, proporciona las direcciones IP Locales mediante DHCP y realizando los debidos rangos de exclusión DHCP para evitar conflictos de IP. ANTIVIRUS: ESET HOME OFFICE SECURITY PACK, Seguridad completa para pequeñas y medianas empresas, Permite combinar la protección desde 5 a 25 equipos + 5 smartphones + 1 o 2 servidores de archivos; todas las opciones incluyen la herramienta de administración remota. • Protección de identidad en línea • Antivirus & Antispyware • Antispam • Protección ante redes públicas • Control de Acceso Web • Administración Remota • Control de dispositivo USB • Protección para servidores de archivos • Gestión de móviles corporativos Este software se renueva cada año donde se adquiere sus licencias y activación. • Controles Físicos: a) Dentro del marco del Sistema de Gestión de Seguridad de la información se han definido políticas de seguridad que pueden ser consultadas en el documento P-SI-08 Procedimientos de Protección de Software Malicioso, Ubicado en la carpeta del sistema de gestión. Red\\\\CDAPFILES1\\ssgt\\SGC2017\\5-SISTEMAS\\PROCEDIMIENTOS\\ Protección de Software Malicioso. El objetivo de la política implementada es Proteger la plataforma informática de la entidad en sus componentes de servidores, equipos de escritorio y portátiles, para que estén libres de virus informáticos y software mal intencionado, para evitar la pérdida, daño o alteración de la información. Condiciones Generales Para garantizar la confidencialidad, integridad y disponibilidad de la información de la red de datos, todo computador/servidor propiedad de la entidad o en su efecto alquilado debe tener instalado el antivirus debidamente licenciado, los computadores que no son propiedad de la entidad y van a Ser conectados a la red de datos, deben contar con un software antivirus que este actualizado o, de lo contrario, se restringirá el acceso. Los usuarios deben cumplir con todas las restricciones que la plataforma antivirus tiene configurada para evitar la propagación de virus informático. El software instalado en las estaciones de trabajo, está debidamente licenciado, en consecuencia está prohibido usar software que no cumpla con las normas legales existentes al respecto. El Área de Sistemas, es la única autorizada para la instalación, de software en las estaciones de trabajo (computadores, portátiles, entre otros), así como la configuración y Administración del mismo. Está prohibida la instalación de software para uso exclusivo del funcionario adquirido por él. Todos los funcionarios son responsables de la integridad de los elementos tecnológicos asignados. Cada funcionario es responsable de la organización e integridad de la información almacenada en las estaciones de trabajo asignadas y/o en el ambiente de red utilizado, ya sea localmente (red interna) o en la nube (internet). Se debe realizar una inspección con el antivirus antes de utilizar medios de almacenamiento extraíbles utilizados en los equipos de cómputo de la entidad con el fin de evitar la propagación de virus informáticos. Tener licenciamiento de software antivirus vigente. b) PROTECCION Y MANTENIMIENTO DE DATOS Protección de Datos: Se basa en varios puntos entre ellos es el cumplimiento del plan de mantenimiento de los equipos de cómputo (P-SI-02), la autenticidad de licencias de software, la verificación o control de mecanismos de prevención de software malicioso mediante firewall y antivirus, , la verificación del almacenamiento de datos tal como lo establece el procedimiento P-SI-01 y la verificación de los mismos.

4. ¿Cuál es el destino final que se le da al software dado de baja en su entidad?	El software del CENTRO DE DIAGNOSTICO AUTOMOTOR DE PALMIRA LIMITADA, generalmente viene asociado a un computador de escritorio, portátil o servidor, es decir que teniendo en cuenta que la entidad adquiere licenciamiento tipo original Equipment Manufacturer (OEM) Fabricante original de equipo, para paquetes ofimáticos y sistemas operativos Windows. Este software está ligado a la vida útil del equipo, razón por la cual cuando los equipos son dados de baja con el formato (F-FI-15), igualmente se le da de baja al software adquirido con él.
Ingrese el Link de la publicación en su entidad del Informe de Software en los términos de la Circular 04 del 22 de diciembre de 2006 del Consejo Asesor del Gobierno Nacional en materia de Control Interno	https://www.cdap.com.co/consulta/informes-meci

Cualquier otra inquietud estaremos atentos a responderla a través del número telefónico (571) 7868220 ext. 1114, o al correo electrónico info@derechodeautor.gov.co

Se ha enviado una copia al correo registrado: sistemas.cdap@gmail.com