Marco de ciberseguridad para los Centros de Diagnóstico Automotor (CDA) en Colombia

Óscar Ricardo Páez Cruz, Jorge Leonardo Pedraza Acevedo, y Sara Palacios Chavarro
o.paezc, j.pedrazaa, s.palaciosc @uniandes.edu.co
MESI, Universidad de los Andes

***Resumen*—Los Centros de Diagnóstico Automotor (CDA) en Colombia operan sobre plataformas tecnológicas esenciales para la revisión técnico–mecánica de vehículos y el registro de información sensible de ciudadanos, pero la mayoría de estas organizaciones presentan características de pequeñas y medianas empresas (PYMEs), con recursos limitados y baja madurez en ciberseguridad. Este artículo presenta el diseño de un marco de ciberseguridad específico para CDA, alineado con el marco NIST Cybersecurity Framework (CSF), las normas ISO/IEC 27001, ISO 27002, ISO/IEC 27701, ISO 22301 y lineamientos OWASP (OWASP Top 10, Testing Guide, IoT Top 10, ASVS) para aplicaciones y servicios, y la normativa colombiana de protección de datos personales.**

Además, se describe el desarrollo de una herramienta tipo SaaS que implementa dicho marco en forma de checklist dinámico, con funcionalidades de cálculo de madurez, panel de control y generación de controles técnicos adicionales a partir de escaneos de seguridad. La herramienta está diseñada para ser utilizada por CDA sin equipos especializados de TI, facilitando la adopción de buenas prácticas de seguridad de la información y el cumplimiento normativo bajo un enfoque de mejora continua.

Abstract-- Vehicle Inspection Centers (CDA, by its acronym in Spanish) in Colombia operate in essential information systems for technical–mechanical inspections and the processing of sensitive personal data. However, most of these organizations behave as small and medium–sized enterprises (SMEs), with limited resources and low maturity in cybersecurity practices. This paper presents the design of a cybersecurity framework tailored to CDA, aligned with the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, ISO 27002, ISO/IEC 27701, ISO 22301 and OWASP guidelines ((OWASP Top 10, Testing Guide, IoT Top 10, ASVS)) for applications and services, and Colombian data protection regulations.

In addition, it describes the development of a SaaS–based tool that implements the framework as a dynamic checklist, including maturity scoring, a security dashboard, and the ability to generate additional technical controls from security scan outputs. The tool is intended to be used by CDA without dedicated IT security teams, thus facilitating the adoption of cybersecurity best practices and regulatory compliance under a continuous improvement approach.

I. Introducción

Los Centros de Diagnóstico Automotor (CDA) en Colombia son actores clave en la seguridad vial, pues certifican el estado técnico–mecánico de los vehículos y generan información que es consumida por autoridades de tránsito, aseguradoras y otras entidades del sector automotor. En este proceso se manejan datos personales, historiales de revisiones y registros operativos que están sujetos a la Ley 1581 de 2012, la Ley 1266 de 2008, el Decreto 1074 de 2015 y las disposiciones del Ministerio de Transporte, entre otras normas.

A pesar de la criticidad de la información que gestionan, muchos CDA funcionan con estructuras organizativas y tecnológicas propias de las PYMEs, sin equipos formales de seguridad, con infraestructuras heterogéneas y con prácticas de TI centradas en la operación diaria más que en la gestión del riesgo. La ausencia de lineamientos específicos de ciberseguridad para este sector genera una brecha entre las exigencias regulatorias y las capacidades reales de implementación.

En este contexto, el presente trabajo propone: (i) un marco de ciberseguridad orientado específicamente a los CDA colombianos, que articula estándares internacionales como NIST CSF, ISO/IEC 27001 y OWASP con la normativa nacional; y (ii) una herramienta software tipo Software as a Service (SaaS) que operacionaliza este marco mediante un checklist estructurado, indicadores de madurez y generación de controles técnicos derivados de escaneos de seguridad. El objetivo es ofrecer un mecanismo práctico, replicable y progresivo para elevar la postura de ciberseguridad de los CDA sin exigir grandes inversiones ni equipos especializados.

II. MARCO DE REFERENCIA

El diseño del marco de ciberseguridad propuesto se fundamenta en un conjunto de estándares internacionales, lineamientos técnicos especializados y normativas colombianas aplicables a los Centros de Diagnóstico Automotor (CDA).

En primer lugar, se adopta el NIST Cybersecurity Framework (CSF v1.1) como estructura base para la gestión del riesgo, organizando las actividades de seguridad en cinco funciones fundamentales: Identificar, Proteger, Detectar, Responder y Recuperar. Este enfoque permite modelar la postura de seguridad de los CDA en un ciclo claro y comunicable, adaptable a organizaciones con recursos limitados.

En segundo lugar, el marco incorpora controles y buenas prácticas provenientes de ISO/IEC 27001, ISO/IEC 27002 y ISO/IEC 27701, que aportan directrices para la gestión de seguridad de la información, la seguridad técnica y organizativa, y la protección de datos personales bajo un enfoque de privacidad. Asimismo, se incluye ISO 22301, que orienta la planificación de la continuidad del negocio y la resiliencia organizacional, aspectos claves para asegurar la operación ininterrumpida y su relación directa con procesos regulatorios del sector transporte.

En materia de seguridad de aplicaciones y tecnologías, se integran múltiples lineamientos del proyecto OWASP: OWASP Top 10, OWASP Testing Guide, OWASP IoT Top 10 y OWASP Application Security Verification Standard (ASVS). Estos marcos permiten identificar vulnerabilidades críticas, evaluar configuraciones inseguras, fortalecer aplicaciones web y mejorar la protección de dispositivos IoT utilizados por los CDA, tales como cámaras, DVR, puntos de acceso y equipos de red.

A partir de este conjunto heterogéneo de estándares se desarrolló un marco unificado específicamente orientado a los CDA. La construcción se basó en una metodología sistemática en tres pasos. El primero fue la descomposición de cada estándar en sus elementos mínimos aplicables, extrayendo únicamente los componentes factibles para organizaciones tipo PYMEs. En este proceso, NIST CSF se desglosó en sus funciones y subcategorías relevantes; ISO/IEC 27001 y 27002 se redujo a controles esenciales como gestión de activos, control de accesos, operación segura y continuidad; ISO/IEC 27701 aportó únicamente los elementos de privacidad exigidos por la normativa colombiana; y los lineamientos OWASP se incorporaron como controles técnicos concretos para aplicaciones, autenticación, criptografía y gestión de vulnerabilidades.

El segundo paso consistió en un mapeo cruzado entre controles normativos y necesidades operativas reales de los CDA, guiado por preguntas clave como: “¿Este control protege información crítica del CDA?”; “¿Mitiga un riesgo observado en la operación diaria o en la infraestructura de diagnóstico?”; “¿Apoya el cumplimiento normativo colombiano?”. Este análisis permitió descartar controles sobredimensionados para el sector e incorporar otros que, aun no siendo obligatorios, resultan estratégicos para su resiliencia técnica.

El tercer paso fue la normalización de todas las recomendaciones en un modelo único de control, estructurado por categoría, dominio, descripción, referencia normativa y nivel de madurez. Este proceso permitió armonizar marcos que, por naturaleza, difieren en granularidad, propósito y enfoque. NIST CSF proporciona capacidades organizacionales de alto nivel; ISO introduce controles formales con evidencia documental; OWASP profundiza en aspectos técnicos; e ISO 27701 amplía la perspectiva hacia la privacidad. La convergencia entre estos enfoques exigió resolver tres desafíos:
(1) Diferencias de granularidad, solucionadas mediante la creación de dominios que agrupan controles complementarios sin perder detalle técnico;
(2) Carga operativa de ISO, mitigada mediante la adopción de un modelo de madurez que permite priorizar progresivamente; y
(3) Heterogeneidad tecnológica entre CDA, lo que llevó a introducir un mecanismo complementario: un assessment de caracterización, que permite activar dinámicamente un subconjunto de controles dedicados según el tamaño, infraestructura, número de sedes o nivel de exposición del CDA.

Este proceso de armonización permitió consolidar un marco adaptable, modular y proporcional a las capacidades reales del sector, preparando el terreno para las siguientes secciones del artículo, donde se describe el desarrollo del marco, la definición de categorías y dominios, y la construcción de la herramienta que implementa estos controles.

III. MARCO DE CIBERSEGURIDAD PROPUESTO PARA CDA

El marco de ciberseguridad propuesto se concibe como un conjunto estructurado de controles que cubren dominios clave para la operación de un CDA: Infraestructura y Redes, Aplicativos y Datos, Gobierno y Cumplimiento, Equipos de Diagnóstico, Personas, Proveedores y Seguridad Física. Cada control se describe mediante un identificador, una descripción clara, una categoría, un dominio, una referencia a estándares o normas aplicables y un nivel de madurez objetivo sobre una escala ordinal.

El diseño del marco se guía por el ciclo PDCA (Plan–Do–Check–Act). En la fase de Planificación se identifican activos, se revisa el marco normativo aplicable y se seleccionan controles mínimos obligatorios para el sector. La fase de Implementación se orienta a la puesta en práctica de controles técnicos y organizativos, incluyendo cifrado de datos, segmentación de redes, control de acceso a software de diagnóstico, gestión de parches y políticas internas de seguridad. En la fase de Verificación se plantea el uso periódico del checklist para medir el nivel de cumplimiento, detectar desviaciones y generar indicadores de madurez. Finalmente, en la fase de Mejora se incorporan ajustes a los controles, nuevas medidas frente a amenazas emergentes y actualizaciones derivadas de cambios regulatorios o tecnológicos.

El marco está diseñado para ser progresivo y priorizado. No se espera que un CDA implemente de forma inmediata todos los controles, sino que pueda avanzar desde niveles básicos hacia niveles más elevados de madurez. Para ello, cada control se asocia con un nivel de madurez objetivo que sirve como referencia para la planificación y la priorización de acciones de mejora. Adicionalmente, se distinguen controles de carácter estructural (por ejemplo, políticas de tratamiento de datos) y controles de carácter técnico (por ejemplo, endurecimiento de TLS en servicios internos), de manera que se pueda modular la adopción de acuerdo con las capacidades del CDA.

IV. DESAROLLO DEL MARCO DE CIBERSEGURIDAD

La selección del conjunto definitivo de controles respondió a criterios sistemáticos basados en cumplimiento normativo, gestión de riesgo y viabilidad operativa. Se priorizaron aquellos controles con impacto directo en el cumplimiento normativo colombiano, incluyendo la Ley 1581 de 2012, el Decreto 1074 de 2015 y los lineamientos de la Superintendencia de Industria y Comercio (SIC). Estos controles fueron considerados no opcionales, ya que garantizan obligaciones legales para todos los CDA; ejemplos de ello son GC01 (*Política de tratamiento de datos personales publicada*) y GC02 (*registro de bases de datos en la SIC*), ambos incluidos en el checkllist[1] final.

Posteriormente, se analizaron los riesgos tecnológicos recurrentes en los CDA, entre los que destacan: exposición de servicios como RDP o MySQL, ausencia de segmentación de red, uso de dispositivos IoT inseguros, carencia de actualizaciones en Tomcat y MySQL, y software propio sin lineamientos de desarrollo seguro. Este diagnóstico permitió complementar el marco con controles altamente específicos derivados de NIST, ISO y OWASP. Entre estos controles se encuentran IR01 (*Segmentación de red*), IR06 *(Inventario y segmentación de IoT*), AD03–AD04 (*prácticas de desarrollo seguro basadas en OWASP ASVS*) y FS01–FS02 (*controles de seguridad física orientados a CCTV*). La selección siguió un criterio de priorización centrado en la mitigación directa de riesgos observados en el sector.

El agrupamiento de controles en categorías y dominios respondió a la necesidad de cubrir el ciclo de vida operativo de un CDA, desde gobierno corporativo hasta infraestructura técnica y seguridad de dispositivos especializados. Las categorías definidas fueron: Gobierno y Cumplimiento, Infraestructura y Redes, Equipos de Diagnóstico, Aplicativos y Datos, Personas, Proveedores y Seguridad Física.

Cada categoría contiene *dominios* derivados directamente de los capítulos temáticos de ISO 27002, de las funciones de NIST CSF y de los componentes técnicos de OWASP. Esta estructura permitió organizar los controles de manera coherente, garantizando que la cobertura normativa se mantuviera sin generar redundancias, y asegurando al mismo tiempo que cada dominio respondiera a riesgos observados en la operación real de los CDA.

Por ejemplo, la categoría *Infraestructura y Redes* incorpora dominios como segmentación de red, firewalling, acceso remoto seguro e IoT, todos ellos esenciales dado que numerosos incidentes en CDA surgen de configuraciones débiles, exposición innecesaria de servicios o dispositivos sin gestión de firmware. La categoría *Aplicativos y Datos*, en contraste, adopta dominios basados en OWASP ASVS y NIST PR.DS para asegurar bases de datos, pruebas de seguridad y uso de criptografía adecuada.

Finalmente, la integración de todas las fuentes normativas, el análisis de riesgos sectoriales y la organización por dominios dio lugar a un checklist consolidado de ciberseguridad compuesto por 23 controles base, distribuidos en las siete categorías descritas. Cada control quedó normalizado bajo una estructura uniforme (identificador, descripción, dominio, referencia normativa y nivel de madurez), permitiendo que el modelo sea auditable, comparable entre CDA y técnicamente accionable. La Ilustración 1 presenta una vista parcial del checklist final, evidenciando cómo los controles se agrupan por categoría y cómo se visualizan sus atributos clave dentro de la herramienta desarrollada.

ID	Control	Descripción	Categoría	Dominio	Referencia	Recomendación	Nivel de Madurez (1-5)
GC01	Política de tratamiento de datc	El CDA debe contar con una pol	Gobierno y Cumplimiento	Privacidad y Cumplimiento Legal	Ley 1581 de 20	Publicar la política e	2
GC02	Registro de bases de datos en	Toda base de datos con inform	Gobierno y Cumplimiento	Privacidad	Ley 1581; Decre	Registrar o actualiza	2
GC03	Oficial o responsable de seguri	Debe existir una persona desig	Gobierno y Cumplimiento	Organización	ISO 27002 §5.2,	Asignar rol formal y	3
GC04	Matriz de riesgos de seguridad	Evaluación de riesgos tecnológi	Gobierno y Cumplimiento	Gestión de Riesgos	ISO 27005	Aplicar metodología	2
GC05	Plan de tratamiento de riesgos	Documento con acciones, prior	Gobierno y Cumplimiento	Gestión de Riesgos	ISO 27005	Definir controles pri	2
GC06	Procedimiento de gestión de ir	Debe existir un procedimiento	Gobierno y Cumplimiento	Continuidad	ISO 27035	Asegurar canal de re	3
GC07	Inventario de activos tecnológ	Listado actualizado de equipos,	Gobierno y Cumplimiento	Gestión de Activos	ISO 27002 §5.9	Incluir responsable,	2
GC08	Clasificación de información	Definir niveles de sensibilidad	Gobierno y Cumplimiento	Gestión de Activos	ISO 27002 §5.1,	Clasificar BD del RUT	3
GC09	Contratos con terceros que inc	Los proveedores deben aceptar	Gobierno y Cumplimiento	Proveedores	ISO 27002 §5.2	Firmar anexos de tr	3
IR01	Segmentación de red administ	La red debe estar dividida lógic	Infraestructura y Redes	Control de Redes	ISO 27002 §8.2(	Crear VLAN admin, I	4
IR02	RDP sin exposición pública	Ningún puerto 3389 debe estar	Infraestructura y Redes	Control de Acceso	NIST CSF PR.AC	Usar VPN y cerrar pu	5
IR03	Routers sin contraseñas por de	Eliminar credenciales de fábrica	Infraestructura y Redes	Config. Segura	OWASP Secure	Contraseñas >12 car	3
IR04	WiFi de invitados aislado	La red de invitados no debe ver	Infraestructura y Redes	Control de Redes	ISO 27002 §8.2	Modo 'Guest' activa	3
IR05	Firewall configurado	Debe existir firewall con reglas	Infraestructura y Redes	Perímetro	NIST CSF PR.AC	Bloquear todo excep	3

Ilustración 1. Resumen del checklist base

V. ARQUITECTURA Y DISEÑO DE LA HERRAMIENTA

La solución propuesta se implementó bajo una arquitectura modular basada en microservicios, diseñada para soportar un modelo SaaS escalable y multientidad. La arquitectura general (ver ilustración *1*) se compone de un frontend liviano, un backend en Python/Flask que expone servicios dedicados para el manejo de controles, procesamiento de escaneos y cálculo de métricas, un módulo de persistencia para almacenar resultados y configuración, y un componente de inteligencia artificial responsable de generar controles adicionales a partir de reportes técnicos. Esta arquitectura permite separar responsabilidades, facilitar la evolución independiente de cada módulo y garantizar que los CDA puedan consumir la solución desde cualquier ubicación sin necesidad de infraestructura local especializada.

[1] https://github.com/SaraPalaciosAndes/CyberCDA/blob/main/checklist_cda.json

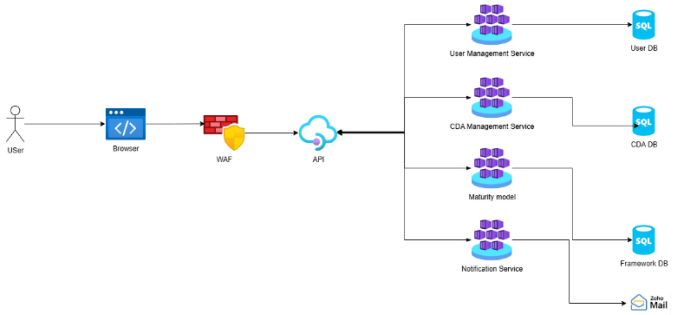

Ilustración 2. Arquitectura de Bloques

En esta arquitectura, el backend Flask opera como el núcleo lógico de la plataforma. Gestiona las rutas principales de la aplicación, incluida la carga del checklist, el cálculo del cumplimiento, el manejo del dashboard, la lectura de archivos JSON y la integración con el motor de IA. El enfoque basado en archivos JSON para almacenar controles permite mantener un repositorio de configuración flexible, fácilmente actualizable y desacoplado del código. Cada control está definido con atributos clave como identificador, categoría, dominio, referencia normativa, recomendación y nivel de madurez objetivo, lo que facilita su procesamiento automático.

La capa de presentación (Ilustración 2) se construye mediante plantillas HTML/Jinja, organizadas en diferentes vistas funcionales. Estas plantillas fueron diseñadas para ser intuitivas y operables por personal no técnico, manteniendo una interfaz limpia, con componentes visuales como barras de progreso, etiquetas de riesgo y navegación lateral por módulos.

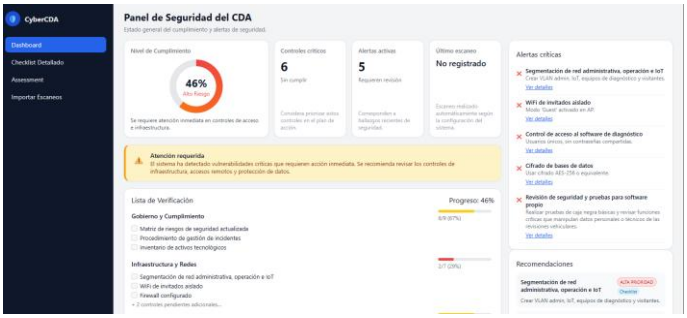

Ilustración 3. Vista del panel de seguridad y checklist automatizado

El checklist detallado (ilustración 3) constituye el núcleo operativo de la herramienta. Esta vista muestra todos los controles del marco, clasificados por categoría y organizados según la estructura definida por NIST CSF, ISO/IEC 27001–27002–27701, ISO 22301 y OWASP. Cada control incluye atributos tales como identificación, dominio, referencia normativa, nivel de madurez esperado y una recomendación específica.

El usuario puede marcar los controles implementados, tras lo cual el sistema recalcula el porcentaje de cumplimiento y la categoría de riesgo (bajo, medio o alto). La vista ofrece un panel lateral para el detalle de cada control y gráficos de cumplimiento por dominio.

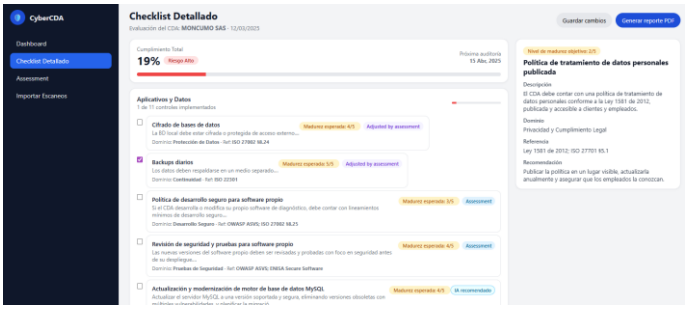

Ilustración 4. Checklist detallado con indicadores de cumplimiento

El assessment (Ilustración 4) permite adaptar el marco de ciberseguridad a la realidad particular de cada CDA, diferenciando entre organizaciones con más personal, mayores requerimientos tecnológicos o riesgos específicos. El cuestionario genera un conjunto de etiquetas (*tags*) que ajustan dinámicamente los controles base, incorporando nuevos requisitos cuando el nivel de complejidad del CDA lo amerita. Esta funcionalidad transforma el marco en un instrumento personalizado y no genérico.

Ilustración 5. Vista del formulario de assessment

El módulo de ingesta de reportes técnicos (Ilustración 6) incorpora un componente de análisis asistido por IA que permite transformar hallazgos de herramientas como Nmap u OpenVAS en controles de ciberseguridad accionables. El proceso inicia con la carga de un archivo XML, TXT o PDF, el cual es sometido a un preprocesamiento donde se eliminan líneas vacías, texto redundante y elementos no relevantes para el análisis. A partir del reporte limpio se extraen únicamente los atributos esenciales de cada vulnerabilidad (host, puerto, nombre, severidad, descripción y solución) con el fin de reducir ruido semántico y optimizar el consumo de tokens en el modelo de IA. Posteriormente, el contenido se divide en fragmentos (“chunks”) de tamaño controlado para garantizar que cada solicitud permanezca dentro del límite aceptado por el modelo OpenAI GPT-5.1.

Ilustración 6. Vista de carga de escaneos y controles generados

Cada uno de estos fragmentos se envía al servicio de IA mediante una consulta estructurada que incluye un *system prompt* y un *user prompt* especializados. El *system prompt (Ilustración 7)* define el rol del modelo como un experto en ciberseguridad para CDA en Colombia, instruyéndolo para analizar vulnerabilidades resumidas y producir controles de seguridad alineados con ISO 27001, NIST CSF y OWASP, asegurando que la salida sea exclusivamente un objeto JSON válido.

```
system_prompt = (
"Eres un experto en ciberseguridad para pequeñas y medianas empresas "
"del sector de Centros de Diagnóstico Automotor (CDA) en Colombia. "
"Recibirás como entrada el TEXTO RESUMIDO de un escaneo de seguridad "
"(por ejemplo, Nmap u OpenVAS), organizado en bloques con el formato:\n\n"
"[VULNERABILIDAD]\n"
"Host: ...\n"
"Puerto: ...\n"
"Nombre: ...\n"
"Severidad: ...\n"
"Descripción:\n"
"... \n"
"Solución recomendada:\n"
"... \n"
"----------------------------------------\n\n"
"Tu tarea es analizar estos bloques y proponer CONTROLES DE CIBERSEGURIDAD "
"concretos, accionables y alineados con estándares como ISO 27001, NIST CSF y OWASP, "
"pensados específicamente para un CDA.\n\n"
"Tu salida DEBE ser EXCLUSIVAMENTE un objeto JSON válido, sin texto adicional."
)
```

Ilustración 7. Contenido de system prompt

El *user prompt* (Ilustración 8) contextualiza el fragmento indicando su número, el tipo de escaneo y el CDA asociado, además de especificar el formato exacto de los bloques de vulnerabilidad y las reglas estrictas para la generación de controles. Entre estas reglas se incluyen: proponer controles específicos basados en el hallazgo (por ejemplo, si existe exposición de RDP recomendar su restricción), asignar niveles de madurez en función de la severidad y etiquetar todos los controles generados con la marca `"requires_tags": ["Scan_AI"]` para diferenciarlos del checklist base.

```
user_prompt = f"""
        El siguiente texto corresponde al BLOQUE {idx+1} de {total_chunks} de los resultados
        de un escaneo de seguridad tipo: {scan_type} para el CDA: {cda_name}.

        El texto ya está resumido en bloques de vulnerabilidades con el siguiente estilo:

        [VULNERABILIDAD]
        Host: <IP o nombre>
        Puerto: <puerto/protocolo>
        Nombre: <nombre de la vulnerabilidad>
        Severidad: <Low/Medium/High/Critical o numérico>
        Descripción:
        <descripción breve>
        Solución recomendada:
        <medida sugerida>
        ----------------------------------------

        INSTRUCCIONES:

        1. Analiza únicamente las vulnerabilidades presentes en este fragmento de texto.
        2. Para cada vulnerabilidad relevante, propone uno o más CONTROLES de ciberseguridad
        que un CDA debería aplicar para mitigar el riesgo (por ejemplo: segmentación de red,
        endurecimiento de servicios, actualización de software, control de accesos remotos, etc.).
        3. No repitas controles genéricos; enfócate en acciones específicas derivadas de estos hallazgos
        (por ejemplo, si hay RDP expuesto, un control para restringir o encapsular RDP).
        4. Si una vulnerabilidad es de severidad alta o crítica, asigna un nivel de madurez objetivo más alto
        (por ejemplo 4 o 5). Si es media, usa 3; si es baja, 2.

        La salida debe tener EXACTAMENTE la siguiente estructura JSON:

        {{
        "Infraestructura_y_Redes": [
            {{
            "id": "IR_SCAN_01",
            "control": "Nombre corto del control",
            "descripcion": "Descripción clara del control, indicando qué debe hacer el CDA.",
            "categoria": "Infraestructura y Redes",
            "dominio": "Subdominio o área (ej. Segmentación, Acceso remoto, Firewall)",
            "referencia": "Referencias a ISO/NIST/OWASP relevantes",
            "recomendacion": "Acción concreta recomendada para este CDA, basada en el hallazgo.",
            "madurez": "calcula el nivel de madurez del control de 1 a 5,
            "requires_tags": ["Scan_AI"]
            }}
        ],
        "Aplicativos_y_Datos": [],
        "Gobierno_y_Cumplimiento": [],
        "Personas": [],
```

Ilustración 8. User prompt utilizado para la generación de controles

El servicio de IA devuelve para cada fragmento un conjunto de controles estructurados por categoría, dominio, recomendación y nivel de madurez, los cuales son posteriormente consolidados en un archivo JSON único (Ilustración 9) y almacenados en el módulo de resultados de escaneo. Estos controles pueden visualizarse en la interfaz y son integrados dinámicamente al checklist del CDA, ampliando su contenido base con recomendaciones especializadas derivadas del análisis del reporte técnico.

Ilustración 9. Ejemplo de control generado por IA

La integración de una arquitectura modular, basada en microservicios y extendida con capacidades de inteligencia artificial, permite que el marco de ciberseguridad se convierta en una herramienta dinámica, automatizada y adaptable. Esto facilita que los CDA avancen hacia la madurez en ciberseguridad sin requerir infraestructura compleja, asegurando conformidad con estándares internacionales y alineación con el marco normativo colombiano.

VI. MODELO DE MADUREZ

El modelo de madurez adoptado en esta propuesta se fundamenta en la medición del nivel de cumplimiento del marco de ciberseguridad, expresado como un porcentaje que refleja los controles implementados respecto al total de controles

aplicables. A diferencia de los modelos tradicionales basados en capacidades (CMMI, COBIT o niveles ISO), este enfoque se construye desde la perspectiva práctica de los Centros de Diagnóstico Automotor (CDA), privilegiando la simplicidad, la comunicación efectiva y la capacidad de reflejar el riesgo operativo de forma directa.

El nivel de cumplimiento se calcula considerando: (1) los controles base del marco de referencia, (2) los controles ajustados por el assessment específico del CDA y (3) los controles generados mediante análisis asistido por IA a partir de reportes técnicos. Cada control tiene un estado binario (implementado/no implementado) y un peso equivalente, lo que permite obtener un porcentaje total de cumplimiento. Este porcentaje se traduce en un nivel de riesgo, que opera simultáneamente como modelo de madurez organizacional, pues representa la capacidad del CDA para sostener prácticas mínimas de ciberseguridad y reducir su exposición a amenazas.

Para facilitar la interpretación y tomar decisiones operativas, el modelo agrupa los resultados en tres niveles de madurez-riesgo, mostrados en la Tabla 1. A mayor cumplimiento, menor riesgo y mayor madurez organizacional. Como resultado, el modelo funciona tanto como un indicador de desempeño como un mecanismo de mejora continua, permitiendo a los CDA avanzar progresivamente hacia niveles de riesgo aceptables.

Nivel	Rango de Cumplimiento	Interpretación de riesgo
Bajo Riesgo (Madurez Alta)	>= 80%	Riesgo reducido
Riesgo Medio (Madurez intermedia)	50% - 79%	Riesgo moderado
Alto Riesgo (Madurez baja)	< 50%	Riesgo elevado

Tabla 1. Modelo de madurez basado en cumplimiento y riesgo

El modelo permite una lectura inmediata del estado de seguridad del CDA, soporta comparaciones interanuales y facilita la toma de decisiones por parte de directivos y auditores. Además, al incorporar controles personalizados derivados del assessment y de los hallazgos técnicos procesados por IA, el nivel de cumplimiento se adapta a la realidad operativa de cada CDA, convirtiéndose en un indicador dinámico que refleja de forma precisa la evolución de su madurez en ciberseguridad.

VII. DISCUSIÓN

El desarrollo del marco de ciberseguridad y de la herramienta SaaS demuestra que es posible adaptar estándares internacionales complejos a sectores altamente regulados, pero con capacidades técnicas limitadas, como los Centros de Diagnóstico Automotor. La integración de múltiples fuentes normativas permitió consolidar un enfoque robusto y orientado a la gestión del riesgo, asegurando cobertura normativa y técnica. A su vez, la implementación tecnológica del marco demuestra que la automatización de procesos de evaluación no solo mantiene la rigurosidad requerida, sino que reduce tiempos, minimiza errores humanos y facilita la adopción en organizaciones con recursos limitados.

Asimismo, el uso de inteligencia artificial para la generación de controles derivados de escaneos técnicos representa una innovación significativa en el fortalecimiento de la seguridad para organizaciones pequeñas. Esta capacidad permite transformar resultados técnicos en acciones concretas y contextualizadas, reduciendo barreras de conocimiento especializado.

Más allá de los aspectos técnicos, la cultura organizacional de los CDA plantea desafíos relevantes, para la adopción del marco. Al tratarse de empresas con características de PYMEs, la gestión del riesgo suele percibirse como un costo adicional y no como un factor estratégico, lo que limita la inversión en medidas preventivas. La ausencia de roles especializados en ciberseguridad y la delegación de estas funciones a personal no técnico incrementan la probabilidad de errores y la dependencia de terceros

Otro reto es la resistencia al cambio. La implementación de controles normativos y técnicos implica modificar procesos arraigados, generar evidencia documental y adoptar nuevas rutinas, lo que puede ser visto como burocracia innecesaria. Sin una estrategia de sensibilización y capacitación, estas iniciativas corren el riesgo de ser cumplidas de manera superficial. Finalmente, la baja conciencia sobre riesgos digitales refuerza la idea de que las amenazas son improbables, lo que dificulta la creación de una cultura de seguridad.

Superar estos retos exige integrar la ciberseguridad en la narrativa organizacional, vinculándola con objetivos estratégicos como la protección de datos, la reputación y la sostenibilidad del negocio. Programas de formación, liderazgo visible y mecanismos de incentivos internos son acciones clave para lograrlo.

Por último, la arquitectura modular y basada en microservicios facilita la evolución futura del sistema y su despliegue en plataformas cloud, garantizando escalabilidad, continuidad y sostenibilidad a largo plazo.

VIII. CONCLUSIONES Y TRABAJO FUTURO

La ausencia de lineamientos específicos en materia de ciberseguridad para los Centros de Diagnóstico Automotor ha generado un escenario de vulnerabilidad que compromete la integridad de los procesos de revisión técnico-mecánica y la protección de datos personales. El marco desarrollado en este proyecto establece políticas, protocolos y controles que permiten garantizar la confidencialidad, integridad y disponibilidad de la información, adaptándose a las necesidades de las PYMES que conforman la mayoría del sector. Su diseño, basado en estándares internacionales como ISO/IEC 27001, NIST CSF y OWASP, asegura la alineación con buenas prácticas globales y con la normativa nacional, reduciendo riesgos de sanciones y mejorando la confianza de los usuarios

El proyecto demuestra que es posible integrar principios avanzados de ciberseguridad en un contexto local sin generar costos prohibitivos. La herramienta de diagnóstico complementaria refuerza esta propuesta, ofreciendo una solución práctica para evaluar el nivel de madurez y priorizar acciones correctivas. Con ello, se logra un avance significativo hacia la creación de una cultura de seguridad en los CDA, donde la protección de datos y la continuidad operativa se convierten en pilares estratégicos.

En cuanto al trabajo futuro, se identifican varias líneas de acción que permitirán consolidar y ampliar el impacto del marco. Una de ellas es el desarrollo de una guía práctica que facilite la implementación del marco en CDA pequeños y medianos, incorporando ejemplos, plantillas y procedimientos simplificados. También se plantea la integración con plataformas gubernamentales como el Registro Único Nacional de Tránsito (RUNT), lo que permitiría automatizar la verificación de cumplimiento normativo y reducir la carga administrativa. Otra línea estratégica consiste en la capacitación continua del personal, mediante programas virtuales y simulaciones de incidentes que fortalezcan la conciencia sobre riesgos y buenas prácticas.

Adicionalmente, se contempla la expansión del marco hacia otros sectores críticos como salud, transporte y servicios, donde la protección de datos y la continuidad operativa son fundamentales. El diseño modular permitirá ajustar los controles según el nivel de madurez digital de cada organización, garantizando flexibilidad y escalabilidad. Asimismo, se proyecta una mayor incorporación de Inteligencia Artificial (IA), mediante algoritmos avanzados para la detección de anomalías, análisis predictivo y predicción temprana de incidentes.

El marco deberá ser objeto de evaluaciones periódicas para incorporar nuevos controles frente a amenazas emergentes y adaptarse a cambios regulatorios. Esto incluye la consideración de tecnologías emergentes como IoT, inteligencia artificial y entornos híbridos, que incrementan la superficie de ataque y exigen medidas adicionales. Asimismo, se proyecta la expansión del marco hacia otros actores del ecosistema automotor, como concesionarios, aseguradoras y talleres especializados, con el fin de crear un estándar sectorial que eleve el nivel de seguridad en toda la cadena de valor.

Finalmente, se contempla la incorporación de módulos de analítica predictiva que permitan anticipar riesgos y optimizar la toma de decisiones, así como la certificación del marco bajo estándares internacionales como ISO 27001, lo que fortalecerá la confianza de clientes, autoridades y gremios. Estas acciones consolidarán el marco como una referencia nacional en ciberseguridad para el sector automotor, contribuyendo a la protección de datos, la continuidad operativa y la competitividad de los CDA en Colombia

REFERENCIAS

[1] *Congreso de la República de Colombia, Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá D.C., Colombia, 2012.*

[2] *Congreso de la República de Colombia, Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del Habeas Data financiero. Bogotá D.C., Colombia, 2008.*

[3] *Congreso de la República de Colombia, Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Bogotá D.C., Colombia, 1999.*

[4] *Ministerio de Comercio, Industria y Turismo, Decreto 1074 de 2015: Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Bogotá D.C., Colombia, 2015.*

[5] *Asamblea Nacional Constituyente, Constitución Política de Colombia. Bogotá D.C., Colombia, 1991.*

[6] *Superintendencia de Industria y Comercio (SIC), Entidad de supervisión en protección de datos personales. Bogotá D.C., Colombia. [En línea]. Disponible en: https://www.sic.gov.co*

[7] *International Organization for Standardization, ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. Ginebra, Suiza: ISO, 2022.*

[8] *National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD, USA: NIST, 2018.*

[9] *OWASP Foundation, OWASP Top 10: The Ten Most Critical Web Application Security Risks, 2021. [En línea]. Disponible en: https://owasp.org*

[10] *Ministerio de Transporte, Resoluciones sobre Centros de Diagnóstico Automotor (CDA). Bogotá D.C., Colombia.*

[11] *Nmap Project. (2024). Nmap Reference Guide. https://nmap.org/book/man.html*

[12] *Von Solms, B. and von Solms, R. (2004) The 10 Deadly Sins of Information Security Management. Computers & Security, 23, 371-376. https://doi.org/10.1016/j.cose.2004.05.002*

[13] *Hollnagel, Erik. (2014). Resilience engineering and the built environment. Building Research and Information. 42. 10.1080/09613218.2014.862607.*

[14] *Cavoukian, Ann & Taylor, Scott & Abrams, Martin. (2010). Privacy by Design: essential for organizational accountability and strong business practices. Identity in the Information Society. 3. 405-413. 10.1007/s12394-010-0053-z.*

[15] Hiatt, J. (2006). *ADKAR: A Model for Change in Business, Government and Our Community*. Prosci Research.

[16] Prosci (2018). *Best Practices in Change Management*. Prosci.
[17] Deming, W. E. (1986). *Out of the Crisis*. MIT Press.