



GRUPO
IPMéxico

INFORMATICA PROFESIONAL DE MEXICO S.A. DE C.V.

*Programación y Desarrollo
de Software a la Medida
Control de Acceso*

SEGURIDAD DE DATOS



GRUPO
IPM México

Informatica Profesional de México S.A. de C.V.

*Programación y Desarrollo
de Software a la Medida
Control de Acceso*



GRUPO
IPM México

Dictamen Técnico de Seguridad Informatica

Nombre de la Empresa: GRUPO IPMEXICO
Director General: Hugo Guevara Ruíz
Domicilio: *Av. Río Churubusco M4. L16. F11, Col. Agrícola Pantitlán, Alc. Iztacalco, Cp. 08100 CDMX, México
Tels./Fax: (800) 841-9871
R.F.C. IPM130219T90 Mail. soporte@grupoipmexico.mx
Escritura Pública. No.31,149, Volumen 629, Folio 048-055, NT00055307

Como antecedente, el que suscribe como director general de GRUPO IPMEXICO, inició labores en el mercado en el año de 1990 como IPCOM mantenimiento preventivo, correctivo y venta a equipos de cómputo.

Para el año 2012 incursionamos como empresa independiente con el nombre de **INFORMÁTICA PROFESIONAL DE MÉXICO, S.A. DE C.V. (IPM)**. Incursionando en desarrollo de software, venta de hardware para control de acceso. así como licencias, mantenimiento preventivo y correctivo, asesoría en software e instalación de redes, elaboración de plataformas dedicadas a el control de acceso.

GRUPO IPMEXICO CONTROL DE ASISTENCIA ESCOLAR Y TRAYECTORIA ACADÉMICA (CAETA), y sus filiales son una marca registrada ante el **Instituto Mexicano de la Propiedad Industrial (IMPI)** con el **registro 251993, folio de salida 20200886678 y expediente No. 2244061**, con fecha de registro el 05 agosto del 2019., teniendo así los **derechos de autor y propiedad intelectual** de dicha plataforma (CAETA) control de acceso, con numero de **registro 03-2025-110411011000-01** ante el **Instituto Mexicano de los Derechos de Autor (INDAUTOR)**. de la misma manera, contamos con el certificado (**US TSA CERTIFICATE**) de la **Unión Europea** con encriptación de datos de proyecto para plataforma control de acceso y seguimiento académico, Y **numero de registro 00d08c14f48e9b2b352a8d8df6fdebb09acd355815** con encriptación de datos internacionales No. (**a32e7f62-8c69-461e-affd-d7e*******), designando a Informatica Integral de Hidalgo como la única autoría de dicha encriptación.

Tipo de Desarrollo de la plataforma Control de Asistencia Escolar Y Trayectoria Académica (CAETA).

En un entorno digital donde la protección de la información es crucial, implementar medidas de seguridad adecuadas para servidores y bases de datos es una prioridad. En este contexto, la combinación de un Servidor operando con PostgreSQL mediante Cloudflare representa una solución robusta y confiable para garantizar la integridad y privacidad de los datos. El uso de **Cloudflare** como intermediario entre los usuarios y el servidor proporciona una capa adicional de protección mediante su sistema de mitigación de ataques DDoS, filtrado de tráfico malicioso y cifrado SSL/TLS, asegurando que cualquier comunicación entre el usuario y el servidor se realice de manera segura. Además, su capacidad para gestionar reglas de acceso y optimizar la distribución de contenido refuerza la seguridad del sistema.

Por otro lado, **PostgreSQL** es reconocido por sus avanzadas características de seguridad, incluyendo autenticación reforzada y mecanismos de cifrado de datos. Para garantizar la protección de la información almacenada, se implementan técnicas como **cifrado transparente de datos (TDE)**, **cifrado a nivel de aplicación** y **cifrado de conexión con SSL**, lo que impide accesos no autorizados y protege la base de datos ante posibles vulnerabilidades.

Además de estas medidas técnicas, este servidor cuenta con **registro ante los derechos de autor**, asegurando la propiedad intelectual que se gestiona en la plataforma. Este registro otorga respaldo legal y protección a los contenidos alojados, evitando usos indebidos y garantizando su autenticidad.

La seguridad informática es un proceso continuo y dinámico. La combinación de un Servidor con PostgreSQL, la protección de Cloudflare y el uso de cifrado avanzado constituye una infraestructura confiable para la gestión y resguardo de datos críticos, reforzada con el reconocimiento legal de la propiedad intelectual. Implementar estas tecnologías y estrategias de seguridad no solo protege la información, sino que también genera confianza en los usuarios y colaboradores.

Es importante mencionar que como máxima protección para la información almacenada contamos con un firewall **SRX-300** de manera física, con las siguientes características.

I-DATOS GENERALES DE LA JUNTA Y EL EXPEDIENTE

Dominio y Hosting Web	Dominio en Neubox. Hosting Web y CDN en CloudFlare.
ISP	Totalplay con Dirección IP Fija.

II. ANÁLISIS DE LA INFRAESTRUCTURA ACTUAL FIREWALL SRX-300 (NGFW)

El análisis de la infraestructura revela los siguientes componentes clave y sus **brechas de seguridad actuales**:

- **Servidor de Base de Datos:** Corre sobre **Windows Server 2022 Datacenter** y utiliza **PostgreSQL** como motor de base de datos. Aloja el *backend* y los datos esenciales del negocio.
- **Conectividad:** Se utiliza un servicio **ISP (Totalplay)** con una **IP Fija**, lo que imposibilita la identificación y el *targeting* directo del servidor por parte de atacantes externos.
- **Aplicativo Móvil:** La existencia de un aplicativo móvil implica que la API de la base de datos nunca este **expuesta**, e imposibilita la superficie de ataque.
- **Seguridad Web (Parcial):** La página web esta beneficiada con la protección por **CloudFlare** (CDN, *Web Application Firewall* básico, mitigación de DDoS), lo cual es positivo, ya que esta protección se extiende al servidor de base de datos o a la API del aplicativo móvil.

el *hardware Juniper SRX-300* debido a sus capacidades nos brinda:

1.**Seguridad de Estado (Stateful Firewall):** Control estricto de las sesiones y el flujo de tráfico.

2.**Filtrado por Aplicación y Usuario:** Capacidad de inspección profunda (*Deep Packet Inspection* - DPI protege la API del aplicativo móvil y la conexión al servidor de PostgreSQL.

3.**Mitigación de Amenazas:** El SRX-300 proporciona servicios de *Intrusion Prevention System* (IPS) que son esenciales para defender el servidor contra *exploits* dirigidos a Windows Server 2022 o a PostgreSQL.

Gestión de Puertos: todos los puertos del servidor están cerrados, excepto aquellos estrictamente necesarios para la administración (vía VPN) y la conexión de la aplicación móvil.

- **Endurecimiento del SO y DB:** aplica políticas de seguridad estrictas en **Windows Server 2022** y en la configuración de **PostgreSQL** (ej. autenticación fuerte, cifrado de tráfico de la DB).

DIAGRAMA DE CONEXIÓN DE FIREWALL SRX-300

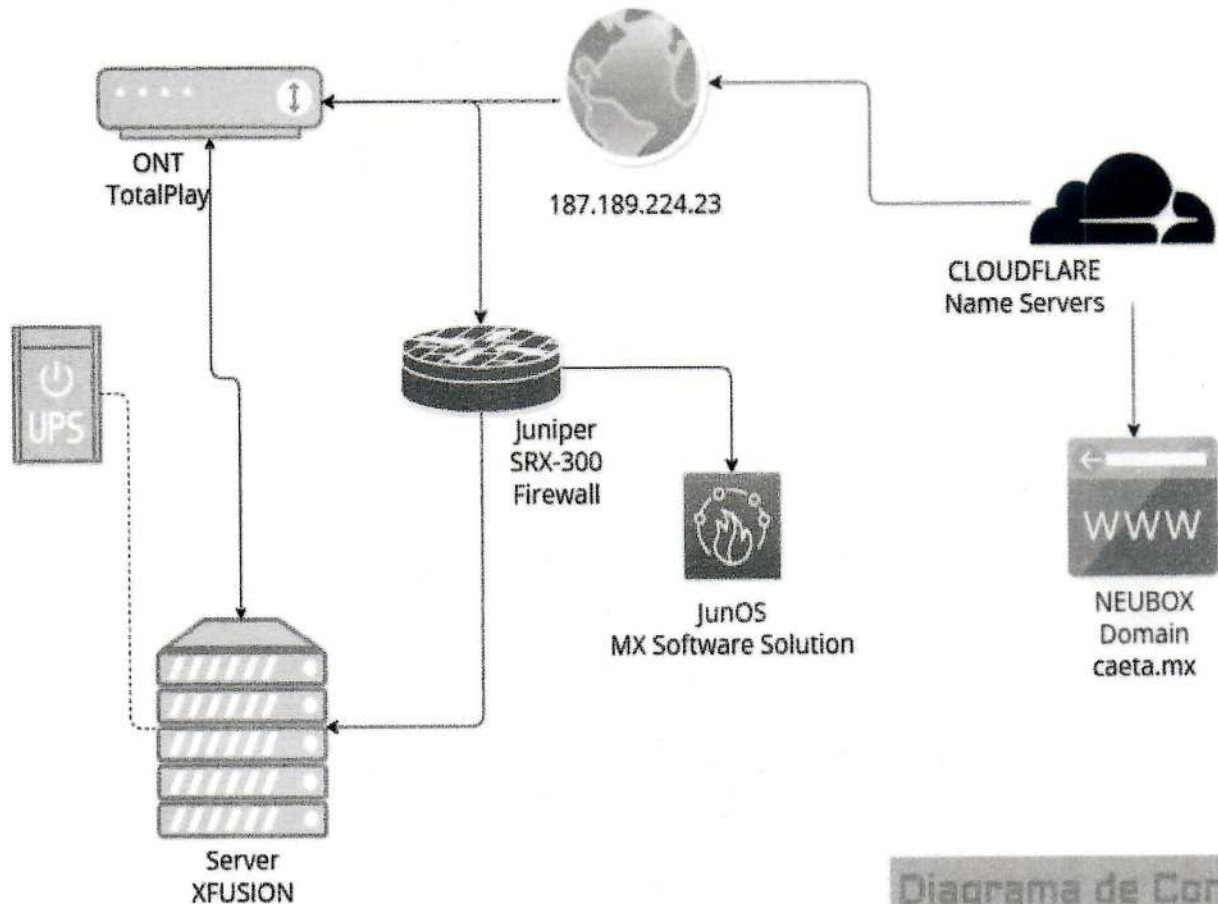


Diagrama de Conexión

A su vez, queremos reiterar que el sistema de control de acceso implementado en su institución es un desarrollo exclusivo de nuestro equipo en Informática Profesional de México S.A. de C.V.

Esta plataforma ha sido diseñada, programada y optimizada completamente por nuestro equipo de especialistas, lo que nos convierte en los únicos con la capacidad y el conocimiento técnico necesario para garantizar su correcto funcionamiento.

Nuestra responsabilidad abarca la actualización, mantenimiento, gestión de datos y evolución del sistema, asegurando así su estabilidad, seguridad y eficiencia. Dado que se trata de una solución propietaria.

Estamos a su disposición para cualquier consulta o requerimiento adicional. Agradecemos su confianza y reiteramos nuestro compromiso con brindarles un servicio de la más alta calidad.

ATENTAMENTE

ING. BRYAN GUEVARA PÉREZ

Desarrollador y PM de Software

www.grupoipmexico.mx

soporte@grupoipmexico.mx

Av. Río Churubusco M.4 L.16 Fracc.11, Col. Agrícola Pantitlán, Alc. Iztacalco, CDMX, Tel. 800 841 9871