DOCUMENTO DE ARQUITECTURA DE LA SOLUCIÓN

Plataforma Krixo — Monitoreo de exposición cibernética y validación ofensiva

Campo	Detalle
Cliente	Federación Colombiana de Municipios
Dominios en alcance	fcm.org.co / simit.org.co
Elaborado por	Rubén Darío Zuluaga — Preventa, Krixo
Fecha	03/09/2026

1. Objetivo

Este documento describe la arquitectura funcional de la solución implementada sobre la plataforma Krixo para la Federación Colombiana de Municipios detallando el flujo de información de cada módulo habilitado, desde la fuente de datos hasta la entrega del hallazgo al equipo de seguridad, y deja constancia de la transferencia de conocimiento realizada al equipo técnico del cliente.

El alcance cubre cuatro frentes: monitoreo de exposición e inteligencia de amenazas sobre los dominios principales, protección de marca y detección de phishing, vigilancia de perfiles VIP, y validación ofensiva a partir de la integración con el escáner de vulnerabilidades del cliente.

2. Arquitectura general

La arquitectura es de tipo SaaS multi-tenant y no requiere agentes desplegados en la infraestructura del cliente para los módulos de monitoreo. Krixo recolecta y correlaciona información desde fuentes externas —dark web, deep web, foros clandestinos, canales de Telegram, marketplaces de credenciales y registros de dominios— y desde las integraciones que el cliente habilita vía API key; todo hallazgo pasa por análisis dentro de la plataforma, se almacena con trazabilidad en el repositorio de evidencias y se notifica por correo. El acceso es por consola web con autenticación y control de acceso basado en roles, de modo que cada perfil solo ve los módulos y la información que le corresponden.

2.1 Módulos habilitados

Módulo	Función principal
Threat Intelligence + Data Vault	Monitoreo de exposición y gestión de evidencias
Phishing Inspector	Detección de dominios fraudulentos y takedown
VIP Threat Watch	Vigilancia de exposición de perfiles ejecutivos
Xploit Studio & Pentesting	Priorización de vulnerabilidades y pentesting

3. Threat Intelligence + Data Vault

El módulo toma como entrada los dominios principales de la organización y ejecuta monitoreo continuo sobre las fuentes de inteligencia de Krixo. Sobre cada dominio se buscan correos corporativos expuestos, contraseñas y credenciales filtradas, sesiones comprometidas provenientes de stealer logs, documentos filtrados, menciones de la organización y activos expuestos identificados en la superficie de ataque externa.

Cada hallazgo se envía al Data Vault, que funciona como repositorio de evidencias con integridad por hash y marca de tiempo. Ahí es donde el equipo gestiona el ciclo de vida del hallazgo: revisión, clasificación, validación de la credencial y cierre. Es importante entender que el Data Vault es un repositorio de evidencia y trazabilidad, no un gestor de contraseñas ni una bóveda de secretos operativa.

La notificación se hace por correo electrónico y se configura por tipo de evento desde el módulo de Settings, de manera que el equipo recibe la alerta apenas se detecta nueva evidencia sin depender de que alguien esté revisando la consola.

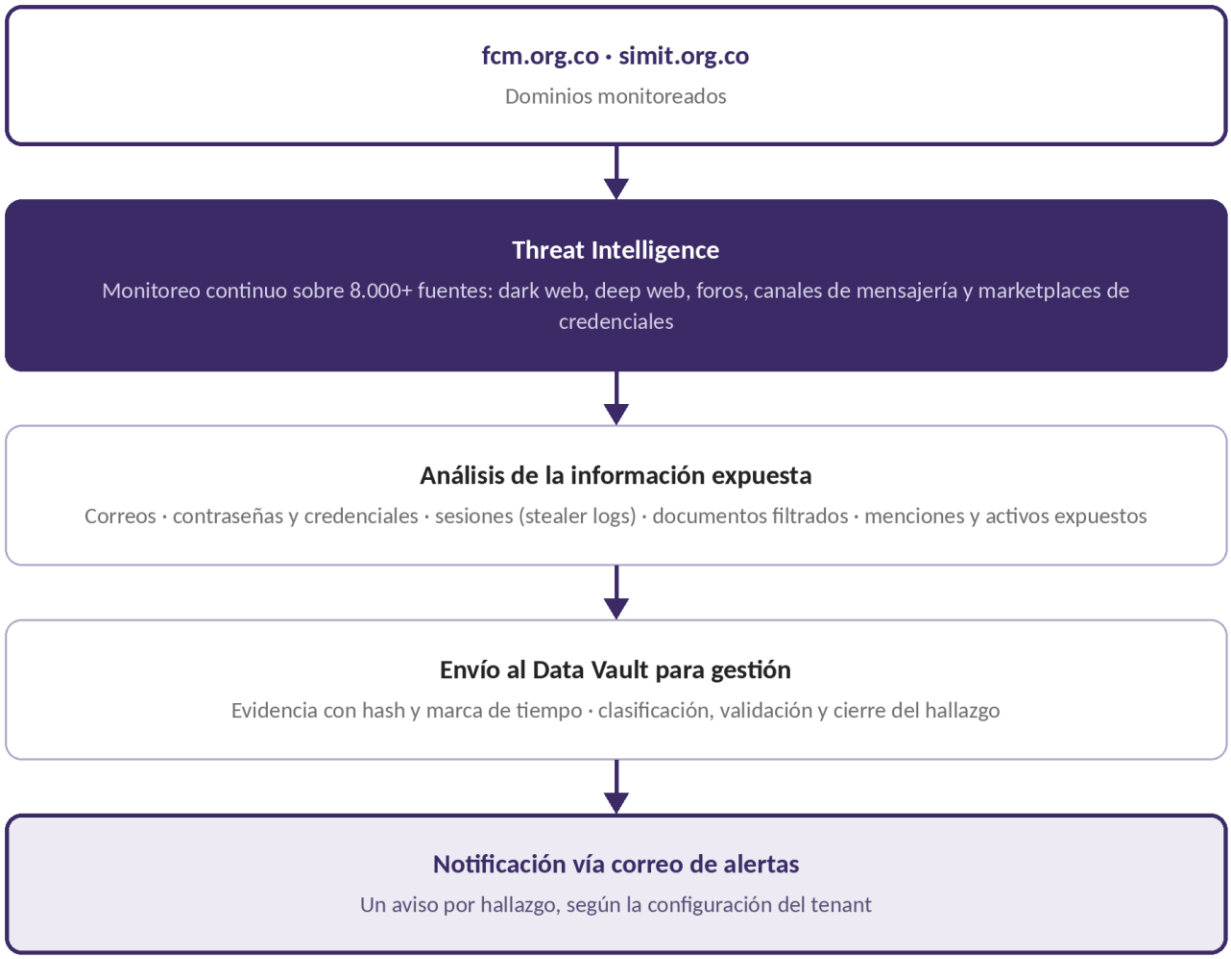


Figura 1. Flujo de Threat Intelligence + Data Vault

4. Phishing Inspector

Partiendo de los mismos dominios principales, el módulo monitorea el registro de dominios similares y variantes de escritura —typosquatting— que puedan usarse para suplantar a la organización, además de detectar defacement sobre los sitios legítimos. La lógica no es solo detectar el dominio parecido, sino determinar si efectivamente está siendo usado para suplantar.

Para eso, sobre cada dominio candidato se levanta evidencia: capturas del sitio, uso de logos y elementos de marca, análisis del código de la página en busca de formularios de captura de credenciales o kits de phishing conocidos, y un análisis asistido por IA que consolida esos elementos y determina el nivel de riesgo y la probabilidad real de suplantación.

Cuando el análisis confirma la suplantación, el caso pasa a takedown. El proceso se puede iniciar desde la plataforma o escalar como solicitud de servicio de takedown a través del equipo de Krixo, y queda registro del estado de la solicitud y de la evidencia que la soporta.

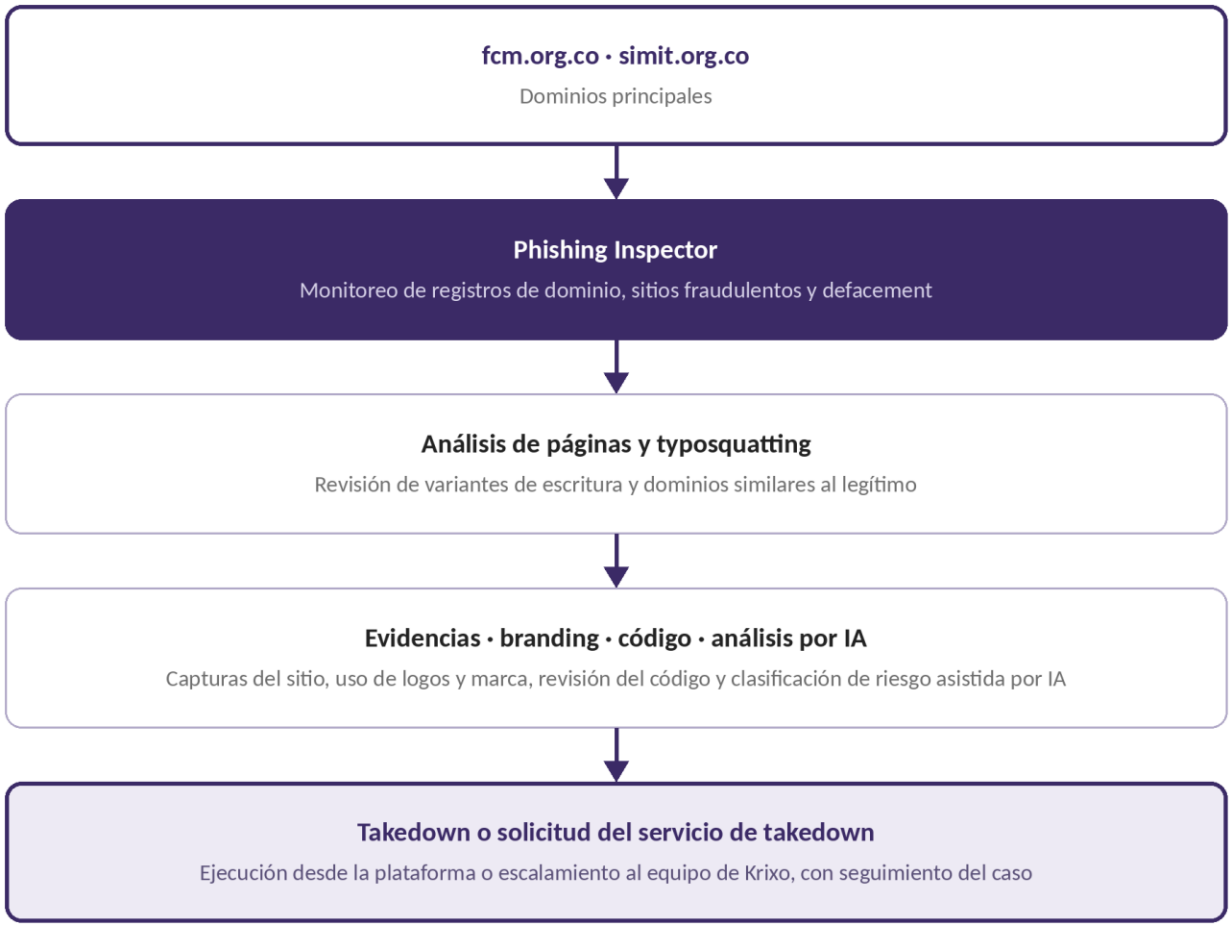


Figura 2. Flujo de Phishing Inspector

5. VIP Threat Watch

El módulo trabaja sobre una lista definida de correos y perfiles VIP —normalmente nivel directivo y cuentas críticas de la operación— y monitorea de forma continua si esas identidades aparecen en filtraciones, brechas de terceros o registros de credenciales expuestas.

Ante una filtración se genera la alerta con el detalle de la fuente, el tipo de dato expuesto y la fecha de la brecha, y a partir de ahí el equipo ejecuta la remediación —cambio de contraseña, cierre de sesiones, habilitación de segundo factor— y el módulo permite verificar y documentar que la contención efectivamente se aplicó, dejando la evidencia del proceso.

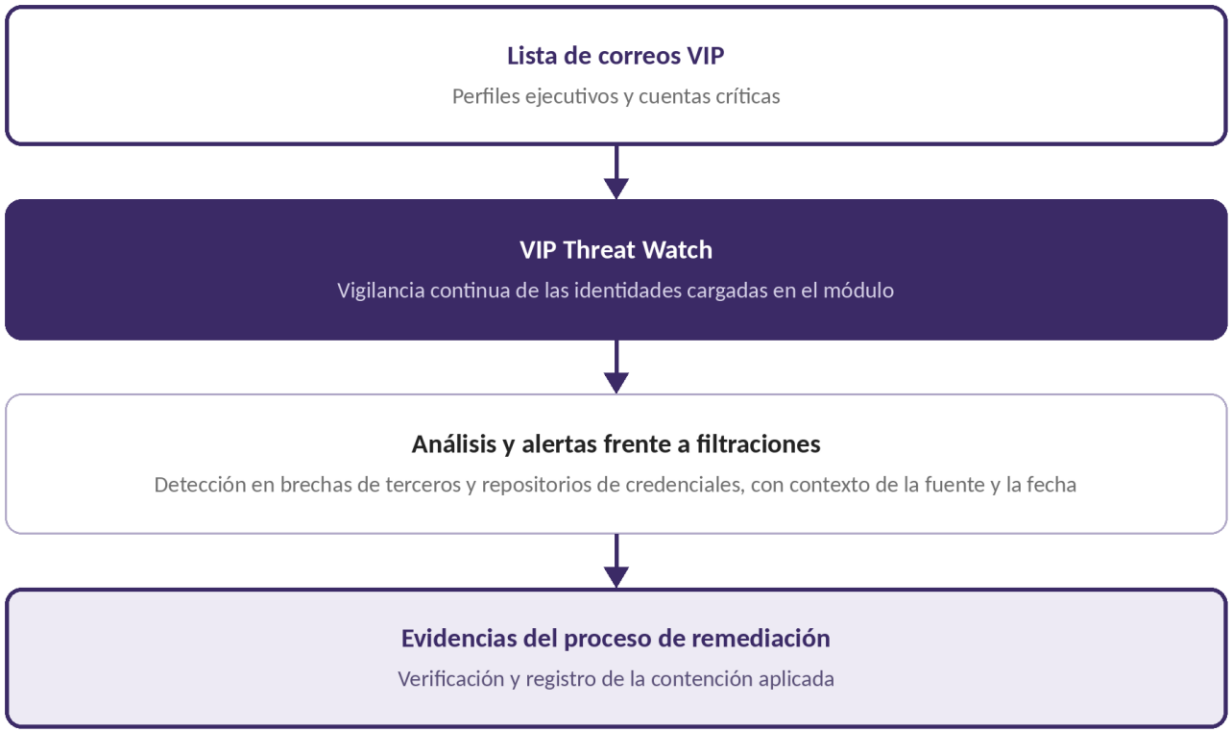


Figura 3. Flujo de VIP Threat Watch

6. Xploit Studio & Pentesting

La integración se establece mediante API key contra la consola de Tenable del cliente, de modo que Krixo consume los resultados de los escaneos existentes sin duplicar el escaneo ni exigir un cambio de herramienta. La conexión se configura desde el módulo de integraciones y el escáner queda disponible para asociarse a los Engagements que se creen.

Una vez ingestados, los hallazgos se correlacionan y deduplican, y se priorizan por Risk Priority Score y porcentaje de explotabilidad, cruzando el catálogo CISA KEV y el mapeo MITRE ATT&CK para separar lo que es realmente explotable de lo que es ruido del escáner. Sobre esa base se ejecutan dos líneas de trabajo: pruebas de penetración autónomas desde la plataforma para validar la explotabilidad real de la vulnerabilidad, y pruebas de consultoría ejecutadas por el equipo de servicios, que se documentan dentro del mismo Engagement.

El resultado se consolida en el submódulo de Deliverables, que genera los reportes y paquetes de evidencia exportables del Engagement, con el detalle técnico de los hallazgos, la validación de explotabilidad y el plan de remediación.

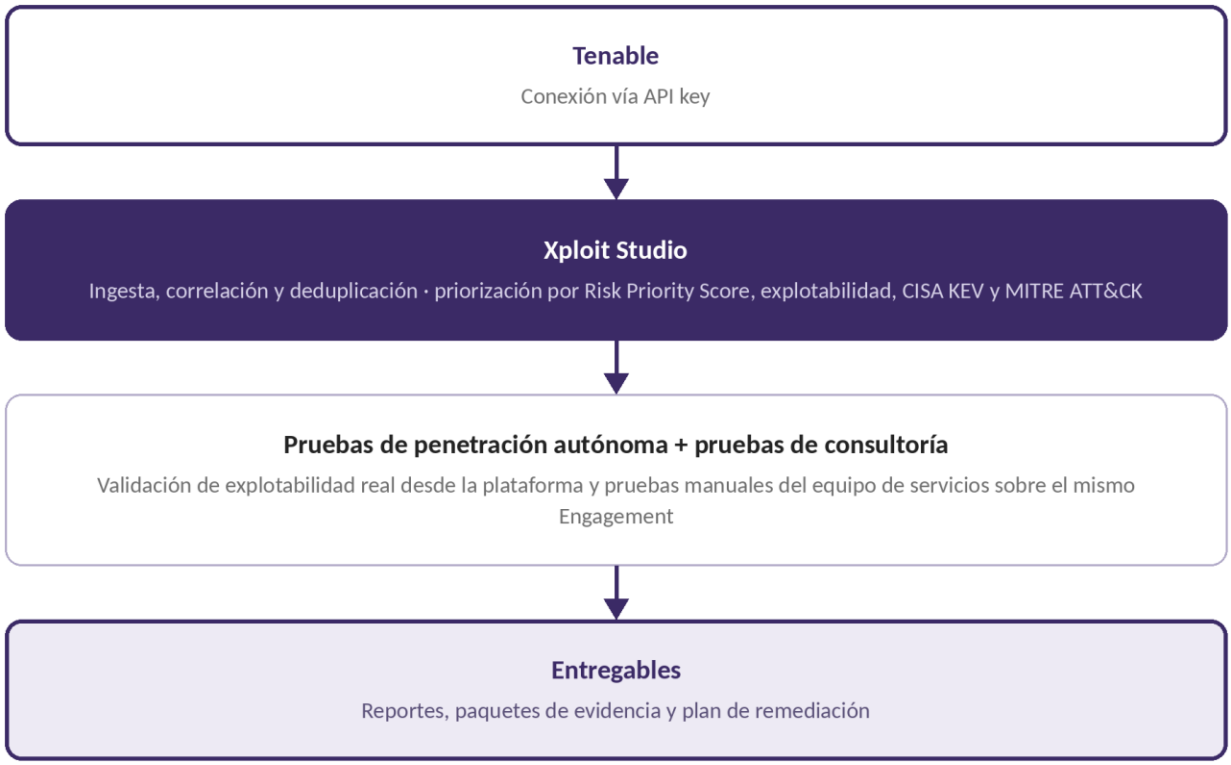


Figura 4. Flujo de Xploit Studio & Pentesting

7. Transferencia de conocimiento

Se realizó sesión de transferencia de conocimiento con el equipo técnico de Federación Colombiana de Municipios **FCM**, cubriendo la configuración inicial, la administración de la plataforma y la operación de cada uno de los módulos habilitados. Los temas trabajados fueron los siguientes.

7.1 Configuración inicial y administración

- Configuración inicial de la plataforma y recorrido por el módulo de administración.
- Creación de perfiles y usuarios en la plataforma, con asignación de roles y permisos por módulo.
- Generación de API Key desde la consola.
- Cambio de contraseña de la cuenta desde el módulo de Settings.

7.2 Visualización de módulos habilitados

Se generó la visualización de los módulos habilitados en la plataforma para el tenant del cliente:

- Threat Intelligence + Data Vault
- VIP Threat Watch
- Phishing Inspector
- Xploit Studio & Pentesting

7.3 Operación y análisis de la información

Se explicó el funcionamiento de cada módulo y se entregaron recomendaciones para el análisis de la información y la administración de los datos: criterios de priorización de hallazgos, manejo del ciclo de vida de la evidencia dentro del Data Vault, uso de los filtros y estados para separar lo crítico del ruido, y buenas prácticas para el manejo confidencial de las exportaciones, dado que contienen información sensible de la infraestructura.

7.4 Configuración de Xploit Studio

Se configuró el módulo de Xploit Studio con la API key de Tenable, dejando la integración establecida y el escáner disponible para asociarse a los Engagements.

8. Pendientes y seguimiento

Durante la sesión se identificó que los datos traídos desde Tenable no se actualizaron en la plataforma después de establecer la integración. Se generó ticket de soporte con el equipo técnico de Krixo para revisar la sincronización y el estado de la ingesta de hallazgos.

Ítem	Descripción	Estado
Sincronización Tenable	Los datos traídos desde Tenable no se reflejaron actualizados en Xploit Studio tras la configuración de la API key. Se generó ticket de soporte para revisión.	Abierto

El seguimiento del caso se hace por la plataforma de tickets de soporte de Krixo hasta el cierre y validación con el cliente.