Caso de éxito

TÍTULO DEL CASO DE USO DE INTELIGENCIA ARTIFICIAL EN EL SECTOR PÚBLICO COLOMBIANO

Programa de Fortalecimiento de Habilidades y Herramientas de Inteligencia Artificial para el Sector Público

Nombre Autor (a): Luis Felipe Boada López

2025

1. Nombre del Caso/Iniciativa

Gobernación de Bolívar: sistema de respuesta automatizada con Inteligencia Artificial (SOAR-IA) para proteger infraestructuras críticas frente a ciberataques.

2. Entidad(es) Responsable(s)

Gobernación de Bolívar, Secretaría TIC – infraestructura

3. Sector Administrativo (Salud, Justicia, Educación, etc.)

Gobierno y administración pública departamental

4. Área de Aplicación

Mejora de la Fiscalización, Seguridad y Justicia

5. Problema Público Abordado

La tarea a optimizar es la gestión de incidentes de seguridad digital y la protección de servicios críticos. La Gobernación ha sido víctima de ciberataques que han comprometido sistemas y generado interrupciones en trámites y servicios, lo que evidencia que los mecanismos de defensa tradicionales, basados en firmas y reglas estáticas, resultan insuficientes frente a amenazas sofisticadas como el ransomware. Estos ataques afectan la continuidad del recaudo, la prestación de servicios en línea y la confianza de la ciudadanía en la capacidad institucional para resguardar datos personales y recursos públicos. Se plantea como punto de partida la necesidad de implementar el Sistema Nacional de Ciberinteligencia y Respuesta Automatizada (SNCRA) y de alinear esta implementación con el marco de gobernanza existente (Resolución 261 de 2023, PSPI 2025, Decreto 338 de 2022)

6. Solución de IA Implementada

La solución se formula como un diseño de sistema basado en IA denominado “Guardián Bolívar”, integrado al SNCRA y orientado a la prevención de pérdidas y a la respuesta rápida ante incidentes. Se describe la solución como un conjunto de módulos de analítica predictiva y orquestación automática de respuesta (SOAR-IA). En una primera fase, la Gobernación identifica activos y datos críticos y prioriza los logs y el tráfico de red de los sistemas de impuestos y trámites en línea, utilizando también los datos de incidentes pasados para entrenar modelos de machine learning que

aprendan patrones específicos de ataque en el entorno de Bolívar. Al mismo tiempo, el Comité de Seguridad de la Información debe aprobar formalmente la adopción del sistema, integrándolo en los procedimientos de gestión de incidentes definidos en el PSPI 2025. En la segunda fase, la solución despliega un módulo de detección de anomalías de red, que monitorea en tiempo real el flujo de datos entre municipios y Gobernación y detecta picos anómalos de tráfico saliente (indicativos de exfiltración de datos) o comportamientos típicos de cifrado malicioso, según la tabla de módulos del SNCRA. En la tercera fase, un componente de priorización inteligente de alertas clasifica los eventos según la criticidad del activo afectado: por ejemplo, una alerta en el servidor de liquidación de impuestos se marca como prioridad crítica (P1) y desencadena una respuesta automatizada inmediata, mientras una alerta en un sitio meramente informativo recibe prioridad baja (P4).

En la cuarta fase, entra en juego la respuesta automatizada (SOAR-IA)**:** el sistema aísla subredes afectadas, bloquea direcciones IP de origen inusual, limita el tiempo de permanencia del atacante en la red a minutos o segundos y ejecuta playbooks de contención de manera autónoma, siempre con registro auditable de cada acción.

Finalmente, la solución incorpora mecanismos de fiabilidad y mitigación de riesgos: validación y enriquecimiento de datos de alerta desde varias fuentes para evitar el efecto GIGO, gestión de falsos positivos y negativos mediante comparación con líneas de base de comportamiento y registro detallado para auditoría y mejora continua. Además, se proponen prompts de análisis estratégico para asistentes de IA generativa, con el fin de elaborar diagnósticos y planes alineados con el marco normativo nacional (CONPES 3995, Decreto 338, MSPI).

7. Tecnologías Utilizadas (ej. PLN, Visión por Computador, Machine Learning)

La solución se basa en analítica predictiva y machine learning aplicados a grandes volúmenes de logs de seguridad, con técnicas de detección de anomalías de red y ciberinteligencia para identificar patrones de ataque. Sobre esa capa de analítica se construye un sistema SOAR-IA (Security Orchestration, Automation, and Response potenciado por IA), que automatiza decisiones de defensa en tiempo real y ajusta las respuestas según la evolución del incidente. Se usaron asistentes de IA generativa mediante prompts específicos para desarrollar análisis estratégicos sobre valor público, innovación, fiabilidad y cumplimiento del marco regulatorio, aunque no menciona marcas comerciales concretas (por ejemplo, ChatGPT o similares). Por tanto, la solución se apoya en modelos de machine learning para la parte operativa

(detección y respuesta) y en modelos de lenguaje para el análisis estratégico y documental, pero no queda claro qué herramientas o proveedores específicos se utilizarían en la implementación.

8. Resultados

Se plantean resultados como metas o KPIs esperados, ya que se trata de una propuesta de implementación. En el escenario previo, la defensa es reactiva y manual, con tiempos de respuesta prolongados, alta carga de trabajo del personal especializado, riesgo de falsos positivos que afectan servicios legítimos, posibilidad de falsos negativos que permiten ataques exitosos, y episodios de caída de servicios que impactan el recaudo de impuestos y los trámites ciudadanos. Con el despliegue de SOAR-IA, se espera una reducción del 90 % en el tiempo medio de respuesta (MTTR), pasando de horas a segundos para contener un ataque; una disminución del 85 % en la tasa de falsos positivos, lo que liberaría aproximadamente el 80 % del tiempo del personal analista para tareas estratégicas; y un aumento de la disponibilidad de servicios críticos hasta niveles cercanos al 99,9 %, según la tabla de indicadores clave incluida en las páginas 10 y 11. Desde la perspectiva del valor público, los beneficios esperados incluyen: protección de ingresos al evitar interrupciones en sistemas de recaudo, fortalecimiento de la confianza de la ciudadanía al saber que sus datos y trámites están bajo un sistema proactivo de seguridad y mejora de la transparencia y el control interno al monitorear accesos a bases de datos financieras y de contratación para detectar patrones inusuales que podrían estar asociados a fraude o corrupción interna, como se resume en la tabla de “Beneficios y valor para el público de Bolívar”.

9. Factor de Sostenibilidad y Escalabilidad

La propuesta sitúa a la Gobernación de Bolívar como modelo regional (CSIRT-Región). El sistema puede replicarse en alcaldías municipales del departamento, que manejan información sensible pero cuentan con menos recursos técnicos y humanos. Se plantea la creación de un Centro de Monitoreo de Seguridad asistido por IA para todo el territorio, con una infraestructura centralizada que presta servicios de ciberseguridad a varias entidades. En términos de sostenibilidad, se destaca el aprovechamiento del programa Talento Tech del MinTIC para formar talento local en ciberseguridad e IA, así como el uso de infraestructura en la nube para entrenar modelos de deep learning, evitando inversiones iniciales elevadas en hardware y permitiendo escalar recursos según la demanda. La solución se alinea con el marco regulatorio nacional (CONPES 3995 de 2020, Decreto 338 de 2022, Modelo de Seguridad y Privacidad de la Información del MinTIC), de modo que la automatización de la respuesta y la verificación contribuye directamente al aumento del índice de madurez de seguridad

digital (FURAG) y al cumplimiento de la Política de Gobierno Digital. Para la ciudadanía, los beneficios se expresan en continuidad de trámites y servicios esenciales, protección de datos personales, menor probabilidad de interrupciones por ataques y fortalecimiento de la confianza en la capacidad del Estado departamental para gestionar riesgos digitales de manera profesional, transparente y auditada.