



DOTLAKE EN LA ADMINISTRACIÓN PÚBLICA

Whitepaper

LA IMPORTANCIA DE LA CIBERSEGURIDAD EN LA ADMINISTRACIÓN PÚBLICA

La Administración Pública desempeña un papel esencial en la **prestación de servicios a los ciudadanos**, la gestión de datos sensibles y la toma de decisiones críticas para el **bienestar de la sociedad**. Sin embargo, este papel crucial también la convierte en un **objetivo atractivo para los ciberdelincuentes** y amenazas cibernéticas en constante evolución

Pero, ¿qué desafíos debe encarar la administración pública?

- **Amenazas Emergentes:** el sector público se enfrenta a amenazas cibernéticas en constante evolución, desde ataques de ransomware hasta robos de identidad.
- **Información Sensible:** el manejo de datos sensibles, como información de ciudadanos y operaciones gubernamentales, requiere medidas de seguridad robustas.
- **Evaluación de Riesgos:** La evaluación efectiva de riesgos de proveedores es esencial para garantizar la integridad y seguridad de los sistemas gubernamentales.

Y con el fin de ayudar a la administración pública nace **Dotlake CTI**, una solución que se encarga de recopilar información de forma automatizada de la **deep web, darknets, ransomsites, telegram y foros ciberdelinquentes** más importantes del mercado para que puedas consumirla de forma rápida y segura y así poder monitorizar y prevenir dichos ataques incluso antes de que puedan suponer una amenaza real.

¿Qué te ofrece Dotlake CTI?

Y no solo eso...

- **Protección Ciudadana:** Dotlake contribuye directamente a la protección de los ciudadanos al salvaguardar su información personal y mantener la confianza en las instituciones gubernamentales.
- **Prevención Proactiva:** La capacidad de anticipar y prevenir amenazas antes de que se materialicen proporciona una ventaja crucial en la defensa cibernética.
- **Cumplimiento Normativo:** Dotlake ayuda al sector público a cumplir con regulaciones de ciberseguridad, garantizando estándares elevados en la protección de datos.
- **Portal de investigación** para evaluar el nivel de riesgo aumentando tu capacidad de análisis de la gravedad de las amenazas, su alcance y su potencial impacto a través de su monitorización constante.
- **Detección de filtración de contraseñas** permite mitigar el riesgo de accesos no autorizados.
- **Prevención proactiva y evaluación de riesgos de proveedores** fortaleciendo las defensas contra amenazas externas.