



**Government
deploys safe,
secure, manageable
solutions to prevent
major breaches**



**Secretaría
de Finanzas,
Inversión y
Administración**

In the face of international accountability and with no room for error, Kaspersky provides the Guanajuato State Government with unerring, reliable, manageable protection.



Public sector

- Guanajuato, Mexico.
- Using **Kaspersky Endpoint For Business Advanced**, **Kaspersky Endpoint Detection and Response Optimum**, **Kaspersky Security for Internet Gateway**, **Kaspersky Managed Detection and Response Expert**, and **Kaspersky Enhanced Support**.
- High levels of transparency and accountability enables safe, secure operations for Guanajuato State's public sector.

2

Major potential security incidents detected and repelled.

\$885 million (USD)

Foreign direct investment (FDI) in the state of Guanajuato.

“Kaspersky MDR successfully detected and halted a zero-day attack that could otherwise have caused severe disruption to our operations.”

Daniel Huerta Santos
Cybersecurity Manager,
Guanajuato State Government.

About the customer

Transparency and data security is of vital importance in the public sector. Citizens need to be confident that their data and information are always fully protected – The Guanajuato Government in Mexico has sought out Kaspersky's proven solutions since 2008.

Challenges

The Guanajuato State Government is committed to providing its citizens with secure, personalized digital services. This commitment is especially significant given Guanajuato's status as a hub for information technology and creative industries, known for its world-class products and services.

Initially, when the government approached Kaspersky, they were facing challenges with secure endpoints, centralized administration, and appropriate levels of technical support. This was a concern due to Guanajuato's robust ITC sector being populated by industries such as automotive and agribusiness, all moving towards digital transformation and industry 4.0.

The region boasts a vibrant ecosystem, ideal for Internet of Things (IoT) companies, making security and transparency paramount. Guanajuato is currently crafting a digital agenda to take advantage of new technologies for social and economic growth. This digital transformation roadmap is vital for creating public policies that strengthen the technological landscape, all built on a foundation of security and risk management.

Managing these new technological solutions effectively required a simplification of its infrastructure, which was only possible with airtight security to avoid breaches and downtime. Cost-effectiveness was also a factor, with the government seeking to minimize expenses through strategic purchasing decisions.

The Kaspersky solution

To meet the organization's broad range of challenges, Kaspersky offered the Government of Guanajuato a range of fully integrated enterprise solutions, covering endpoint protection, threat intelligence, incident detection and response, and technical support.

- **Kaspersky Endpoint For Business Advanced**
Kaspersky Endpoint for Business Advanced provides The Guanajuato Government adaptive security that detects advanced threats. Server hardening enhances its protection with additional application, web, and device controls, to prevent the theft of organizational and financial information.
- **Kaspersky Endpoint Detection and Response Optimum**
Kaspersky Endpoint Detection and Response (EDR) Optimum delivers advanced detection, simple investigation, and automated response in an easy-to-use package, protecting government systems against the latest threats.



Security

When acting with and for the public sector, there is no room for error.



Detection

Kaspersky solutions boost confidence, agility and transparency.



Management

Each of the five deployed solutions is secure and highly manageable.



Confidence

The state's population can be assured of the safety and security of its data.

▪ **Kaspersky Security for Internet Gateway**

Secure internet access for employees is critical to all organizations today, and the Guanajuato Government is certainly no exception. [The Kaspersky Security for Internet Gateway](#) product delivers fast internet access to assist employees with their workload but with the added protection required by the organization through the following features:

- Clear visibility – Discovers threats on endpoints.
- Avoids getting stuck in the black box – Providing vital information on automatic detects and lurking threats with Indicators of Compromise (IoC).
- Simple analysis.
- Root cause analysis in a single incident card to understand where a threat came from.
- Automated response – Acting quickly to avoid damage.
- Easy 'single-click' actions and in-product guidance to prevent threats from spreading.

▪ **Kaspersky Managed Detection and Response Expert**

[Kaspersky Managed Detection and Response Expert](#) solution continuously hunts, detects, and responds to threats targeting Guanajuato's Government's entire IT infrastructure. The organization required a cost-effective and flexible managed service, including manual and automated security monitoring, threat hunting, detection, and response – all of which Kaspersky's cyber security analysts and experts provide round the clock.

▪ **Kaspersky Enhanced Support**

The Kaspersky professional services team also provides advanced training to the company's team on how to manage and optimize these solutions. The Kaspersky team also delivered training for IT administrators and operators on managing the installation, performing updates, and troubleshooting.



“The Kaspersky solutions are fully deployed and provide us with an excellent level of security.”

Daniel Huerta Santos
Cybersecurity Manager,
Guanajuato State Government.

Outcomes

The implementation of Kaspersky’s suite of solutions has led to significant benefits for the Guanajuato State Government both in the overall security, visibility, and management of their systems and in repelling attacks. Post implementation, the organization highlights two specific incidents where Kaspersky’s solutions helped to protect their systems from significant damage.

The first incident was a zero-day attack where even without a pre-existing signature, Kaspersky’s technology detected and stopped a large-scale attack. The support team then promptly investigated and updated the system with the necessary malware signature.

In the second case, an external computer infected with ransomware was identified upon connection to the government network. Kaspersky’s solutions quickly detected unusual behavior and alerted the relevant parties, allowing for a rapid response that prevented the situation from escalating.

The solutions offered by Kaspersky have simplified threat management and allowed for efficient handling of complex situations, supported by Kaspersky’s professional service. This ease of management, combined with the confidence instilled by the close relationship with Kaspersky and its channels, significantly enhances the Guanajuato State Government’s cybersecurity posture.

Key benefits noted by the organization include the reliability of Kaspersky’s tools, the quality of professional services, and the heightened confidence among users in performing their duties without the fear of malware. These outcomes collectively underscore Kaspersky’s critical role in bolstering the digital security framework of the Guanajuato State Government.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

kaspersky BRING ON
THE FUTURE

2024 AO Kaspersky Lab. All rights reserved.
Registered trademarks and service marks are the property of their respective owners.