NEO

IDEAS E INNOVACIÓN

3. INTELIGENCIA APLICADA A LA PROTECCIÓN DE INFRAESTRUCTURAS

INTELIGENCIA APLICADA A LA PROTECCIÓN DE INFRAESTRUCTURAS

En la última década, la mayor conciencia sobre las amenazas potenciales hacia la seguridad sobre las personas y las infraestructuras han hecho que el concepto de seguridad nacional haya adquirido un elevado protagonismo. Recientemente se han publicado un gran número de documentos sobre estrategias de seguridad nacional en EE.UU., Reino Unido, Francia, Holanda... que revisan el concepto de seguridad nacional y proclaman la importancia de contemplarlo como un concepto global, es decir, algo que no sólo compete al estado, sino que exige la participación de empresas privadas, ciudadanos y otras instituciones. Esta mayor importancia de la seguridad se ha traducido en un aumento de la demanda de soluciones en este ámbito, en las que tienen particular relevancia las tecnologías de la información y de las comunicaciones (TIC).

Las TIC permiten desarrollar soluciones innovadoras para anticipar los riesgos, prevenirlos, protegerse frente a ellos y responder de modo más eficaz ante las emergencias. Disponer de la información a tiempo y poder analizarla permite identificar, comprender y evaluar los riesgos y vulnerabilidades y determinar su impacto potencial. Contar con las herramientas y procedimientos adecuados facilita una actuación de forma eficaz y coordinada en caso de alarma o emergencia.

Las TIC pueden gestionar la protección de las personas, las infraestructuras críticas, los recursos económicos y tecnológicos, así como el patrimonio natural (bosques, ríos, acuíferos, etc.). Son, asimismo, la base para coordinar la adecuada respuesta ante una emergencia.

SISTEMAS "INTELIGENTES" DE PROTECCIÓN DE INFRAESTRUCTURAS

Más allá de la espectacularidad de los atentados de Nueva York, Madrid, Londres o Bombay, que contribuyeron a atraer las alarmas hacia la seguridad internacional, el problema del terrorismo es mucho más profundo: anualmente hay aproximadamente 11.800 ataques terroristas contra civiles en el Mundo, con el resultado de 54.000 muertos, heridos o secuestrados.

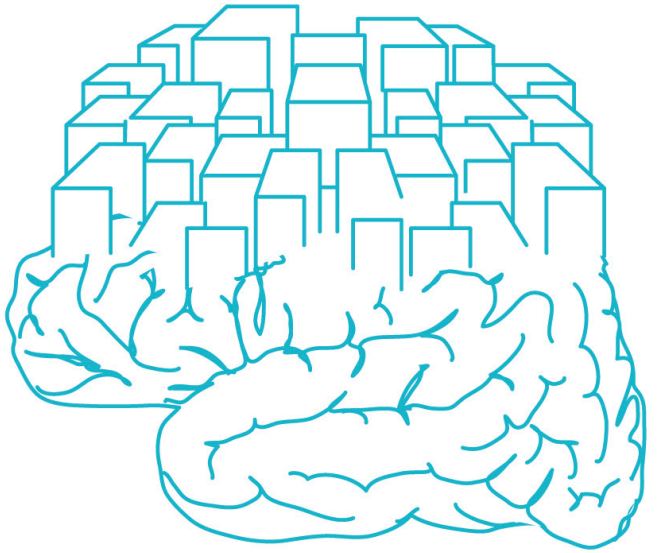
Pese a que el 40% de los ataques y el 35% de las víctimas se concentra en Oriente Medio , el problema no nos es tan ajeno: en el último año, la Unión Europea registró 300 ataques terroristas .

En este contexto, las soluciones para la protección de infraestructuras cobran un enorme protagonismo.

Obviamente, el principal objetivo de los sistemas para la protección de infraestructuras es, ante todo, proteger la vida humana, pero también subyace en ellos un importante componente de protección de intereses económicos y recursos que permiten el desarrollo de la actividad económica y social.

Pero el valor de estos sistemas no es única y meramente la protección de infraestructuras en sus distintas vertientes técnicas y en los distintos ámbitos de la actividad económica. El valor surge cuando dotamos a estos sistemas de inteligencia, ya que esto nos permite poder correlacionar y combinar la información proporcionada por los propios sistemas de protección y nos otorga un nuevo prisma de actuación: la anticipación.

Ya no hablamos de proteger, ahora hablamos de prevenir.



EL VALOR SURGE CUANDO DOTAMOS A ESTOS SISTEMAS DE INTELIGENCIA

¿QUÉ DEBE APORTAR UN SISTEMA DE INTELIGENCIA A LA PROTECCIÓN DE INFRAESTRUCTURAS?

La información que proporcionan los sistemas de protección de infraestructuras, en si misma, no permite obtener ninguna conclusión. Y esto resulta crucial cuando en el 60% de los ataques terroristas, no se ha podido determinar el responsable del ataque .

Por eso, es necesario un sistema que permita correlacionar y combinar la información. Pero, en concreto, ¿qué debe aportar un sistema de inteligencia a la protección de infraestructuras?

Recopilar la mayor cantidad de información disponible

Evaluar todas las posibles fuentes de información disponibles para valorar su adecuación de cara a permitir que el sistema se anticipe a los riesgos. Sobre todo, hay que tener en cuenta que la mejor herramienta para evitar la pérdida de información relevante es la integración de las fuentes de datos.

Adaptar la información recogida

Parte de la información obtenida de distintas fuentes de datos será de tipo no estructurado, por lo que se hace necesario su adaptación a una estructura que permita manejarla: fotografías, vídeos, documentos, transcripciones, etc.

La puesta en valor de la información se puede realizar con sistemas de reconocimiento de imágenes, almacenes de huellas, informes de vigilancia perimetral o similares, o sistemas de extracción de entidades en documentos.

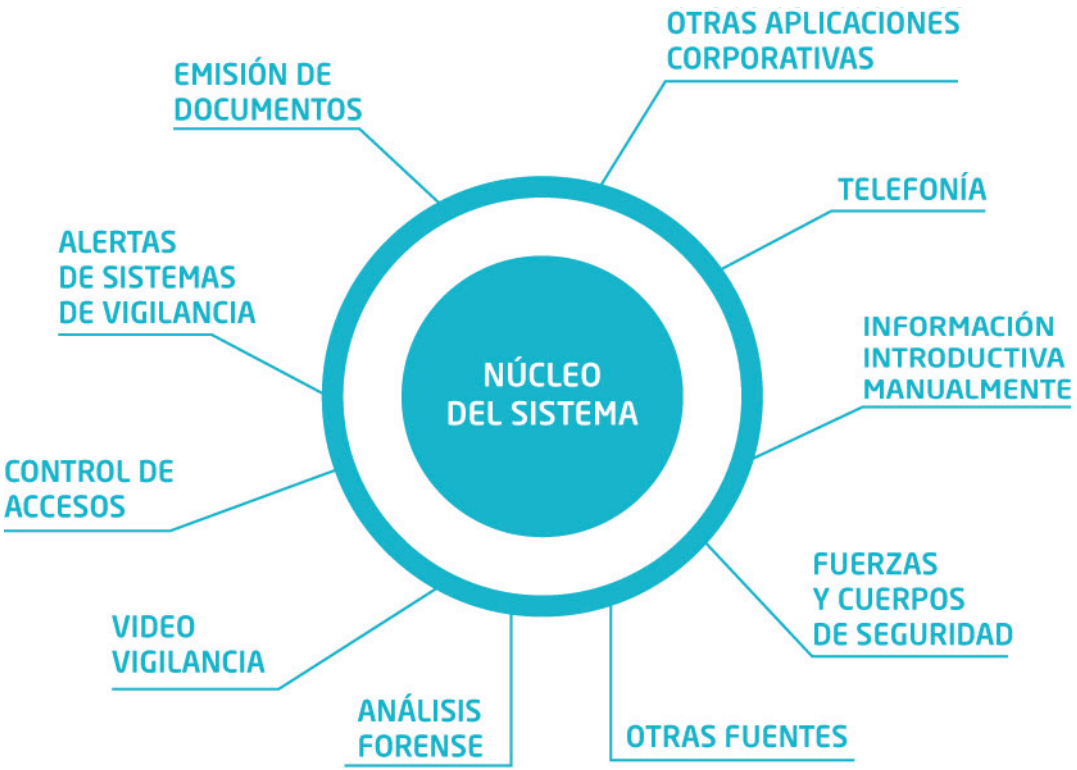
Buscar patrones, coincidencias y seguimientos

Este es el punto donde el sistema aporta inteligencia real.
A través de estos métodos, en base a algoritmos de búsqueda complejos, se evalúa la información y se comprueban posibles duplicidades de información que permiten encontrar patrones comunes, generar coincidencias entre datos dispersos o simplemente marcar información susceptible de ser objeto de especial atención debido a sus características particulares.

Ayudar a la toma de decisiones y a las operaciones

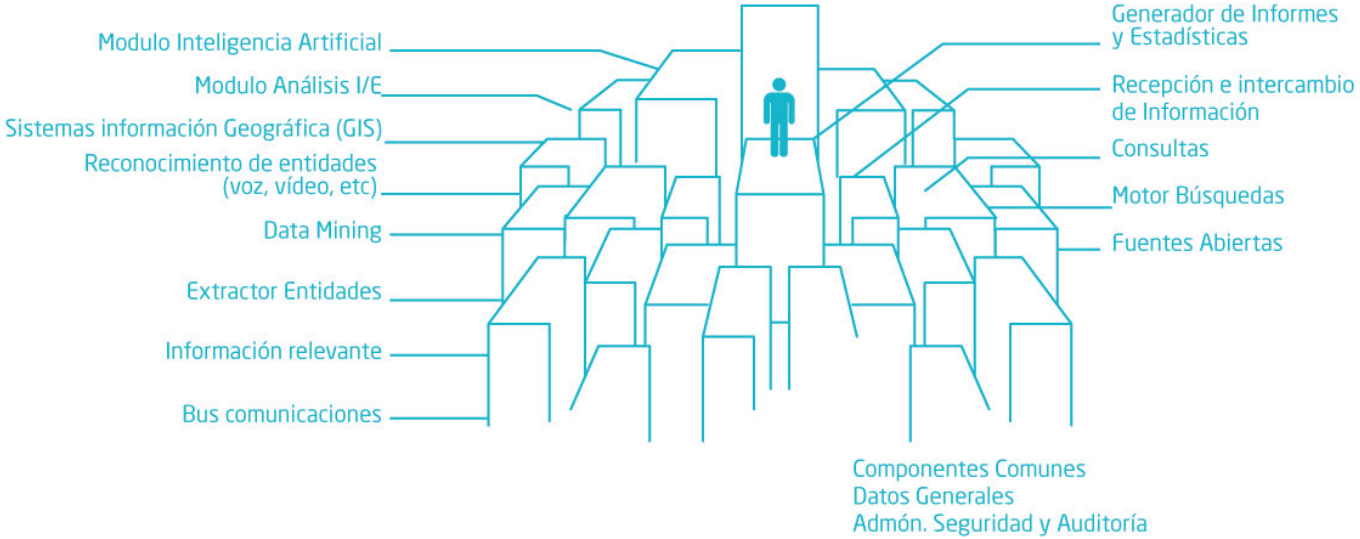
Proporciona las herramientas necesarias para evaluar estadísticamente la información de la que se dispone y para la generación de informes. Incluye funcionalidades de ayuda a los investigadores (alertas, mensajería interna, sistemas de intercambio de información, sistemas de gestión de dossieres/operaciones, etc.).

¿QUÉ INFORMACIÓN ALIMENTA AL SISTEMA DE INTELIGENCIA?



- **Sistemas de emisión de documentos**:
  Número de documentos emitidos e identidad.
- **Identificación mediante sistemas biométricos o tradicionales:**
  Tráfico de personas y vehículos. Controles de presencia
- **Otros sistemas de vigilancia:**
  Detectores de intrusión, sistemas anti-incendio, etc.
- **Video vigilancia tradicional:**
  Los datos recogidos por estos sistemas se complementan con la información complementaria proporcionada por los operadores (identificación de personas, vehículos, hechos, etc.).
- **Sistemas de video vigilancia inteligente:**
  Estos sistemas pueden proporcionar información sobre el tráfico de personas por un punto determinado, detectan intrusiones, realizan seguimientos e incluyen su propio sistema inteligente de detección de comportamientos sospechosos.
- **Aplicaciones corporativas y sistemas de auditoria de sistemas:**
  Integración de información gestionada con otras aplicaciones y sistemas corporativos, incluyendo la información recopilada por sus sistemas de auditoria.
- **Información introducida manualmente:**
  Datos introducidos por personal de seguridad sobre hechos que puedan resultar relevantes.
- **Análisis forense:**
  Búsqueda de información en equipos informáticos asignados a personas sospechosas.

¿CÓMO SE TRATA LA INFORMACIÓN Y QUÉ SE OBTIENE DE ELLA?



- **Tratamiento de datos:**
  Se realiza una integración sencilla de repositorios y de fuentes nuevas, así como un tratamiento específico de información no estructurada, aportando la herramienta necesaria a cada caso.
  Ejemplo: Controles de Presencia.

- **Extracción de Entidades:**
  Los datos son extraídos y unificados para relacionarlos.
  Ejemplo: Relacionar video y texto.

- **Búsqueda de patrones:**
  Se identifican patrones de relaciones entre entidades y hechos y de relaciones ocultas utilizando, entre otras, Herramientas de análisis gráfico de relaciones y Sistemas de Inteligencia Artificial.

- **Consultas y Cuadros de Mando:**
  Consultas en toda la información almacenada en local o en repositorios externos, incluyendo motores de búsqueda que permitan integrar distintas fuentes.
  Ejemplo: Consultas sobre visitas a un edificio.

- **GIS:**
  Se integra con sistemas de representación geográfica y refleja el entorno de la/s infraestructura/s a ser supervisadas por el sistema.

- **Estadísticas e informes:**
  Sistema flexible de generación de informes y de estadísticas de análisis estratégico.

- **Correladores de Eventos:**
  Herramienta para la concatenación de sucesos que permite una reacción ante una situación compleja o de alarma.

CONCLUSIONES

La aplicación de inteligencia de forma sistemática proporciona un salto cualitativo en la protección de infraestructuras que hasta ahora no había sido posible acometer por impedimentos tecnológicos o presupuestarios.

En Indra, disponemos una amplia oferta en el ámbito de la seguridad que va desde la seguridad civil a la militar, y desde la seguridad lógica a la física, con soluciones que gestionan las múltiples fuentes de información disponibles para facilitar la toma de decisiones en tiempo real.

En concreto, nuestras soluciones de investigación e inteligencia permiten capitalizar los activos de información para su puesta en valor y, además, contamos con una solución propia, el sistema iThink, que aúna todo nuestro conocimiento y supone la herramienta perfecta para facilitar la toma de las mejores decisiones.