

## Monitorización y gestión de la seguridad TI en Gobierno de Aragón.



© Aragonese de Servicios Telemáticos, Zaragoza

### Objetivos del proyecto:

- Capacitar a AST de un sistema de gestión de logs altamente cualificado para la centralización y explotación de los mismos.
- Dotar a AST de una visión global del estado de la seguridad que ayude en la toma de decisiones.
- Dar cumplimiento a requerimientos legales en materia de trazabilidad, salvaguarda y persistencia de la información.
- Optimizar el tiempo de respuesta ante incidentes de seguridad y gestionarlos en base a procedimientos de notificación y actuación preestablecidos.
- Gestionar remotamente dispositivos de comunicaciones.
- Definir un modelo de monitorización y gestión avanzado, en 24 x 7, que se apoye en información proveniente de análisis exhaustivos de los eventos, la CMDB y sistema de ticketing corporativo.

Aragonesa de Servicios Telemáticos (AST), entidad responsable de la provisión de infraestructuras y servicios telemáticos de Gobierno de Aragón, apuesta por S21sec para la monitorización y gestión de la seguridad de sus servicios e infraestructuras TI. El modelo garantiza un servicio integral de **seguridad gestionada basada en eventos** con capacidad de reducir los tiempos de detección de incidentes y la gestión inmediata para su neutralización dentro de su ciclo de vida. La solución es posible gracias a Bitacora Log Management, que actúa como plataforma integral de recolección, análisis y explotación de logs y los servicios de monitorización y operación de los dispositivos de seguridad ofrecidos en 24 x 7.

### Aragonesa de Servicios Telemáticos

Aragonesa de Servicios Telemáticos es la entidad de derecho público que, desde su puesta en marcha en 2002, participa activamente en la cadena de prestación de servicios con objeto de cubrir las necesidades operativas de la Diputación General de Aragón (DGA). Este modelo presenta importantes beneficios a la Administración Pública, así como al territorio y al ciudadano: optimización del uso de infraestructuras y servicios; homogeneidad, compatibilidad e interoperabilidad de soluciones; facilita la focalización en su actividad principal (servicios públicos, sanitarios, educativos, etc.); mayor extensión territorial de los servicios; más puntos de acceso a los servicios, etc.

En los últimos años, Gobierno de Aragón y AST se han posicionado a la vanguardia autonómica en innovación TIC. En mayo se inauguró el Centro de Innovación en Tecnologías Audiovisuales en el Parque Tecnológico Walqa, así como el modelo de gestión de servicios e infraestructuras global. Ahora, de la mano de S21sec, apuesta por una seguridad integral de la actividad de negocio, con el despliegue de Bitacora Log Management y los servicios 24x7 de monitorización y gestión de dispositivos que operan de forma conjunta.

### Seguridad para los servicios críticos

AST provee de infraestructuras y servicios telemáticos a todos los Departamentos y Organismos de la Administración de la Comunidad Autónoma de Aragón. Los servicios internos y públicos prestados a día de hoy, su evolución, complejidad, así como la previsión de crecimiento, requieren un elevado número de sistemas de información altamente heterogéneos que deben ser gestionados y administrados en su conjunto.

“Gracias a la solución implantada por S21sec, AST puede proveer al Gobierno de Aragón de un servicio de monitorización y gestión de la seguridad que actúa ininterrumpidamente las 24 horas del día, ofreciendo así a la administración y al ciudadano una garantía y una confianza basada en la calidad de nuestros servicios. ”

D. Fernando García Mongay,  
Director Gerente de Aragonesa de Servicios Telemáticos (AST).

**Áreas del proyecto:**

- Bitacora Log Management.
- Plataforma para la gestión de la seguridad:
  - Servicio de monitorización 24x7.
  - Servicio de gestión de dispositivos 24x7.
- Personalización e integración de la tecnología de S21sec con las de AST.

La existencia de servicios de carácter crítico, como por ejemplo, diversos servicios sanitarios o la e-Administración, están sujetos a requerimientos legales específicos, cuya existencia marcan las necesidades de desarrollo en cuanto a generación, protección y disponibilidad de los registros de actividad que deban proveer las aplicaciones de los sistemas utilizados.

Además, la evolución de ataques, riesgos y nuevas amenazas procedentes de Internet y de dentro de las grandes redes, hace necesaria una gestión eficiente de la seguridad de la red y de los sistemas corporativos.

El alcance de la solución comprende todos los componentes tecnológicos de Gobierno de Aragón (sistemas, dispositivos de comunicaciones, aplicaciones, aplicaciones de desarrollo interno, etc.) en su arquitectura distribuida en varios CPDs.

**Seguridad basada en la gestión de logs**

Bitacora Log Management es la plataforma que facilita la gestión y análisis de cualquier tipo de evento, posibilitando el empleo de los logs de auditoría como posibles evidencias en un proceso judicial. Bitacora Log Management está certificado por Common Criteria, estándar en seguridad que en España otorga el Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia del Ministerio de Defensa Español. AST, dispone de un amplio entorno distribuido, por lo que la escalabilidad de la plataforma ha resultado una característica decisiva para lograr un despliegue integral en sus infraestructuras.



Imagen: Esquema de servicios AST.

El motor de correlación de Bitacora Log Management analiza en tiempo real toda la información recolectada, generando alertas y categorizándolas según su gravedad: cambios de configuración fuera del horario laboral, ataques por fuerza bruta, accesos ilegítimos, escaneo de puertos, spam, propagación de malware, etc. Adicionalmente, se interactúa con la CMDB de AST para la obtención de la criticidad del activo afectado en la alarma. En base a estos valores se propaga la alerta para su correspondiente gestión y resolución.

### Plataforma:

Los logs son centralizados y explotados para reducir miles de eventos inconexos diarios a indicadores precisos y sintetizados que ayuden a la toma de decisiones. Esta información se entrega en dos formatos:

- Cuadros de mando, para información reciente que varía de entre 6 a 48 horas en función de las necesidades.
- Informes consistentes en listados y datos de mayor extensión para periodos de una semana o incluso meses atrás según las necesidades.



Imagen: Plataforma para la gestión de la seguridad.

Los servicios de seguridad gestionada de S21sec se ofrecen ininterrumpidamente las 24 horas del día desde el Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) y cuentan con la combinación de recursos humanos, procesos, inteligencia (información) y tecnología para la gestión de riesgos de seguridad y la monitorización y mitigación de los efectos de las amenazas de seguridad. La plataforma para la gestión de la seguridad, actúa como punto único de acceso desde el que gestionar todos los aspectos relativos a la seguridad de las organizaciones.

En base a los procedimientos de notificación y actuación definidos conjuntamente entre AST y S21sec, los operadores de SOC actúan según la alerta recibida, activo afectado, franja horaria, umbrales de normalidad, sucesos en otros entornos similares, etc. realizando las acciones pertinentes que van desde la notificación, hasta la operación de dispositivos para detener o mitigar un ataque o incidente de mayor gravedad. Todo el proceso, desde la recepción de la alerta, su gestión, así como su cierre, queda debidamente registrado tanto en el sistema de gestión de incidentes y cambios corporativo de AST, como en la plataforma para la gestión de la seguridad de S21sec. Esta operativa es beneficiosa tanto para AST, que le permite conocer el estado de la seguridad actual y disponer de indicadores reales de la gestión que se realiza de la misma, como para S21sec que, a través de la plataforma para la gestión de la seguridad, tiene visibilidad del estado de la seguridad y de los eventos e incidentes en multitud de organizaciones, con el valor añadido de inteligencia de negocio que supone.

### La monitorización y gestión de la seguridad han permitido a AST:

- Consulta de la información por parte de los responsables de AST de forma segura a través de una plataforma de gestión de logs.
- Centralización de logs y acceso a los mismos de forma homogénea y segura basada en perfiles.
- Desarrollo de una política corporativa en materia de los registros de actividad y estandarización de los mecanismos de exportación de logs por tecnología.
- Cumplimiento de requerimientos legales. Almacenamiento de logs con validez legal y retención de los mismos por el periodo de retención establecido por ley (para cada servicio).
- Visión unificada del estado de la seguridad de la organización.
- Análisis y explotación de eventos en tiempo real.
- Un servicio monitorización de la seguridad 24x7.
- Un servicio de operación de dispositivos 24x7.
- Reacción temprana ante incidentes de seguridad.
- Definición de procedimientos de notificación y actuación según la alerta y activo afectado.
- Gestión por personal especializado con visión e inteligencia de negocio.