WHITEPAPER

SIRAM OCR7 LPR Y LA CIBERSEGURIDAD EN LOS SISTEMAS LPR MODERNOS

La ciberseguridad de un sistema LPR no consiste en aislarlo de la red, sino en diseñarlo para conectarse de forma segura, actualizarse de forma controlada, gestionar vulnerabilidades y mantener la disponibilidad durante todo su ciclo de vida

CONTENIDOS

1. INTRODUCCIÓN

Los sistemas LPR han evolucionado desde simples motores de reconocimiento de matrículas hasta convertirse en componentes críticos de infraestructuras de aparcamientos, ciudades inteligentes, instalaciones industriales, puertos, aeropuertos y centros logísticos. En todos estos escenarios, la disponibilidad del servicio es tan importante como la precisión del reconocimiento.

Durante años, la elección de un sistema LPR se centró casi exclusivamente en la tasa de acierto, la velocidad de lectura, el rendimiento nocturno o el comportamiento en condiciones adversas. Todo eso sigue siendo importante: nadie quiere un sistema que no sea capaz de leer correctamente una matrícula. Sin embargo, el mercado empieza a formular preguntas que hace poco tiempo apenas aparecían en una conversación técnica: cómo se actualiza el firmware de las cámaras, qué ocurre cuando aparece una vulnerabilidad, cómo se protegen las comunicaciones, cuánto tiempo recibirá soporte el sistema y quién garantiza que la instalación siga siendo segura dentro de cinco o diez años.

La razón es sencilla: un sistema LPR moderno ya no es solo una cámara ni solo un algoritmo OCR. Es un conjunto de dispositivos conectados que controlan accesos físicos e intercambian información con plataformas de gestión, sistemas de pago, aplicaciones cloud y otros servicios corporativos. Por eso, hoy ya no basta con que un sistema funcione correctamente el día de la puesta en marcha: debe estar diseñado para protegerse, actualizarse y mantenerse operativo durante toda su vida útil.

Este documento describe la visión de Innova sobre la ciberseguridad aplicada a OCR7 y explica cómo la combinación de OCR7, SCAP, las cámaras Axis y los servicios Access y Alarm permite construir una arquitectura preparada para afrontar este nuevo escenario.

2. CIBERSEGURIDAD EN SISTEMAS LPR

Un sistema LPR controla accesos físicos e interactúa con barreras, plataformas PMS, sistemas de pago, soluciones VMS y servicios corporativos. Una vulnerabilidad ya no afecta únicamente a la lectura de matrículas: puede comprometer la continuidad de la operación, alterar configuraciones críticas, bloquear un carril o convertirse en un punto de entrada hacia otras redes.

Entre los riesgos más relevantes destacan los siguientes:

Riesgo	Descripción
Manipulación de configuraciones	Cambios no autorizados en parámetros críticos del sistema.
Apertura o bloqueo no autorizado de accesos	Control indebido de barreras o puntos de paso.
Indisponibilidad de dispositivos	Cámaras o servicios fuera de servicio que interrumpen la operación.
Explotación de vulnerabilidades conocidas	Uso de fallos ya publicados y no corregidos a tiempo.
Cámara como punto de entrada a la red	La cámara se usa como puerta de acceso a otros sistemas corporativos.
Firmware o software no autorizado	Instalación de versiones no verificadas o maliciosas.

En instalaciones distribuidas, además, estos riesgos se multiplican si no existe una visión centralizada del estado de los equipos.

Por ello, la ciberseguridad debe contemplarse como un requisito funcional del sistema y no como una característica adicional. En un entorno de parking, logística, industria o infraestructura crítica, la disponibilidad del servicio es parte de la seguridad. Un sistema perfectamente protegido desde el punto de vista criptográfico deja de aportar valor si una incidencia impide operar el acceso. La seguridad no debe limitarse a proteger información; también debe contribuir a mantener el servicio operativo.

3. PRINCIPIOS DE DISEÑO DE OCR7

OCR7 se desarrolla siguiendo una filosofía Security by Design. Esto significa que la autenticación, el control de accesos, la protección de las comunicaciones, el registro de eventos y la capacidad de actualización forman parte de la arquitectura desde el inicio del desarrollo. No se añaden al final como elementos externos, sino que condicionan la forma en que se diseña, despliega y mantiene el sistema.

Este enfoque se complementa con Secure by Default: configuraciones iniciales orientadas a reducir riesgos, minimizar servicios innecesarios y facilitar una puesta en marcha más controlada. En la práctica, esto ayuda al integrador a evitar errores habituales, como dejar servicios abiertos, compartir credenciales entre usuarios o mantener dispositivos con versiones antiguas de firmware.

El objetivo no consiste únicamente en proteger OCR7 el día de la instalación, sino en facilitar que la instalación continúe siendo segura durante todo su ciclo de vida. Para ello son esenciales la trazabilidad de cambios, la gestión de perfiles, la posibilidad de actualizar versiones y la reducción de la superficie de ataque.

4. CONECTIVIDAD SEGURA: ACCESS & ALARM

En el pasado era habitual considerar que un sistema seguro era un sistema completamente aislado de Internet. Hoy esa afirmación ya no es válida para muchas instalaciones: la gestión remota, la monitorización centralizada, la actualización continua y la explotación de servicios cloud aportan un valor operativo muy elevado cuando se implementan de forma segura.

La cuestión ya no es si un sistema está conectado, sino cómo lo está. Las comunicaciones deben realizarse mediante canales autenticados y cifrados, limitando el acceso a los servicios estrictamente necesarios y aplicando el principio de mínimo privilegio. Una cámara conectada de forma controlada a Access o Alarm no es equivalente a una cámara expuesta sin control a Internet.

Access Cloud permite centralizar la gestión de instalaciones distribuidas y ofrecer acceso remoto controlado. Alarm Cloud complementa esta arquitectura proporcionando una visión continua del estado operativo y de mantenimiento de los dispositivos. Juntas, estas plataformas permiten evolucionar desde una instalación aislada y difícil de mantener hacia una infraestructura conectada de forma segura y gestionable a largo plazo.

5. SEGURIDAD CONTINUA CON SCAP Y ALARM

SCAP, el módulo SIRAM Camera Application Platform, permite estandarizar el despliegue y mantenimiento de aplicaciones sobre cámaras Axis. Su valor no reside únicamente en simplificar la instalación, sino en reducir variabilidad operativa: menos procedimientos manuales, menos configuraciones improvisadas y mayor control sobre qué versión del software se encuentra instalada en cada dispositivo.

La seguridad no termina cuando finaliza la puesta en marcha. Durante los años siguientes aparecerán nuevas versiones de firmware, actualizaciones de OCR7, vulnerabilidades conocidas, certificados que caducan, cambios de red y dispositivos que entran en fin de soporte. Mantener la instalación protegida exige una gestión continua, no una configuración inicial.

En este contexto, Alarm evoluciona desde una plataforma de monitorización hacia una herramienta de gestión continua del ciclo de vida. Sus funciones previstas incluyen:

- Inventario centralizado de dispositivos.
- Identificación de versiones de firmware Axis.
- Seguimiento de versiones de OCR7.
- Detección de equipos fuera de soporte.
- Ayuda al despliegue de actualizaciones.
- Generación de información útil para responder ante vulnerabilidades conocidas.

Este enfoque transforma la gestión de la ciberseguridad en un proceso operativo. No se trata solo de saber si una cámara está conectada, sino de conocer si está actualizada, si ejecuta una versión soportada, si requiere intervención o si forma parte de una instalación que necesita una acción preventiva.

6. VALOR DE OCR7 EN CÁMARAS AXIS

La plataforma sobre la que se ejecuta el software también es determinante. OCR7 puede ejecutarse embebido en cámaras Axis, aprovechando una plataforma de red diseñada para operar en entornos profesionales y mantener un ciclo de vida de seguridad activo.

Capacidad de Axis	Beneficio de seguridad
AXIS OS	Base mantenida mediante actualizaciones y versiones de soporte.
Firmware firmado y arranque seguro	Ayudan a garantizar que el dispositivo ejecute software autorizado.
Axis Edge Vault	Protección de identidad del dispositivo y almacenamiento seguro de claves criptográficas.
HTTPS, certificados digitales e IEEE 802.1X	Facilitan la integración en redes corporativas con requisitos avanzados de seguridad.

Otro aspecto clave es la gestión de vulnerabilidades. Que un fabricante publique avisos de seguridad y parches no elimina la responsabilidad del integrador o del operador, pero proporciona una base transparente para actuar. Una actualización solo protege si se aplica; por ello, la combinación de plataforma Axis, SCAP y Alarm permite cerrar el círculo entre detección, disponibilidad de parche y despliegue controlado.

Ejecutar OCR7 sobre Axis no significa que la seguridad venga resuelta automáticamente. Significa partir de una base sólida sobre la que Innova puede desarrollar capacidades LPR, integración cloud y mantenimiento continuo con menor exposición y mayor trazabilidad.

7. ZERO TRUST APLICADO AL LPR

La filosofía Zero Trust parte de una idea sencilla: no confiar implícitamente en ningún usuario, dispositivo o servicio. Estar dentro de la red no debería ser suficiente para obtener acceso. Cada petición debe verificarse, autorizarse y limitarse según la función real que debe cumplir.

Aplicado a OCR7, esto implica segmentación de red, privilegios mínimos, autenticación fuerte, uso de certificados y supervisión continua del estado de los dispositivos. Por ejemplo:

Rol / componente	Acceso que debería tener
Operador	Consultar eventos, sin poder modificar configuraciones críticas.
Técnico de mantenimiento	Acceso temporal a una cámara concreta, no a otros sistemas.
Aplicación / integración	Comunicación únicamente con los servicios estrictamente necesarios.

Zero Trust no debe entenderse como un producto, sino como una forma de diseñar la arquitectura. En un sistema LPR moderno ayuda a reducir la superficie de ataque y limita el impacto de una credencial comprometida, un dispositivo mal configurado o una integración excesivamente permisiva.

8. DISPONIBILIDAD Y RESILIENCIA OPERATIVA

En ciberseguridad suele hablarse de confidencialidad e integridad, pero en sistemas LPR la disponibilidad tiene un peso especialmente alto. Un parking ticketless, un acceso industrial o un puerto no pueden depender de un único elemento si la interrupción del servicio bloquea la operación diaria.

Por este motivo, la resiliencia debe formar parte de la arquitectura. TwinPlate P2P Master/Master es un ejemplo de cómo una arquitectura distribuida puede reducir puntos únicos de fallo: si una cámara deja de prestar servicio por una avería, una desconexión o un incidente, la otra puede contribuir a mantener el carril operativo y minimizar el impacto.

No se trata solo de aumentar la disponibilidad técnica, sino de reducir el impacto operativo de fallos o incidentes. En este sentido, la resiliencia es también una dimensión de la ciberseguridad.

9. RECOMENDACIONES: INTEGRADORES Y CLIENTES

Una arquitectura segura requiere buenas prácticas de implantación. En muchas instalaciones, el usuario administrador se crea una vez, se comparte entre varias personas y permanece sin cambios durante años. Esta práctica elimina la trazabilidad y dificulta saber quién modificó una configuración o ejecutó una acción crítica.

Es recomendable definir perfiles diferenciados según la función real de cada persona. Un operador que consulta movimientos no debería modificar parámetros de cámara. Un técnico de mantenimiento debería disponer de permisos suficientes para su tarea, pero no de acceso administrativo permanente. Cuando sea posible, la integración con directorios corporativos o proveedores de identidad ayuda a evitar cuentas locales olvidadas y facilita la baja de usuarios.

También deben aplicarse medidas de red y mantenimiento:

- Segmentar cámaras y servicios.
- Usar HTTPS y desplegar certificados.
- Cerrar servicios innecesarios.
- Mantener firmware y OCR7 actualizados.
- Revisar configuraciones periódicamente.
- Proteger las copias de seguridad.

Las actualizaciones no son una molestia operativa, sino una parte esencial de la seguridad del sistema.

La responsabilidad es compartida:

Actor	Responsabilidad
Innova	Diseñar productos seguros y publicar actualizaciones, que faciliten el despliegue, la integración y el mantenimiento del sistema LPR
Integrador	Instalar siguiendo buenas prácticas.
Cliente	Operar la infraestructura con políticas claras de usuarios, red y mantenimiento.

10. RELACION CON NIS2 ET Y CYBER RESILIENCE ACT

La ciberseguridad está adquiriendo un papel cada vez más relevante en la gestión de las infraestructuras conectadas. En este contexto, la Directiva NIS2 y el Cyber Resilience Act (CRA) marcan la dirección que seguirá el mercado en los próximos años.

Mientras que NIS2 refuerza los requisitos de seguridad para las organizaciones que operan infraestructuras y servicios esenciales, el Cyber Resilience Act establece nuevas exigencias para los fabricantes de productos digitales conectados. Entre ellas destacan la gestión de vulnerabilidades, la publicación de actualizaciones de seguridad y el mantenimiento del producto durante todo su ciclo de vida.

Calendario de aplicación del CRA

- 10 de diciembre de 2024: entrada en vigor del Cyber Resilience Act.
- 11 de septiembre de 2026: comienzan las obligaciones de notificación de vulnerabilidades explotadas e incidentes graves.
- 11 de diciembre de 2027: aplicación plena de los requisitos relacionados con el soporte, las actualizaciones de seguridad y la gestión de vulnerabilidades.

Fuente: Comisión Europea – Cyber Resilience Act.

Para los usuarios finales, el mensaje es sencillo: un sistema LPR ya no debe valorarse únicamente por su precisión de lectura. También es importante que pueda mantenerse seguro a lo largo del tiempo mediante actualizaciones periódicas, una gestión adecuada de las vulnerabilidades y una arquitectura diseñada para reducir los riesgos operativos.

En definitiva, la capacidad de un sistema para evolucionar de forma segura será un criterio de decisión cada vez más importante, al mismo nivel que su rendimiento o su fiabilidad.

11. CONCLUSIONES

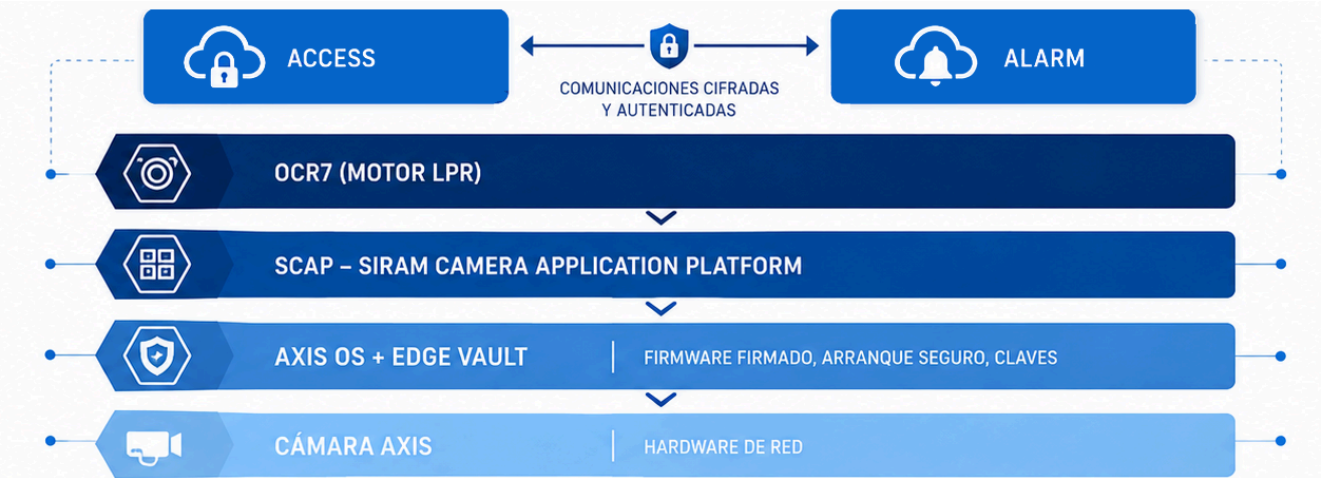
La ciberseguridad está dejando de ser un elemento diferenciador para convertirse en un requisito imprescindible en cualquier sistema LPR profesional. La precisión del reconocimiento seguirá siendo un factor clave, pero cada vez tendrá más peso la capacidad del sistema para mantenerse seguro a lo largo del tiempo mediante actualizaciones, comunicaciones protegidas, gestión de vulnerabilidades y una arquitectura resiliente.

Con OCR7, Innova apuesta por un enfoque Security by Design, integrando mecanismos de protección desde el diseño de la solución. Esta estrategia combina una arquitectura segura, comunicaciones cifradas, una gestión continua del ciclo de vida del software y el aprovechamiento de las funciones de ciberseguridad incorporadas en las cámaras Axis. Soluciones como SCAP, SIRAM Access Cloud y SIRAM Alarm complementan esta estrategia, facilitando una operación más segura y una administración centralizada de las instalaciones.

La seguridad de un sistema LPR no finaliza con su puesta en marcha. Al contrario, comienza una etapa en la que resulta fundamental mantener el software actualizado, supervisar el estado de la infraestructura y gestionar de forma proactiva las posibles vulnerabilidades. Solo mediante una estrategia continua de mantenimiento y mejora es posible garantizar la disponibilidad, la resiliencia y la protección del sistema durante toda su vida útil.

12. **ANEXO. DIAGRAMAS Y PREGUNTAS DE EVALUACIÓN**

Arquitectura segura OCR7 + Axis + Alarm



Ciclo de vida de seguridad operativa

Cinco preguntas antes de elegir un sistema LPR

¿Cómo se actualiza el firmware de las cámaras y el software OCR?
A través de SCAP (SIRAM Camera Application Platform), que estandariza el despliegue y mantenimiento de aplicaciones sobre cámaras Axis, y de Alarm , que ayuda al despliegue de las actualizaciones y hace seguimiento de qué versión de OCR7 y de firmware Axis tiene cada dispositivo. La base de firmware es AXIS OS, mantenida con actualizaciones y versiones de soporte, con firmware firmado y arranque seguro para garantizar que el dispositivo ejecute software autorizado.

¿Cómo se gestionan las vulnerabilidades conocidas?
Axis publica avisos de seguridad y parches; Alarm genera información útil para responder ante esas vulnerabilidades conocidas (detectando qué equipos están afectados); y SCAP facilita el despliegue controlado del parche. Innova lo resume como "cerrar el círculo entre detección, disponibilidad de parche y despliegue controlado" — publicar un parche no basta, solo protege si se aplica.

¿Qué mecanismos protegen las comunicaciones entre dispositivos y servicios cloud?
Canales autenticados y cifrados hacia Access y Alarm, con acceso limitado a los servicios estrictamente necesarios (mínimo privilegio). A nivel de plataforma, Axis aporta HTTPS, certificados digitales e IEEE 802.1X, más Edge Vault para protección de identidad del dispositivo y almacenamiento seguro de claves. Todo esto bajo una filosofía Zero Trust: ninguna petición se confía por estar dentro de la red.

¿Cómo se supervisa el estado de la instalación durante toda su vida útil?
Con Alarm, que evoluciona de plataforma de monitorización a herramienta de gestión continua del ciclo de vida: inventario centralizado de dispositivos, identificación de versiones de firmware Axis, seguimiento de versiones OCR7 y detección de equipos fuera de soporte.

¿Qué ocurre cuando un dispositivo queda fuera de soporte o deja de estar disponible?
Alarm Cloud detecta los equipos que entran en fin de soporte para que se puedan planificar renovaciones (última etapa del ciclo de vida: "renovación tecnológica"). Y si una cámara deja de prestar servicio por avería, desconexión o incidente, arquitecturas como TwinPlate P2P Master/Master permiten que otra cámara mantenga el carril operativo, minimizando el impacto — la resiliencia se trata como parte de la ciberseguridad, no solo como un tema de continuidad técnica.

Innova Systems Group
C/ Joaquim Mir 55
08100 Mollet del Vallès
Barcelona (SPAIN)
Tel. +34 93 5797238
www.innovagroupbcn.com