

La obsolescencia de los Sistemas Electrónicos de Seguridad y sus implicaciones



Hoy en día los avances tecnológicos suceden a gran velocidad, y estos avances no son una excepción en el campo de los Sistemas Electrónicos de Seguridad, al contrario, los avances se suceden a gran velocidad. En un contexto donde las soluciones tecnológicas son imprescindibles para la protección de bienes y personas, la obsolescencia de los elementos que forman parte de los Sistemas Electrónicos de Seguridad se ha convertido en un punto crítico que hay que tener en cuenta a la hora de diseñar, implantar y mantener estos sistemas.

Las causas de la obsolescencia en los Sistemas Electrónicos de Seguridad podemos agruparlas en tres grandes grupos, tecnológicos, económicos y normativos.

Factores tecnológicos, el continuo desarrollo de nuevos equipos que implementan nuevas soluciones, tanto hardware como software hacen que las tecnologías empleadas en Sistemas Electrónicos de Seguridad queden rápidamente superadas. La aparición de nuevos estándares de comunicación,

protocolos más seguros y dispositivos con mayor capacidad de procesamiento hace que los dispositivos existentes dejen de ser compatibles con los nuevos desarrollos, y su eficacia y eficiencia sea inferior a la de los nuevos dispositivos que aparecen en el mercado.

Factores económicos, la presión del mercado fuerza a los fabricantes a centrarse en ofrecer a sus clientes soluciones innovadoras y a mejorar continuamente las capacidades de los productos de su catálogo, lo que implica que el tiempo en que un producto concreto aparece en el catálogo de un fabricante es muy corto, en ocasiones solo de unos pocos meses, siendo sustituido rápidamente por otro producto evolucionado, este procesos de renovación, en ocasiones, puede dificultar la obtención de repuestos, acelerando el proceso de obsolescencia.

Los cambios en la legislación vigente también pueden convertir en obsoletos sistemas que no cumplen con los nuevos requisitos. La entrada en vigor de nueva legislación o cambios en la existente pueden obligar a las empresas a actualizar o reemplazar sus sistemas, para adecuarlos a los nuevos requisitos legales.

El problema de la obsolescencia se agrava especialmente en los Sistemas Electrónicos de Seguridad cerrados, aquellos cuyas arquitecturas, protocolos y componentes están restringidos al fabricante original, lo que impide o limita la interoperabilidad con equipos de otros proveedores.

La dependencia de un Sistema Electrónico de Seguridad cerrado, con tecnologías propietarias dificulta la integración de nuevas funcionalidades o la actualización frente a nuevas amenazas y necesidades, si no es de la mano del fabricante. Cualquier necesidad de ampliación, actualización de software o reparación suele requerir la intervención directa del fabricante, cuyas políticas comerciales puede que no garanticen la continuidad del soporte o la disponibilidad de repuestos a largo plazo.

Desde un punto de vista económico, los Sistemas Electrónicos de Seguridad cerrados incrementan el coste de propiedad y de mantenimiento. La falta de competencia en el suministro de componentes y servicios restringe las opciones de los usuarios, quienes pueden verse obligados a aceptar precios elevados o condiciones contractuales poco favorables. A medida que la plataforma cerrada envejece, el riesgo de quedar “trapado” en una tecnología con un futuro incierto crece, incrementando el coste de migrar a soluciones más innovadoras y abiertas. El riesgo de quedar “trapado” puede llegar a suponer la necesidad de realizar grandes inversiones en equipamiento y en el rediseño de los sistemas e infraestructura a la hora de migrar un sistema abierto.

La obsolescencia tecnológica genera costes importantes, la necesidad de reemplazar equipos, actualizar software o invertir en nuevos sistemas implica costes económicos directos. Además, los costes indirectos de la gestión de incidencias derivados de la pérdida de eficiencia y eficacia de los sistemas pueden llegar a ser elevados.

Uno de los aspectos más relevantes de la obsolescencia tecnológica de los Sistemas Electrónicos de Seguridad, que hay que tener en cuenta, es el impacto económico que genera a lo largo del ciclo de vida de los sistemas. A la hora de calcular el coste total de un sistema, no solo hay que tener en cuenta la inversión inicial y los costes de mantenimiento recurrentes, hay que contemplar los costes derivados de la actualización de capacidades y la obsolescencia, lo que puede implicar la ampliación del número de elementos o el reemplazo de algunos de ellos, e incluso la migración parcial o total del sistema. Estos costes suelen ser subestimados cuando se elaboran los presupuestos de inversión, lo que puede llevar a decisiones financieras poco eficientes y a una reducción del retorno de inversión (ROI) esperado.

Es necesario incorporar el análisis de la obsolescencia en la valoración de los proyectos de implantación de Sistemas Electrónicos de Seguridad y en su planificación presupuestaria. La previsión de gastos futuros, la estimación de la vida útil real de los sistemas, los sistemas no son eternos, y la evaluación de riesgos asociados a la obsolescencia son elementos clave para calcular el ROI de manera precisa. Ignorar estos factores puede llevar a la necesidad de inversiones adicionales inesperadas, afectar la operatividad y comprometer la seguridad de bienes y personas.

Incremento del riesgo y pérdida de eficacia y eficiencia: la falsa sensación de seguridad

Una de las consecuencias de la obsolescencia en los Sistemas Electrónicos de Seguridad es el incremento gradual del riesgo y la disminución de la capacidad real para proteger a personas y bienes. A medida que los sistemas envejecen, pierden eficacia en la detección y respuesta ante amenazas. Las funciones críticas pueden fallar, los tiempos de reacción pueden alargarse y las posibilidades de integración con nuevas tecnologías se reducen, afectando tanto la eficiencia operativa como el nivel de protección ofrecido.

La falta de actualizaciones de seguridad y la imposibilidad de integrar nuevas funciones limitan su capacidad de respuesta ante las amenazas. Además, la incompatibilidad con otros sistemas dificulta la interoperabilidad y la escalabilidad, reduciendo la eficacia de la solución de seguridad implantada.



Por otra parte, hay que tener en cuenta que hoy en día los Sistemas Electrónicos de Seguridad, no son sistemas aislados, son sistemas OT e IoT interconectados, expuestos a ciberamenazas de todo tipo, en el caso de un sistema obsoleto, sin soporte, sin parches, ni actualizaciones el riesgo de que un ciberataque comprometa su funcionamiento es alto. Si a esto se une la ausencia de compatibilidad con nuevas soluciones impide la utilización de herramientas de monitorización y respuesta ante ciberincidentes, la situación se convierte en crítica.

Sin embargo, muchas organizaciones siguen confiando en la presencia física de estos sistemas obsoletos, generando una falsa sensación de seguridad entre el personal y los responsables de la gestión. Esta percepción errónea puede llevar a tomar decisiones inadecuadas ante situaciones de riesgo, subestimando la vulnerabilidad real del entorno protegido.

La confianza en dispositivos obsoletos puede tener consecuencias graves, desde el acceso no autorizado a las instalaciones, hasta el daño a personas y bienes, pasando por la interrupción de operaciones críticas. Por ello, es esencial revisar periódicamente la eficacia de los Sistemas Electrónicos de Seguridad, evaluando objetivamente su eficacia, su eficiencia y el grado de protección que están ofreciendo, para evitar caer en una falsa sensación de seguridad.

Tampoco podemos obviar los retos que supone la legislación vigente, como puede ser la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, las Directivas Europeas NIS2 y CER, que establecen requisitos que en muchos casos son muy difíciles de cumplir con un sistema que empieza a dar muestras de obsolescencia.

Estrategias para mitigar la obsolescencia



La actualización constante de software y hardware es fundamental para prolongar la vida útil de los Sistemas Electrónicos de Seguridad. Los programas de mantenimiento preventivo, la monitorización de vulnerabilidades y la aplicación de parches permiten anticipar problemas y reducir riesgos. Disponer de contratos de soporte facilita el acceso a recursos técnicos y actualizaciones.

Una estrategia eficaz para gestionar la obsolescencia es la planificación del ciclo de vida de los sistemas. Definir periodos de actualización, evaluar la compatibilidad con nuevas tecnologías y programar el reemplazo de equipos críticos contribuye a evitar interrupciones y costes imprevistos. La adopción de soluciones escalables y

modulares favorece la adaptación a futuras necesidades sin necesidad de sustituciones masivas.

La capacitación del personal en el uso y mantenimiento de los Sistemas Electrónicos de Seguridad es muy importante a la hora de identificar señales de obsolescencia y poder actuar con rapidez. Disponer de una cultura de mejora continua y de una vigilancia tecnológica permite anticipar tendencias y tomar decisiones informadas sobre la actualización o reemplazo de equipos.

A la hora de diseñar e implantar Sistemas Electrónicos de Seguridad es necesario optar por tecnologías abiertas y estandarizadas, por productos y soluciones de proveedores que garanticen soporte a largo plazo, lo que va a reducir el riesgo de una obsolescencia prematura. Utilizar tecnologías abiertas que faciliten la integración, la actualización y la interoperabilidad es una forma de maximizar la vida útil de un sistema y por lo tanto de la rentabilidad de las inversiones en seguridad electrónica.

La obsolescencia de los Sistemas Electrónicos de Seguridad plantea retos significativos afectando a la protección de personas y bienes. Comprender sus causas y consecuencias es el primer paso para abordar los riesgos asociados y diseñar estrategias efectivas de mitigación. La gestión proactiva, basada en la planificación y actualización, es clave para garantizar la eficacia y eficiencia de los Sistemas Electrónicos de Seguridad en un entorno tecnológico en constante evolución. En definitiva, la anticipación y el compromiso con la mejora continua son esenciales para la seguridad de personas y bienes.



Ricardo Cañizares Sales

Asesor de AES FUNDACIÓN