



## La Ciberseguridad de los Sistemas Electrónicos de Seguridad es un asunto demasiado importante para dejarlo en manos de los técnicos

Parafraseando a Georges Clemenceau al que se le atribuye la frase “La guerra es un asunto demasiado serio para dejarla en manos de los militares”, hoy podríamos decir que “La Ciberseguridad los Sistemas Electrónicos de Seguridad es un asunto demasiado importante para dejarlo en manos de los técnicos”.

Es un reto tan trascendental para cualquier organización, que dejarlo solo en las manos expertas de los técnicos sería un error que podría tener consecuencias impredecibles. Con esta analogía queremos resaltar que para hacer frente a desafíos muy complejos es necesario aunar pensamiento estratégico, visión de conjunto y liderazgo decidido.



No podemos olvidar que, dentro de la ciberseguridad, destaca la de los Sistemas Electrónicos de Seguridad (SES) que, como la de cualquier otro sistema de nuestra organización, debe ser una de las prioridades de la alta dirección que debe asumirla como un elemento clave de negocio y no solo como un reto tecnológico.

Hace tiempo ya que los Sistemas Electrónicos de Seguridad abandonaron el mundo analógico para pasar al mundo digital por lo que hoy en día, podemos considerarlos como sistemas OT y muchos de sus componentes son elementos IoT e incluso AIoT, formando parte del ciberespacio.

Esto los convierte en parte de la frontera entre el ciberespacio y el mundo físico, lo que convierte a la ciberseguridad de los SES en un elemento clave no solo para la protección de ellos mismos, sino para la protección del resto de sistemas de la organización, de los activos físicos y de las personas.

Tal como establece el Esquema Nacional de Seguridad y las directivas europeas NIS2 y CER, la protección efectiva de estos sistemas trasciende de la mera implementación de soluciones técnicas; exige una visión estratégica y un compromiso decidido de la alta dirección, lo que supone su implicación directa en la toma de decisiones sobre ciberseguridad, su responsabilidad en la gestión de riesgos, la asignación de recursos y la gobernanza de la seguridad.

Las empresas de seguridad que se dedican a instalar y mantener Sistemas Electrónicos de Seguridad no solo son responsables de instalar y mantener dichos sistemas correctamente con eficacia y eficiencia, sino que deben realizar dichas tareas aplicando criterios y medidas de ciberseguridad. Además, tienen la obligación de transmitir a sus clientes la necesidad de contemplar la ciberseguridad como un elemento central en los proyectos de instalación de los SES.

Hoy en día nos encontramos en un entorno complejo de seguridad en el que la superficie expuesta a un ciberataque crece con cada nueva conexión, ya no basta con securizar los sistemas, también es imprescindible que las empresas de seguridad que diseñan, los SES informen y sensibilicen a los clientes de que, a la hora de tomar decisiones de inversión, tengan en cuenta la importancia de integrar las medidas y los servicios de ciberseguridad desde la definición de necesidades del proyecto.

De esta manera, las empresas instaladoras y mantenedoras se convierten en agentes clave para impulsar la transformación cultural y garantizar que la seguridad digital no sea una idea abstracta, sino una práctica concreta desde la concepción del proyecto hasta su operación continua. Esta obligación va más allá del cumplimiento normativo y debe responder a la visión estratégica de defender tanto los intereses del cliente como la reputación del propio sector.

Uno de los principales problemas a los que nos enfrentamos a la hora de proteger adecuadamente nuestros Sistemas Electrónicos de Seguridad, es la percepción errónea de la ciberseguridad como un gasto prescindible cuando la realidad es que se trata de una inversión estratégica. Es imprescindible entender que cada euro invertido en la ciberseguridad de nuestros sistemas tiene repercusión directa en la protección de los activos y las personas a las que protegen esos sistemas, lo que al final se traduce en un aumento de la resiliencia del negocio, la reputación de la compañía y la confianza de los clientes y el resto de las partes interesadas. Las directivas NIS2 y CER refuerzan este enfoque exigiendo pruebas fehacientes de la asignación de recursos suficientes, de la implicación de la alta dirección en la supervisión de las inversiones y de la implantación de medidas de protección, tanto técnicas como organizativas.

Y es que, aunque la máxima responsabilidad recae sobre la alta dirección “La ciberseguridad es tarea de todos”, y es fundamental reconocer que debe involucrar a todas las personas que forman parte de la organización lo que incluye tanto al personal que utiliza y opera los SES como a las personas a las que ofrece protección.



Esta corresponsabilidad implica que la formación, la sensibilización y la vigilancia en el cumplimiento de las políticas y procedimientos de ciberseguridad deben estar presentes en todos los niveles. La cultura de ciberseguridad debe ser impulsada desde la alta dirección, pero debe permear cada proceso, cada decisión y cada acción cotidiana. Solo así se crea un entorno verdaderamente resiliente, donde el error humano, a menudo el eslabón más débil, se minimiza gracias a la concienciación y la implicación colectiva.

La visión y la percepción de la necesidad de ciberseguridad por parte de los equipos técnicos son esenciales a la hora de diseñar, instalar y mantener los Sistemas de Seguridad Electrónica, pero su perspectiva suele estar limitada al ámbito tecnológico. La ciberseguridad, como subrayan el ENS, NIS2 y CER, requiere una visión interdisciplinar, integrando la gestión de riesgos, el cumplimiento normativo, la formación, la respuesta a incidentes y la alineación con los objetivos estratégicos de la organización. Los técnicos, por sí solos, carecen de la autoridad para coordinar la estrategia global que debe emanar desde la dirección y ser respaldada por políticas y recursos adecuados.



Abordar el problema de la ciberseguridad únicamente desde un punto de vista técnico puede llevar a soluciones tecnológicamente avanzadas pero desalineadas con las necesidades reales de los Sistemas Electrónicos de Seguridad a los que tienen que proteger. Esta protección debe realizarse aplicando las políticas y procedimientos promulgadas por la dirección de la organización, que debe crear estructuras de gobernanza que integren la seguridad en todos los niveles bajo la supervisión directa de los órganos de gobierno.

Debido a todo lo anterior, un temor habitual es que la ciberseguridad pueda restar agilidad u obstaculizar la eficacia y eficiencia de los Sistemas Electrónicos de Seguridad, sin embargo, tanto la experiencia como la regulación internacional demuestran que una estrategia bien diseñada debe (y puede) garantizar la ciberseguridad sin sacrificar la operatividad. Los principios de “*seguridad por diseño*” y “*seguridad por defecto*”, recogidos en las directivas europeas y en el Esquema Nacional de Seguridad, promueven la integración de la protección desde el diseño de los sistemas, logrando que la ciberseguridad sea un facilitador y no un obstáculo para que los SES cumplan con su objetivo de proteger a personas y bienes. El reto se encuentra en proteger sin paralizar, adaptándose a los cambios tecnológicos y a las nuevas amenazas manteniendo siempre un rumbo firme que persiga la mejora continua.

Garantizar la ciberseguridad de los SES es uno de los mayores retos para cualquier organización ya que si alguno se viera comprometido por un ciberataque supondría un riesgo sobre el objeto de protección, las personas y los bienes que ninguna organización puede obviar.

En resumen, las empresas deben tener claro que dejar la ciberseguridad en manos exclusivas de los técnicos es insuficiente y que esta responsabilidad recae en la alta dirección. Ahora bien, garantizar un adecuado nivel de ciberseguridad solo es posible si todos los miembros de la organización comprenden que “La ciberseguridad es cosa de todos”.

Además, una de las piezas fundamentales para abordar la protección de los SES son las empresas de seguridad, que juegan un papel esencial a la hora de garantizar la ciberseguridad de estos y deben informar y asesorar a sus clientes sobre la importancia de tener en cuenta las necesidades de ciberseguridad durante todo el ciclo de vida del sistema, desde la definición de necesidades, hasta pasando por el diseño y, la instalación, hasta y el mantenimiento.

Ricardo Cañizares Sales  
Vocal de la Junta Directiva de AES  
Miembro del área de ciberseguridad de AES