Retos y oportunidades de la Ciberseguridad en Sistemas de Seguridad Física

Conclusiones de la I Jornada

Policy Brief ESYS | Alfonso Bilbao y Maite Arcos – noviembre 2022

El 10 de noviembre de 2022, la Fundación ESYS organizó la 1ª Jornada sobre Ciberseguridad de los Sistemas de Seguridad Física (enlace a la descripción del evento). Se resumen aquí las principales conclusiones, retos y oportunidades que la ciberseguridad de los sistemas de seguridad física presenta en el ámbito empresarial español. Al final del documento se plantean una serie de recomendaciones para mejorar el abordaje de este tema tan crítico.

La importancia de entender el concepto de seguridad integral

La Jornada comenzó con una introducción del Presidente de ESYS, Carlos López Blanco, subrayando el concepto de seguridad integral, un ámbito que se ha convertido en estratégico dada la importancia que es abordar conjuntamente la seguridad física y la ciberseguridad. Su diferencia radica únicamente en el medio en que se materializan las amenazas, de forma física o informática, y muchas veces lo hacen de forma conjunta. La seguridad ante estas amenazas hace ya mucho tiempo que se considera como una única disciplina, y con una estrategia común en las empresas y los usuarios en general.

Como destacó el Presidente de ESYS: "En una sociedad digital las cuestiones relacionadas con seguridad deben considerarse desde un enfoque integral o híbrido. A medida que avanza el proceso de digitalización, la ciberseguridad ha ido ganando protagonismo, pero la pandemia nos ha recordado que también las cuestiones de seguridad física son relevantes".

La asociación Española de Ingenieros de Seguridad (AINSE) también subrayó que es necesario dejar de hablar de ciberseguridad y comenzar a hablar de seguridad como concepto único y global, "hace 20 o 30 años la seguridad eran vallas físicas, hoy ya no es suficiente".

Los sistemas electrónicos físicos tienen una parte digital, lo que los hace más cibervulnerables. AIENSE ha elaborado una Guía de buenas prácticas de ciberseguridad en proyectos de seguridad física que trata de ayudar a esa coordinación.

Sin embargo, no siempre se siguen estas pautas y, aunque sí está asumida la necesidad de aplicar metodología de seguridad física a la protección de acceso o intrusión a activos Informáticos (CPDs, cuartos con electrónica de red y otros, tal y como recoge el capítulo 11 de la norma ISO 27001), sensu contrario no lo está, es decir, **no siempre se atiende la protección de los sistemas de seguridad física ante los ataques informáticos**. Estos ataques pueden tener como objetivo el propio sistema de seguridad e, incluso, su utilización como vehículo de entrada a otros sistemas informáticos de su propietario.

Sobre este tema, ESYS convocó a destacadas personas expertas en la materia en una mesa redonda, moderada por Alfonso Bilbao, Presidente de la Comisión Técnica de la Fundación ESYS, con los siguientes participantes:

- Representantes de empresas propietarias de Sistemas de Seguridad Física: Cándido Arregui, RSI de AENA y Justo López, RSI de ENDESA.
- Una empresa de Instalación de Sistemas de Seguridad: Javier Rubio, Director Global de Ventas de Tecnología de PROSEGUR.
- Un representante de la Administración: Alberto Santos, Analista de la Oficina de Coordinación de la Ciberseguridad (OCC), Ministerio del Interior.
- Una entidad generadora de una de las pocas *Guías sobre mejores prácticas del diseño e instalación de este tipo de Ciberseguridad* en esta aplicación concreta: Álvaro Ubierna, miembro del Grupo de Trabajo de Ciberseguridad de la Asociación Española de Ingenieros de Seguridad (AEINSE).

Regulación y público objetivo: ¿freno o incentivo?

Las obligaciones regulatorias pueden orientar a las empresas a considerar este concepto evolucionado dentro del enfoque de seguridad en la que se integran aspectos físicos y lógicos. Sin embargo, la regulación no está reaccionando a tiempo, ni de forma coordinada entre los diferentes Ministerios competentes.

ENDESA manifestó su dedicación específica a la consideración de los sistemas de seguridad física como un importante activo dentro del OT (*Operation Technology*) de la compañía, así como la facilidad encontrada para la adopción de las medidas necesarias por parte de los equipos responsables de Seguridad Física.

AENA también está en el proceso de asegurar sus importantes sistemas de seguridad de los Aeropuertos ante los ciberataques. En ese sentido, ha contado con la existencia de una regulación específica, tanto de la Agencia Europea de Seguridad Aérea (EASA), como de la correspondiente Agencia española (AESA), lo que ha facilitado la labor. El trabajo de AENA se presenta como ingente y muy relacionado con los cambios en la disposición de medidas de Seguridad.

Cándido Arregui, RSI de AENA, considera que “las obligaciones regulatorias en algunos sectores muy específicos, como es el de la gestión de servicios aeroportuarios, sí avanza en esa dirección de evaluación de la seguridad integral, en el que los sistemas de seguridad física deben tener en cuenta las vulnerabilidades lógicas”.

Durante la Jornada quedó patente que tanto AENA como ENDESA sí son conscientes de la necesaria atención a la ciberseguridad de los sistemas de seguridad físicos, por convencimiento y porque forma parte de su *compliance* regulatorio (por normativa sectorial de gestión aeroportuaria o por ser gestores de infraestructuras críticas).

No obstante, la regulación también provoca algunas disfuncionalidades.

Alberto Santos manifestó que, desde la Oficina de Coordinación de Ciberseguridad, en el marco de la normativa de protección de infraestructuras críticas, ya tienen en cuenta las vulnerabilidades lógicas de los sistemas físicos en relación a la protección de las infraestructuras críticas. El análisis de las vulnerabilidades de los sistemas de seguridad frente a ciberataques se está considerando de forma efectiva en sus auditorías e inspecciones, que están dirigidas a su ámbito de competencias (las empresas afectadas por la normativa de infraestructuras críticas). Ahora bien, según su experiencia, queda una importante labor por hacer.

Sin embargo, entre los asistentes al acto se señaló la dificultad de encontrar referencias a la ciberseguridad y a esta necesidad de considerar la seguridad desde un punto de vista integral en la Ley de Seguridad Privada y en lo que se conoce del borrador de reglamento en el que se está trabajando. Esta falta de apoyo en el marco normativo puede ser una dificultad para que las empresas que quedan fuera del ámbito de las obligaciones de las infraestructuras críticas compartan también esta visión integral sobre la seguridad de sus sistemas OT.

Esta falta de peso de la ciberseguridad en la normativa de seguridad contrasta con el incremento de peso de la figura del CISO en las Directivas NIS (ya traspuesta a la legislación española y la inminente sucesora, la NIS 2.0), por ejemplo.

Parece que la normativa progresa y se adapta a las nuevas realidades digitales, pero sin que exista esa necesaria coordinación entre los entes competentes que incorporen los diferentes aspectos desde un punto de vista de seguridad integral. Estas dos medidas -capacidad regulatoria y coordinación interinstitucional- debe ir de la mano.

Por otro lado, es importante abordar los retos que la normativa puede estar generando, en especial debido a la multiplicidad de obligaciones derivadas de varias normativas dirigidas a las empresas españolas que ofrecen servicios de seguridad integral, si bien las empresas que únicamente prestan servicios de ciberseguridad quedan libres de la mayoría de esas obligaciones. Esta discriminación puede ser un lastre para las empresas españolas en el sector. Esto es especialmente grave en el caso de las PyMES, que representan el 99 por ciento de las empresas españolas y que no son conscientes de esa necesidad.

Ciertamente la normativa europea que viene, en concreto la Directiva NIS 2.0, va en la dirección de extender la obligación de considerar todo tipo de vulnerabilidades de forma integral y de extender estas obligaciones a empresas distintas de las infraestructuras críticas a través de la obligatoriedad de considerar, no solo las vulnerabilidades de la propia empresa, sino también las de su cadena de suministro, en la que pueden participar muchas PyMES.

En definitiva, no podemos confiar que únicamente la regulación sea el motor de la evolución hacia la consideración de la seguridad integral porque la evolución normativa es lenta y parcial, no tiene en cuenta todos los aspectos necesarios ni ofrece soluciones a toda la posible problemática en un mundo de amenazas globales.

Álvaro Ubierna, de AEINSE, manifestó que la preocupación de la Asociación se centraba en la puesta al día de los conocimientos de sus ingenieros asociados y de la divulgación de buenas prácticas como es el apoyo en el caso de falta de guía regulatoria. Los cambios tecnológicos continuos exigen una formación continua al colectivo tanto en la estrategia de cómo afrontar las nuevas amenazas, como la evolución permanente de los medios técnicos a utilizar.

En definitiva, todos los participantes coincidieron en que el nivel de conocimiento y concienciación en general sobre la necesidad de dotar a los sistemas de seguridad de ciberseguridad es muy limitado, por lo que se necesita seguir trabajando en la labor de divulgación y formación. Es necesario continuar el esfuerzo de concienciación y que las buenas prácticas de las empresas líderes ayuden a extender el ejemplo de unos modelos de seguridad avanzados. En este sentido, se manifestó el deseo de que este tema sea tratado en el Foro Nacional de Ciberseguridad, como plataforma de colaboración público-privada.

Cómo repensar la gestión de responsabilidades en las empresas proveedoras de servicios de seguridad

En cuanto a la oferta de servicios de seguridad desde esta perspectiva integral, Alfonso Bilbao abrió el debate planteando el siguiente dilema: "Los clientes dicen que los proveedores no saben hacerlo y los proveedores dicen que los clientes no saben pedirlo".

En general los participantes coincidieron en que no todas las empresas prestadoras de servicios de seguridad ofrecen este tipo de servicios integrales y avanzados, con un enfoque holístico pero cada vez va a ser más necesario que las empresas usuarias de estos servicios demanden ese enfoque integral. En la medida en la que los usuarios demanden este tipo de servicios más avanzados, un mayor número de empresas los incorporarán a sus ofertas.

Si bien es cierto que la presión competitiva y los departamentos financieros y de compras pueden presionar hacia las ofertas más económicas, los directivos al más alto nivel deben ser conscientes de que la seguridad no es un gasto, sino una inversión. Hay que recordar que el coste medio de un ciberataque a una pequeña empresa ronda los 75.000 euros y eso explica que más de la mitad de las empresas atacadas no sobreviva.

Algunas empresas, sobre todo las de mayor tamaño, sí ofrecen servicios de seguridad integral. Javier Rubio, de PROSEGUR, hizo hincapié en su estrategia de considerar la seguridad como un elemento transversal en sus servicios. Siendo una de las empresas de seguridad física que ha desarrollado de forma más importante la especialidad de ciberseguridad entre las tradicionales de instalación y mantenimiento de sistemas, de tratamiento de efectivo, de vigilancia o recepción de alarmas. Actualmente su oferta al mercado no distingue tanto en qué tipo de servicio se ofrece, sino en soluciones completas hechas a medida de las necesidades.

Según Javier Rubio, "antes de conectar los sistemas, se hace un análisis previo de vulnerabilidades y, en caso de encontrar alguna, Prosegur actúa entre fabricante y cliente para solventarlas antes de la integración. Es una filosofía de "*security by design*" que además se complementa con un control constante de la operación en tiempo real y auditorías sucesivas. Es un proceso continuo". Además, el representante de Prosegur subrayó que no se trata únicamente de disponer de un departamento de ciberseguridad, sino de poner en práctica una filosofía de seguridad integral en todos sus servicios, que considere las tecnologías y también las personas.

Es cierto que esto puede encarecer el servicio, pero es una mejora necesaria para garantizar la seguridad de manera integral.

Por otro lado, hay que tener en cuenta que en el mundo OT puede existir una restricción del número de proveedores que limite la capacidad de elección de las empresas que tienen que adquirir determinados equipamientos muy específicos. En ese caso la dependencia de los prestadores de servicios de los fabricantes de sus equipos es mayor y a menudo no progresa a la velocidad adecuada en materia de ciberseguridad. En este sentido se señaló que la propuesta de Reglamento de Ciberresiliencia, que define responsabilidades de los fabricantes y desarrolladores en materia de ciberseguridad, ayudará a sofisticar este asunto. Otro aspecto relevante sería una certificación a nivel de la Unión Europea que aún no está disponible.

Coordinación interna en la empresa

La comunicación y coordinación entre las personas Responsables de Seguridad de la Información (RSI) y la Dirección de Seguridad Física (Responsables de Seguridad y Enlace en los Operadores Críticos) no siempre es idónea y dificulta en parte la disposición de las medidas de ciberseguridad (responsabilidad de los RSI) en los sistemas cuya responsabilidad pertenece a la Dirección de Seguridad.

Es necesario mejorar el nivel de coordinación entre los responsables de la información, la figura del CISO, y los responsables de la seguridad tradicional. Son profesionales que vienen de comunidades y lenguajes distintos, pero es imprescindible que colaboren e intercambien información. Es un cambio cultural muy necesario.

En el mundo de OT los equipos eran los protagonistas de la seguridad. Sin embargo, en cuanto esos equipos se conectan a una red, más del 90% de las vulnerabilidades están vinculadas a la ciberseguridad y es necesario tener en cuenta aspectos adicionales de seguridad IT, como la disponibilidad de los sistemas, la integridad de los datos o la autenticidad de los mismos. Y esta situación es novedosa y aún no ha sido asimilada en toda su extensión por los responsables de seguridad. De ahí, que sea necesario seguir trabajando en concienciación.

No obstante, también los participantes coincidieron en señalar que las nuevas normativas, como la propuesta de Directiva NIS 2.0 y su refuerzo del papel del CISO en la empresa, ayudan a que los máximos responsables empresariales asignen más recursos a la seguridad de la empresa, sin necesidad de esperar a que ocurra un incidente.

Manuel Carpio, miembro del Consejo Asesor de la Fundación ESYS, comentó que "existen muchas sinergias para la inteligencia de la empresa que combina la información de los sistemas de seguridad físicos y lógicos". - AEINSE también coincidió en señalar que hay mucho camino por recorrer a la hora de generar una cultura de la seguridad integral en las empresas españolas. Según Álvaro Ubierna, "el mundo IT ha aterrizado muy rápidamente en el mundo OT pero aún falta mucha concienciación".

Recomendaciones de mejora para abordar los retos de la ciberseguridad de los sistemas de seguridad física

Tras escuchar a las personas expertas que participaron en la mesa redonda, así como a las opiniones manifestadas por el público, la Fundación ESYS extrae las siguientes conclusiones:

- **Necesidad de divulgación y concienciación**. El nivel de conocimiento y concienciación en general en el sector de la seguridad privada sobre la necesidad de dotar a los sistemas de seguridad de ciberseguridad es muy limitado, por lo que se necesita una labor de divulgación y formación extensa e intensa.

- **Necesidad de incorporación a la regulación**. La regulación existente sobre medidas de seguridad, encuadradas en la legislación de seguridad privada no tiene en cuenta estas necesidades, por lo que se debe trabajar para incorporar en la regulación esta visión de seguridad integral y evitar disfuncionalidades.

- **Modelo de protección de infraestructuras críticas**. Una excepción interesante es la normativa de protección de infraestructuras críticas, solo aplicable a las empresas encuadradas en su ámbito, que sí se guía por el enfoque de seguridad integral. Usar como modelo esta normativa para la regulación de otros aspectos en materia de seguridad sería una solución eficaz.

- **Generalización de la seguridad integral en el mercado de servicios de seguridad**. Las empresas propietarias de sistemas de seguridad no siempre cuentan con este tipo de protecciones y las empresas instaladoras y, también en su gran mayoría, no incorporan elementos de ciberseguridad como parte de su oferta de los sistemas a instalar. Se precisa la difusión de buenas prácticas tanto para la demanda como para la oferta para que se acometa de forma general.

- **Gran potencial de mejora a través de la coordinación interna en las empresas.** La comunicación entre los equipos Responsables de Seguridad de la Información (RSI) y la Dirección de Seguridad Física (Responsables de Seguridad y Enlace en los Operadores Críticos) no siempre es idónea y a veces dificulta la disposición de las medidas de ciberseguridad (responsabilidad de los RSI) en los sistemas cuya responsabilidad es de la Dirección de Seguridad. Se precisa un esfuerzo divulgación sobre los potenciales beneficios al respecto y una concienciación de los estamentos directivos de las empresas para facilitar el entendimiento necesario.

Estas conclusiones alcanzadas animan a la Fundación ESYS en seguir profundizando en esta dirección, con estudios y jornadas que permitan avanzar según estas líneas de acción.