¿Qué Formación en Ciberseguridad necesitamos en Seguridad Privada?

En un escenario donde los sistemas de seguridad que protegen domicilios, empresas, administraciones públicas e infraestructuras críticas son digitales y por tanto potenciales objetivos de ciberataques, la Formación en Ciberseguridad es una necesidad estratégica para la Seguridad Privada. Instalar una cámara o configurar una central de alarmas requiere entender los riesgos digitales en cada uno de los procesos y en todas nuestras actividades. Es indispensable saber cómo proteger los dispositivos conectados y cómo reaccionar ante un incidente de ciberseguridad.

Las Administraciones y las Fuerzas de Seguridad alertan de que el crecimiento de los ciberataques es exponencial y las ciberamenazas se incrementan en varios frentes, desde la ciberdelincuencia común, los grupos y amenazas avanzadas, hasta el ciberterrorismo o ciberactivismo derivado de un escenario geopolítico muy inestable.

La Ciberseguridad debe formar parte de la formación esencial del personal de las empresas de seguridad así como de los usuarios que gestionen sus sistemas, pero no existe una fórmula única sino que debemos planificar el tipo de formación que resulta más adecuada para cada perfil y organización.

La Convergencia de la Seguridad Física y la Ciberseguridad

Tradicionalmente, la Seguridad Física y la Ciberseguridad han sido mundos separados. Una se ocupaba de proteger lo tangible —ersonas, edificios, bienes—y otra exclusivamente de lo digital —atos, redes, software— Si el bien a proteger es digital se dejaba al cuidado del departamento de IT. Ahora sabemos que plantearlo así es un error, ya que las tecnologías, como el Internet de las Cosas (IoT), los sistemas de videovigilancia IP o las centrales de alarmas inteligentes, han eliminado esa separación.

Un ataque a un sistema de seguridad ya no requiere necesariamente estar en el lugar para forzar una puerta o desactivar una alarma. Basta con vulnerar un router mal configurado, acceder remotamente a una cámara IP con una contraseña débil o explotar un fallo en el software de una central receptora de alarmas (CRA). Los ciberdelincuentes pueden atacar desde cualquier parte del mundo.

Debemos ser conscientes de los riesgos que para nuestras organizaciones supondría dejar cámaras de videovigilancia sin la suficiente protección, o sistemas de control de acceso que puedan ser indebidamente manipulados a distancia, o instalaciones de seguridad integral comprometidas por técnicas de ransomware, spoofing o denegación de servicio. Todo esto nos lleva a pensar que sin una capa sólida de Ciberseguridad, incluso el sistema de seguridad más sofisticado es vulnerable.

Las Brechas de Formación en el Sector de la Seguridad Privada

A pesar de esta realidad, la mayoría de los profesionales del sector de la seguridad privada no cuenta con una formación sólida en ciberseguridad. Instaladores, vigilantes, operadores de CRAs, técnicos comerciales y directores de seguridad siguen recibiendo, en muchos casos, una capacitación centrada exclusivamente en la seguridad física o en la tecnología desde un punto de vista funcional, pero no desde una perspectiva del riesgo digital.

La normativa actual en Seguridad Privada no exige conocimientos específicos de ciberseguridad a los profesionales del sector, lo que genera una peligrosa brecha. Como bien sabemos en el sector, los mínimos exigidos por la normativa suelen ir por detrás de las capacidades (y vulnerabilidades) tecnológicas, los riesgos y las amenazas reales.

Incluso cuando se trabaja con sistemas tecnológicamente avanzados, el conocimiento sobre configuraciones seguras, gestión de contraseñas robustas, detección de accesos no autorizados o actualizaciones de firmware suele ser demasiado superficial o inexistente.

Este vacío formativo y falta de concienciación expone a clientes (pensemos en industrias, servicios esenciales, o infraestructuras críticas), y puede provocar incidentes que impacten en la reputación y responsabilidad de las propias empresas de seguridad. Un fallo de ciberseguridad en un sistema instalado por una empresa puede derivar en consecuencias legales, económicas y de imagen.

¿Qué Formación en Ciberseguridad necesita el Sector?

En primer lugar, como toda formación, la de ciberseguridad debe estar adaptada a los distintos perfiles profesionales del sector de la seguridad privada.

No todo el personal puede ni debe profundizar en los aspectos más técnicos del hacking ético o el pentesting. Se trata de ofrecer conocimientos adecuados adaptados al puesto, y para ello, debemos analizar los objetivos y temarios contemplados en la formación para asegurarnos que es la más conveniente.

Competencias de Ciberseguridad según Perfil Profesional

Perfil Profesional	Competencias Clave de Ciberseguridad
Instaladores / Técnicos de Sistemas	• Configuración segura de equipos y dispositivos. • Gestión de contraseñas y credenciales de acceso. • Segmentación de redes y uso de VPN. • Actualización de firmware.
Operadores de CRA	• Conocimiento básico de ciberamenazas: phishing, spoofing, denegación de servicio. • Reconocimiento de señales sospechosas y anomalías digitales. • Protocolos de respuesta ante incidentes digitales.
Vigilantes de Seguridad / Supervisores	• Concienciación sobre amenazas digitales (ingeniería social, dispositivos USB maliciosos). • Identificación de posibles intentos de sabotaje tecnológico. • Coordinación con equipos técnicos ante anomalías digitales.
Directores de Seguridad, responsables y mandos intermedios	• Gestión del riesgo. • Cumplimiento (RGPD, ENS, ISO 27001, NIS, etc.). • Desarrollo de políticas internas. • Planes de Continuidad y Resiliencia. • Protección de Infraestructuras Críticas (PIC)
Gestión, Comerciales / Preventa	• Conocimiento de normativas y exigencias legales aplicables. • Concienciación frente a ciberamenazas actuales • Argumentario de ciberseguridad para clientes. • Evaluación de riesgos tecnológicos en instalaciones.

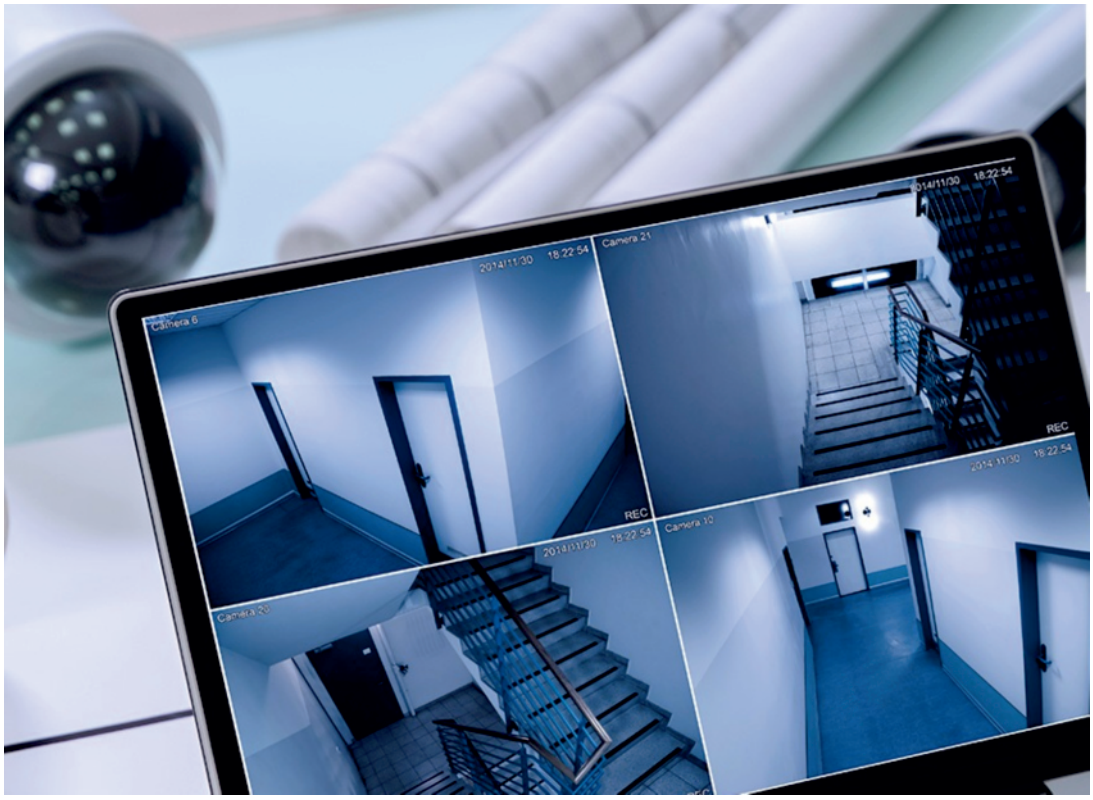
Dificultades al escoger los recursos formativos adecuados

Dependiendo del nivel de profundidad requerido, existen recursos que pueden ayudar a los profesionales de la seguridad privada a adquirir las competencias en Ciberseguridad que necesitan.

El problema principal es distinguir la formación adecuada ante la ausencia actual de una Formación reglada claramente identificada. Muchos centros ofrecen módulos de Ciberseguridad, pero los ciclos reglados, de grado medio o superior de sistemas de telecomunicación pueden ser muy extensos, costosos y resultar poco operativos.

También existen cursos básicos de concienciación gratuitos o de bajo coste disponibles a través de plataformas y Administraciones Públicas como INCIBE, pero su objetivo es la concienciación a nivel de entrada y pueden no ser suficientes al nivel necesitado en cada caso por las empresas.

Dado que existen múltiples centros generalistas que ofrezcan formación en ciberseguridad, ante la falta de regulación actual es recomendable consultar con formadores que entiendan las particularidades de la Seguridad Física y la Seguridad Privada, el funcionamiento de las empresas y como adaptar las necesidades a aspectos concretos, como los Centros de Control y las CRA, las tecnologías utilizadas en videovigilancia, el control de accesos o los sistemas de alarmas, así como la normativa específica.



Además, al estar familiarizados con los perfiles profesionales concretos del sector —igilantes, instaladores, operadores, directores—pueden adaptar los contenidos a su contexto operativo real. Esta orientación práctica y sectorial maximiza la eficacia de la formación y permite una integración más rápida y natural de los conceptos de ciberseguridad en el día a día de los equipos.

Debemos reclamar a nuestros centros de formación, que propongan programas sobre Ciberseguridad lo más adaptados posible a nuestro sector y a sus perfiles profesionales.

La formación en Ciberseguridad no es única, debe estar adaptada a los conocimientos previos y objetivos específicos del personal, y aprovechar metodologías online que permitan realizar itinerarios personalizados y que sean compatibles con la actividad profesional.

Para los casos en los que se requieran certificaciones técnicas, debemos tener un conocimiento previo para distinguir las más relevantes o reconocidas, como ISO 27001, CompTIA, C-Council, CISM o CISA.

Por último, debemos tener en cuenta la formación específica proporcionada por los fabricantes de seguridad electrónica, que ofrecen módulos sobre la Ciberseguridad, aplicada a sus productos.

En todos los casos, será esencial que las empresas de seguridad fomenten la formación continua de su personal, asignen presupuestos específicos y evalúen periódicamente el nivel de Ciberseguridad de sus equipos.

La Formación en Ciberseguridad como mejora competitiva

Además, los clientes están cada vez más informados y preocupados por la ciberseguridad. Incluir esta dimensión en la propuesta de valor de una empresa de seguridad privada ya no es un extra, sino una necesidad.

Invertir en formación no es solo una cuestión de prevención y protección, también representa una oportunidad competitiva para las empresas de seguridad que puede traer beneficios directos para las empresas y los profesionales, como:

- **Mejora de la calidad del servicio:** ofrecer soluciones seguras, robustas y con garantías digitales.
- **Diferenciación comercial:** destacar frente a competidores que no cubren la dimensión cibernética.
- **Reducción de incidentes:** menor riesgo de brechas, reclamaciones o sanciones.
- **Adaptación a futuras normativas:** estar preparados ante posibles exigencias regulatorias.
- **Confianza del cliente:** transmitir una imagen de profesionalidad y responsabilidad digital.

Conclusiones y recomendaciones para las empresas de seguridad

La frontera entre la Seguridad Física y la Ciberseguridad ya no existe. En la práctica, todo sistema de seguridad es hoy también un sistema informático, y por tanto, susceptible de ser atacado digitalmente. Profesionales y empresas del sector de la seguridad privada deben tomar conciencia de esta realidad y prepararse en consecuencia.

La formación en ciberseguridad no es una opción, sino una responsabilidad y también una oportunidad de mejora competitiva. No solo para proteger los activos de los clientes, sino también para garantizar la integridad de las empresas proveedoras y la

continuidad de negocio. Mejorar la Formación en Ciberseguridad con determinación nos prepara mejor para ofrecer un servicio más completo y seguro, contribuyendo al objetivo de la Seguridad Privada que es elevar el nivel general de protección (y también ciberprotección) en nuestra sociedad.

Para una ello, las empresas de seguridad privada deben tener planes de formación para adoptar una cultura de ciberseguridad, para todos los empleados y realizar algunas estrategias concretas.

Las empresas deberían empezar por evaluar el nivel actual de ciberpreparación de sus equipos de profesionales y Diseñar planes de formación escalables, comenzando por los perfiles técnicos y directivos.

De esta forma estarán preparados para establecer políticas de ciberseguridad internas, con protocolos claros y permanentemente actualizados. Si es necesario, las empresas pueden contar con expertos externos en ciberseguridad para auditorías, simulacros o formaciones específicas.

Las empresas pueden contar actualmente con la ayuda de las Asociaciones y las Administraciones Públicas, conocer como impulsan programas de formación, y generan marcos normativos que incluyen la ciberseguridad a la vez que fomentan promover buenas prácticas entre los profesionales.

Fernando Sánchez Raya
Miembro del área de trabajo de ciberseguridad de AES

en los medios

La protección de infraestructuras críticas es esencial

Riesgos seguridad

¿Cuáles serán los grandes retos del sector de la seguridad en los próximos años y cómo superarlos? La industria de la seguridad se enfrenta a varios retos importantes en los próximos años: la ciberseguridad, la privacidad de datos, la atracción y fidelización del talento, las amenazas internas, la adaptación a nuevas tecnologías, y la sobrerregulación.

https://www.ifema.es/sicur/noticias/entrevista-aes-fundacion-antonio-escamilla