AES
FUNDACIÓN

Guía Seguridad Hospitalaria

Índice

Guía Seguridad Hospitalaria

Elaborada por el Área de Trabajo de Seguridad electrónica de AES

Nombre	Empresa	Papel en la elaboración de la guía
Agustín Rodríguez	CHUBB	
Alberto Alonso	AXIS	
Alberto Moreno	FEIX	
Alberto Trigo	SECURITAS DIRECT	
Alejandro García	OBSERVATORIO SEET	
Angel Reyes	TRABLISA	
Antonio Gómez	ILUNION	
David Alonso	TELEFÓNICA	
David del Rey	SECURITAS	Coordinador
Emilio Castro	ILUNION	
Eva Plana	MOTOROLA	Redactora
Felix Rizo	CHUBB	
Guilherme Ribeiro	ADVANCIS	
José Luis Andrés	SECURITAS DIRECT	
Juan de la Fuente	PROSEGUR	Redactor
Juan José López	TRABLISA	
Julio Pérez	EULEN	
Manuel Pérez	SECURITAS	
Mariano Casado	SECURITAS	
Nacho Jiménez	SECURITAS DIRECT	
Óscar Téllez	PYCSECA	
Rafael González	SECURITAS	
Ricardo Cañizares	AES FUNDACIÓN	Colaborador
Roberto Otero	AJAX	
Manuel Yanguas	INTERLOCUTOR POLICIAL SANITARIO	Colaborador en esta guía
Santiago García	OSICH	Colaborador en esta guía
Santiago Riaño	OSICH	Colaborador en esta guía

Presentación

En la Industria de la Seguridad en España y como asociación decana, AES siempre ha desarrollado un papel vital. Representamos a nuestro país tanto en los Comités Nacionales y Europeos donde se crean las normas como en las dos principales asociaciones europeas como son Eurosafe y Euralarm. Todo ello es posible gracias a la dedicación y conocimiento de nuestros expertos pertenecientes a las diferentes Áreas de Trabajo que disponemos. La información es poder y por supuesto vital para la competitividad de nuestras empresas asociadas. El compromiso social es parte de nuestro ADN y para ello creamos continuamente guías, recomendaciones y publicaciones desde donde transmitimos nuestro conocimiento. En nombre de toda la Junta Directiva de AES esperamos que disfrutes de este trabajo que con tanto cariño hemos realizado.

Iñigo Ugalde Blanco –Presidente de AES.

Después de muchos meses de trabajo y dedicación, el 27 de junio de 2024 quedó registrada AES FUNDACIÓN en el Registro Nacional de Fundaciones. Uno de los objetivos establecidos para la Fundación es la difusión de los documentos elaborados por las áreas de trabajo de AES.

Es por ello por lo que todas las publicaciones de nuestras áreas de trabajo (ya tenemos incorporadas varias guías que puedes consultar sin coste en Publicaciones AES Fundación así como la Newsletter y el Boletín, han empezado a aparecer con el color naranja distintivo de la Fundación, y en el caso de Newsletter y Boletín, con una nueva numeración de segunda época.

Todo ello forma parte del desarrollo #UniversoAES y #HaciendoIndustria. Espero que esta nueva publicación que os traemos hoy sirva de ayuda y siga contribuyendo con nuestra propuesta de valor **"dinamizando la seguridad ciudadana"**

Antonio Escamilla Recio –Presidente de AES FUNDACIÓN.

La elaboración de una Guía de Seguridad Electrónica de aplicación en Seguridad Hospitalaria se enmarca en la habitual dinámica de trabajo del Área de Seguridad Electrónica de AES. Al igual que el resto de las iniciativas de las diferentes Áreas de trabajo de AES, esta surge como propuesta de uno de los miembros del Área. Dicha propuesta fue aprobada por unanimidad en una de las reuniones del Área y, de la misma forma que en otras ocasiones, se procedió a crear un grupo de trabajo que liderara la confección de dicha guía.

El espíritu del trabajo no es tanto elaborar un documento que recoja todos los detalles de aplicación, algo que habría resultado poco menos que inabordable en un breve espacio de tiempo, sino generar buenas prácticas en la industria y a la vez recopilar diferentes fuentes autorizadas que permitan al lector profundizar en la materia tanto como sea necesario.

Tras sucesivas versiones por parte del grupo de trabajo, con sus correspondientes revisiones y aportes por parte del resto de miembros del grupo, así como de otros grupos de trabajo involucrados en la materia, este trabajo ve finalmente la luz. Desde el Área de Seguridad Electrónica de AES tenemos el firme deseo de que sirva de guía y orientación para aquellos profesionales o empresas (asociados o no) que busquen la excelencia en el servicio diario que proporcionamos a nuestros clientes.

David del Rey

Coordinador del área de seguridad electrónica.

1 Objetivos y alcance

La seguridad hospitalaria busca garantizar la protección de trabajadores, pacientes, infraestructura y equipos frente a riesgos de diversa naturaleza. Este documento ofrece una guía integral con énfasis en sistemas electrónicos, complementados con medidas físicas y protocolos de actuación.

Ejemplos concretos incluyen la prevención de accesos no autorizados, como intrusiones en áreas de alta sensibilidad como farmacias o laboratorios, así como la mitigación de fallos en la seguridad de datos mediante sistemas robustos de ciberseguridad.

Esta guía incorpora experiencias contrastadas en otros ámbitos de la seguridad.

2.1. Situación del Sector

La seguridad hospitalaria abarca desde pequeños centros de atención primaria hasta complejos hospitalarios considerados infraestructuras críticas. Factores clave incluyen:

- **Alta concurrencia de personas:** Los centros médicos reciben a diario a numerosos pacientes, visitantes y personal, lo que aumenta la complejidad en la gestión de la seguridad.
- **Zonas restringidas:** Áreas como laboratorios, quirófanos y almacenes de medicamentos requieren controles de acceso estrictos para garantizar su seguridad.
- **Preocupación creciente por la seguridad del personal sanitario:** Según el informe de agresiones a profesionales del sistema nacional de salud del Ministerio de Sanidad en 2024 se notificaron un total de 17.070 agresiones a profesionales sanitarios en el conjunto del Sistema Nacional de Salud, lo que supuso un aumento de 2.364 respecto a 2023 (+16 %). Del total, 7.450 agresiones (el 44 %) se produjeron en atención hospitalaria.
- **Seguridad del paciente:** La Organización Mundial de la Salud (OMS) estima que uno de cada 10 pacientes sufre daños durante su estancia hospitalaria, y que el 50% de estos incidentes podrían prevenirse. Además, un informe de la Organización Mundial de la Salud (OMS) subraya que las fallas en la seguridad de los pacientes afectan al 10% de los ingresos hospitalarios a nivel mundial.

Estos datos enfatizan la necesidad de implementar medidas robustas de seguridad.

2.2. Principales Riesgos y Amenazas

- ⚠ **Violencia:** Tensiones en urgencias o conflictos entre pacientes y personal. En junio de 2024, familiares de una paciente agredieron a 16 trabajadores de un hospital de Terrassa tras complicaciones en un parto: se produjo violencia física y verbal. Se destrozó material sanitario, y varios empleados sufrieron lesiones físicas y psicológicas.
- ⚠ **Accesos No Autorizados:** Ingreso indebido a áreas restringidas (radiología, farmacia, etc.). En 2025, un individuo fue detenido en un hospital de Elche tras acceder a habitaciones de pacientes y a zonas restringidas al personal sanitario. Se forzaron taquillas de trabajadores y se llevó material médico.

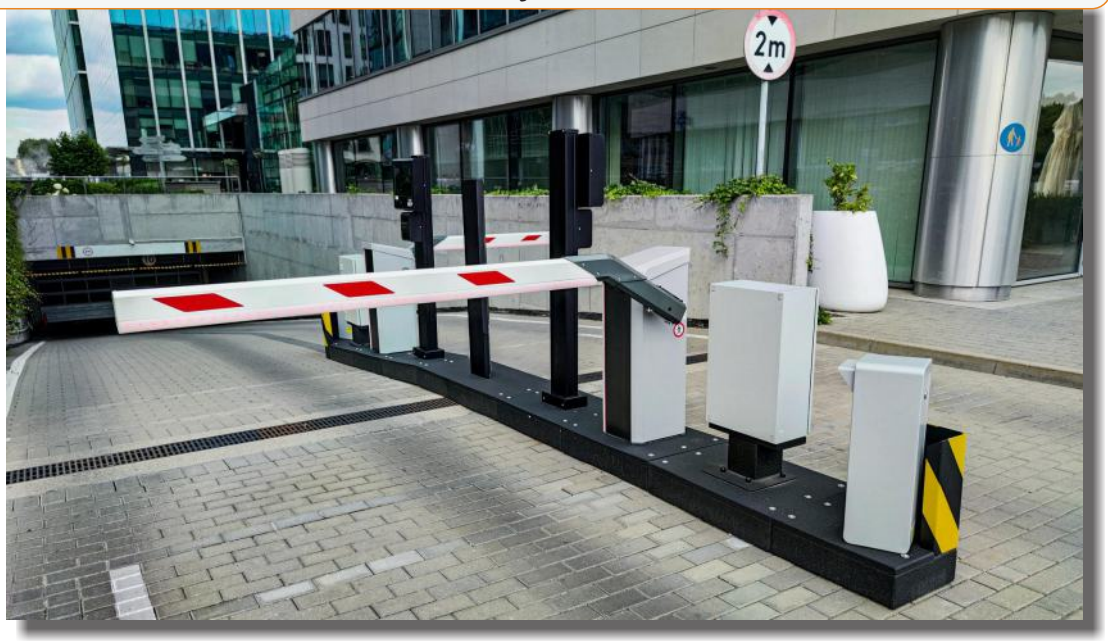
- ⚠ Desastres y Emergencias: Incendios, cortes eléctricos o inundaciones que afectan la operatividad. Un incendio declarado en noviembre de 2025 en la terraza de un Hospital de Cartagena activó el plan de autoprotección y emergencias, y los pacientes de las cuatro plantas superiores fueron trasladados a zonas seguras dentro del propio recinto.
- ⚠ Ciberseguridad: Protección de datos de pacientes frente a ataques. En 2023, un ataque de ransomware a un gran hospital en Barcelona, afectó servicios esenciales: urgencias, laboratorio y farmacia. Como consecuencia se cancelaron más de 150 operaciones no urgentes, unas 3.000 consultas externas y cientos de pruebas analíticas. También se dejó inaccesible la historia clínica digital de pacientes; el personal tuvo que recurrir a métodos "nalógicos"(papel), con el retraso operativo que ello conllevó.
- ⚠ Alta dependencia tecnológica: La continuidad asistencial depende cada vez más de la electricidad y las comunicaciones para el funcionamiento de los sistemas vitales.

2.3. Normativa Aplicable

- Protección contra Incendios (PCI): Reglamento de Instalaciones de Protección contra Incendios (RIPCI), Código Técnico de la Edificación (CTE). Por ejemplo, en el Hospital General de Valencia, el uso de sistemas avanzados de detección temprana permitió contener un incendio en 2021 sin necesidad de evacuación masiva.
- Seguridad Privada: Ley 5/2014, de 4 de abril, de Seguridad Privada y normativa complementaria. Un caso práctico es la implementación de controles de acceso en el Hospital de la Paz, Madrid, donde se utilizan tarjetas RFID para restringir el acceso a áreas críticas como quirófanos y farmacias.
- Ciberseguridad: Esquema Nacional de Seguridad (ENS), ISO 27001, y directiva NIS2. Por ejemplo, el Hospital Clínico de Barcelona recientemente reforzó sus medidas de protección de datos con certificaciones de ciberseguridad tras un ataque de ransomware en 2023.
- Fuentes Radiológicas: Norma IS-41 del Consejo de Seguridad Nuclear sobre protección de Fuentes Radiológicas. Se establece la obligatoriedad de presentar planes de protección física para fuentes radiológicas de nivel 3, 2 y 1, siendo necesaria la revisión de estos planes tanto por el Consejo de Seguridad Nuclear (CSN) como por las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

3.1. Medios Físicos de Protección Pasiva

Perímetro: Cercas, muros y control de acceso vehicular.



Accesos: Puertas reforzadas y señalización clara de áreas restringidas.

3.2. Sistemas Electrónicos de Seguridad

3.2.1. Videovigilancia (CCTV)

- Objetivos: Monitorear actividades, prevenir incidentes y registrar evidencia.
- Recomendaciones:
  - Requisitos de Infraestructura y Fiabilidad
    - **Arquitectura:** El sistema debe ser de arquitectura cliente-servidor y basarse en una red de comunicaciones e infraestructura de TI prevista.
    - **Grabadores (NVR):** Deben ser de formato rack y contar con mecanismos de redundancia (discos de SO, discos de almacenamiento de video, fuente de alimentación) para asegurar la continuidad del servicio y evitar la pérdida de grabaciones o interrupciones.
    - **Failover:** Debe existir una lógica de failover (conmutación por error) entre los grabadores, de modo que si uno falla, sus cámaras se transfieran automáticamente a los grabadores restantes sin interrupción de la grabación.
    - **Escalabilidad:** El sistema debe ser escalable para futuras ampliaciones de cámaras y/o servidores y debe soportar cámaras IP de terceros.
  - Funcionalidades Clave del Software (VMS)
    - **Video Análisis (IA):** Debe incluir analíticas de última generación basadas en IA, con detección y clasificación de personas y vehículos, calibración automática y autoaprendizaje. Las analíticas pueden estar integradas en las cámaras o llevarse a cabo en el grabador.
    - **Búsqueda Inteligente:** Debe contar con herramientas avanzadas para búsqueda por movimiento, presencia de objetos clasificados, cambios en la escena y búsqueda por apariencia.
    - **Motor de Reglas:** Debe permitir crear flujos de trabajo integrales para la supervisión, asignación y confirmación de alarmas.
    - **Gestión Centralizada:** Permitirá la gestión de roles y grupos de usuarios, asignando privilegios para grabación, visualización, exportación y configuración.
    - **ONVIF:** Compatibilidad con los perfiles ONVIF® S, T y G para garantizar la interoperabilidad. La funcionalidad del perfil G permite la grabación local ante pérdida de conexión y la recuperación de imágenes consolidadas posteriormente.

Nota: Consulte el Glosario de términos en la página 24 para definiciones técnicas.

- **Actualización de Firmware:** El software debe actualizar el firmware de las cámaras automáticamente.
- **Acceso Remoto y Móvil:** Debe disponer de una aplicación móvil gratuita (iOS y Android) para acceso unificado a video en vivo, grabado y notificaciones de alarmas. También debe disponer de un entorno cloud para gestión, acceso a video y estado de salud de los grabadores (sin almacenar video).

- Integración Unificada de Sistemas

  La interfaz de usuario principal para los operadores de seguridad será el propio *software* de CCTV (VMS).

  - **Con Control de Accesos (CCAA):**
    - Supervisión y actuación sobre eventos y mapas de CCAA desde la interfaz de CCTV.
    - Asociación de cámaras de CCTV a cada puerta para supervisión visual.
    - Búsqueda por Identidades: Búsqueda de un individuo por nombre/ID y visualización del video asociado a su paso por las puertas.
  - **Con Detección de Intrusión:**
    - Visualización de panel sinóptico, estados de zonas y grupos.
    - Supervisión de alarmas del sistema de intrusión con el video asociado al momento de la alarma.
    - Representación gráfica de elementos en mapas, permitiendo actuar sobre ellos y visualizar las cámaras asociadas.
  - Con los **pulsadores de agresión** instalados en Urgencias y Controles de Enfermería.
    - **Respuesta Inmediata:** Al activarse un pulsador, el sistema debe activar una alarma y situar inmediatamente la cámara más cercana en el centro de control, enfocando automáticamente el incidente

- Tipos de Cámara Incluidos
  - Cámaras Bullet: Diseñadas para exterior , con iluminación IR, resolución de 5MP y analíticas embebidas (detección/clasificación de vehículos/personas).
  - Cámara Minidomo: Para interiores, con detección de sabotaje, audio y movimiento, y resolución de 2MP.
  - Cámara Multisensor Exterior: Cobertura de 270º con una resolución total de 24MP (3 sensores de 8MP) o 360º con una resolución total de 32MP para vigilancia de amplias áreas perimetrales.
  - Cámara de Esquina: Con lente fija, iluminación infrarroja invisible (940 nm) y analíticas embebidas.

- Ubicaciones específicas:
  - Entradas de emergencia: Cámaras de alta definición con capacidad para operar en condiciones de baja luz, asegurando una vigilancia continua.
  - Quirófanos: Cámaras diseñadas para registrar el acceso y salida del personal, con integración a sistemas de control de accesos.
  - Pasillos principales y áreas comunes: Cámaras con visión panorámica para cubrir amplias áreas de tránsito.
  - Áreas de almacenamiento de medicamentos: Cámaras enfocadas en puertas de acceso y pasillos internos para detectar cualquier actividad inusual.
  - Accesos a Urgencias, Admisión y Controles de Enfermería/Psiquiatría: Clave para la prevención y respuesta ante agresiones al personal.
  - Áreas de Instalaciones Críticas (Climatización, Calderas, etc.): Cámaras con detección de intrusión perimetral y analíticas para prevenir sabotajes que comprometan la operatividad asistencial.
  - Accesos a CPD (Centro de Procesamiento de Datos).

3.2.2. Control de Accesos

- Soluciones: Cerraduras electrónicas, biometría y tarjetas RFID. Por ejemplo, el Hospital General de Madrid ha implementado sistemas biométricos de reconocimiento facial para controlar el acceso a sus quirófanos, garantizando que solo el personal autorizado pueda entrar. Además, el uso de tarjetas RFID en el Hospital Clínico de Barcelona permite gestionar el acceso a áreas restringidas, como farmacias y laboratorios, con registro automático de entradas y salidas.
    - El uso de biometría (como el reconocimiento facial o de huella dactilar) debe estar estrictamente alineado con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, ya que implica el tratamiento de datos personales de categorías especiales. Se debe justificar la necesidad, asegurar el consentimiento explícito y cumplir con los requisitos de la AEPD (Agencia Española de Protección de Datos) o equivalente.
- Zonas Críticas: Farmacias, quirófanos y áreas de almacenamiento.
- Integración: Con sistemas de videovigilancia y gestión hospitalaria.

3.2.3. Detección de Intrusión

- Tecnologías: Sensores de movimiento, contactos magnéticos y detectores de rotura de cristales.
- Funcionalidad para Prevención de Agresiones: Integración de pulsadores de agresión instalados en Urgencias y Controles de Enfermería con el sistema de CCTV.
  - Al activarse un pulsador, el sistema activa inmediatamente una alarma y sitúa la cámara más cercana en el centro de control, enfocando automáticamente el incidente
- Ubicación: Entradas principales, áreas de almacenaje y zonas sensibles.
- Ejemplos Prácticos: En 2022, un hospital en Sevilla evitó un robo en su área de farmacia gracias a un sistema de detección de intrusión que activó una alerta inmediata al centro de control, permitiendo la intervención del personal de seguridad antes de que el incidente escalara. Asimismo, sensores de movimiento en un hospital de Valencia identificaron intentos de acceso no autorizado a un quirófano, reforzando la seguridad del área.

3.2.4. Sistemas de Comunicaciones

- Funciones: Comunicación entre sistemas de alarma, videovigilancia y control de accesos.
- Redundancia: Sistemas de respaldo para asegurar operatividad continua.

3.3. Centro de Control de Seguridad

- Diseño: Equipado con tecnología de monitoreo y registro, como pantallas de alta resolución para la supervisión en tiempo real de todas las áreas del hospital.
- Tecnologías Utilizadas: Software de gestión de seguridad integrado que centraliza las alarmas, videovigilancia, control de accesos y detección de intrusión.
- Funciones: Supervisar sistemas integrados, coordinar respuestas a incidentes y gestionar simulacros de emergencia.
- Funciones Adicionales del Software de Integración:
  - Apertura Remota de Cerraduras Electrónicas: Permite aperturas en remoto de cerraduras, lo que mejora la seguridad en centros de salud al eliminar la dependencia de celadores con llaves físicas.
  - Gestión de Zonas: Permite la apertura y el cierre completo de áreas o plantas, logrando que todos los despachos de una zona queden abiertos o cerrados a una hora determinada, facilitando tanto el acceso del personal como la evacuación del edificio en caso de emergencia.

- Ubicación: En un área segura y de acceso restringido, con redundancia energética para garantizar operatividad continua incluso en situaciones críticas.

3.4. Innovaciones Tecnológicas y Tendencias

- IA y Biometría: Reconocimiento facial para acceso y verificación de identidad. Por ejemplo, el Hospital Universitario de Madrid ha implementado un sistema de reconocimiento facial en su zona de quirófanos, lo que ha reducido significativamente los intentos de acceso no autorizado.
  - Consideración Adicional: En línea con el punto 3.2.2, la adopción de tecnologías biométricas debe realizarse respetando el RGPD y las directrices de las autoridades de protección de datos, minimizando riesgos de privacidad.
- Dispositivos IoT: Sensores para control de temperatura y humedad en áreas críticas, En un hospital de Barcelona, estos sensores han permitido alertas tempranas de fallos en sistemas de refrigeración para medicamentos. Actualmente estos dispositivos permiten detectar virus que pueden ayudar a prevenir el contagio masivo o agresiones en aquellas zonas en las que las cámaras no están permitidas por privacidad.
- Análisis Predictivo: Identificación de patrones de riesgo. Por ejemplo, el uso de IA en el Hospital Clínico de Sevilla ha facilitado la detección de comportamientos sospechosos en tiempo real en áreas de alta concurrencia, mejorando la seguridad.
- Analíticas de Safety: Seguridad y Salud para hospitales, detección de caídas de pacientes o personal en pasillos solitarios.

3.5. Plan de Autoprotección

- Componentes: Inventario de riesgos, protocolos de emergencia y simulacros periódicos.
- Cumplimiento: Normativa vigente (RD 393/2007) y guías de protección civil.
- Ejemplos de simulacros incluyen un ejercicio de evacuación realizado en el Hospital Universitario de Zaragoza en 2022, que permitió reducir los tiempos de salida en un 15% tras identificar puntos de congestión en los pasillos principales. Otro caso destacado es el simulacro de respuesta ante incendios llevado a cabo en el Hospital Clínico de Salamanca, donde el personal sanitario logró coordinarse con los servicios de emergencia locales para evacuar a más de 50 pacientes simulados en menos de 20 minutos, demostrando la efectividad de su plan de emergencia.

3.6. Matriz de Riesgos y Soluciones de Seguridad Hospitalaria

Matriz de Riesgos y Soluciones de Seguridad Hospitalaria: Integración de sistemas (CCTV, Accesos e Intrusión) bajo un VMS responde a las amenazas actuales.

Riesgo Identificado	Impacto en el Sector	Solución Tecnológica Propuesta
Violencia y agresiones al personal	Aumento del 16% en agresiones notificadas en 2024; el 44% ocurre en hospitales.	Integración de pulsadores de agresión en Urgencias y Enfermería que activan alarmas y enfocan automáticamente la cámara de CCTV más cercana.
Accesos no autorizados a áreas restringidas	Intrusiones en quirófanos, farmacias o laboratorios para robo de material o taquillas.	Sistemas de Control de Accesos mediante tarjetas RFID o biometría. Uso de cámaras de esquina con analíticas en zonas críticas.
Robos en farmacias y almacenes	Pérdida de material médico y medicamentos sensibles.	Sensores de movimiento y contactos magnéticos de intrusión integrados con el VMS. Cámaras específicas para el control de pasillos de medicación.
Incendios y emergencias	Necesidad de evacuación de pacientes críticos y protección de infraestructura.	Sistemas de detección temprana (PCI). Gestión centralizada de zonas para apertura remota de cerraduras y facilitar la evacuación.
Ataques de ciberseguridad (Ransomware)	Bloqueo de historias clínicas, cancelación de operaciones y retrasos operativos masivos.	Cumplimiento del ENS e ISO 27001. Monitoreo continuo de redes IT/OT e implementación de seguridad desde el diseño.
Caídas y seguridad del paciente	El 10% de los ingresos mundiales sufre daños prevenibles durante la estancia.	Implementación de **Analíticas de Safety** para la detección automática de caídas de pacientes en pasillos o áreas comunes.

4.1. El Entorno Tecnológico en los Centros Sanitarios: Una Infraestructura en Evolución

La transformación digital ha alcanzado de lleno al entorno sanitario, donde actualmente conviven una gran variedad de tecnologías. Desde dispositivos de electromedicina como electrocardiógrafos, audiómetros y espirómetros, hasta sistemas de diagnóstico por imagen, tratamiento radiológico y radioterapia, todos ellos forman parte esencial del equipamiento de un centro sanitario moderno.

A este ecosistema se suman los sistemas informáticos de gestión hospitalaria, soluciones de domótica para el control ambiental y de instalaciones, y los Sistemas Electrónicos de Seguridad (SES), como videovigilancia (CCTV), control de accesos y detección de intrusiones. Este conjunto conforma un entorno complejo en el que interactúan tecnologías de la información (IT), tecnologías de operación (OT) e Internet de las Cosas (IoT), que a menudo comparten infraestructuras de red y comunicación.

La creciente dependencia de estos sistemas y su integración es clave para mejorar la eficiencia, la capacidad diagnóstica y la calidad asistencial. Sin embargo, esta interconectividad también expone a los centros sanitarios a nuevos riesgos, especialmente en el ámbito de la ciberseguridad.

4.2. Ciberseguridad en el Entorno Sanitario

La protección de estos sistemas tecnológicos no es solo una cuestión técnica, sino un componente fundamental de la seguridad del paciente, de la continuidad asistencial y de la protección de la información clínica.

La convergencia de IT, OT e IoT plantea retos significativos en materia de ciberseguridad, dado que cualquier brecha puede comprometer datos sensibles, alterar servicios críticos o poner en riesgo la integridad física de los pacientes.

Es imprescindible contar con políticas de seguridad sólidas, mecanismos de monitorización continua, y medidas tanto técnicas como organizativas que contemplen la seguridad desde el diseño. En este contexto, la gestión de riesgos cobra un papel esencial, adaptándose a la realidad específica de cada centro y evaluando la exposición potencial de cada sistema.

4.3. Sistemas Electrónicos de Seguridad: Consideraciones Clave

La instalación de un nuevo sistema electrónico de seguridad en un entorno hospitalario requiere un enfoque riguroso desde el punto de vista de la ciberseguridad. No basta con evaluar los riesgos del sistema en sí, sino que es necesario considerar su posible impacto sobre el conjunto de la infraestructura tecnológica del centro.

Antes de la implementación de un sistema electrónico de seguridad, es esencial evaluar los requisitos normativos específicos que aplican en el entorno hospitalario. Los sistemas de seguridad deben cumplir con las leyes y regulaciones relacionadas con la protección de la información sanitaria, como el Reglamento General de Protección de Datos (RGPD) en Europa, y las normativas locales que puedan estar vigentes.

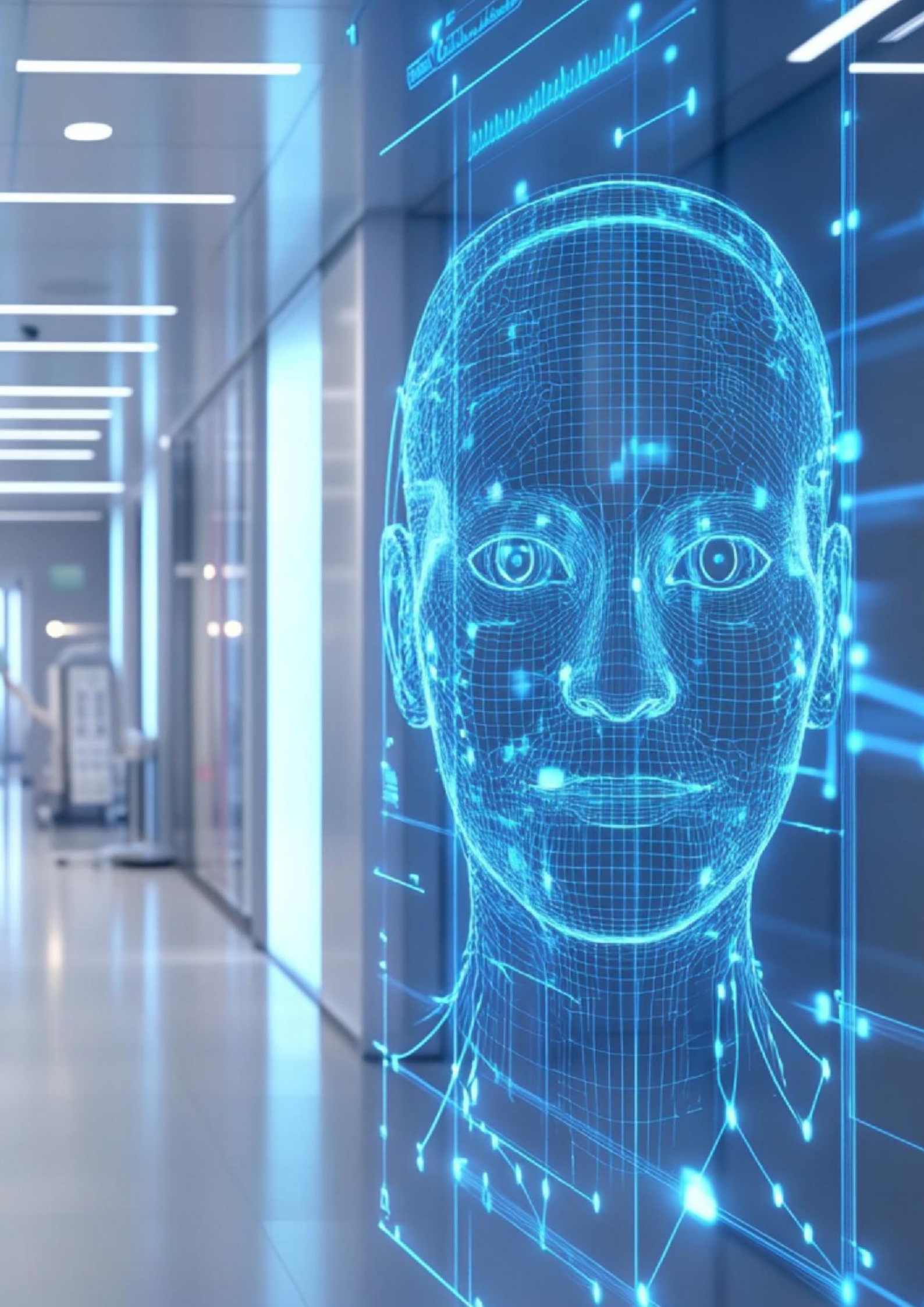
Además de las regulaciones relacionadas con la protección de datos personales, el sistema de seguridad debe cumplir con los estándares internacionales de ciberseguridad, como los definidos por la Organización Internacional de Normalización (ISO), como la norma ISO/IEC 27001, que establece los requisitos para un sistema de gestión de seguridad de la información

El segundo paso es determinar si el sistema que se va a implantar estará completamente aislado o si, por el contrario, compartirá elementos o conexiones con otros sistemas IT, OT o IoT. Esta clasificación no siempre es evidente, y una falsa percepción de aislamiento puede generar vulnerabilidades ocultas.

- Si el sistema es verdaderamente aislado, deberá someterse a un análisis de riesgos específico y aplicarse las correspondientes medidas de protección, incluyendo herramientas de monitorización.
- Si el sistema está interconectado, será necesario un análisis de riesgos conjunto que contemple todas las interdependencias con el resto de sistemas del centro. En este caso, el nuevo sistema deberá cumplir, como mínimo, con los mismos estándares y requisitos de ciberseguridad que los sistemas con los que interactúa.

Una vez que se ha determinado si el sistema es aislado o interconectado, y se han implementado las medidas de ciberseguridad adecuadas, es crucial que el sistema electrónico de seguridad sea sometido a un proceso de monitoreo continuo. Esto no solo ayuda a identificar vulnerabilidades emergentes, sino que también permite detectar comportamientos anómalos que puedan indicar un posible ataque. Las herramientas de monitorización deben ser capaces de integrar y analizar datos provenientes tanto del propio sistema de seguridad como de otros sistemas interconectados en la infraestructura hospitalaria.

El monitoreo proactivo también incluye la actualización constante de los sistemas de seguridad. Las amenazas evolucionan con el tiempo, y es fundamental que los sistemas de seguridad se mantengan al día con las últimas actualizaciones de software y parches de seguridad. Además, se deben realizar auditorías periódicas para garantizar que todos los controles de seguridad estén siendo efectivos y no existan brechas inadvertidas en el sistema.



4.4. Resiliencia y recuperación ante desastres

La resiliencia de los sistemas electrónicos de seguridad es otro aspecto crucial. En un entorno hospitalario, los sistemas de seguridad deben ser capaces de seguir operando, incluso en el caso de un ataque o fallo crítico en los sistemas. Esto requiere el diseño de sistemas redundantes, de modo que, si un componente del sistema falla, otro pueda tomar el control de inmediato sin interrumpir la seguridad o el funcionamiento del centro.

Es imprescindible también contar con un plan de recuperación ante desastres que permita restaurar los sistemas de seguridad a su estado óptimo tras un incidente. Este plan debe incluir estrategias para asegurar la disponibilidad de la información crítica y garantizar que el sistema de seguridad continúe funcionando incluso en condiciones extremas. La simulación de incidentes y la realización de ejercicios prácticos en los que se simule un ataque o un fallo del sistema, pueden ayudar a validar la efectividad del plan y la capacidad de respuesta del personal.

4.5. Validación y pruebas Post-Implementación

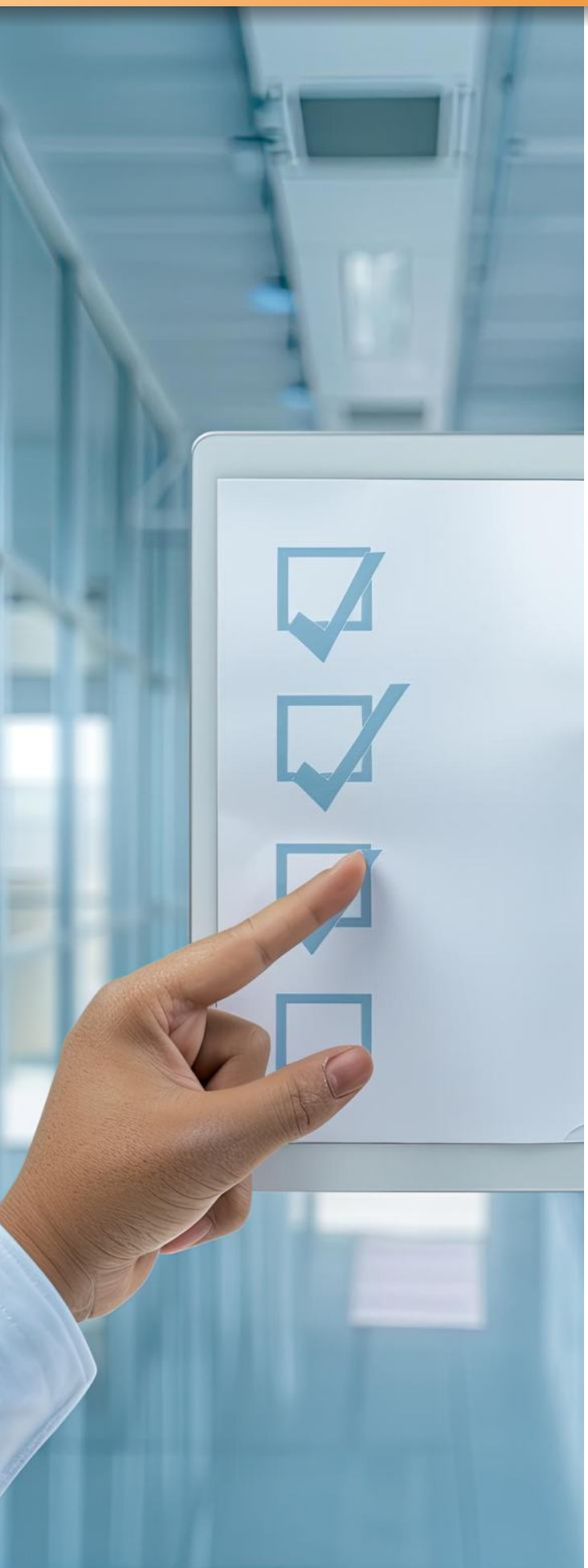
Una vez instalado el sistema electrónico de seguridad, se deben realizar pruebas de penetración para identificar posibles vulnerabilidades que no hayan sido detectadas durante la fase de planificación y diseño. Estas pruebas consisten en simular un ataque de un actor malicioso con el fin de evaluar la robustez del sistema y la efectividad de las medidas de protección implementadas.

Además de las pruebas de penetración, se deben realizar validaciones post-implementación para asegurarse de que el sistema cumple con todos los requisitos normativos y estándares de ciberseguridad aplicables, como los establecidos por organizaciones internacionales o las leyes locales de protección de datos e información sanitaria (por ejemplo, el Reglamento General de Protección de Datos, RGPD en Europa).

4.6. Concienciación y capacitación del personal

La efectividad de cualquier sistema electrónico de seguridad no solo depende de la tecnología, sino también de las personas que interactúan con él. Por ello, es esencial formar y capacitar al personal sobre los riesgos cibernéticos y las mejores prácticas en ciberseguridad. Esto incluye desde el personal de seguridad encargado de la supervisión del sistema, hasta los usuarios finales que podrían, sin querer, comprometer la seguridad al interactuar con el sistema.

La capacitación debe ser continua y adaptada a los roles y responsabilidades de cada miembro del personal, asegurando que todos comprendan la importancia de seguir los protocolos de seguridad. Además, deben implementarse políticas claras sobre el uso de dispositivos y sistemas, acceso a información confidencial y la gestión de contraseñas.



- Capacitación: profesionales del ámbito sanitario, incluyendo módulos de negociación, comunicación asertiva y gestión de situaciones conflictivas adaptados a las necesidades de diferentes tipos de hospitales.
- En pequeños centros clínicos, enfocarse en protocolos básicos de evacuación y gestión de conflictos.
- En grandes complejos hospitalarios, incluir simulacros avanzados de respuesta ante emergencias y ciberataques.
- Mantenimiento Preventivo: Revisiones periódicas de sistemas electrónicos y físicos.
- En hospitales de menor tamaño, priorizar la funcionalidad de sistemas esenciales como alarmas de incendio y cámaras básicas de vigilancia.
- En grandes complejos, asegurar la integración de múltiples sistemas de seguridad y realizar auditorías externas.
- Evaluación Continua: Actualización de análisis de riesgos y adaptación a nuevas amenazas.
- Los pequeños centros pueden realizar evaluaciones anuales simplificadas.
- Los hospitales más grandes deben implementar sistemas de análisis predictivo para monitorear amenazas en tiempo real.
- Colaboración Interinstitucional: Coordinación con autoridades locales y organismos de protección civil.
- En hospitales rurales, establecer convenios con cuerpos de emergencia locales para respuestas rápidas.
- En entornos urbanos, participar en redes de seguridad integradas con otras infraestructuras críticas.
- Esta guía busca establecer un marco de referencia que permita a los hospitales no solo cumplir con las exigencias normativas, sino también garantizar un entorno seguro y resiliente ante riesgos emergentes.

6 Referencias Bibliográficas

- Informe de agresiones a profesionales del sistema nacional de salud de 2024. Recuperado de [https:// www.sanidad.gob.es]
- Organización Mundial de la Salud (OMS). (2023). Seguridad del paciente: Una prioridad global.
- Real Decreto 393/2007. Norma Básica de Autoprotección.
- Real Decreto 513/2017. Reglamento de Instalaciones de Protección contra Incendios.
- Ley 5/2014 de Seguridad Privada y normativa asociada.
- Esquema Nacional de Seguridad. Ministerio de Asuntos Económicos y Transformación Digital.
- Reglamento (UE) 2016/679 (RGPD)
- Ley Orgánica 3/2018 (L.O.P.D.G.D.D.)
- Guías y Criterios de la AEPD (Agencia Española de Protección de Datos)

AEPD: Agencia Española de Protección de Datos, autoridad encargada de velar por el cumplimiento de la normativa sobre protección de datos personales.

CCTV: Circuito Cerrado de Televisión (Videovigilancia), sistema de cámaras para la supervisión y registro de actividades en áreas críticas.

CPD: Centro de Procesamiento de Datos, ubicación donde se concentran los recursos informáticos necesarios para el procesamiento de la información del hospital.

ENS: Esquema Nacional de Seguridad, marco normativo que establece las condiciones necesarias para garantizar la confianza en el uso de los medios electrónicos.

FQDN: Fully Qualified Domain Name (Nombre de Dominio Completamente Cualificado), dirección de internet completa que especifica la ubicación exacta de un servidor en la red.

IA: Inteligencia Artificial, tecnología que permite a los sistemas de seguridad realizar análisis avanzados, como la clasificación de personas y vehículos.

IoT: Internet of Things (Internet de las Cosas), red de objetos físicos con sensores y software que se conectan para intercambiar datos, como los sensores de temperatura o humedad.

NVR: Network Video Recorder (Grabador de Vídeo de Red), equipo encargado de gestionar y almacenar las grabaciones de las cámaras IP en formato rack.

ONVIF: Open Network Video Interface Forum, estándar global que garantiza la interoperabilidad entre productos de vídeo IP de distintos fabricantes.

PCI: Protección Contra Incendios, conjunto de medidas y sistemas destinados a prevenir, detectar y extinguir incendios en el recinto hospitalario.

RFID: Radio Frequency Identification (Identificación por Radiofrecuencia), tecnología de comunicación inalámbrica utilizada en tarjetas de acceso para restringir la entrada a áreas críticas.

RGPD: Reglamento General de Protección de Datos, normativa europea que regula el tratamiento de datos personales, especialmente sensible en el entorno sanitario.

VMS: Video Management System (Sistema de Gestión de Vídeo), plataforma de software que centraliza la visualización, grabación y análisis de todo el sistema de cámaras.

Guía elaborada por el Área de
Trabajo de Seguridad electrónica de:

AES
ASOCIACIÓN ESPAÑOLA
EMPRESAS DE SEGURIDAD

C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225
www.aesfundacion.es
patronato@aesfundacion.es

@FundacionAES AES Fundación aes_fundacion_