

Estándar de competencias profesionales

Implantar y mantener equipos y dispositivos en sistemas de control de accesos y presencia, y de videovigilancia

Familia Profesional	Electricidad y Electrónica
Nivel	3
Código	ECP1220_3
Estado	BOE
Publicación	RD 546/2023

Competencia profesional

Elementos de la competencia

EC1 Implementar el sistema de control de accesos y presencia y/o videovigilancia, verificando previamente arquitectura, infraestructura, componentes y ubicaciones, atendiendo a los procedimientos de la entidad responsable de la instalación y de acuerdo con los requisitos del proyecto y la normativa aplicable electrotécnica, sobre prevención de riesgos y de protección de datos.

IC1.1 La arquitectura y componentes del sistema a implementar se verifican, a partir del análisis de riesgos, comprobando sus características funcionales, elementos y zonas a proteger para asegurar la funcionalidad del sistema, proponiendo alternativas en su caso.

IC1.2 La infraestructura:

- cableado,
- cuadro o armario principal y secundarios o subcuadros,
- registros de conexiones,
- alimentaciones eléctricas

IC1.2 y los equipos de control, elementos de captación y de accionamiento:

- barreras,
- cerraderos eléctricos,

- portillones de paso,
- tornos y molinillos,
- cámaras de videovigilancia, entre otros, de los sistemas de control de accesos y presencia, se verifican antes del proceso de implantación, para garantizar la viabilidad de su instalación en las canalizaciones existentes y ubicaciones señaladas en la documentación del proyecto del sistema, proponiendo alternativas en caso de encontrar alguna incompatibilidad.

IC1.3 Los monitores de visualización de las imágenes procedentes de los elementos de captación se verifican, comprobando que su ubicación es acorde con la normativa de protección de datos y que los elementos y zonas a proteger se capten sin excluir áreas de interés.

IC1.4 La arquitectura y conexionado de los equipos de tratamiento de señales de videovigilancia tales como multiplexores, secuenciadores, matrices, videograbadores, 'videowall', entre otros se comprueba, verificando que se ajusta a lo definido en el proyecto.

IC1.5 Las operaciones a desarrollar se planifican de acuerdo con los recursos humanos y materiales disponibles, asignando tareas, optimizando el proceso de implementación de los sistemas, minimizando el impacto operativo de las actividades realizadas en el emplazamiento objeto de la instalación.

IC1.6 Los equipos y dispositivos que componen el sistema se configuran, efectuando ajustes tales como ángulo de visualización de cámaras y parámetros que establezca el fabricante, entre otros, para comprobar su funcionalidad y asegurar su funcionamiento, instalando carteles de aviso del sistema de grabación en las ubicaciones, de modo que sean visibles, conforme la normativa aplicable de protección de datos.

IC1.7 La pasarela de conexión externa ('gateway' o 'router'), en su caso, se configura para conectar las redes internas que componen el sistema con las redes públicas de datos, para acceder a los servicios que proporcionan y permitir el acceso al sistema desde el exterior, según las especificaciones del proyecto.

IC1.8 El inventario se recoge en un documento para su registro, almacenamiento y posterior tratamiento, anotando tipo de dispositivo, modelo, marca y número de serie de los componentes instalados, siguiendo el formato establecido por la entidad responsable de la instalación.

IC1.9 Las actividades realizadas se documentan en el parte de instalación, recogiendo los detalles de las actuaciones tales como fecha, horas, tipo de operación, datos del operario, entre otras, usando el formato que estipule la entidad responsable de la instalación.

EC2 Efectuar la puesta en servicio de los sistemas de control de accesos y presencia, instalando las aplicaciones de control y gestión, programando y parametrizando los terminales, siguiendo los requisitos y especificaciones de diseño del proyecto para obtener un sistema

funcional en condiciones de seguridad y cumpliendo la normativa aplicable de prevención de riesgos y de protección de datos.

IC2.1 Las aplicaciones de control y gestión de usuarios en los equipos informáticos se instalan, configurándolas de acuerdo con los perfiles de acceso, para garantizar la seguridad y fiabilidad de la información del sistema.

IC2.2 Los terminales de control de accesos y presencia de los usuarios y sus elementos biométricos se programan, parametrizándolos de acuerdo con los perfiles y niveles de acceso prescritos y las normas de control de accesos y presencia especificadas en el proyecto.

IC2.3 La aplicación 'software' que centraliza el control del sistema se instala, bien configurándola asignando permisos y parámetros tales como horarios, entre otros, bien ejecutando una carga inicial de los datos desde un archivo compatible, asegurando su integridad y verificando la funcionalidad del sistema de control de accesos y presencia.

IC2.4 La información registrada en el sistema se trata con herramientas de consulta y generación de informes, garantizando la seguridad en los accesos y usos de dicha información, de acuerdo con los planes de contingencias y seguridad de la entidad responsable de la instalación.

IC2.5 La generación de copias de seguridad de los controles y registros realizados se integra con el sistema, configurándola para su acceso en su caso, estableciendo el tipo y alcance de la copia y la periodicidad, entre otros, de acuerdo con los planes de seguridad y a la normativa aplicable sobre protección de datos.

IC2.6 El informe de puesta en servicio de los sistemas de control de accesos y presencia se documenta, recogiendo los parámetros de funcionalidad y configuración, así como los ajustes realizados y las modificaciones introducidas en su caso.

EC3 Efectuar la puesta en servicio del sistema de videovigilancia, instalando y configurando aplicaciones de control, gestión y planimetría, y grabación de la información, siguiendo los requisitos y especificaciones de diseño del proyecto para obtener un sistema funcional en condiciones de seguridad y cumpliendo la normativa aplicable de prevención de riesgos y de protección de datos.

IC3.1 Las aplicaciones de control, gestión y planimetría, se instalan en los equipos informáticos, configurándolas de acuerdo con las secuencias de visualización y la calidad de las imágenes requeridas, para garantizar la funcionalidad del sistema y la integración de sus elementos.

IC3.2 La aplicación 'software' para gestión de cámaras, proceso de grabación, planimetría y acceso remoto, entre otros, que centraliza el control del sistema de videovigilancia, se instala, configurándola con los parámetros prefijados y comprobando que es compatible con los

equipos que tiene que controlar, de acuerdo con los parámetros establecidos por el fabricante.

IC3.3 La información de imagen y/o sonido se registra, guardándola en un dispositivo de almacenamiento, garantizando la confidencialidad, asegurando la continuidad de la prestación de los servicios de visualización y grabación de imágenes de las zonas establecidas, según el plan de contingencia aplicable en la entidad responsable de la instalación para los sistemas de información.

IC3.4 La generación de copias de seguridad de las grabaciones realizadas se integra con el sistema, configurándola para su acceso en su caso, parametrizando el tipo y alcance de la copia y la periodicidad, entre otros, de acuerdo con los planes de seguridad y a la normativa aplicable sobre protección de datos.

IC3.5 El informe de puesta en servicio del sistema de videovigilancia se documenta, recogiendo los parámetros de funcionalidad y configuración, así como los ajustes realizados y las modificaciones introducidas en su caso.

EC4 Mantener los sistemas de control de accesos y presencia y de videovigilancia, previniendo, localizando, diagnosticando y solucionando las incidencias, conforme la documentación técnica del proyecto y el plan de mantenimiento y los procedimientos establecidos en la entidad responsable de la instalación para asegurar su funcionalidad.

IC4.1 Los procedimientos específicos de mantenimiento preventivo requeridos por los equipos y componentes que conforman los sistemas tales como calibrados, reajustes y limpieza entre otros se ejecutan, para garantizar la funcionalidad del sistema y la continuidad en la prestación del servicio, respetando la periodicidad de su aplicación.

IC4.2 El plan de mantenimiento se revisa, identificando deficiencias mediante análisis de riesgos y proponiendo, en su caso, la adaptación del sistema de control de acceso y presencia y de videovigilancia según el procedimiento establecido por la entidad responsable de la instalación.

IC4.3 Los componentes 'hardware' y 'software' de los sistemas de control de acceso y presencia y de videovigilancia se actualizan, descargando en su caso los parches y/o sustituyendo componentes, para añadir mejoras y corregir posibles fallos, comprobando las recomendaciones del fabricante.

IC4.4 Las averías de los sistemas de control de accesos y presencia y de videovigilancia se detectan, localizando el dispositivo afectado, averiguando la posible causa del fallo, consultando el histórico de incidencias y averías del equipo o sistema registrado en la entidad responsable de la instalación y apoyándose en la documentación técnica específica de los fabricantes de los equipos.

IC4.5 Los sistemas de control de accesos y presencia y de videovigilancia se reparan, aplicando las soluciones propuestas en la documentación técnica específica de los fabricantes de los equipos, respetando las normas de seguridad y los tiempos de respuesta indicados en el plan de mantenimiento, para evitar interrupciones en la prestación del servicio y minimizar el impacto operativo cuando se produzcan.

IC4.6 La aplicación de los procedimientos de mantenimiento, así como las intervenciones realizadas, se documentan en el histórico incidencias y averías, recogiendo los detalles de las actuaciones realizadas tales como fecha, horas, tipo de operación, datos del operario, entre otras, siguiendo el modelo que establezca la entidad responsable de la instalación para su registro, almacenamiento y posterior tratamiento.

Contexto profesional

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

Medios de producción

Equipos informáticos y periféricos. Sistemas de video híbrido y distribuidos. Monitores interactivos para aplicaciones de seguridad y videovigilancia y dispositivos móviles de acceso al sistema. Herramientas ofimáticas. Herramientas 'software' de planificación. Aplicaciones informáticas para la gestión de los sistemas de control de accesos y detección de presencia. Aplicaciones informáticas para la gestión de cámaras de videovigilancia y planimetría. Herramientas de análisis de video integrable con los controles de accesos y detección de presencia. Monitor de vídeo portátil, luxómetro. Equipos para control de accesos y presencia: cabezales lectores de tarjetas (banda magnética, proximidad, chip), lectores biométricos, centrales de control, actuadores (electrocerraderos, barreras), detectores de presencia. Equipos para sistemas de videovigilancia: cámaras analógicas, cámaras IP, ópticas para las cámaras, cabinas para las cámaras, posicionadores, teclados y centros de control, multiplexores, secuenciadores, grabadores de imagen analógicos y digitales, monitores, soportes de grabación y almacenamiento.

Información utilizada o generada

Normas externas de trabajo (normativa aplicable sobre prevención de riesgos laborales, normativa de protección de datos, propiedad intelectual e industrial, normativa aplicable de seguridad privada y de infraestructuras de comunicaciones). Normas internas de trabajo (documentación de proyectos y planes

de mantenimiento; análisis de riesgos; especificaciones técnicas de los proyectos de instalación; información sobre la configuración de red y direccionamiento IP; informes de puesta en marcha de los sistemas; partes de averías; parte de instalación; histórico incidencias y averías; informe de puesta en servicio; manuales de mantenimiento y protocolos de acceso a los datos almacenados -capturas de video e históricos de controles de acceso y presencia-. Documentación técnica (Documentación de los equipos y dispositivos de los fabricantes. Manuales de instalación y guías de usuario. Manuales de uso y funcionamiento de los equipos y dispositivos).