

DATOS IDENTIFICATIVOS DE LA UNIDAD FORMATIVA

| | | | |
|--|---|------------|-----|
| UNIDAD FORMATIVA | INSTALACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE CONTROL DE ACCESO Y PRESENCIA | Duración | 90 |
| | | Específica | |
| Código | UF1138 | | |
| Familia profesional | INFORMÁTICA Y COMUNICACIONES | | |
| Área Profesional | Sistemas y Telemática | | |
| Certificado de profesionalidad | Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia | Nivel | 3 |
| Módulo formativo | Implantación y mantenimiento de sistemas de control de accesos y presencia, y de videovigilancia | Duración | 220 |
| Resto de unidades formativas que completan el módulo | Instalación y puesta en marcha de un sistema de videovigilancia y seguridad | Duración | 90 |
| | Mantenimiento y gestión de incidencias en proyecto de videovigilancia, control de accesos, y presencia | | 40 |

Apartado A: REFERENTE DE COMPETENCIA

Esta unidad formativa se corresponde con la RP1 en lo referente a control de accesos y presencia y con la RP2 de la UC1220_3 IMPLANTAR Y MANTENER SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA.

Apartado B: ESPECIFICACIÓN DE LAS CAPACIDADES Y CONTENIDOS

Capacidades y criterios de evaluación

C1: Interpretar las especificaciones técnicas y funcionales de un proyecto de instalación de sistemas de control de accesos y presencia así como del análisis de riesgo identificando la información necesaria para llevar a cabo su implantación.

CE1.1 Describir las características y especificaciones técnicas del proyecto de instalación del sistema de control de accesos y presencia.

CE1.2 Explicar las características, funciones y elementos del análisis de riesgo para llevar a cabo la implantación y el mantenimiento de un sistema de control de accesos y presencia teniendo en cuenta las especificaciones técnicas del proyecto.

CE1.3 Describir las técnicas de planificación de proyectos necesarias para llevar a cabo la implantación del sistema: recursos humanos, plazos de entrega, costes establecidos y justificación de variaciones entre otros.

CE1.4 En un caso práctico, a partir de la documentación técnica que define el proyecto de instalación y mantenimiento de un sistema de control de accesos y presencia, debidamente caracterizado, identificar y describir:

- La ubicación de los equipos y dispositivos de los distintos subsistemas.
- Los medios y herramientas necesarios para aplicar los procesos de implementación.
- El sistema de distribución de energía, los elementos de protección y el sistema de alimentación ininterrumpida.
- Las envolventes, cuadros, armarios y elementos del cableado.
- El tipo de canalizaciones y su distribución en plantas, distribución horizontal y vertical.
- Las características de los cableados y conexionado de los elementos.
- Los sistemas de identificación y señalización de conductores y de los elementos de conexión de los equipos presentes en la instalación.
- Los equipos informáticos y periféricos utilizados para la administración del sistema.
- La aplicación informática de configuración, gestión y supervisión de los drivers debidamente actualizados.

C2: Identificar la infraestructura y verificar la instalación de los sistemas de control de accesos y presencia para su implantación, de acuerdo a especificaciones técnicas.

CE2.1 Identificar los equipos, dispositivos y elementos que componen la infraestructura de los sistemas de control de accesos y presencia así como las conexiones con otros sistemas o redes de comunicación.

CE2.2 Describir la interconexión entre los recintos de cableado y/o entre los edificios donde se encuentran los equipos del sistema de control de accesos y presencia.

CE2.3 Explicar técnicas de ajuste físico de los equipos, dispositivos y elementos que componen la infraestructura de los sistemas de control de accesos y presencia así como las conexiones con otros sistemas o redes de comunicación.

CE2.4 Explicar la necesidad de integrar el sistema de control de accesos y presencia.

CE2.5 En un caso práctico, debidamente caracterizado, verificar la instalación de los sistemas de control de accesos y presencia, y de videovigilancia, según especificaciones técnicas del proyecto:

- Identificar los equipos y dispositivos que componen los sistemas.

- Comprobar las conexiones eléctricas y de cableado entre equipos y dispositivos.
- Verificar el ajuste de los equipos y dispositivos de los sistemas.
- Documentar los trabajos realizados según formatos especificados.

C3: Poner en servicio los equipos y dispositivos del sistema de control de accesos y presencia, así como sus aplicaciones y configuraciones, teniendo en cuenta las especificaciones técnicas asociadas.

CE3.1 Describir las características y funcionalidades de los dispositivos y equipos que forman el sistema de control de accesos y presencia, identificando sus parámetros de configuración.

CE3.2 Identificar las funciones principales que realiza el sistema informático que se utiliza para la gestión y supervisión del sistema de control de accesos y presencia.

CE3.3 Explicar las características y funcionalidades de las aplicaciones software del sistema de control de accesos y presencia, tanto el software que centraliza el sistema como el software de control y gestión de usuarios, identificando sus parámetros de instalación y configuración.

CE3.4 Programar y parametrizar los terminales de control de accesos y presencia, y sus elementos biométricos, siguiendo prescripciones técnicas del proyecto.

CE3.5 Explicar los procesos de carga inicial del sistema de control de accesos y presencia.

CE3.6 Describir la funcionalidad de las herramientas de generación de copias de seguridad que se utilizan en los sistemas de control de accesos y presencia, identificando los parámetros de instalación y configuración.

CE3.7 Realizar consultas e informes de la información registrada en el sistema de control de accesos y presencia, utilizando herramientas específicas propias del sistema, teniendo en cuenta la legislación sobre protección de datos.

CE3.8 En un caso práctico, debidamente caracterizado, poner en servicio el sistema de control de accesos y presencia, de acuerdo a especificaciones técnicas del proyecto:

- Identificar los dispositivos y equipos del sistema.
- Configurar el sistema informático.
- Instalar las aplicaciones software de todo el sistema de control de accesos y presencia.
- Configurar los parámetros del sistema de control de accesos en las controladoras y terminales de control de accesos.
- Configurar los parámetros del sistema de control de accesos en los servidores.
- Configurar los parámetros del sistema de control de accesos en los portillones.
- Probar la funcionalidad del sistema.
- Elaborar el plan de documentación a través del diario de ingeniería.
- Elaborar el documento de seguridad teniendo en cuenta las normas marcadas por la LOPD.

CE3.9 Interpretar la documentación inherente a los equipos y dispositivos, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda.

Contenidos

1. Sistemas de control de acceso y presencia.

- o Definición de los sistemas de control de acceso y presencia. Características más importantes.
- o Valoración de las necesidades y razones para la integración de un sistema de control de accesos y presencia.
- o Identificación de los principales campos de aplicación mediante el estudio de casos reales.

2. Componentes y características de los sistemas y dispositivos que forman el control de acceso y presencia.

- o Sistemas mecánicos automatizados integrados en la gestión de accesos.
 - Electro cerraduras.
 - Puertas y Barreras .
 - Torniquetes y Tornos .
 - Rampas y Elevadores .
 - Sistemas diseñados para minusválidos.
 - Otros tipos de activaciones o eventos.
- o Dispositivos, Sistemas y tecnologías de identificación / autenticación.
 - Relojes de control y / o tarificación.
 - Teclados: Códigos y contraseñas de acceso.
 - Lectores de tarjeta.
 - o Códigos de barra.
 - o Banda Magnética.
 - Lectores de proximidad.
 - o Tarjetas o chips de proximidad. Tecnología RFID.
 - o Bluetooth.
 - o Otras.
 - Sensores Biométricos e Identidad biométrica; Como identificar a través de rasgos y factores únicos en cada persona.
 - o Lector de Huella digital.
 - o Lector de Palma o estructura de la mano.

- Reconocimiento Facial.
- Reconocimiento del Iris.
- Reconocimiento de retina.
- Sistemas de reconocimiento de voz.
- Dispositivos, Software y datos de control del sistema.
 - Hardware de control e integración de sistema
 - Conectividad y cableado. Infraestructura, funcionamiento y topología de los sistemas de control de acceso y presencia.
 - Punto de gestión y monitorización del sistema:
 - Configuración y parametrización del sistema.
 - Solución Hardware o Software.
 - Herramientas de extracción de informes.
 - Software de tratamiento de datos.
 - Bases de datos e información de control.

3. Funcionalidades y Aplicaciones de los sistemas de control de acceso y presencia.

- Control, monitorización y gestión de prioridades de acceso en instalaciones, identificación de las personas y datos relevantes que acceden, conocer el estado de los accesos y tener la posibilidad de gestionarlos.
- Control de horarios y eficiencia en empresas o procesos productivos.
- Tratamiento de datos:
 - Generación de estadísticas y datos de ocupación.
 - Tarifificación de servicios y tiempos.
- Sistemas de localización, control y detección de personas en un entorno cerrado; control de errantes no intrusivo.
- Sistemas de control médico, acceso a datos y posibilidad de actualización de información automatizado. (Aplicable o otros procesos similares).
- Gestión de alarmas y eventos.
 - Accesos no deseados.
 - Alertas no permitidos o fuera de horario.
 - Alarmas de averías o mal funcionamiento del sistema.
 - Interacción con otros sistemas y/o redes de comunicación o CRA (Centrales receptoras de alarmas).
- Soluciones de control logístico y de distribución.
- Soluciones de Gestión de Asistencia a Eventos.

4. Protección y seguridad del sistema y de los datos e información aportada por el sistema:

- Protección, mediante un sistema de alimentación ininterrumpida, de los dispositivos de toda la instalación de control de accesos y presencia.
- Copias de seguridad y sistemas de prevención de pérdidas de datos.
- Redundancia.
- Acceso protegido y gestión de privilegios en los sistemas de gestión y monitorización del sistema de control de accesos y presencia.
 - Copias seguridad actualizadas de la información de control del sistema. Accesos, zonas de vigilancia, Bases de datos, horarios, etc.

5. Proceso de acometida e implantación de un proyecto de control de accesos y presencia.

- Evaluación de las recomendaciones y puntos clave previos a acometer un proyecto de control de accesos y presencia.
 - Restricciones de los sistemas y de su funcionalidad.
 - Problemática del medio de comunicación (número máximo de dispositivos, distancias, interferencias, atenuaciones, etc.).
 - Problemática debida al medio y la localización del sistema (entorno).
 - Protecciones de los aparatos (lps).
 - Factor Humano.
- Evaluación de los niveles de riesgo y tipos de amenazas.
- Evaluación de las necesidades y definición del servicio y funcionalidades a implantar.
- Interpretación y evaluación del proyecto y la infraestructura necesaria para acometerlo.
- Estimación de tiempos de ejecución, recursos y personal necesario.
- Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas).
- Análisis de la situación: ¿Qué accesos hay que controlar?
- Planteamiento y planificación: ¿Cómo y cuándo se controlan? ¿Desde dónde controlar y gestionar el sistema?
- Estructuración del sistema y búsqueda de la ubicación óptima de los dispositivos.
- Planteamiento de las funcionalidades del sistema.
- Integración con otros sistemas y redes: Reacciones y posibilidades ante una detección o evento.
- Comprobación el cumplimiento de la normativa y reglamentación sobre seguridad privada y Ley Orgánica de Protección de Datos.

- Configuración del sistema y puesta en marcha tanto del software como del hardware, según las especificaciones y funcionalidades requeridas.
- Documentación generada o utilizada en el proceso:
 - Procesada:
 - Proyecto: memoria, planos, pliego de condiciones y requisitos necesarios.
 - Proyecto de las instalaciones a controlar.
 - Normativa técnica.
 - Normativa legal aplicada.
 - Generada.
 - Informe de puesta en marcha.
 - Libro de Seguimiento e incidencias.
 - Reflejo fiel del estado final de la instalación.
 - Informe de Configuración del sistema.
 - Informe de seguridad acorde con la LOPD.

6. Simulación del desarrollo de un proyecto de control de accesos y presencia siguiendo las pautas que se indiquen.

- Observación del proyecto de forma global: sistemas que involucra, dispositivos a instalar, espacios reservados, infraestructura, canalizaciones y conectividad de los elementos para hacerse a la idea del alcance del mismo.
- Realización de un estudio previo de las necesidades, características y funcionalidades del proyecto a implantar. Comprobación que el sistema nos aporta todo lo que necesitamos.
- Análisis de la solución propuesta e instalación física de los dispositivos y la totalidad de sus conexiones, tanto con el sistema de control de accesos como con el resto de sistemas involucrados.
- Parametrización y ajuste del sistema de control de accesos.
- Comprobación de que el sistema funcione según exigencias del proyecto, y en caso contrario, aplicación de los métodos de detección y corrección de errores, para posteriormente volver a comprobar el sistema.
- Realización del informe de la puesta en marcha y la documentación necesaria.

Apartado C: REQUISITOS Y CONDICIONES

Deberá cumplir alguno de los requisitos siguientes:

- Estar en posesión del título de Bachiller.
- Estar en posesión de algún certificado de profesionalidad de nivel 3.
- Estar en posesión de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional.
- Cumplir el requisito académico de acceso a los ciclos formativos de grado superior o haber superado las correspondientes pruebas de acceso a ciclos de grado superior.
- Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
- Tener, de acuerdo con la normativa que se establezca, los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.

En relación con las exigencias de los formadores o de las formadoras, instalaciones y equipamientos se atenderá las exigencias solicitadas para el propio certificado de profesionalidad: Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia.