CUALIFICACIÓN PROFESIONAL:
Implantación y gestión de elementos informáticos en sistemas domóticos-inmóticos, de control de accesos y presencia, y de videovigilancia

Familia Profesional:	***Informática y Comunicaciones***
Nivel:	***3***
Código:	***IFC365_3***
Estado:	***59{/!¢![hD!5!***
{dzLJNXYˆlŘI·:	***w5 рпскнлно***

Competencia general

Integrar y mantener elementos informáticos y de comunicaciones en sistemas de automatización de edificios domóticos e inmóticos, de control de accesos y presencia y de videovigilancia a nivel de hardware y software, asegurando el funcionamiento de los distintos módulos que los componen, en condiciones de calidad y seguridad, cumpliendo la normativa y reglamentación aplicables.

Unidades de competencia

UC0490_3: GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO
UC1219_3: Implantar y mantener sistemas domóticos/inmóticos
UC1220_3: Implantar y mantener sistemas de control de accesos y presencia, y de videovigilancia

Entorno Profesional

Ámbito Profesional

Desarrolla su actividad profesional en el área de soporte informático dedicado al diseño, implementación y mantenimiento de sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia, en entidades de naturaleza pública o privada, empresas de tamaño pequeño/mediano/grande o microempresas, tanto por cuenta propia como ajena, con independencia de su forma jurídica. Desarrolla su actividad dependiendo, en su caso, funcional y/o jerárquicamente, de un superior. Puede tener personal a su cargo en ocasiones, por temporadas o de forma estable. En el desarrollo de la actividad profesional se aplican los principios de accesibilidad universal de acuerdo con la normativa aplicable.

Sectores Productivos

Se ubica sobre todo en el sector servicios, en el subsector de provisión y mantenimiento de servicios relacionados con la automatización de viviendas, edificios y seguridad privada, relativos a la implementación y mantenimiento de sistemas de control de accesos y presencia y de videovigilancia.

Ocupaciones y puestos de trabajo relevantes

Los términos de la siguiente relación de ocupaciones y puestos de trabajo se utilizan con carácter genérico y omnicomprensivo de mujeres y hombres.

- Integradores de elementos informáticos en sistemas domóticos/inmóticos
- Integradores de elementos informáticos en sistemas de control de accesos y presencia, y en sistemas de videovigilancia

- Expertos en mantenimiento de elementos informáticos en sistemas de control de accesos y presencia y en sistemas de videovigilancia

Formación Asociada (510 horas)

Módulos Formativos

MF0490_3: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO (90 horas)

MF1219_3: Implantación y mantenimiento de sistemas domóticos/inmóticos (150 horas)

MF1220_3: Implantación y mantenimiento de sistemas de control de accesos y presencia, y de videovigilancia (270 horas)

UNIDAD DE COMPETENCIA 1
GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel: *3*
Código: *UC0490_3*
Estado: *BOE*

Realizaciones profesionales y criterios de realización

RP1: Gestionar la configuración del sistema para asegurar el rendimiento de los procesos según las necesidades de uso, considerando despliegues en arquitecturas dedicadas o distribuidas, con y sin virtualización y cumpliendo las directivas de la organización.

CR1.1 Los procesos que intervienen en el sistema se identifican de forma que permitan evaluar parámetros de rendimiento, diferenciando los procesos que se encuentran repartidos en diferentes nodos, (si la arquitectura es distribuida) y/o si están asociados al software de gestión de la virtualización, al hipervisor de los host físicos o a los propios servicios virtualizados (si se trata de un modelo virtualizado).

CR1.2 Los parámetros que afectan a los componentes del sistema: memoria, procesador y periféricos, entre otros, se ajustan a las necesidades de uso asignándoles la configuración que maximice el rendimiento.

CR1.3 Las prioridades de ejecución de los procesos se adecuan en función de las especificaciones del plan de explotación de la organización (tipo de proceso, usuario, perfil, entre otros).

CR1.4 Las herramientas de monitorización se implantan, configurándolas y determinando los niveles de las alarmas.

CR1.5 La conectividad y el ancho de banda que se necesita en arquitecturas distribuidas, se proporcionan según las especificaciones y/o manuales de fabricantes y de la organización.

CR1.6 La distribución de la información en arquitecturas distribuidas se gestiona, siguiendo las especificaciones y/o manuales de fabricantes y de la organización, para maximizar el rendimiento del sistema.

CR1.7 El software de gestión de virtualización y el hipervisor, de los hosts físicos y los propios servicios virtualizados, en el caso de despliegues virtualizados, se gestiona, revisando la configuración y monitorizando el rendimiento, siguiendo las especificaciones y/o manuales de fabricantes y de la organización, y maximizando el rendimiento del sistema.

RP2: Administrar el almacenamiento según las necesidades de uso, considerando despliegues en arquitecturas dedicadas o distribuidas, con y sin virtualización y cumpliendo las directivas de la organización.

CR2.1 Los dispositivos de almacenamiento se configuran para ser usados, asignando los parámetros propios del sistema operativo utilizado en el sistema informático.

CR2.2 El almacenamiento se configura, teniendo en cuenta la posible necesidad de arquitecturas distribuidas que requieran distribución de la información, así como la necesidad de entornos virtualizados que requieren software de gestión de virtualización, hipervisores y los propios servicios virtualizados.

CR2.3 La estructura de almacenamiento se define, implantándose, atendiendo a las necesidades de los sistemas de archivos y a las especificaciones de uso de la organización.

CR2.4 Los requerimientos de nomenclatura de objetos y restricciones de uso del almacenamiento se documentan, siguiendo el formato (tipo de documento, tamaño, maquetación, tipografía, entre otros) y otras indicaciones establecidas por la organización.

CR2.5 El almacenamiento se integra para ofrecer un sistema funcional al usuario, siguiendo las especificaciones de la organización, con independencia del tipo de arquitectura (distribuida o dedicada) y de la existencia o no de capa de virtualización.

RP3: Gestionar las tareas de usuarios para garantizar los accesos al sistema y la disponibilidad de los recursos según especificaciones de explotación del sistema informático.

CR3.1 El acceso de los usuarios al sistema informático se configura, asignando métodos de autenticación y perfiles, entre otros, para garantizar la seguridad e integridad del sistema.

CR3.2 El acceso de los usuarios a los recursos se administra mediante la asignación de permisos en función de las necesidades de la organización.

CR3.3 Los recursos disponibles (dispositivos, espacio, número de conexiones, caudal/ancho de banda, entre otros) para los usuarios se limitan, usando las herramientas instaladas en el sistema, en base a lo especificado en las normas de uso de la organización.

RP4: Gestionar los servicios de red para asegurar la comunicación entre sistemas informáticos según necesidades de explotación.

CR4.1 Los servicios de comunicación se establecen con un sistema de calidad de servicio, garantizándose las comunicaciones de los mismos.

CR4.2 Los dispositivos de comunicaciones se verifican en lo que respecta a su configuración y rendimiento, siguiendo las especificaciones de la organización.

CR4.3 Los consumos de recursos de los servicios de comunicaciones se analizan, verificando que se encuentran dentro de los límites permitidos por las especificaciones.

CR4.4 Las incidencias detectadas en los servicios de comunicaciones se documentan para informar a los responsables de la explotación del sistema y de la gestión de las mismas según los protocolos de la organización indicando, entre otros, el momento, la descripción y la solución aplicadas al problema.

Contexto profesional

Medios de producción

Sistemas operativos. Herramientas de administración de usuarios y gestión de permisos a recursos. Herramientas de control de rendimiento. Herramientas de monitorización de procesos. Herramientas de monitorización de uso de memoria. Herramientas de monitorización de gestión de dispositivos de almacenamiento. Herramientas de gestión de usuarios.

Productos y resultados

Dispositivos de almacenamiento configurados y estructurados. Sistema configurado y operando. Rendimiento del sistema según los parámetros de explotación. Usuarios gestionados. Sistema seguro e íntegro en el acceso y utilización de servicios y recursos. Servicios de comunicaciones en funcionamiento.

Información utilizada o generada

Normas externas de trabajo (normativa aplicable de protección de datos y publicación de la información). Normas internas de trabajo (plan de explotación de la organización; gráficas y análisis de rendimiento; listados de acceso y restricciones de usuarios; informe de incidencias; protocolo de actuación ante incidencias). Documentaciones técnicas (manuales de explotación del sistema operativo y de los dispositivos; manuales de las herramientas de monitorización utilizadas).

UNIDAD DE COMPETENCIA 2

Implantar y mantener sistemas domóticos/inmóticos

Nivel: *3*
Código: *UC1219_3*
Estado: *BOE*

Realizaciones profesionales y criterios de realización

RP1: Configurar los equipos y dispositivos para la puesta en servicio del sistema domótico/inmótico cumpliendo los requisitos funcionales del proyecto.

CR1.1 Las especificaciones recogidas en el proyecto de instalación y/o de integración del sistema domótico/inmótico a implantar se interpretan con objeto de identificar la arquitectura, componentes y tecnologías que intervienen en el sistema.

CR1.2 La ubicación e instalación de los equipos, dispositivos e infraestructura se revisa, comprobando que garantiza la configuración, programación y puesta en marcha del sistema domótico/inmótico, de acuerdo con los requisitos funcionales del proyecto.

CR1.3 La configuración y parametrización física y lógica de los equipos y dispositivos que forman el sistema domótico/inmótico se planifica y se realiza, para su puesta en servicio, cumpliendo los requisitos funcionales fijados por el proyecto y según los procedimientos establecidos por la organización.

CR1.4 La pasarela residencial, en su caso, se configura para conectar las distintas redes internas que componen el sistema domótico/inmótico 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.

CR1.5 El sistema domótico/inmótico se pone en marcha, siguiendo el protocolo de pruebas establecido por la organización y de acuerdo con las especificaciones funcionales del proyecto.

CR1.6 El informe de puesta en marcha del sistema domótico/inmótico se elabora, incluyendo la configuración de los equipos, de los dispositivos y las pruebas de puesta en marcha realizadas, con objeto de registrar la información para su uso posterior, según normas de la organización.

RP2: Elaborar los inventarios de los equipos, dispositivos y del software que componen el sistema domótico/inmótico, para garantizar su identificación y localización, aplicando las normas establecidas por la organización.

CR2.1 El inventario de componentes hardware y aplicaciones software se elabora para registrar las características, localización y estado de los mismos, según las normas de la organización.

CR2.2 Las configuraciones de los equipos y aplicaciones del sistema domótico/inmótico se registran en el inventario, según procedimiento establecido por la organización, para facilitar las labores de recuperación en caso de fallos.

CR2.3 El inventario se mantiene actualizado registrando todos los cambios producidos en el sistema domótico/inmótico, tanto a nivel de hardware, como de software y de configuración, según procedimiento establecido por la organización.

CR2.4 Los manuales técnicos de los dispositivos y equipos del sistema domótico/inmótico se registran y se referencian en la documentación generada, para su uso posterior, según el procedimiento establecido por la organización.

RP3: Adaptar el software de control a los cambios de funcionalidades del sistema domótico/inmótico de acuerdo con especificaciones técnicas y necesidades.

CR3.1 La configuración y parametrización del software de control del sistema se planifica y se realiza para su puesta en funcionamiento, de acuerdo con los requisitos funcionales fijados por el proyecto, los protocolos de configuración establecidos por los elementos software del sistema domótico/inmótico y los procedimientos establecidos por la organización.

CR3.2 La ubicación e instalación de los equipos de monitorización y control del sistema se revisa, comprobando que garantiza la configuración, programación y puesta en marcha del sistema domótico/inmótico, de acuerdo con los requisitos funcionales del proyecto.

CR3.3 Las funcionalidades del software de control se programan teniendo en cuenta las distintas técnicas y lenguajes de desarrollo y estándares de referencia de sistemas de control domótico/inmótico, utilizando las herramientas proporcionadas por el sistema, según especificaciones técnicas y necesidades de uso.

CR3.4 La pasarela residencial, en su caso, se configura implementando nuevos servicios y aplicaciones, utilizando estándares software de desarrollo de estos servicios, según necesidades especificadas.

CR3.5 Las pruebas de puesta en marcha de las funcionalidades de visualización y control del sistema, se realizan para verificar que cumplen las especificaciones del proyecto, siguiendo el protocolo establecido por la organización.

CR3.6 El informe de puesta en marcha de la aplicación de monitorización y control se elabora, incluyendo las actividades realizadas y las incidencias detectadas, para su uso posterior, siguiendo las normas establecidas por la organización.

RP4: Mantener el sistema domótico/inmótico tanto a nivel hardware como software para garantizar su funcionamiento, de acuerdo con requisitos funcionales y criterios de calidad establecidos en el proyecto.

CR4.1 Los procedimientos específicos de mantenimiento de los equipos y dispositivos que componen el sistema domótico/inmótico se definen para garantizar su funcionalidad, teniendo en cuenta las especificaciones técnicas de los mismos.

CR4.2 El plan de mantenimiento preventivo del sistema domótico/inmótico se elabora para garantizar la continuidad en la prestación del servicio, de acuerdo con los procedimientos específicos requeridos por los componentes del sistema, y por la organización.

CR4.3 La localización de averías y reparación o sustitución de los componentes hardware y software del sistema informático que soporta el sistema domótico/inmótico se realiza para mantenerlo operativo, utilizando herramientas específicas, aplicando los procedimientos normalizados y cumpliendo las normas de seguridad establecidas por la organización.

CR4.4 El manual de identificación y resolución de incidencias del sistema domótico/inmótico se elabora y se actualiza cada vez que se detecte una incidencia nueva, indicando la información más relevante respecto a la misma, de acuerdo con los procedimientos específicos requeridos por los componentes del sistema, indicando tareas, tiempos y resultados previstos.

Contexto profesional

Medios de producción

Equipos informáticos, dispositivos móviles y periféricos. Aplicaciones informáticas propietarias para configuración de sistemas domóticos. Bases de datos software de elementos hardware. Aplicaciones informáticas para diseño 2D y 3D. Aplicaciones informáticas para la gestión del mantenimiento. Pasarelas residenciales para sistemas domóticos. Instrumentos de medida: polímetro, cronómetro,

luxómetro, entre otras. Estándares de referencia para desarrollo de sistemas domóticos/inmóticos. Equipos y dispositivos de sistemas domóticos/inmóticos. Software de control de sistemas domóticos/inmóticos. Telemandos para el control local de instalaciones domóticas inalámbricas (teléfonos inteligentes o tabletas).

Productos y resultados

Configuración y puesta en marcha del sistema inmótico/domótico. Mantenimiento preventivo y correctivo de los componentes hardware y software del sistema domótico/inmótico.

Información utilizada o generada

Proyecto de ingeniería del sistema domótico/inmótico. Documentación técnica, manuales de instalación y uso de elementos hardware y las aplicaciones software del sistema domótico/inmótico. Documentación de instalación eléctrica de los elementos hardware del sistema domótico/inmótico. Reglamentos aplicables en materia de baja tensión y de infraestructuras de comunicaciones. Pliegos de especificaciones del sistema domótico/inmótico. Planificación de la configuración y parametrización del sistema domótico/inmótico. Documentación de la topología, configuración de los elementos (parámetros, valores, direcciones IP, direcciones físicas) del sistema domótico/inmótico. Documento de procedimiento de pruebas de puesta en marcha del sistema domótico/inmótico. Acta de puesta en marcha y entrega del sistema. Documento de procedimiento de acciones de mantenimiento del sistema domótico/inmótico. Informes/actas/partes de mantenimiento preventivo y correctivo del sistema domótico/inmótico. Manual de usuario de funcionamiento del sistema domótico: hardware y software de control del sistema domótico/inmótico.

UNIDAD DE COMPETENCIA 3

Implantar y mantener sistemas de control de accesos y presencia, y de videovigilancia

Nivel: *3*
Código: *UC1220_3*
Estado: *BOE*

Realizaciones profesionales y criterios de realización

RP1: Implementar el sistema de control de accesos y presencia y videovigilancia para atender a los requerimientos de la organización de acuerdo con las especificaciones técnicas del proyecto.

CR1.1 La arquitectura y componentes del sistema a implantar se determinan, a partir del análisis de riesgo y las especificaciones recogidas en el proyecto de instalación del sistema de control de accesos y presencia, y videovigilancia a implementar.

CR1.2 Las operaciones a desarrollar se planifican de acuerdo con los recursos humanos y materiales disponibles, optimizando el proceso de implementación de los sistemas, teniendo en cuenta el marco de la normativa aplicable y las especificaciones del diseño.

CR1.3 La infraestructura (cableado, armarios de conexiones, alimentaciones eléctricas) y los equipos de control, los elementos de captación y de accionamiento (barreras, cerraderos eléctricos, portillones de paso, tornos y molinillos, entre otros) de los sistemas de control de accesos y presencia, se verifican a lo largo del proceso de implantación para garantizar su integración y funcionalidad, siguiendo especificaciones descritas en la documentación del proyecto del sistema.

CR1.4 La infraestructura (cableados, armarios de conexiones, alimentaciones eléctricas), las características y ubicación de las cabinas de los elementos de captación de imagen (cámaras y domos, entre otros), de los detectores de presencia, de los equipos de tratamiento de señales(multiplexores, secuenciadores, matrices, videograbadores, videowall y teclados, entre otros) y dispositivos de visualización (monitores) de los sistemas de videovigilancia, se verifican a lo largo del proceso de montaje en lo que respecta a características funcionales, elementos y zonas a proteger para asegurar la funcionalidad del sistema, siguiendo las especificaciones de proyecto del sistema.

CR1.5 Los equipos y dispositivos instalados que componen el sistema de control de accesos y presencia se ajustan y configuran, para probar su funcionalidad y asegurar su funcionamiento, de acuerdo con especificaciones técnicas de proyecto del sistema.

CR1.6 Los equipos y dispositivos instalados, así como los elementos motorizados del sistema de videovigilancia se ajustan y configuran, para garantizar la integración de los mismos y la consecución de los objetivos del sistema, de acuerdo con las características funcionales y técnicas prescritas en la documentación técnica y de diseño.

CR1.7 Las actividades realizadas se documentan en formato normalizado para su uso posterior, siguiendo el procedimiento establecido por la organización.

RP2: Efectuar la puesta en servicio de los sistemas de control de accesos y presencia en la organización, siguiendo los requisitos y especificaciones de diseño del proyecto.

CR2.1 Los equipos informáticos y periféricos asociados se configuran físicamente, y se instalan y configuran las aplicaciones de control y gestión de usuarios de acuerdo con los perfiles de acceso establecidos en las especificaciones del diseño, para garantizar la seguridad y fiabilidad de la información del sistema, teniendo en cuenta las especificaciones de la organización y la normativa aplicable.

CR2.2 Los terminales de control de accesos y presencia de los usuarios y sus elementos biométricos se programan y parametrizan para cumplimentar las normas de control de accesos y presencia, de acuerdo con los perfiles y niveles de acceso prescritos en las especificaciones del proyecto del sistema.

CR2.3 La aplicación software que centraliza el control del sistema se instala y configura, y se verifica que es compatible con los equipos que tiene que controlar, para ratificar la funcionalidad del sistema de control de accesos y presencia, de acuerdo con los parámetros prefijados en las especificaciones de diseño.

CR2.4 La carga inicial de los datos del sistema de control de accesos y presencia se realiza y verifica para asegurar su integridad y el cumplimiento de la normativa aplicable sobre protección de datos, según la política de seguridad de la organización.

CR2.5 La información registrada en el sistema se trata con herramientas de consulta y generación de informes para una distribución de la misma, garantizando la continuidad de la prestación de los servicios y la seguridad en los accesos y usos de dicha información, cumpliendo las normas de protección de datos y de acuerdo con los planes de contingencias y seguridad de la organización.

CR2.6 La herramienta de generación de copias de seguridad de los controles y registros realizados se integra con el sistema y se configura para que los usuarios tengan acceso, de acuerdo con los planes de seguridad y a la normativa aplicable sobre protección de datos.

CR2.7 El informe de puesta en servicio de los sistemas de control de accesos y presencia se confecciona para que recoja con precisión los parámetros de funcionalidad, de acuerdo con lo establecido en la documentación del sistema, así como los ajustes realizados y las modificaciones que se sugieren para el análisis de riesgo.

RP3: Efectuar la puesta en servicio del sistema de videovigilancia en la organización, siguiendo los requisitos y especificaciones de diseño del proyecto.

CR3.1 Los equipos informáticos y periféricos asociados se configuran físicamente, se instalan y configuran las aplicaciones de control, gestión y planimetría, de acuerdo con las secuencias de visualización y la calidad de las imágenes requeridas establecidas en las especificaciones, para garantizar la funcionalidad del sistema y la integración de sus elementos.

CR3.2 La aplicación software (gestión de cámaras, proceso de grabación, planimetría, acceso remoto) que centraliza el control del sistema de videovigilancia se instala, configura y verifica para comprobar que cumple los parámetros prefijados y es compatible con los equipos que tiene que controlar, de acuerdo con especificaciones técnicas.

CR3.3 La información registrada y grabada se trata con parámetros de confidencialidad, para garantizar la continuidad de la prestación de los servicios de visualización y grabación de imágenes de las zonas establecidas, según el plan de contingencia vigente en la organización para los sistemas de información y teniendo en cuenta la normativa aplicable sobre protección de datos.

CR3.4 La herramienta de generación de copias de seguridad de las grabaciones realizadas se integra con el sistema y se configura, para que los usuarios tengan acceso al sistema, de acuerdo con los planes de seguridad y cumpliendo la normativa aplicable sobre protección de datos.

CR3.5 El informe de puesta en servicio del sistema de videovigilancia se confecciona para que recoja con precisión los parámetros de funcionalidad de acuerdo con lo establecido en la documentación del sistema, así como los ajustes realizados y las modificaciones que se sugieren para el análisis de riesgo.

RP4: Mantener los sistemas de control de accesos y presencia y de videovigilancia, siguiendo la documentación técnica del proyecto para asegurar su funcionalidad.

CR4.1 El plan de mantenimiento preventivo se interpreta para garantizar la continuidad en la prestación del servicio, de acuerdo con los procedimientos específicos requeridos por los componentes del sistema, indicando claramente la periodicidad de su aplicación.

CR4.2 Los procedimientos específicos de mantenimiento preventivo de los sistemas de control de acceso y presencia se ejecutan, para garantizar la funcionalidad óptima de los mismos, según lo indicado en el plan de mantenimiento.

CR4.3 Los procedimientos específicos de mantenimiento preventivo de los sistemas de videovigilancia se ejecutan, de acuerdo con los equipos y dispositivos que conforman las distintas partes del sistema, para garantizar la continuidad en la prestación del servicio y la funcionalidad de cada uno de los componentes, según lo indicado en las especificaciones funcionales y el plan de mantenimiento.

CR4.4 Los procedimientos específicos de mantenimiento se revisan periódicamente para adaptar el sistema a los cambios incluidos en el análisis de riesgo, detectar deficiencias y proponer mejoras de seguridad, siguiendo las indicaciones de los fabricantes y normativa de la organización.

CR4.5 La localización de averías y reparación de los sistemas de control de accesos y presencia y de videovigilancia se realiza aplicando sistemáticamente los procedimientos normalizados por la organización, respetando las normas de seguridad y los tiempos establecidos, para evitar interrupciones en la prestación del servicio y minimizar el impacto de éstas cuando se produzcan.

CR4.6 Las actualizaciones de los componentes hardware y software de los sistemas de control de acceso y presencia y de videovigilancia, se realizan para añadir mejoras y corregir posibles fallos, teniendo en cuenta las especificaciones técnicas de los fabricantes y normativa de la organización.

CR4.7 El plan de mantenimiento preventivo de los sistemas de control de accesos y presencia y de videovigilancia, se actualiza para recoger con precisión los resultados obtenidos en la aplicación del plan de mantenimiento preventivo, así como las intervenciones realizadas frente a disfunciones y averías del sistema, de acuerdo a los planes de contingencias de la organización.

CR4.8 La documentación generada en la aplicación de los procedimientos de mantenimiento se recoge en los registros normalizados para su almacenamiento y posterior tratamiento y distribución, siguiendo el protocolo establecido por la organización.

Contexto profesional

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. Instrumentos de medida: polímetro, téster de cableado coaxial y par trenzado, certificador de cableado, 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.

Productos y resultados

Planificación, ejecución y seguimiento de la implementación de los sistemas de control de accesos y presencia y de videovigilancia. Definición de los sistemas de videovigilancia para entornos de seguridad avanzados basados en sistemas abiertos (analógico e IP) integrados con los datos generados en el control de acceso, presencia, y en su caso, controles de procesos industriales con video para seguridad física, calidad, trazabilidad y productividad. Verificación y puesta en marcha de los sistemas de control de accesos y presencia y de videovigilancia. Procedimientos de intervención preventiva y correctiva requeridos para el mantenimiento de los sistemas de control de accesos y presencia y de videovigilancia. Mantenimiento preventivo de los sistemas de control de accesos y presencia y de videovigilancia. Reparación de averías en los sistemas de control de accesos y presencia y de videovigilancia.

Información utilizada o generada

Análisis de riesgo. Especificaciones técnicas de los proyectos de instalación. Documentación técnica de los equipos y dispositivos y recomendaciones de los fabricantes, en soporte impreso o electrónico. Manuales de instalación y guías de usuario. Reglamentación sobre seguridad privada. Manuales de uso y funcionamiento de los equipos y dispositivos. Manuales del software asociado. Información sobre la configuración de red y direccionamiento IP. Informes de puesta en marcha de los sistemas. Partes de servicio e intervención para el mantenimiento de los sistemas. Normativa aplicable sobre protección de datos y seguridad privada. Manuales de mantenimiento y protocolos de acceso a los datos almacenados (capturas de video e históricos de controles de acceso y presencia).

MÓDULO FORMATIVO 1

GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel:	*3*
Código:	*MF0490_3*
Asociado a la UC:	*UC0490_3 - GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO*
Duración (horas):	*90*
Estado:	*BOE*

Capacidades y criterios de evaluación

C1: Analizar procesos del sistema, asegurando un rendimiento acorde a los parámetros especificados en el plan de explotación considerando despliegues en arquitecturas dedicadas o distribuidas, con y sin capa de virtualización.

CE1.1 Identificar procesos del sistema, analizando los parámetros que los caracterizan (procesos padre, estado del proceso, consumo de recursos, prioridades y usuarios afectados entre otros) para determinar su influencia en el rendimiento del sistema.

CE1.2 Describir cada una de las herramientas provistas por el sistema para la gestión de procesos, con objeto de permitir la intervención en el rendimiento general del sistema explicando sus características y funciones.

CE1.3 Explicar técnicas de monitorización y herramientas destinadas a evaluar el rendimiento del sistema, indicando qué parámetros se miden y qué funciones se controlan.

CE1.4 En un supuesto práctico de análisis del rendimiento de un sistema informático con una carga de procesos concreta:

- Utilizar herramientas del sistema, monitorizando sus parámetros para identificar cuantos procesos activos existen y las características particulares de alguno de ellos.
- Realizar operaciones de activación, desactivación y modificación de prioridad entre otras con un proceso, utilizando las herramientas del sistema.
- Monitorizar el rendimiento del sistema, mediante herramientas específicas y definir alarmas, que indiquen situaciones de riesgo.

C2: Aplicar procedimientos de administración del almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, confidencial y disponible.

CE2.1 Identificar sistemas de archivo utilizables en un dispositivo de almacenamiento dado, para optimizar los procesos de registro y acceso a los mismos.

CE2.2 Explicar las características de un sistema de archivo, en función de la arquitectura hardware (dedicada o distribuida), los dispositivos de almacenamiento y sistemas operativos empleados.

CE2.3 Describir la estructura general de almacenamiento asociando, para cada nodo o sistema informático final, los dispositivos con los sistemas de archivos existentes.

CE2.4 Describir la distribución del almacenamiento en nodos, dispositivos y sistemas de archivo, comprobando que se garantice la funcionalidad y el rendimiento del conjunto.

CE2.5 En un supuesto práctico de aplicación de procedimientos de administración de almacenamiento de la información con varios dispositivos:

- Particionar los dispositivos, en los casos que se requiera distribuir la información de manera separada, generando la infraestructura de los sistemas de archivo a instalar.
- Distribuir la información en diferentes nodos, integrándolos en un sistema de almacenamiento común, garantizando las comunicaciones y el rendimiento cuando la distribución del almacenamiento sea un requisito de implementación.
- Implementar la estructura general de almacenamiento, integrando todos los nodos, dispositivos y sus correspondientes sistemas de archivos.
- Documentar los requerimientos y restricciones de cada sistema de archivos implantado, indicando la restricción o el requerimiento y el tipo de dispositivo afectado.
- Aplicar los puntos anteriores sobre sistemas virtualizados.

C3: Administrar accesos al sistema y a los recursos para asegurarlos, restringiendo su uso en función del perfil de acceso.

CE3.1 Identificar posibilidades de acceso al sistema, distinguiendo los accesos remotos de los accesos locales.

CE3.2 Describir herramientas que se utilizan en la gestión de permisos a usuarios para el uso de los recursos del sistema.

CE3.3 En un supuesto práctico de administración del acceso al sistema en el que se cuenta con derecho de administración de usuarios:
- Identificar los posibles accesos de un usuario al sistema, monitorizando mediante visionado de log o usando herramienta software.
- Modificar los permisos de utilización de un recurso del sistema a un usuario, estableciendo otros que se hayan solicitado.
- Definir limitaciones de uso de un recurso del sistema a los usuarios, verificando dicha limitación simulando el acceso.

C4: Evaluar el uso y rendimiento de los servicios de comunicaciones para mantenerlos dentro de los parámetros especificados.

CE4.1 Explicar parámetros de configuración y funcionamiento de los dispositivos de comunicaciones, indicando los servicios afectados por cada uno para asegurar su funcionalidad dentro del sistema.

CE4.2 Relacionar servicios de comunicaciones activos en el sistema con los dispositivos utilizados por ellos, analizando y evaluando el rendimiento.

CE4.3 En un supuesto práctico de evaluación de uso y rendimiento de un sistema informático conectado con el exterior por medio de varias líneas de comunicaciones:
- Identificar los dispositivos de comunicaciones, describiendo sus características.
- Verificar el estado de los servicios de comunicaciones, comprobando su funcionalidad.
- Evaluar el rendimiento de los servicios de comunicaciones, midiendo los parámetros de conectividad y caudal.
- Detectar las incidencias producidas en el sistema, documentando las que se produzcan.

Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.4; C2 respecto a CE2.5; C3 respecto a CE3.3; C4 respecto a CE4.3.

Otras Capacidades:

Mantener el área de trabajo con el grado apropiado de orden y limpieza.
Demostrar cierto grado de autonomía en la resolución de contingencias relacionadas con su actividad.

Demostrar creatividad en el desarrollo del trabajo que realiza.
Interpretar y ejecutar instrucciones de trabajo.
Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.
Valorar el talento y el rendimiento profesional con independencia del sexo.
Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.
Cumplir las medidas que favorezcan el principio de igualdad de trato y de oportunidades entre hombres y mujeres.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Procesos en el sistema informático

Estados de un proceso.
Manejo de señales entre procesos.
Administración de procesos.
Cambio de prioridades.
Monitorización de procesos.
Gestión del consumo de recursos.

2 Almacenamiento de información en la gestión de servicios

Dispositivos de almacenamiento.
Sistemas de archivo.
Estructura general de almacenamiento.
Herramientas del sistema para gestión del almacenamiento.

3 Gestión de usuarios en la gestión de servicios

Acceso al sistema.
Permisos y acceso a los recursos.
Limitaciones de uso de recursos.

4 Servicios de comunicaciones en la gestión de servicios

Dispositivos de comunicaciones.
Protocolos de comunicaciones.
Servicios de comunicaciones.
Rendimientos de los servicios de comunicaciones.

Parámetros de contexto de la formación

Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos, salud laboral, accesibilidad universal y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la gestión de servicios en el sistema informático, que se acreditará mediante una de las dos formas siguientes:

- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior), Ingeniero Técnico, Diplomado o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.

2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

MÓDULO FORMATIVO 2

Implantación y mantenimiento de sistemas domóticos/inmóticos

Nivel: *3*
Código: *MF1219_3*
Asociado a la UC: *UC1219_3 - Implantar y mantener sistemas domóticos/inmóticos*
Duración (horas): *150*
Estado: *BOE*

Capacidades y criterios de evaluación

C1: Interpretar las especificaciones técnicas y funcionales de un proyecto de instalación y/o de integración de sistemas domóticos/inmóticos.

CE1.1 Describir los requisitos funcionales del proyecto domótico/inmótico, detallando los equipos y dispositivos involucrados en cada una de las funcionalidades, e identificando las distintas redes del sistema y las interconexiones entre los elementos de cada una de ellas.

CE1.2 Identificar las distintas tecnologías utilizadas en instalaciones de sistemas domóticos/inmóticos, indicando las características de cada una.

CE1.3 Distinguir y clasificar las distintas arquitecturas y medios de transmisión utilizados (par trenzado, vía radio, red eléctrica) en los sistemas domóticos.

CE1.4 Verificar los elementos que componen la instalación e infraestructura de un sistema domótico/inmótico para la puesta en servicio y su configuración, de acuerdo con las especificaciones funcionales del proyecto.

CE1.5 En un supuesto práctico, debidamente caracterizado, de interpretación de un proyecto de instalación y/o integración de un sistema domótico/inmótico, a partir de la documentación técnica que define el proyecto:
- Identificar los requisitos funcionales del proyecto.
- Identificar los elementos del sistema domótico/inmótico, tanto hardware como software.
- Identificar las distintas redes que forman el sistema domótico/inmótico.
- Comprobar que los elementos del sistema cumplen con los requisitos funcionales.
- Verificar visualmente la instalación.
- Documentar los trabajos realizados según unas especificaciones dadas.

C2: Identificar los parámetros funcionales de los equipos y dispositivos del sistema domótico/inmótico y, en un caso práctico, realizar su puesta en servicio, de acuerdo con las especificaciones técnicas del proyecto.

CE2.1 Identificar las características de los estándares y protocolos implicados en el sistema domótico/inmótico para su correcta configuración.

CE2.2 Describir las características técnicas y funcionales de los equipos y dispositivos del sistema domótico/inmótico, incluyendo el estándar domótico o sistema propietario al que pertenecen, identificando los parámetros de configuración e indicando el impacto que supone en un proyecto una modificación del mismo.

CE2.3 Configurar los componentes hardware y software del sistema domótico/inmótico, utilizando las herramientas específicas del sistema al que pertenecen.

CE2.4 Explicar las características y funcionalidades de las pasarelas residenciales identificando los tipos, tecnologías y parámetros de configuración y conexión del sistema domótico con las redes externas.

CE2.5 En un supuesto práctico, debidamente caracterizado, de configuración y parametrización de los equipos y dispositivos que forman el sistema domótico/inmótico para su puesta en servicio, según unas especificaciones técnicas:

- Identificar los equipos y dispositivos del sistema domótico a implantar y poner en servicio.
- Configurar los elementos hardware y software del sistema domótico/inmótico utilizando las herramientas software propietarias.
- Configurar, en su caso, la pasarela residencial, e integrar las distintas redes del sistema, utilizando herramientas software específicas.
- Probar la funcionalidad de los equipos del sistema.
- Elaborar un informe de puesta en marcha del sistema.

C3: Identificar los procedimientos y herramientas de gestión de inventarios, y elaborar y mantener el inventario del sistema domótico/inmótico siguiendo especificaciones dadas.

CE3.1 Identificar los pasos que se deben seguir en el procedimiento de inventariado de un sistema domótico/inmótico, tanto durante su implantación inicial como durante su posterior mantenimiento.

CE3.2 Describir las características y funcionalidades de las herramientas software que se utilizan para la gestión de inventarios.

CE3.3 Describir los procedimientos de extracción de información a inventariar de los elementos que componen los sistemas domóticos/inmóticos, en función de sus especificaciones técnicas.

CE3.4 En un supuesto práctico, debidamente caracterizado, de elaboración y mantenimiento del inventario de los equipos y dispositivos que forman el sistema domótico/inmótico:

- Identificar los equipos y dispositivos, así como las configuraciones y software asociado a inventariar.
- Utilizar herramientas software específicas de gestión de inventarios.
- Registrar toda la información del sistema y los cambios que se produzcan en el inventario.

C4: Identificar los parámetros y herramientas de configuración del software de control, y añadir nuevas funcionalidades al sistema domótico/inmótico, siguiendo especificaciones técnicas dadas.

CE4.1 Explicar las características y funcionalidades del software de configuración del sistema domótico/inmótico, en función de sus especificaciones técnicas.

CE4.2 Identificar los equipos y el software de control del sistema domótico/inmótico, con sus características y funcionalidades, incluyendo el estándar domótico o sistema propietario al que pertenecen.

CE4.3 Describir los parámetros de configuración de cada módulo del software de control del sistema domótico/inmótico, indicando el impacto que supone en un proyecto una modificación del mismo, teniendo en cuenta especificaciones técnicas y funcionales.

CE4.4 Identificar las herramientas de programación que proporcionan los sistemas domóticos/inmóticos, en función de los estándares domóticos y sistemas propietarios a los que pertenecen.

CE4.5 Describir los servicios que se pueden añadir al sistema domótico/inmótico a través de la pasarela residencial.

CE4.6 En un supuesto práctico, debidamente caracterizado, de configuración del software de control y adición de nuevas funcionalidades al sistema domótico/inmótico, según unas especificaciones técnicas dadas:
- Verificar los equipos que van a contener el software de control.
- Instalar y configurar el software de control.
- Añadir nuevas funcionalidades utilizando las herramientas de programación o configuración propias del sistema.
- Aplicar técnicas de desarrollo para añadir las nuevas funcionalidades al sistema.
- Aplicar técnicas de prueba para verificar las funcionalidades del software de control.
- Elaborar el informe de puesta en marcha siguiendo los formatos especificados.

C5: Elaborar y aplicar procedimientos de mantenimiento del sistema domótico/inmótico, teniendo en cuenta los criterios de calidad establecidos en el proyecto y las recomendaciones de fabricantes de los elementos que lo componen.

CE5.1 Identificar y detallar las operaciones de mantenimiento preventivo del sistema domótico/inmótico y de cada uno de los equipos y dispositivos que lo forman, en función de las especificaciones técnicas de los mismos.

CE5.2 Describir los procedimientos normalizados y las herramientas que se utilizan para localizar y solucionar las averías de los componentes del sistema domótico/inmótico, tanto a nivel hardware como software.

CE5.3 En un supuesto práctico, debidamente caracterizado, de mantenimiento del sistema domótico/inmótico según unas especificaciones técnicas dadas:
- Identificar las tareas de mantenimiento de los equipos y dispositivos implicados.
- Elaborar el plan de mantenimiento de cada uno de los elementos del sistema.
- Utilizar herramientas específicas para localizar averías hardware y software.
- Resolver las incidencias que se produzcan aplicando los procedimientos normalizados.
- Actualizar el manual de identificación y detección de incidencias.

Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.5; C2 respecto a CE2.5; C3 respecto a CE3.4; C4 respecto a CE4.6; C5 respecto a CE5.3.

Otras Capacidades:

Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Demostrar cierto grado de autonomía en la resolución de contingencias relacionadas con su actividad.
Adaptarse a la organización, a sus cambios organizativos y tecnológicos así como a situaciones o contextos nuevos.
Interpretar y ejecutar instrucciones de trabajo.
Demostrar flexibilidad para entender los cambios.
Respetar los procedimientos y normas internas de la organización.

Contenidos

1 Domótica/inmótica

Aspectos generales de la domótica/inmótica: confort, seguridad, ahorro energético, multimedia.
Infraestructura de los sistemas domóticos/inmóticos, pequeñas y grandes instalaciones.
Arquitecturas del sistema de control de un edificio.

Climatización: ventilación, refrigeración y calefacción. Iluminación: conceptos generales, sistemas de iluminación.
Sistemas de seguridad: intrusión, alarmas técnicas, conexión a CRA.
Componentes de un sistema domótico-inmótico.
Sensores, actuadores, transmisores, unidades de control, pasarelas de comunicación.
Topologías de los sistemas domóticos/inmóticos.
Medios físicos de transmisión: par trenzado, corrientes portadoras, radiofrecuencia, infrarrojos, bus compartido, fibra óptica.
Conceptos de atenuación, interferencias, velocidad de transmisión.
Proyectos domóticos/inmóticos: documentación y su interpretación.

2 Dispositivos y protocolos de redes de comunicación aplicados a los domótica/inmótica

Protocolos en sistemas domóticos/inmóticos: protocolos estandarizados: EIB/KNX, 'lonworks', entre otros, herramientas de configuración, programación, visualización y control.
Sistemas propietarios cableados: herramientas de configuración, programación, visualización y control. Sistemas propietarios vía radio: herramientas de configuración, programación, visualización y control. Otras tecnologías de apoyo a la domótica/inmótica (enocean, zigbee, RFID -RadioFrequency IDentification-, entre otras).
Funciones lógicas: puertas, tablas de la verdad, mapas de Karnaugh.
Protocolos TCP/IP: direccionamiento IP, puertos TCP/UDP, protocolos: FTP, TFTP, NTP, http. Concepto de routers, conmutadores, 'hubs' y firewalls.
Técnicas de planificación.

3 Inventarios en sistemas domóticos/inmóticos

Características de los inventarios en sistemas domóticos/inmóticos.
Metodologías de realización y actualización de inventarios en sistemas domóticos/inmóticos.
Herramientas para la gestión de inventarios.

4 Mantenimiento de sistemas domóticos/inmóticos

Procedimientos de mantenimiento de equipos y dispositivos de sistemas domóticos/inmóticos.
Herramientas software y hardware de diagnóstico: características y usos.
Entorno normativo aplicable.

Parámetros de contexto de la formación

Espacios e instalaciones

Los espacios e instalaciones darán respuesta, en forma de aula, aula-taller, taller de prácticas, laboratorio o espacio singular, a las necesidades formativas, de acuerdo con el Contexto Profesional establecido en la Unidad de Competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos, salud laboral, accesibilidad universal y protección medioambiental.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la implantación y el mantenimiento de sistemas domóticos/inmóticos, que se acreditará mediante una de las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior), Ingeniero Técnico, Diplomado o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo

2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

MÓDULO FORMATIVO 3

Implantación y mantenimiento de sistemas de control de accesos y presencia, y de videovigilancia

Nivel:	*3*
Código:	*MF1220_3*
Asociado a la UC:	*UC1220_3 - Implantar y mantener sistemas de control de accesos y presencia, y de videovigilancia*
Duración (horas):	*270*
Estado:	*BOE*

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 y de videovigilancia, 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 y de videovigilancia.

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 y de videovigilancia, 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 supuesto práctico, debidamente caracterizado, de identificación y descripción de un sistema de control de accesos y presencia y de videovigilancia, a partir de la documentación técnica de su instalación y mantenimiento:

- Identificar la ubicación de los equipos y dispositivos de los distintos subsistemas, y los medios y herramientas necesarios para aplicar los procesos de implementación.
- Identificar y describir el sistema de distribución de energía, los elementos de protección y el sistema de alimentación ininterrumpida, y las envolventes, cuadros, armarios y elementos del cableado.
- Reconocer y detallar el tipo de canalizaciones y su distribución en plantas, distribución horizontal y vertical, y las características de los cableados y conexionado de los elementos.
- Reconocer y describir los sistemas de identificación y señalización de conductores y de los elementos de conexión de los equipos presentes en la instalación.
- Identificar y detallar los equipos informáticos y periféricos utilizados para la administración del sistema.
- Identificar y describir la aplicación informática de configuración, gestión y supervisión de los subsistemas, así como los controladores (manejadores de dispositivos o 'drivers') debidamente actualizados.

C2: Identificar la infraestructura y verificar la instalación de los sistemas de control de accesos y presencia y de videovigilancia 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 y de videovigilancia, así como las conexiones entre los mismos.

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 y de videovigilancia.

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 y de videovigilancia, así como las conexiones entre ellos.

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

CE2.5 En un supuesto práctico, debidamente caracterizado, de verificación de la instalación de los sistemas de control de accesos y presencia y de videovigilancia, y a partir de unas especificaciones técnicas dadas:

- 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 normativa aplicable sobre protección de datos.

CE3.8 En un supuesto práctico, debidamente caracterizado, de puesta en servicio el sistema de control de accesos y presencia:

- Configurar el sistema informático.
- Instalar las aplicaciones software de todo el sistema de control de accesos y presencia, teniendo identificados todos los dispositivos y equipos del sistema.
- 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 y en los portillones.
- Probar la funcionalidad del sistema, comprobando que se ajusta a las especificaciones recibidas.
- Elaborar el plan de documentación a través del diario de ingeniería.
- Elaborar el documento de seguridad teniendo en cuenta la normativa aplicable en materia de protección de datos.

C4: Poner en servicio los equipos y dispositivos del sistema de videovigilancia, así como sus aplicaciones y configuraciones, teniendo en cuenta las especificaciones técnicas asociadas.

CE4.1 Describir las características y funcionalidades de los dispositivos y equipos que forman el sistema de videovigilancia, identificando sus parámetros de configuración.

CE4.2 Identificar las funciones principales que realiza el sistema informático que se utiliza para la gestión y supervisión del sistema de videovigilancia.

CE4.3 Explicar las características y funcionalidades de las aplicaciones de control, gestión y planimetría que se utilizan en el sistema de videovigilancia, identificando los parámetros de instalación y configuración.

CE4.4 Describir la funcionalidad de la aplicación software que centraliza el control del sistema de videovigilancia, identificando los parámetros de instalación y configuración.

CE4.5 Citar la legislación sobre protección de datos a la hora de tratar la información registrada y grabada en el sistema de videovigilancia.

CE4.6 Describir la funcionalidad de las herramientas de generación de copias de seguridad que se utilizan en los sistemas de videovigilancia, identificando los parámetros de instalación y configuración.

CE4.7 En un supuesto práctico, debidamente caracterizado, de puesta en servicio de un sistema de videovigilancia, según las especificaciones del proyecto:
- Configurar el sistema informático.
- Instalar las aplicaciones software de todo el sistema de videovigilancia, identificando todos los dispositivos y equipos del sistema implicados.
- Configurar los parámetros del sistema de CCTV en las controladoras y en los servidores de grabación.
- Probar la funcionalidad del sistema.
- Elaborar el plan de documentación a través del diario de Ingeniería.
- Elaborar el documento de seguridad teniendo en cuenta la normativa aplicable en materia de protección de datos.

C5: Describir los procedimientos de mantenimiento y resolver las incidencias de los sistemas de control de accesos y presencia y de videovigilancia, para mantener operativo el sistema.

CE5.1 Describir los procesos de mantenimiento de los equipos y dispositivos que forman los sistemas de control de accesos y detección de presencia y de videovigilancia identificando los parámetros de funcionalidad óptima.

CE5.2 Elaborar y actualizar los procedimientos de mantenimiento estableciendo el número de revisiones preventivas y las acciones a realizar en cada revisión del sistema.

CE5.3 Identificar nuevas funcionalidades y mejoras de los componentes hardware y software de los sistemas de control de accesos y detección de presencia y de videovigilancia que existen en el mercado, para proponer actualizaciones compatibles.

CE5.4 Clasificar la tipología y características de las averías de naturaleza física y lógica que se presentan en los sistemas de control de accesos y detección de presencia y de videovigilancia.

CE5.5 Describir las técnicas generales y los medios técnicos específicos necesarios para la localización de averías de naturaleza física y lógica en los sistemas de control de accesos y detección de presencia y de videovigilancia.

CE5.6 En un supuesto práctico, debidamente caracterizados, de diagnóstico, localización y resolución de averías en los sistemas de control de accesos y presencia y de videovigilancia:

- Interpretar la documentación del sistema, identificando los distintos bloques funcionales y componentes específicos que lo componen.
- Identificar los síntomas de la avería caracterizándola por los efectos que produce y realizar un plan de intervención en el sistema para determinar su causa o causas.
- Localizar el elemento (físico o lógico) responsable de la avería y realizar la sustitución (mediante la utilización de componentes similares o equivalentes) o modificación del elemento, configuración y/o programa, aplicando los procedimientos requeridos y en un tiempo adecuado.
- Realizar las comprobaciones, modificaciones y ajustes de los parámetros del sistema, según las especificaciones de la documentación técnica del mismo, utilizando las herramientas apropiadas, que permitan su puesta a punto en cada caso.
- Elaborar un informe-memoria de las actividades desarrolladas y resultados obtenidos, estructurándolo en los apartados necesarios para su adecuada documentación (descripción del proceso seguido, medios utilizados, medidas, explicación funcional y esquemas).

Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.4; C2 respecto a CE2.5; C3 respecto a CE3.8; C4 respecto a CE4.7; C5 respecto a CE5.6.

Otras Capacidades:

Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Demostrar cierto grado de autonomía en la resolución de contingencias relacionadas con su actividad.
Adaptarse a la organización, a sus cambios organizativos y tecnológicos así como a situaciones o contextos nuevos.
Interpretar y ejecutar instrucciones de trabajo.
Demostrar flexibilidad para entender los cambios.
Respetar los procedimientos y normas internas de la organización.

Contenidos

1 El análisis de riesgo

La rueda de seguridad.
La categorización del riesgo.
Los niveles de riesgo.
Los activos a proteger: recursos humanos, bienes tangibles y protección de la información.
Analizando el riesgo de una compañía.
La importancia de la seguridad física en una empresa e integración con los restantes departamentos. La amenaza de la intrusión: mitigación del riesgo de intrusión.

2 Proyectos de seguridad física, sistemas de control de accesos y presencia y videovigilancia

Proyectos y especificaciones.

Documentación técnica de un proyecto: memoria, planos, pliego de condiciones y presupuesto.
Planificación de las tareas propias de un proyecto de seguridad integral.

3 El sistema de seguridad integral y sus componentes

Necesidad de integrar un sistema de seguridad.
El sistema de seguridad integral y sus subsistemas.
Examinando el sistema de control de accesos y presencia.
Examinando el sistema de videovigilancia.
Integrando un sistema de control de accesos y presencia y videovigilancia.

4 Entorno legal

Normativa aplicable en materia de protección de datos.
Normativa aplicable en materia de seguridad privada.

5 Interconexión de los elementos que integran el sistema integral de seguridad

Infraestructura de los sistemas de seguridad física, sistemas de control de accesos y presencia y videovigilancia.
Dispositivos y protocolos de redes de comunicaciones IP.
Tipo de cableado y conexiones para el sistema de control de accesos, presencia y videovigilancia.
Tipos de tecnologías para el sistema de control de accesos, presencia y videovigilancia.
Tipos de protocolos para el sistema de control de accesos, presencia y videovigilancia.

6 Sistemas de control de accesos y presencia

Función de un sistema de control de accesos y presencia en la empresa.
Elementos que componen un sistema de control de accesos y presencia, componentes hardware y software: características, funcionalidades, parámetros, herramientas de configuración.
Configuración y parametrización del sistema de control de accesos y presencia.
La biometría como elemento potenciador del control de accesos.
Los soportes de acreditación personal.
Más allá de los sistemas de control de accesos: compatibilidad con los sistemas de seguridad lógica.

7 Sistemas de videovigilancia

Función de un sistema de videovigilancia en la empresa.
Elementos que componen un sistema de control de accesos y presencia, componentes hardware y software: características, funcionalidades, parámetros, herramientas de configuración.
Configuración y parametrización del sistema de videovigilancia.
Conexión a CRA (Central Receptora de Alarmas).

8 Mantenimiento de los sistemas de control de accesos y presencia y videovigilancia

Tipos y procedimientos de supervisión y mantenimiento preventivo de los equipos.
Tipos de alarmas y averías de los equipos de los sistemas de control de accesos y presencia y videovigilancia.
Técnicas y herramientas de diagnóstico y resolución de averías en sistemas de control de accesos y presencia y videovigilancia.
El plan de contingencia: análisis e interpretación.

Parámetros de contexto de la formación

Espacios e instalaciones

Los espacios e instalaciones darán respuesta, en forma de aula, aula-taller, taller de prácticas, laboratorio o espacio singular, a las necesidades formativas, de acuerdo con el Contexto Profesional establecido en la Unidad de Competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos, salud laboral, accesibilidad universal y protección medioambiental.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la implantación y el mantenimiento de sistemas de control de accesos y presencia y de videovigilancia, que se acreditará mediante una de las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior), Ingeniero Técnico, Diplomado o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.