Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico-sanitaria correspondiente y responderán a medidas de accesibilidad universal y seguridad de los participantes.

El número de unidades que se deben disponer de los utensilios, máquinas y herramientas que se especifican en el equipamiento de los espacios formativos, será el suficiente para un mínimo de 15 alumnos y deberá incrementarse, en su caso, para atender a número superior.

En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

ANEXO IV

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: IMPLANTACIÓN Y GESTIÓN DE ELEMENTOS INFORMÁTICOS EN SISTEMAS DOMÓTICOS/INMÓTICOS, DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

Código: IFCT0409

Familia profesional: Informática y Comunicaciones

Área profesional: Sistemas y Telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC365_3 Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia (RD 1701/2007, de 14 diciembre)

Relación de unidades de competencia que configuran el certificado de profesionalidad:

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

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 vigentes.

cve: BOE-A-2011-10055

Entorno Profesional:

Ámbito profesional:

Desarrolla su actividad profesional tanto por cuenta propia, como por cuenta ajena en empresas o entidades publicas o privadas de cualquier tamaño, dedicadas al diseño, implementación y mantenimiento de sistemas domóticos/inmóticos, de control de accesos y presencia, y videovigilancia.

Sectores productivos:

Se ubica sobre todo en el sector servicios, y principalmente en empresas cuya actividad tenga como objetivo el proveer y mantener servicios relacionados con la automatización de viviendas y edificios, así como con la seguridad privada, relativos a la implementación y mantenimiento de sistemas de control de accesos y presencia, y de videovigilancia.

Ocupaciones o puestos de trabajo relacionados:

Integrador de elementos informáticos en sistemas domóticos/inmóticos.
Integrador de elementos informáticos en sistemas de control de accesos y presencia, y en sistemas de videovigilancia.
Experto de mantenimiento de elementos informáticos en sistemas de control de accesos y presencia, y en sistemas de videovigilancia.

Duración de la formación asociada: 540 horas.

Relación de módulos formativos y de unidades formativas:

MF0490_3: (Transversal) Gestión de servicios en el sistema informático (90 horas)
MF1219_3: Implantación y mantenimiento de sistemas domóticos/inmóticos (150 horas)
- UF1134: Instalación y puesta en marcha de un proyecto domótico / inmótico (80 horas)
- UF1135: Conectividad del proyecto domótico: redes, sistemas y protocolos de comunicación; pasarelas (40 horas)
- UF1136: Documentación, mantenimiento y gestión de incidencias en un proyecto domótico (30 horas)

MF1220_3: Implantación y mantenimiento de sistemas de control de accesos y presencia, y de video vigilancia (220 horas)
- UF1137: Instalación y puesta en marcha de un sistema de Video Vigilancia y seguridad (90 horas)
- UF1138: Instalación y puesta en marcha de un sistema de Control de Acceso y presencia (90 horas)
- UF1139: Mantenimiento y gestión de Incidencias en proyectos de Video Vigilancia, control de accesos, y presencia (40 horas)

MP0236: Módulo de prácticas profesionales no laborales de Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia (80 horas)

cve: BOE-A-2011-10055

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel: 3

Código: UC0490_3

Realizaciones profesionales y criterios de realización

RP1: Gestionar la configuración del sistema para asegurar el rendimiento de los procesos según las necesidades de uso y dentro de las directivas de la organización.

CR1.1. Los procesos que intervienen en el sistema son identificados para evaluar parámetros de rendimiento.

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

CR1.3. Las prioridades de ejecución de los procesos se adecuan en función de las especificaciones del plan de explotación de la organización.

CR1.4. Las herramientas de monitorización se implantan y configuran determinando los niveles de las alarmas en función del plan de explotación de la organización.

RP2: Administrar los dispositivos de almacenamiento según las necesidades de uso y dentro de las directivas de la organización.

CR2.1. Los dispositivos de almacenamiento se configuran para ser usados en los distintos sistemas operativos utilizados en el sistema informático.

CR2.2. La estructura de almacenamiento se define y se implanta atendiendo a las necesidades de los distintos sistemas de archivos y a las especificaciones de uso de la organización.

CR2.3. Los requerimientos de nomenclatura de objetos y restricciones de uso de cada dispositivo de almacenamiento se documentan adecuadamente.

CR2.4. Los dispositivos de almacenamiento se integran para ofrecer un sistema funcional al usuario según las especificaciones de la organización.

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 para garantizar la seguridad e integridad del sistema según las especificaciones de la organización.

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 para los usuarios se limitan con las herramientas adecuadas 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 dispositivos de comunicaciones son verificados en lo que respecta a su configuración y rendimiento según las especificaciones de la organización.

CR4.2. Los servicios de comunicaciones son identificados en el sistema con sus procesos correspondientes para analizar los consumos de recursos y verificar que están dentro de lo permitido por las especificaciones del plan de explotación de la organización.

cve: BOE-A-2011-10055

CR4.3. Las incidencias en los servicios de comunicaciones se detectan y se documentan para informar a los responsables de la explotación del sistema y de la gestión de las comunicaciones según los protocolos de la organización

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
Sistema operando correctamente. Rendimiento del sistema adecuado a los parámetros de explotación. Sistema seguro e íntegro en el acceso y utilización de recursos. Servicios de comunicaciones en funcionamiento.

Información utilizada o generada
Manuales de explotación del sistema operativo y de los dispositivos. Plan de explotación de la organización. Manuales de las herramientas de monitorización utilizadas. Gráficas y análisis de rendimiento. Listados de acceso y restricciones de usuarios. Informe de incidencias. Protocolo de actuación ante incidencias.

Unidad de competencia 2

Denominación: IMPLANTAR Y MANTENER SISTEMAS DOMÓTICOS/INMÓTICOS

Nivel: 3

Código: UC1219_3
Realizaciones profesionales y criterios de realización

RP1: Configurar y parametrizar los equipos y dispositivos del sistema domótico/inmótico para su puesta en servicio, de acuerdo a 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 comprobación y verificación de la ubicación e instalación de los equipos, dispositivos e infraestructura se realiza para garantizar la configuración, programación y puesta en marcha del sistema domótico / inmótico, de acuerdo a 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 de acuerdo a los procedimientos establecidos por la organización.

CR1.4 La configuración de las diferentes pasarelas residenciales, en su caso, se realiza 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 bidireccional al sistema desde el exterior de acuerdo a especificaciones del proyecto.

CR1.5 La puesta en marcha del sistema domótico/inmótico se realiza, siguiendo el protocolo de pruebas establecido por la organización y de acuerdo a las especificaciones funcionales del proyecto.

cve: BOE-A-2011-10055

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.
CR1.7 La documentación técnica específica asociada, se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP2: Elaborar y mantener inventarios de los equipos y dispositivos, y del software que componen el sistema domótico/inmótico, para garantizar su identificación y localización, siguiendo 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, de acuerdo al procedimiento establecido por la organización.

RP3: Ajustar el software de control y crear programas para añadir funcionalidades al sistema domótico/inmótico, integrándolas en la aplicación de monitorización y control (software de control) utilizando herramientas de programación y estándares software de desarrollo, de acuerdo a especificaciones técnicas y necesidades del sistema.
CR3.1 La configuración y parametrización del software de control del sistema se planifica y se realiza para su puesta en funcionamiento, de acuerdo a 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 comprobación y verificación de la ubicación e instalación de los equipos de monitorización y control del sistema, se realizan para garantizar su configuración, programación y puesta en marcha, siguiendo especificaciones técnicas del proyecto.
CR3.3 La programación de funcionalidades del software de control se realiza 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 a requisitos funcionales y criterios de calidad establecidos en el proyecto.

cve: BOE-A-2011-10055

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
Ordenador portátil, PC de sobremesa 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. 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/inmódicos.

Productos y resultados
Configuración y puesta en marcha del sistema inmótico/domótico. Mantenimiento preventivo de los componentes hardware y software del sistema domótico/inmótico. Mantenimiento 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 del sistema domótico/inmótico. Documentación técnica, manuales de instalación y uso de las aplicaciones software del sistema domótico/inmótico. Documentación de instalación eléctrica de los elementos hardware del sistema domótico/inmótico. Reglamento electrotécnico de baja tensión (REBT). Reglamento de infraestructuras comunes de telecomunicaciones (ICT). 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.

cve: BOE-A-2011-10055

Unidad de competencia 3

Denominación: IMPLANTAR Y MANTENER SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

Nivel: 3

Código: UC1220_3

Realizaciones profesionales y criterios de realización

RP1: Interpretar las especificaciones técnicas del proyecto y verificar su instalación para implementar el sistema de control de accesos y presencia, y videovigilancia, según necesidades de la organización.

CR1.1 El análisis de riesgo y las especificaciones recogidas en el proyecto de instalación del sistema de control de accesos y presencia, y videovigilancia a implementar, se interpretan con objeto de identificar la arquitectura y componentes del sistema a implantar.

CR1.2 La planificación de las operaciones a desarrollar se realiza de acuerdo con los recursos humanos y materiales disponibles, para optimizar el proceso de implementación de los sistemas, teniendo en cuenta el marco de la reglamentación vigente 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 a 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 a 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: Implementar los sistemas de control de accesos y presencia en la organización, de acuerdo a los requisitos y especificaciones de diseño establecidos en el 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,

cve: BOE-A-2011-10055

para garantizar la seguridad y fiabilidad de la información del sistema, teniendo en cuenta las especificaciones de la organización y la normativa vigente.

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 legal vigente 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 normativas de protección de datos y de acuerdo a 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 a los planes de seguridad y a la normativa legal vigente sobre protección de datos.

CR2.7 El informe de puesta en marcha 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.

CR2.8 La documentación técnica específica asociada, se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP3: Implementar los sistemas de videovigilancia en la organización, de acuerdo a los requisitos y especificaciones de diseño establecidos en el proyecto.

CR3.1 Los equipos informáticos y periféricos asociados se configuran físicamente, y 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 a 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 legislación 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 a los planes de seguridad y cumpliendo la normativa legal vigente sobre protección de datos.

CR3.5 El informe de puesta en marcha del 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.

cve: BOE-A-2011-10055

CR3.6 La documentación técnica específica asociada, se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP4: Mantener los sistemas de control de accesos y presencia, y de videovigilancia, para asegurar su funcionalidad, de acuerdo con lo establecido en la documentación técnica del proyecto.

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 accesos 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 y, para 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 accesos 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 preventivo 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. 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. Instrumentos de medida: polímetro, téster de cableado coaxial, 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 de control, multiplexores, secuenciadores,

cve: BOE-A-2011-10055

grabadores de imagen analógicos y digitales, monitores analógicos y TFT, soportes de grabación (cintas, CD, DVD).

Productos y resultados
Planificación, ejecución y seguimiento de la implementación de los sistemas de control de accesos y presencia, y de videovigilancia. 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. Legislación vigente sobre protección de datos y seguridad privada.

III. FORMACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

MÓDULO FORMATIVO 1

Denominación: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Código: MF0490_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0490_3: Gestionar servicios en el sistema informático

Duración: 90 horas

Capacidades y criterios de evaluación

C1: Analizar los procesos del sistema con objeto de asegurar un rendimiento adecuado a los parámetros especificados en el plan de explotación.

CE1.1 Identificar los procesos del sistema y 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.

CE1.3 Explicar técnicas de monitorización y herramientas destinadas a evaluar el rendimiento del sistema.

CE1.4 En un supuesto práctico en el que se cuenta con un sistema informático con una carga de procesos debidamente caracterizada:

cve: BOE-A-2011-10055

- Utilizar las herramientas del sistema para identificar cuantos procesos activos existen y las características particulares de alguno de ellos.
- Realizar las 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 a dispositivos de almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, seguro y disponible.

CE2.1 Identificar los distintos 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 los sistemas de archivo en función de los dispositivos de almacenamiento y sistemas operativos empleados.

CE2.3 Describir la estructura general de almacenamiento en el sistema informático asociando los dispositivos con los distintos sistemas de archivos existentes.

CE2.4 En un supuesto práctico en el que se dispone de un sistema de almacenamiento de la información con varios dispositivos:

- Realizar el particionamiento, en los casos que sea necesario, y la generación de la infraestructura de los sistemas de archivo a instalar en cada dispositivo.
- Implementar la estructura general de almacenamiento integrando todos los dispositivos y sus correspondientes sistemas de archivos.
- Documentar los requerimientos y restricciones de cada sistema de archivos implantado.

C3: Administrar el acceso al sistema y a los recursos para verificar el uso adecuado y seguro de los mismos.

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

CE3.2 Describir las 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 en el que se cuenta con derecho de administración de usuarios:

- Identificar los posibles accesos de un usuario al sistema.
- Modificar los permisos de utilización de un recurso del sistema a un usuario.
- Definir limitaciones de uso de un recurso del sistema a los usuarios.

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

CE4.1 Explicar los parámetros de configuración y funcionamiento de los dispositivos de comunicaciones para asegurar su funcionalidad dentro del sistema.

CE4.2 Relacionar los servicios de comunicaciones activos en el sistema con los dispositivos utilizados por ellos con objeto de analizar y evaluar el rendimiento.

CE4.3 En un supuesto práctico en el que tomamos un sistema informático conectado con el exterior por medio de varias líneas de comunicaciones:

- Identificar los dispositivos de comunicaciones y describir sus características.
- Verificar el estado de los servicios de comunicaciones.
- Evaluar el rendimiento de los servicios de comunicaciones.
- Detectar y documentar las incidencias producidas en el sistema.

cve: BOE-A-2011-10055

Contenidos

1. **Seguridad y normativas en sistemas informáticos**
   - Norma ISO 27002 Código de buenas practicas para la gestión de la seguridad de la información
   - Metodología ITIL Librería de infraestructuras de las tecnologías de la información
   - Ley orgánica de protección de datos de carácter personal.
   - Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

2. **Procesos de sistemas informáticos**
   - Identificación de procesos de negocio soportados por sistemas de información
   - Características fundamentales de los procesos electrónicos
     - □ Estados de un proceso,
     - □ Manejo de señales, su administración y los cambios en las prioridades
   - Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
   - Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
   - Técnicas utilizadas para la gestión del consumo de recursos

3. **Sistemas de almacenamiento de sistemas informáticos**
   - Tipos de dispositivos de almacenamiento más frecuentes
   - Características de los sistemas de archivo disponibles
   - Organización y estructura general de almacenamiento
   - Herramientas del sistema para gestión de dispositivos de almacenamiento

4. **Utilización de métricas e indicadores de monitorización de rendimiento de sistemas**
   - Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información
   - Identificación de los objetos para los cuales es necesario obtener indicadores
   - Aspectos a definir para la selección y definición de indicadores
   - Establecimiento de los umbrales de rendimiento de los sistemas de información
   - Recolección y análisis de los datos aportados por los indicadores
   - Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

5. **Confección del proceso de monitorización de sistemas y comunicaciones**
   - Identificación de los dispositivos de comunicaciones
   - Análisis de los protocolos y servicios de comunicaciones
   - Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
   - Procesos de monitorización y respuesta
   - Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
   - Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
   - Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
   - Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

cve: BOE-A-2011-10055

6. **Selección del sistema de registro de en función de los requerimientos de la organización**
   - Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
   - Análisis de los requerimientos legales en referencia al registro
   - Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
   - Asignación de responsabilidades para la gestión del registro
   - Alternativas de almacenamiento para los registros del sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
   - Guía para la selección del sistema de almacenamiento y custodia de registros

7. **Administración del control de accesos adecuados de los sistemas de información**
   - Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
   - Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
   - Requerimientos legales en referencia al control de accesos y asignación de privilegios
   - Perfiles de de acceso en relación con los roles funcionales del personal de la organización
   - Herramientas de directorio activo y servidores LDAP en general
   - Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
   - Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0490_3	90	40

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo

MÓDULO FORMATIVO 2

Denominación: IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS DOMÓTICOS/INMÓTICOS

Código: MF1219_3

Nivel de cualificación profesional: 3

cve: BOE-A-2011-10055

Asociado a la Unidad de Competencia:

UC1219_3 Implantar y mantener sistemas domóticos/inmóticos.

Duración: 150 horas

UNIDAD FORMATIVA 1

Denominación: INSTALACIÓN Y PUESTA EN MARCHA DE UN PROYECTO DOMÓTICO / INMÓTICO

Código: UF1134

Duración: 80 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 y RP3 excepto en lo referente a la configuración y conectividad de las pasarelas de comunicación.

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.

CE1.2 Identificar las distintas tecnologías utilizadas en instalaciones de sistemas domóticos / inmóticos.

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 caso práctico, debidamente caracterizado, a partir de la documentación técnica que define el proyecto de instalación y/o integración de un sistema domótico/inmótico:

- 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 a 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

cve: BOE-A-2011-10055

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 En un caso práctico, debidamente caracterizado, configurar y parametrizar los equipos y dispositivos que forman el sistema domótico/inmótico, a poner en servicio, de acuerdo a 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.
- Probar la funcionalidad de los equipos del sistema.
- Elaborar un informe de puesta en marcha del sistema.

CE2.5 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.

C3: Identificar los parámetros y herramientas de configuración del software de control, y añadir nuevas funcionalidades al sistema domótico/inmótico, de acuerdo a especificaciones técnicas dadas.

CE3.1 Explicar las características y funcionalidades del software de configuración del sistema domótico/inmótico, en función de sus especificaciones técnicas.
CE3.2 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.
CE3.3 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.
CE3.4 Identificar las herramientas de programación que proporcionan los sistemas domóticos/inmóticos, en función de los estándares domóticos y sistemas propietarios a los que pertenecen.
CE3.5 En un caso práctico, debidamente caracterizado, configurar el software de control y añadir nuevas funcionalidades al sistema domótico/inmótico, de acuerdo a 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.
- Realizar pruebas para verificar las funcionalidades del software de control.
- Elaborar el informe de puesta en marcha siguiendo los formatos especificados.

Contenidos

1. Conceptos generales de la domótica / Inmótica
- Definición de conceptos relacionados con domótica.
- Aplicación de la domótica a la vivienda como parte del “hogar digital”.
- Descripción de las diferentes redes que forman un edificio y su integración con la domótica.
- Análisis del ámbito de aplicación y ejemplos de aplicación.
- Desarrollo histórico y estado actual de la domótica.
- Análisis de los actores Influyentes de la domótica.

cve: BOE-A-2011-10055

- Identificación de los organismos y asociaciones relacionados con la domótica.

2. Aplicación de Electricidad y Electrónica a los Sistemas Domóticos
- Relación de los conceptos y elementos electrónicos / eléctricos básicos.
- Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes (incluso en otros idiomas).
- Análisis de los sistemas de control básicos (autómatas) y su evolución hacia sistemas domóticos.

3. Estudio y Clasificación de los diferentes Sistemas Domóticos más representativos
- Clasificación de los sistemas domóticos según su medio de transmisión.
- Clasificación según su arquitectura.
- Clasificación según su Topología.
- Clasificación según su protocolo.
  - Sistemas estándar.
  - Sistemas Propietarios.
- Análisis, evaluación y acometida de un proyecto domótico:
  - Restricciones del protocolo y de su funcionalidad.
  - Restricciones propias de los aparatos y dispositivos.
  - Parámetros a evaluar del medio físico de comunicación (distancias, interferencias, atenuaciones, etc.).
  - Identificación de la problemática debida al medio y la localización del sistema (entorno).
  - Protecciones de los aparatos (Ips).
  - Valoración de la influencia del factor humano.

4. Elementos del Proyecto / Sistema domótico
- Descripción de los componentes HARDWARE (Dispositivos) del sistema domótico.
- Descripción y características del Medio de transmisión (soporte de comunicación) del sistema domótico.
- Análisis, descripción y características del SOFTWARE Programación y parametrización de los elementos del sistema domótico.
- Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas).
- Interpretación de un proyecto domótico.

5. Requisitos y necesidades del sistema domótico
- Definición de la topología de las instalaciones convencionales.
- Análisis de las necesidades de adaptación de las instalaciones a las nuevas tecnologías.
- Modificaciones y requisitos necesarios para integrar sistemas domóticos.
- Estudio de la aplicación de la normativa aplicable en instalaciones domóticas:
  - REBT “Reglamento Electrónico de Baja tensión”.
  - ICT “Infraestructura Común de Telecomunicaciones”.
  - Normativa Mundial y Europea.
- Análisis de la relación de las instalaciones domóticas y la actual normativa ICT.
  - Necesidades de normalización y reglamentación.
  - Adaptación para llegar a la IHD “Infraestructura del Hogar Digital”.

cve: BOE-A-2011-10055

6. **Funcionalidades y valores añadidos de la domótica**
   - Funcionalidad de las instalaciones previo a los sistemas domóticos.
   - Aportaciones y mejoras en seguridad.
   - Mejoras en el confort.
   - Eficiencia energética y control de recursos.
   - Comunicación y redes, ocio y multimedia.

7. **Control y gestión de un sistema domótico:**
   - Diseño de una visualización o unidad funcional de control y gestión del sistema.
   - Gestión de la climatización e iluminación.
   - Gestión inteligente de recursos: eficiencia energética.
   - Tratamiento de datos en la red domótica: horarios y eventos.
   - Definición y estudio de necesidades de escenas y macros en un sistema domótico.
   - Descripción y definición de los sistemas de captura de medidas y almacenamiento de datos, consumos e históricos en un sistema domótico.
   - Definición de las funciones lógicas y temporizaciones del sistema domótico.

8. **Simulación del desarrollo de un proyecto domótico 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 domótico como con el resto de sistemas involucrados.
   - Programación del sistema domótico.
   - 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.

UNIDAD FORMATIVA 2

Denominación: CONECTIVIDAD DEL PROYECTO DOMÓTICO: REDES, SISTEMAS Y PROTOCOLOS DE COMUNICACIÓN; PASARELAS

Código: UF1135

Duración: 40 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 y RP3 en lo referente a pasarelas de comunicación.

Capacidades y criterios de evaluación

C1: Dotar de comunicación (monodireccional o bidireccional) a una instalación domótica mediante la configuración y parametrización de las diferentes pasarelas, redes de comunicación y/o sistemas con los que se necesita interacción según las especificaciones y necesidades del proyecto técnico para permitir los servicios y funcionalidades allí definidos.

cve: BOE-A-2011-10055

CE1.1 Identificar las distintas redes del sistema así como las interconexiones entre los elementos de cada una de ellas y las necesidades de comunicación del sistema.
CE1.2 Explicar las características y funcionalidades de las pasarelas de comunicación identificando los diferentes tipos, tecnologías y parámetros de configuración y conexión del sistema domótico con las redes externas.
CE1.3 Describir los servicios que se pueden añadir al sistema domótico/inmótico a través de las pasarelas de comunicación.
CE1.4 En un caso práctico, debidamente caracterizado, configurar y parametrizar y poner en servicio las pasarelas que dotan al sistema domótico/inmótico de conectividad, de acuerdo a especificaciones técnicas.

Contenidos

1. **Relación de las redes de comunicación con la domótica**
   - Descripción de las diferentes redes de comunicación existentes en el mercado.
   - Evaluación de las necesidades del sistema según las indicaciones del proyecto.
   - Valoración de las posibilidades y ventajas de una vivienda / edificio inteligente con capacidad de comunicación bidireccional.

2. **Integración de la domótica con redes de comunicación y otras tecnologías a gestionar y / o monitorizar: Configuración de la/s pasarela/s:**
   - Red TCP/IP (WAN y LAN)
   - Red telefónica RTC
   - Red multimedia – Hogar Digital
   - Red GSM / GPRS
   - Redes PAN: BlueTooth
   - Red IR
   - Integración de cámaras y sistemas de seguridad
   - Tecnologías Inalámbricas
   - Sistemas de proximidad y control de acceso
   - Pasarelas a otras redes de gestión: Iluminación, Clima.
   - Sistemas de Interacción para personas con discapacidades o minusvalías. Parametrización de interfaces de control adaptado del entorno, avisos y vigilancia.
   - Otras tecnologías a considerar

UNIDAD FORMATIVA 3

Denominación: DOCUMENTACIÓN, MANTENIMIENTO Y GESTIÓN DE INCIENCIAS EN UN PROYECTO DOMÓTICO

Código: UF1136

Duración: 30 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP2 y RP4.

Capacidades y criterios de evaluación

C1: Identificar los procedimientos y herramientas de gestión de inventarios, y elaborar y mantener el inventario del sistema domótico/inmótico siguiendo especificaciones dadas.

cve: BOE-A-2011-10055

CE1.1 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.
CE1.2 Describir las características y funcionalidades de las herramientas software que se utilizan para la gestión de inventarios.
CE1.3 Describir los procedimientos de extracción de información a inventariar de los elementos que componen los sistemas domóticos/inmóticos, en función de sus especificaciones técnicas.
CE1.4 En un caso práctico, debidamente caracterizado, elaborar y mantener el 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.
- Realizar pruebas para verificar las funcionalidades del software de control.
- Elaborar el informe de puesta en marcha siguiendo los formatos especificados.

C2: 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.
CE2.1 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.
CE2.2 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.
CE2.3 En un caso práctico, debidamente caracterizado, mantener el sistema domótico/inmótico de acuerdo a 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.

Contenidos

1. Documentación de una instalación domótica/inmótica.
- Uso de Herramientas de generación de informes
- Verificación del estado final de la instalación y actualización del proyecto incluyendo las modificaciones respecto al proyecto original
- Desarrollo del Inventario final de dispositivos y aparatos: Software y Hardware
- Realización de una copia de seguridad y respaldo de configuraciones de los diferentes dispositivos y sistemas integrados en el proyecto.
- Creación y mantenimiento del libro de incidencias
- Creación del manual de usuario de la instalación
- Elaboración de la documentación correspondiente al proyecto que se indique

cve: BOE-A-2011-10055

2. **Mantenimiento de una instalación domótica/inmótica.**
   - Puesta a punto de la instalación y protocolo de pruebas.
   - Mantenimiento de un sistema domótico a Nivel Hardware
   - Mantenimiento de un sistema domótico a Nivel Software
   - Tele-mantenimiento (Programación y mantenimiento a distancia)
   - Mantenimiento de prevención de la instalación mediante gestión domótica.

3. **Gestión de incidencias en una instalación domótica/inmótica.**
   - Detección de fallos en un sistema domótico
   - Localización de problemática debida al hardware:
     - □ Fallo de Dispositivos o conexiones
     - □ Fallos en el medio de transmisión
     - □ Fallos originados por el entorno y la localización del sistema
   - Localización de problemática debida al software:
     - □ Fallos de comunicación y protocolo
     - □ Fallos de funcionalidad
     - □ Estados no evaluados previamente
   - Solución: Procedimientos y recomendaciones para reponer dispositivos (o añadirlos) en la instalación
   - Solución: Procedimientos y recomendaciones para actualizar, modificar software o firmware en la instalación

Orientaciones metodológicas

Formación a distancia:

Unidades formativas	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Unidades formativa 1 – UF1134	80	30
Unidades formativa 2 – UF1135	40	10
Unidades formativa 3 - UF1136	30	20

Secuencia

Para acceder a la unidad formativa 2 debe haberse superado la unidad formativa 1.
Para acceder a la unidad formativa 3 debe haberse superado la unidad formativa 2.

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo

MÓDULO FORMATIVO 3

Denominación: IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEO VIGILANCIA

Código: MF1220_3

cve: BOE-A-2011-10055

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC1220_3 Implantar y mantener sistemas de control de accesos y presencia, y de videovigilancia.

Duración: 220 horas

UNIDAD FORMATIVA 1

Denominación: INSTALACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE VIDEO VIGILANCIA Y SEGURIDAD

Código: UF1137

Duración: 90 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 en lo referente a videovigilancia y con la RP3.

Capacidades y criterios de evaluación

C1: Interpretar las especificaciones técnicas y funcionales del proyecto de instalación del sistema 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 videovigilancia.

CE1.2 Explicar las características, funciones y elementos del análisis de riesgo para llevar a cabo la implantación de un sistema 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 caso práctico, a partir de la documentación técnica que define el proyecto de instalación de videovigilancia, 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 subsistemas, así como los controladores (manejadores de dispositivos o drivers) debidamente actualizados.

C2: Identificar la infraestructura y verificar la instalación del sistema de videovigilancia para su implantación, de acuerdo a especificaciones técnicas.

cve: BOE-A-2011-10055

CE2.1 Identificar los equipos, dispositivos y elementos que componen la infraestructura del sistema de videovigilancia, 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 videovigilancia.
CE2.3 Explicar técnicas de ajuste físico de los equipos, dispositivos y elementos que componen la infraestructura del sistema de videovigilancia, así como las conexiones con otros sistemas o redes de comunicación.
CE2.4 Explicar la necesidad de integrar el sistema de videovigilancia.
CE2.5 En un caso práctico, debidamente caracterizado, verificar la instalación del sistema 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 videovigilancia, 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 videovigilancia, 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 videovigilancia.
CE3.3 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.
CE3.4 Describir la funcionalidad de la aplicación software que centraliza el control del sistema de videovigilancia, identificando los parámetros de instalación y configuración.
CE3.5 Citar la legislación sobre protección de datos a la hora de tratar la información registrada y grabada en el sistema de videovigilancia.
CE3.6 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.
CE3.7 En un caso práctico, debidamente caracterizado, de poner en servicio el sistema de videovigilancia, de acuerdo a las especificaciones del proyecto:
- Identificar los dispositivos y equipos del sistema de videovigilancia.
- Configurar el sistema informático.
- Instalar las aplicaciones software de todo el sistema de videovigilancia.
- Configurar los parámetros del sistema de CCTV en las controladoras.
- Configurar los parámetros del sistema de CCTV 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 las normas marcadas por la LOPD.

CE3.8 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.

cve: BOE-A-2011-10055

Contenidos

1. **Sistemas de videovigilancia**
   - Definición de sistemas de CCTV y video vigilancia
   - Aplicación de los sistemas de video a la seguridad
   - Identificación de los principales campos de aplicación mediante el estudio de casos reales
   - Descripción de la evolución de los sistemas de video vigilancia

2. **Video y tratamiento de la imagen**
   - Definición de los conceptos de luz, imagen y video
   - Descripción de los tipos de lentes y sus características principales
   - Análisis de la señal de video e imagen analógica
     - □ Formación, tratamiento y transmisión de la imagen analógica
     - □ Características y formatos de video analógico
     - □ Ventajas e inconvenientes del video analógico
   - Análisis de la señal de video e imagen Digital
     - □ Formación, tratamiento y transmisión de la imagen digital
     - □ Características y formatos de video analógico
     - □ Ventajas e inconvenientes del video digital
   - Parámetros de evaluación de las señales de video

3. **Sistemas de Video Vigilancia y seguridad Analógicos**
   - Hardware: cámaras y dispositivos de sistema
   - Soporte, cableado y topología del sistema analógico de video vigilancia
   - Configuración, métodos de gestión y visualización en sistemas analógicos
   - Topología, escalabilidad e Infraestructura de un sistema analógico
   - Características del sistema analógico

4. **Sistemas de Video Vigilancia y seguridad Digitales**
   - Hardware: cámaras y dispositivos de sistema
   - Soporte, cableado, tecnologías de transporte y topología del sistema digital de video vigilancia
   - Configuración, métodos de gestión y visualización en sistemas digitales
   - Topología, escalabilidad e Infraestructura de un sistema digital
   - Características del sistema digital y conectividad con otras redes
   - Integración analógica en el mundo digital: Sistemas mixtos

5. **Almacenamiento de la Información obtenida**
   - Sistemas de almacenamiento en formato analógico
   - Sistemas de almacenamiento formato digital
   - Dimensionado del sistema de almacenamiento en función de los requerimientos del proyecto
   - Protección y seguridad de los datos e información aportada por el sistema:
     - □ Protección mediante un sistema de alimentación ininterrumpida los dispositivos de toda la instalación de video vigilancia
     - □ Copias de seguridad y sistemas de prevención de pérdidas de datos
     - □ Redundancia
     - □ Acceso protegido y gestión de privilegios en los sistemas de videovigilancia
     - □ Autentificación de la información. Marca de Agua
     - □ Copias seguridad actualizadas de la información de control del sistema. Accesos, zonas de vigilancia, Bases de datos, horarios, etc.

cve: BOE-A-2011-10055

6. Funcionalidades y Gestión del sistema de Video Vigilancia

- Métodos de Grabación
  - □ A demanda
  - □ Planificada
  - □ Continua
  - □ Por eventos
  - □ Detección de movimiento
- Configuraciones de visualización
- Búsqueda inteligente de eventos
- Generación de eventos
- Seguridad: Gestión de alertas y avisos; Interacción con otros sistemas y/o redes de comunicación o CRA (Centrales receptoras de alarmas)
- Análisis, proceso y obtención de información relevante: Video Inteligente: Video procesado por herramientas de software informático:
  - □ Conteo de personas
  - □ Reconocimiento Facial
  - □ Seguimiento de objetos y personas
  - □ Lector de Matriculas
  - □ Avisos sobre objetos que desaparecen / aparecen
  - □ Análisis de trayectorias y recorridos
  - □ Obtención de informes y estadísticas
  - □ Detección de situaciones anómalas
  - □ Procesado de Imagen
  - □ Otras

7. Planificación del proceso de acometida e implantación de un proyecto de video vigilancia

- Evaluación de las recomendaciones y puntos clave previos a acometer un proyecto de video vigilancia
  - □ Restricciones de los sistemas y de funcionalidad
  - □ Limitaciones de los dispositivos de captación de video, transmisión de video, comunicación y almacenamiento.
  - □ Problemática del medio de comunicación (distancias, interferencias, atenuaciones, etc.)
  - □ Problemática debida al medio y la localización del sistema (entorno)
  - □ Protecciones de los aparatos (Ips)
  - □ Factor Humano
- Evaluación de los niveles de riesgo y tipos de amenazas
- Evaluación de las necesidades de vigilancia y nivel de protección
- Análisis de la situación: ¿Qué hay que vigilar?
- Planteamiento: ¿Cómo y cuándo vigilar? ¿Desde dónde vigilar? ¿Quién ha de vigilar?
- Estructuración del sistema y búsqueda de la ubicación optima de los dispositivos
- Planteamiento de las funcionalidades del sistema
- Integración con otros sistemas y redes: reacciones y posibilidades ante una detección o evento
- Criterios de selección del dispositivos
- 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)
- Comprobación del cumplimiento de la Normativa y reglamentación sobre Seguridad Privada y Ley Orgánica de Protección de Datos

cve: BOE-A-2011-10055

- 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:
  - □ Usada:
    - Proyecto: memoria, planos, pliego de condiciones y requisitos necesarios
    - Proyecto de las instalaciones a Vigilar
    - 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

8. **Simulación del desarrollo de un proyecto de videovigilancia 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 videovigilancia como con el resto de sistemas involucrados
   - Parametrización y ajuste del sistema de videovigilancia
   - 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

UNIDAD FORMATIVA 2

Denominación: INSTALACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE CONTROL DE ACCESOS Y PRESENCIA

Código: UF1138

Duración: 90 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 en lo referente a control de accesos y presencia y con la RP2.

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.

cve: BOE-A-2011-10055

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

cve: BOE-A-2011-10055

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**
   - Definición de los sistemas de control de acceso y presencia. Características más importantes.
   - Valoración de las necesidades y razones para la integración de un sistema de control de accesos y presencia
   - 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.**
   - 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
   - Dispositivos, Sistemas y tecnologías de identificación / autentificación
     - □ Relojes de control y / o tarificación
     - □ Teclados: Códigos y contraseñas de acceso

cve: BOE-A-2011-10055

- □ Lectores de tarjeta
  - Códigos de barra
  - Banda Magnética
- □ Lectores de proximidad
  - Tarjetas o chips de proximidad. Tecnología RFID
  - Bluetooth
  - Otras
- □ Sensores Biométricos e Identidad biométrica; Como identificar a través de rasgos y factores únicos en cada persona
  - Lector de Huella digital
  - 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
  - □ Tarificación 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

cve: BOE-A-2011-10055

- 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 (Ips)
  - □ 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 optima 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:
  - □ Usada:
    - 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.

cve: BOE-A-2011-10055

- 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

UNIDAD FORMATIVA 3

Denominación: MANTENIMIENTO Y GESTIÓN DE INCIDENCIAS EN PROYECTOS DE VIDEO VIGILANCIA, CONTROL DE ACCESOS Y PRESENCIA

Código: UF1139

Duración: 40 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP4.

Capacidades y criterios de evaluación

C1: 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.

CE1.1 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.

CE1.2 Elaborar y actualizar los procedimientos de mantenimiento estableciendo el número de revisiones preventivas y las acciones a realizar en cada revisión del sistema.

CE1.3 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.

CE1.4 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.

CE1.5 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.

CE1.6 En varios casos prácticos simulados, debidamente caracterizados, para el 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.
- Realizar un plan de intervención en el sistema para determinar la causa o causas que producen la avería.

cve: BOE-A-2011-10055

- 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 una adecuada documentación de las mismas (descripción del proceso seguido, medios utilizados, medidas, explicación funcional y esquemas).

Contenidos

1. Procesos de mantenimiento en sistemas de videovigilancia

- Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento de los dispositivos hardware del sistema.
  - □ Mantenimiento de cámaras y dispositivos hardware de tratamiento de video
  - □ Comprobación de dispositivos de interconexión, sujeción, cableado e infraestructura de monitorización y control
  - □ Mantenimiento de sistemas de almacenamiento
  - □ Mantenimiento de los Sistemas de protección y alimentación ininterrumpida o SAI.
- Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento del software del sistema. Verificación de que funciona según los requisitos especificados
  - □ Comprobación del funcionamiento del software de gestión, visualización, grabación y tratamiento de datos del sistema de videovigilancia
  - □ Comprobación de la correcta parametrización a nivel software de los dispositivos del sistema: cámaras, servidores, comunicación, etc.
  - □ Actualización en caso necesario del software de gestión
  - □ Comprobación del sistema de copias de seguridad y el acceso a información del sistema.
  - □ Comprobación del sistema de seguridad, nivel de privilegios y protección del sistema
  - □ Actualización del firmware de los dispositivos que lo requieran
- Comprobación del correcto funcionamiento de integración con los sistemas y redes de comunicación conectados y certificación del cumplimiento de la Ley Orgánica de protección de datos y normativas técnicas.
  - □ Mantenimiento del hardware y dispositivos físicos de comunicación o integración con otras redes:
    - Pasarelas de comunicación
    - Módulos de entradas y salidas interconectadas entre sistemas
  - □ Pruebas y protocolos de evaluación y correcto funcionamiento de la comunicación a nivel software
  - □ Actualizar el sistema para seguir cumpliendo con la normativa técnica y legal en el momento de realizar el mantenimiento en caso de necesitarla
- Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de mantenimiento
- Comprobar que el personal al cargo hace un correcto uso del sistema, en caso negativo, aconsejar alternativas correctas, enseñar o referencias a los manuales de manejo.

cve: BOE-A-2011-10055

2. **Incidencias y alertas en proyectos de video vigilancia**
   - Incidencias de fallos en hardware: Proceso de reinstalación de dispositivos averiados
   - Incidencias de fallos en Software: Proceso de reconfiguración / actualización / sustitución del software de gestión.
   - Tratamiento de errores o alertas de mal funcionamiento.
     - □ Sistemas y herramientas de detección de errores, tanto a nivel de hardware como software
     - □ Procesos de depuración y reconfiguración del sistema
     - □ Prueba y puesta en marcha de la nueva configuración del sistema
   - Incidencias de Modificación del entorno. Adaptación a las nuevas configuraciones.
     - □ Cambio de escenario a vigilar debido a muebles, árboles, arbustos u otros obstáculos físicos para el correcto funcionamiento del sistema.
     - □ Alteración de la estructura a vigilar. Procesos de reposicionamiento y nueva configuración del sistema
     - □ Gestión de cambios en la configuración requerida por la dirección del lugar
   - Avisos, Gestión y modificaciones en remoto del sistema de video vigilancia
   - Generación de la nueva documentación o actualización de la documentación ya existente tras las operaciones de gestión de incidencias
   - Actualización y mejora del estado del sistema de videovigilancia
   - Evaluación del estado del sistema
   - Propuestas de mejora del sistema
   - Aplicación de nuevas funcionalidades: Procesos para la actualización / ampliación / integración del sistema de video vigilancia

3. **Procesos y tareas de mantenimiento en sistemas de control de accesos y presencia**
   - Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento de los dispositivos hardware del sistema.
     - □ Mantenimiento mecánico de los dispositivos físicos de control de accesos: Barreras, puertas, tornos y resto de dispositivos mecánicos del sistema
     - □ Mantenimiento eléctrico y electrónico de las automatizaciones de control: Cerraduras, tarjetas y componentes electrónicos e informáticos del sistema
     - □ Comprobación de los sistemas de identificación y autentificación: Verificar funcionamiento y funcionalidad de teclados, lectores de tarjetas, proximidad, biométricos y resto de dispositivos identificación y autentificación
     - □ Comprobación de Dispositivos de interconexión, sujeción, Cableado e infraestructura de monitorización, avisos y control
     - □ Mantenimiento de Soporte del sistema de Gestión y almacenamiento de datos
     - □ Mantenimiento de los Sistemas de protección y alimentación ininterrumpida o SAI.
   - Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento del software del sistema. Verificación de que funciona según los requisitos especificados
     - □ Comprobación del funcionamiento del software de gestión, monitorización y herramientas de tratamiento de datos, creación de informes y estadísticas, etc. Para que funcionen según las especificaciones de proyecto
     - □ Comprobación la correcta parametrización a nivel software de los dispositivos del sistema
     - □ Actualización en caso necesario del software de gestión
     - □ Comprobación del sistema de copias de seguridad y el acceso a información del sistema.

cve: BOE-A-2011-10055

- □ Comprobación del sistema de seguridad, nivel de privilegios y protección del sistema
- □ Actualización del firmware de los dispositivos que lo requieran

- Comprobación del correcto funcionamiento de integración con los sistemas y redes de comunicación conectados y certificación del cumplimiento de la Ley Orgánica de protección de datos y normativas técnicas.
  - □ Mantenimiento del hardware y dispositivos físicos de comunicación o integración con otras redes:
    - Pasarelas de comunicación
    - Módulos de entradas y salidas interconectadas entre sistemas
  - □ Pruebas y protocolos de evaluación y correcto funcionamiento de la comunicación a nivel software
  - □ Actualizar el sistema para seguir cumpliendo con la normativa técnica y legal en el momento de realizar el mantenimiento en caso de necesitarla
- Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de mantenimiento
- Comprobación que el personal al cargo hace un correcto uso del sistema, en caso negativo, aconsejar alternativas correctas, enseñar o referencias a los manuales de manejo.

4. Gestión de incidencias y alertas

- Incidencias de fallos en hardware: Proceso de Re instalación de dispositivos averiados
- Incidencias de fallos en Software: Proceso de reconfiguración / actualización / sustitución del software de gestión.
- Tratamiento de errores o alertas de mal funcionamiento.
  - □ Sistemas y herramientas de Detección de errores, tanto a nivel de hardware como software
  - □ Procesos de Depuración y reconfiguración del sistema
  - □ Prueba y puesta en marcha de la nueva configuración del sistema
- Incidencias de Modificación del entorno. Adaptación a las nuevas configuraciones.
  - □ Alteración de la estructura a controlar. Procesos de reposicionamiento y nueva configuración del sistema
  - □ Gestión de cambios en la configuración requerida por la dirección del lugar
- Avisos, Gestión y modificaciones en remoto del sistema de control de accesos y presencia
- Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de gestión de incidencias
- Actualización y mejora del estado del sistema de control de accesos
- Evaluación del estado del sistema
- Propuestas de mejora del sistema
- Aplicación de nuevas funcionalidades: Procesos para la actualización / ampliación / integración del sistema de control de accesos

Orientaciones metodológicas

Formación a distancia:

Unidades formativas	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Unidades formativa 1 – UF1137	90	40
Unidades formativa 2 – UF1138	90	40
Unidades formativa 3 – UF1139	40	20

cve: BOE-A-2011-10055

Secuencia

Para acceder a la unidad formativa 3 debe haberse superado la unidad formativa 1 y la 2.

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo

MÓDULO DE PRÁCTICAS PROFESIONALES NO LABORALES IMPLANTACIÓN Y GESTIÓN DE ELEMENTOS INFORMÁTICOS EN SISTEMAS DOMÓTICOS/ INMÓTICOS, DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

Código: MP0236

Duración: 80 horas

Capacidades y criterios de evaluación

C1: Analizar un proyecto de domótica e inmótica, de video vigilancia, y control de accesos y presencia en un caso real.

CE1.1 Analizar los distintos protocolos y procesos llevados a cabo desde el planteamiento inicial de un proyecto hasta su finalización, poniendo especial atención en la forma profesional de realizar todas las operaciones implicadas en el proceso. Tanto desde el punto de vista de hardware (conexiones, empalmes, distribución inteligente de aparatos, precauciones a tomar, etc.) como software, métodos de programación, formas de mejorar la eficiencia de la instalación, etc.
CE1.2 Identificar los dispositivos o los sistemas con los que trabaje la empresa y saber concretar su ámbito de aplicación y las funcionalidades que aportan al proyecto.
CE1.3 Justificar el diseño y la documentación de un proyecto nuevo, ya sea de Domótica y/o Video Vigilancia y/o Control de Accesos y Presencia.
CE1.4 Identificar el conexionado físico de una instalación de acuerdo con la documentación de proyecto.
CE1.5 Participar en la programación de los distintos dispositivos, recibiendo información tutelada mientras se lleva a cabo la puesta a punto de una instalación real.

C2: Proporcionar soporte técnico y gestionar la incidencias en sistemas de Domótica, Video Vigilancia, y Control de Accesos y Presencia.

CE2.1 Reconocer un sistema instalado y en funcionamiento, identificar los diferentes dispositivos que lo componen y la topología que conforman.
CE2.2 Analizar la infraestructura del sistema, las canalizaciones y cableados de alimentación y comunicación de los diferentes dispositivos que forman el sistema.
CE2.3 Detectar el origen de un mal funcionamiento, así como identificar los métodos de reparación realizando las operaciones de sustitución, reconfiguración o integración que fuesen necesarias.
CE2.4 Realizar las tareas de mantenimiento y supervisión periódicas necesarias para el correcto funcionamiento de los sistemas instalados, ayudando a redactar la documentación necesaria.

cve: BOE-A-2011-10055

C3: Actualizar, ampliar e integrar nuevos sistemas o funcionalidades en instalaciones existentes

CE3.1 Aprender a evaluar el impacto que produce en una instalación existente la implementación de un nuevos sistemas o funcionalidades.
CE3.2 Evaluar las necesidades de infraestructura al implementar nuevos sistemas en instalaciones existentes.
CE3.3 Participar en la integración de un nuevo sistema dentro de una instalación existente
CE3.4 Ayudar a evaluar y comprobar el correcto funcionamiento e interacción funcional óptima de los nuevos sistemas con las instalaciones existentes.
CE3.5 Aprender a detectar los posibles conflictos que pueden presentarse al implementar un nuevo sistema con los sistemas ya dispuestos en la instalación.

C4: Participar en los procesos de trabajo de la empresa, siguiendo las normas e instrucciones establecidas en el centro de trabajo.

CE4.1 Comportarse responsablemente tanto en las relaciones humanas como en los trabajos a realizar.
CE4.2 Respetar los procedimientos y normas del centro de trabajo.
CE4.3 Emprender con diligencia las tareas según las instrucciones recibidas, tratando de que se adecuen al ritmo de trabajo de la empresa.
CE4.4 Integrarse en los procesos de producción del centro de trabajo.
CE4.5 Utilizar los canales de comunicación establecidos.
CE4.6 Respetar en todo momento las medidas de prevención de riesgos, salud laboral y protección del medio ambiente.

Contenidos

1. **Desarrollo de nuevos proyectos domoticos e inmóticos**
   - Análisis detallado de los diferentes sistemas que ofrece el mercado con los que trabaja la empresa en cuestión.
   - Utilización de las herramientas necesarias para la instalación de esos sistemas. Tanto hardware como software
   - Análisis de las necesidades, características y peculiaridades de un nuevo proyecto.
   - Desarrollo de los diferentes documentos que conforman el proyecto.
   - Observación del proceso de Instalación y conexión de los diferentes dispositivos.
   - Análisis de la programación y puesta a punto del sistema. Cooperación de manera no intrusiva siguiendo las indicaciones del tutor de empresa
   - Participación en los procesos de detección y gestión de incidencias
   - Participación en la redacción y actualización de la documentación relevante para el proyecto y final de obra.

2. **Mantenimiento de instalaciones domóticas e inmóticas existentes.**
   - Identificación de los sistemas instalados y en funcionamiento. Identificando los diferentes dispositivos y redes que integran el sistema
   - Análisis de la infraestructura de registros, conductos y espacios de reserva que forman la instalación.
   - Análisis de la topología de la red de alimentación y comunicación del sistema.
   - Detección de fallos en el sistema, ya sean de software o hardware.
   - Subsanación de los fallos detectados.
   - Desarrollo de la documentación necesaria para el registro documental del proyecto.
   - Realización de tareas de mantenimiento para el correcto funcionamiento de los sistemas.

cve: BOE-A-2011-10055

- Análisis de las funcionalidades que ofrece un sistema instalado, así como de las posibles mejoras que podrían incorporarse.
- Optimización de las funcionalidades de los diferentes dispositivos.

3. Implantación de nuevos sistemas en instalaciones domóticas e inmóticas
- Compatibilidad entre sistemas existentes y sistemas a implantar.
- Análisis de las necesidades de infraestructura al implementar nuevos sistemas.
- Identificación de los valores añadidos que surgen al implementar nuevos sistemas en combinación con los ya existentes.
- Solución de conflictos entre los sistemas recién implementados y los ya existentes.
- Creación de la documentación necesaria para reflejar correctamente las modificaciones realizadas en la instalación al implementar un nuevo sistema.

4. Integración y comunicación en el centro de trabajo.
- Comportamiento responsable en el centro de trabajo.
- Respeto a los procedimientos y normas del centro de trabajo.
- Interpretación y ejecución con diligencia las instrucciones recibidas.
- Reconocimiento del proceso productivo de la organización.
- Utilización de los canales de comunicación establecidos en el centro de trabajo.
- Adecuación al ritmo de trabajo de la empresa.
- Seguimiento de las normativas de prevención de riesgos, salud laboral y protección del medio ambienta

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	Experiencia profesional requerida en el ámbito de la unidad de competencia
MF0490_3: Gestión de servicios en el sistema informático	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes.	2 años
MF1219_3: Implantación y mantenimiento de sistemas domóticos/inmóticos	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes.	2 años
MF1220_3: Implantación y mantenimiento de sistemas de control de accesos y presencia, y de videovigilancia.	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes.	2 años

cve: BOE-A-2011-10055

V. REQUISITOS MÍNIMOS DE ESPACIOS, INSTALACIONES Y EQUIPAMIENTO

Espacio Formativo	Superficie m² 15 alumnos	Superficie m² 25 alumnos
Aula de gestión	45	60
Taller de comunicaciones	80	150

Espacio Formativo	M1	M2	M3
Aula de gestión	X	X	X
Taller de comunicaciones		X	X

Espacio Formativo	Equipamiento
Aula de gestión	- Equipos audiovisuales - Cañón con proyección - Pantalla para proyección - Rotafolios o pizarra con rotuladores - Ordenador en funciones de servidor para casos prácticos - Ordenadores en funciones de puesto en red para los casos prácticos - Material de aula - Mesa y silla para formador - Mesas y sillas para alumnos
Taller de comunicaciones	- Instrumentos de medida: polímetro, téster de cableado coaxial, certificador de cableado, monitor de vídeo portátil, luxómetro. - Instrumentos de Taller de Electricidad, Electrónica e Informática. - Paneles de trabajo adaptados según el sistema o sistemas domóticos seleccionados para la formación - Equipos para control de accesos y presencia: cabezales lectores de tarjetas (banda magnética, proximidad, chip), lectores biométricos, centrales de control, actuadores (electro cerraduras, barreras), detectores de presencia. - Equipos para sistemas de videovigilancia: cámaras analógicas, cámaras IP, ópticas para las cámaras, cabinas para las cámaras, posicionadores, teclados de control, multiplexores, secuenciadores, grabadores de imagen analógicos y digitales, monitores analógicos y TFT, soportes de grabación (cintas, CD,DVD) - Ordenador configurado específicamente para la impartición de este certificado (del mismo modo que los ordenadores del aula de gestión) - Acceso a Internet, telefónico y conectividad GSM/GPRS/UMTS (tarjetas SIM)

No debe interpretarse que los diversos espacios formativos identificados deban diferenciarse necesariamente mediante cerramientos.

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico sanitaria correspondiente y responderán a medidas de accesibilidad universal y seguridad de los participantes.

El número de unidades que se deben disponer de los utensilios, máquinas y herramientas que se especifican en el equipamiento de los espacios formativos, será el suficiente para un mínimo de 15 alumnos y deberá incrementarse, en su caso, para atender a número superior.

cve: BOE-A-2011-10055

En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

ANEXO V

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: ADMINISTRACIÓN DE SERVICIOS DE INTERNET

Código: IFCT0509

Familia profesional: Informática y Comunicaciones

Área profesional: Sistemas y telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC156_3 Administración de servicios Internet (RD 1087/05, de 16 de septiembre)

Relación de unidades de competencia que configuran el certificado de profesionalidad:

UC0495_3: Instalar, configurar y administrar el software para gestionar un entorno Web.
UC0496_3: Instalar, configurar y administrar servicios de mensajería electrónica.
UC0497_3: Instalar, configurar y administrar servicios de transferencia de archivos y multimedia.
UC0490_3: Gestionar servicios en el sistema informático.

Competencia general:

Instalar, configurar, administrar y mantener servicios comunes de provisión e intercambio de información utilizando los recursos de comunicaciones que ofrece Internet.

Entorno Profesional:

Ámbito profesional:

Desarrolla su actividad profesional en empresas o entidades de naturaleza pública o privada de cualquier tamaño que cuenten con infraestructura de redes intranet, internet o extranet para realizar intercambio de informaciones, la actividad se realiza en el área de sistemas del departamento de informática desempeñando su trabajo tanto por cuenta ajena como por cuenta propia.

Sectores productivos:

Dada la amplia distribución de los servicios de Internet se observa un fundamento transectorial en esta cualificación, con especial relevancia en el sector servicios, ubicándose en los siguientes tipos de empresas:
Organismos públicos y empresas de cualquier sector productivo que por su tamaño y organización necesiten disponer de servicios propios basados en tecnologías de Internet.

cve: BOE-A-2011-10055