

ANEXO

CUALIFICACIÓN PROFESIONAL: IMPLANTACIÓN Y GESTIÓN DE SISTEMAS DOMÓTICOS-INMÓTICOS, DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

Familia Profesional: Informática y Comunicaciones

Nivel: 3

Código: IFC---_3

Competencia general:

Configurar, implantar y mantener 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 elementos que los componen, en condiciones de calidad y seguridad, cumpliendo la normativa y reglamentación vigentes.

Unidades de competencia:

UC0490_3: Gestionar servicios en el sistema informático.

UC2---_3: Implantar y mantener sistemas domóticos/inmóticos.

UC3---_3: Implantar y mantener sistemas de control de accesos y presencia, y de videovigilancia.

Entorno profesional:

Ámbito profesional:

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

Sectores productivos:

Se ubica sobre todo en el sector servicios, 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 y puestos de trabajo relevantes:

Implantador - mantenedor de sistemas domóticos/inmóticos.

Implantador - mantenedor de sistemas de control de accesos y presencia.

Implantador - mantenedor de sistemas de videovigilancia.

Formación asociada: (510 horas)

Módulos Formativos:

MF0490_3: Gestión de servicios en el sistema informático. (90 horas)

MF2---_3: Implantación y mantenimiento de sistemas domóticos/inmóticos. (150 horas)

MF3---_3: Implantación y mantenimiento de sistemas de control de accesos y presencia, y de videovigilancia. (270 horas)

UNIDAD DE COMPETENCIA 1: GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel: 3

Código: UC0490_3

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.

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: IMPLANTAR Y MANTENER SISTEMAS DOMÓTICOS/INMÓTICOS

Nivel: 3

Código: UC1---_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 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 la pasarela residencial, 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 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.

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

RP2: Elaborar 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.

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 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/inmóticos

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.

UNIDAD DE COMPETENCIA 3: IMPLANTAR Y MANTENER SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

Nivel: 3

Código: UC2---_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, portillos 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, 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.

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.

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. 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, 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.

MÓDULO FORMATIVO 1: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel: 3

Código: MF0490_3

Asociado a la UC: 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:

- *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 caso 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 caso 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 caso 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.*

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

Otras capacidades:

- Adaptarse a la organización específica de la empresa integrándose en el sistema de relaciones técnico-laborales.
- Interpretar y ejecutar las instrucciones que recibe y responsabilizarse de la labor que desarrolla, comunicándose de forma eficaz con la persona adecuada en cada momento.
- Organizar y ejecutar la intervención de acuerdo a las instrucciones recibidas, con criterios de calidad y seguridad, aplicando los procedimientos específicos de la empresa.
- Habituar al ritmo de trabajo de la empresa cumpliendo los objetivos de rendimiento diario definidos en la organización.
- Mostrar en todo momento una actitud de respeto hacia los compañeros, procedimientos y

normas internas de la empresa.

Contenidos:

1. Procesos

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

2. Sistemas de almacenamiento

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

3. Gestión de usuarios

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

4. Servicios de comunicaciones

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

Requisitos básicos del contexto formativo:

Espacios e instalaciones:

- Aula de informática de 45 m².

Perfil profesional del formador:

1. Dominio de los conocimientos y las técnicas relacionadas con gestionar servicios en el sistema informático, en lengua propia y extranjera, que se acreditará mediante una de las formas siguientes:
 - Formación académica de Diplomado o Ingeniero Técnico y de otras de superior nivel relacionadas con este campo profesional.
 - Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

MÓDULO FORMATIVO 2: IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS DOMÓTICOS/INMÓTICOS

Nivel: 3

Código: MF2--- 3

Asociado a la UC: Implantar y mantener sistemas domóticos/inmóticos.

Duración: 150 horas.

Capacidades y criterios de evaluación:

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

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

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 de un sistema domótico / inmótico:

- *Identificar los requisitos funcionales del proyecto.*
- *Identificar los elementos del sistema domótico/inmótico, tanto hardware como software.*
- *Comprobar que los elementos del sistema cumplen con los requisitos funcionales.*
- *Verificar visualmente la instalación.*
- *Documentar los trabajos realizados según procedimientos establecidos.*

C2: Describir los parámetros funcionales de los equipos y dispositivos del sistema domótico/inmótico y realizar su puesta en servicio, de acuerdo a las especificaciones técnicas del proyecto.

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

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

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

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

CE2.5 En un 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.*

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

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

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

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

CE3.4 En un 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.*

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

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

CE4.2 Identificar los equipos y el software de control del sistema domótico/inmótico, con sus características y

funcionalidades, incluyendo el estándar domótico o sistema propietario al que pertenecen.

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

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

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

CE4.6 En un 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.*

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

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

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

CE5.3 En un 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.*

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

Otras capacidades:

- Adaptarse a la organización específica de la empresa, integrándose en el sistema de relaciones técnico-laborales.
- Interpretar y ejecutar las instrucciones que recibe y responsabilizarse de la labor que desarrolla, comunicándose de forma eficaz con la persona adecuada en cada momento.
- Organizar y ejecutar las operaciones de acuerdo con las instrucciones recibidas, con criterios de calidad y seguridad, aplicando los procedimientos específicos de la organización.
- Habitarse al ritmo de trabajo de la organización cumpliendo los objetivos de rendimiento diario definidos en la organización.
- Mostrar en todo momento una actitud de respeto hacia los compañeros, procedimientos y normas internas de la organización.
- Interpretar la documentación técnica específica tanto si está editada en castellanos, como en las lenguas oficiales de las Comunidades Autónomas donde se ubique profesionalmente y/o en la lengua extranjera de uso más frecuente en el sector.

Contenidos:

1. Domótica/inmótica

Aspectos generales de la domótica/inmótica: confort, seguridad, ahorro energético, multimedia.

Infraestructura de los sistemas domóticos – inmóticos, pequeñas y grandes instalaciones.

Arquitecturas del sistema de control de un edificio.

Climatización: ventilación, refrigeración y calefacción.

Iluminación: conceptos generales, sistemas de iluminación.

Sistemas de seguridad: intrusión, alarmas técnicas, conexión a CRA.

Componentes de un sistema domótico-inmótico. Sensores, actuadores, transmisores, unidades de control, pasarelas de comunicación.

Topologías de los sistemas domóticos/inmóticos.

Medios físicos de transmisión: par trenzado, corrientes portadoras, radiofrecuencia, infrarrojos, bus compartido, fibra óptica. Conceptos de atenuación, interferencias, velocidad de transmisión.

Proyectos domóticos/inmóticos: documentación y su interpretación.

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

Protocolos en sistemas domóticos/inmóticos:

- Protocolos estandarizados: EIB/KNX, Lonworks, entre otros, herramientas de configuración, programación, visualización y control.
- Sistemas propietarios cableados, herramientas de configuración, programación, visualización y control.
- Sistemas propietarios vía radio, herramientas de configuración, programación, visualización y control.

Otras tecnologías de apoyo a la domótica/inmótica: enocean, zigbee, RFID (RadioFrequency Identification).

Funciones lógicas: puertas, tablas de la verdad, mapas de Karnaugh.

Protocolos TCP/IP : direccionamiento IP, puertos TCP/UDP, protocolos: FTP, TFTP, NTP, http.

Concepto routers, conmutadores, hubs y firewalls.

Técnicas de planificación.

3. Inventarios en sistemas domóticos/inmóticos

Inventarios. Metodologías. Herramientas para la gestión de inventarios.

4. Mantenimiento de sistemas domóticos/inmóticos

Procedimientos de mantenimiento de equipos y dispositivos de sistemas domóticos/inmóticos.

Herramientas software y hardware de diagnóstico: características y usos.

Entorno legal y normativo.

Requisitos básicos del contexto formativo:

Espacios e instalaciones:

- Taller de comunicaciones de 80 m².

Perfil profesional del formador:

1.- Dominio de los conocimientos y las técnicas relacionadas con implantar y mantener sistemas domóticos/inmóticos, que se acreditará mediante una de las formas siguientes:

- Formación académica de Diplomado o Ingeniero Técnico y de otras de superior nivel relacionadas con este campo profesional.
- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo

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

MÓDULO FORMATIVO 3: IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

Nivel: 3

Código: MF3---_3

Asociado a la UC: Implantar y mantener sistemas de control de accesos y presencia, y de videovigilancia.

Duración: 270 horas.

Capacidades y criterios de evaluación:

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

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

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

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

CE1.4 En un 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, y 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. Describir la infraestructura y verificar la instalación de los sistemas de control de accesos y presencia, y de videovigilancia para su implantación, de acuerdo a especificaciones técnicas.

CE2.1 Identificar los equipos, dispositivos y elementos que componen la infraestructura de los sistemas de control de accesos y presencia, y de videovigilancia, así como las conexiones entre los mismos.

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

CE2.3 Explicar técnicas de ajuste físico de los equipos, dispositivos y elementos que componen la infraestructura de los sistemas de control de accesos y presencia, y de videovigilancia, así como las conexiones entre ellos.

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

CE2.5 En un 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: Describir y poner en servicio los equipos y dispositivos del sistema de control de accesos y presencia, así como sus aplicaciones y configuraciones, teniendo en cuenta las especificaciones técnicas asociadas.

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

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

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

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

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

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

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

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

- *Identificar los dispositivos y equipos del sistema.*
- *Configurar el sistema informático.*
- *Instalar las aplicaciones software de todo el sistema de control de accesos y presencia.*
- *Configurar los parámetros del sistema de control de accesos en las controladoras y terminales de control de accesos.*
- *Configurar los parámetros del sistema de control de accesos en los servidores.*
- *Configurar los parámetros del sistema de control de accesos en los portillos.*
- *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.*

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

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

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

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

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

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

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

CE4.7 En un 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.*

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

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

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

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

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

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

CE5.6 En 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.*
- *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).*

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

Otras capacidades:

- Adaptarse a la organización específica de la empresa, integrándose en el sistema de relaciones técnico-laborales.
- Interpretar y ejecutar las instrucciones que recibe y responsabilizarse de la labor que desarrolla, comunicándose de forma eficaz con la persona adecuada en cada momento.
- Organizar y ejecutar las operaciones de acuerdo con las instrucciones recibidas, con criterios de calidad y seguridad, aplicando los procedimientos específicos de la organización.
- Habitarse al ritmo de trabajo de la organización cumpliendo los objetivos de rendimiento diario definidos en la organización.
- Mostrar en todo momento una actitud de respeto hacia los compañeros, procedimientos y normas internas de la organización.
- Interpretar la documentación técnica específica tanto si está editada en castellanos, como en las lenguas oficiales de las Comunidades Autónomas donde se ubique profesionalmente y/o en la lengua extranjera de uso más frecuente en el sector.

Contenidos:

1. El análisis de riesgo

La rueda de seguridad.

La categorización del riesgo.

Los niveles de riesgo.

Los activos a proteger: recursos humanos, bienes tangibles y protección de la información.

Analizando el riesgo de una compañía.

La importancia de la seguridad física en una empresa e integración con los restantes departamentos.

La amenaza de la intrusión: mitigación del riesgo de intrusión.

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

Proyectos y especificaciones.

Documentación técnica de un proyecto: memoria, planos, pliego de condiciones y presupuesto.

Planificación de las tareas propias de un proyecto de seguridad integral.

3. El sistema de seguridad integral y sus componentes

Necesidad de integrar un sistema de seguridad.

El sistema de seguridad integral y sus subsistemas.
Examinando el sistema de control de accesos y presencia.
Examinando el sistema de videovigilancia.
Integrando un sistema de control de accesos y presencia y videovigilancia.
Entorno legal y normativa: LOPD y ley de seguridad privada.

4. Interconexión de los elementos que integran el sistema integral de seguridad

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

5. Sistemas de control de accesos y presencia

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

6. Sistemas de videovigilancia

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

7. Mantenimiento de los sistemas de control de accesos y presencia y videovigilancia

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

Requisitos básicos del contexto formativo:

Espacios e instalaciones:

- Taller de comunicaciones de 80 m².

Perfil profesional del formador:

1.- Dominio de los conocimientos y las técnicas relacionadas con implantar y mantener sistemas de control de accesos y presencia, y de videovigilancia, que se acreditará mediante una de las formas siguientes:

- Formación académica de Diplomado o Ingeniero Técnico y de otras de superior nivel relacionadas

- con este campo profesional.
 - Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo
- 2.- Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes