959 830 780 / 640 798 742

info@inafe.es

IFCT0409 IMPLANTACIÓN Y GESTIÓN DE ELEMENTOS INFORMÁTICOS EN SISTEMAS DOMÓTICOS/INMÓTICOS, DE CONTROL DE ACCESOS Y ...(ONLINE)

500,00 € - 686,00 €

Este curso se ajusta al itinerario formativo del Certificado de Profesionalidad IFCT0409 Implantación y Gestión de Elementos Informáticos en Sistemas Domóticos/Inmóticos, de Control de Accesos y Presencia, y de Videovigilancia certificando el haber superado las distintas Unidades de Competencia en él incluidas, y va dirigido a la acreditación de las Competencias profesionales adquiridas a través de la experiencia laboral y de la formación no formal que permitirá al alumnado adquirir las habilidades profesionales necesarias para gestionar servicios en el sistema informático, así como implantar y mantener sistemas domóticos-inmóticos.

Categorías: Informática y Comunicaciones |

INFORMACIÓN

Duración	540 h

Modalidad	Online
Docencia	TUTOR PERSONAL
Prácticas	GESTIÓN DE PRÁCTICAS EN EMPRESAS
Método de pago	FINANCIACIÓN SIN INTERESES
Centro de empleo	AGENCIA DE COLOCACIÓN
Formación acreditada	CENTRO ACREDITADO POR EL SEPE
Precio	Particular, Empresa

DESCRIPCIÓN DEL PRODUCTO

FICHA TÉCNICA 1 MF0490_3 Gestión de Servicios en el Sistema Informático (Online)

MÓDULO 1. GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

UNIDAD DIDÁCTICA 1. GESTIÓN DE LA SEGURIDAD Y NORMATIVAS

1. Norma ISO 27002 Código de buenas practicas para la gestión de la seguridad de la información
2. Metodología ITIL Librería de infraestructuras de las tecnologías de la información
3. Ley orgánica de protección de datos de carácter personal.
4. Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

UNIDAD DIDÁCTICA 2. ANÁLISIS DE LOS PROCESOS DE SISTEMAS

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

UNIDAD DIDÁCTICA 3. DEMOSTRACIÓN DE SISTEMAS DE ALMACENAMIENTO

1. Tipos de dispositivos de almacenamiento más frecuentes
2. Características de los sistemas de archivo disponibles
3. Organización y estructura general de almacenamiento
4. Herramientas del sistema para gestión de dispositivos de almacenamiento

UNIDAD DIDÁCTICA 4. UTILIZACIÓN DE MÉTRICAS E INDICADORES DE MONITORIZACIÓN DE RENDIMIENTO DE SISTEMAS

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

UNIDAD DIDÁCTICA 5. CONFECCIÓN DEL PROCESO DE MONITORIZACIÓN DE SISTEMAS Y COMUNICACIONES

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

UNIDAD DIDÁCTICA 6. SELECCIÓN DEL SISTEMA DE REGISTRO DE EN FUNCIÓN DE LOS REQUERIMIENTOS DE LA ORGANIZACIÓN

1. Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
2. Análisis de los requerimientos legales en referencia al registro
3. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros

4. Asignación de responsabilidades para la gestión del registro
5. Alternativas de almacenamiento para los registros del sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
6. Guía para la selección del sistema de almacenamiento y custodia de registros

UNIDAD DIDÁCTICA 7. ADMINISTRACIÓN DEL CONTROL DE ACCESOS ADECUADOS DE LOS SISTEMAS DE INFORMACIÓN

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

FICHA TÉCNICA 2 MF1219_3 Implantación y Mantenimiento de Sistemas Domóticos/Inmóticos (Online)

1. MÓDULO 1. IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS DOMÓTICOS/INMÓTICOS

UNIDAD FORMATIVA 1. INSTALACIÓN Y PUESTO EN MARCHA DE UN PROYECTO DOMÓTICO / INMÓTICO

UNIDAD DIDÁCTICA 1. RELACIÓN DE LAS REDES DE COMUNICACIÓN CON LA DOMÓTICA

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

UNIDAD DIDÁCTICA 2. INTEGRACIÓN DE LA DOMÓTICA CON REDES DE COMUNICACIÓN Y OTRAS TECNOLOGÍAS A GESTIONAR Y / O MONITORIZAR: CONFIGURACIÓN DE LA/S PASARELA/S:

1. Red TCP/IP (WAN y LAN)
2. Red telefónica RTC

3. Red multimedia - Hogar Digital
4. Red GSM / GPRS
5. Redes PAN: BlueTooth
6. Red IR
7. Integración de cámaras y sistemas de seguridad
8. Tecnologías Inalámbricas
9. Sistemas de proximidad y control de acceso
10. Pasarelas a otras redes de gestión: Iluminación, Clima.
11. Sistemas de Interacción para personas con discapacidades o minusvalías. Parametrización de interfaces de control adaptado del entorno, avisos y vigilancia.
12. Otras tecnologías a considerar

UNIDAD FORMATIVA 2. CONECTIVIDAD DEL PROYECTO DOMÓTICO: REDES, SISTEMAS Y PROTOCOLOS DE COMUNICACIÓN; PASARELAS.

UNIDAD DIDÁCTICA 1. RELACIÓN DE LAS REDES DE COMUNICACIÓN CON LA DOMÓTICA

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

UNIDAD DIDÁCTICA 2. INTEGRACIÓN DE LA DOMÓTICA CON REDES DE COMUNICACIÓN Y OTRAS TECNOLOGÍAS A GESTIONAR Y / O MONITORIZAR: CONFIGURACIÓN DE LA/S PASARELA/S:

1. Red TCP/IP (WAN y LAN)
2. Red telefónica RTC
3. Red multimedia - Hogar Digital
4. Red GSM / GPRS
5. Redes PAN: BlueTooth
6. Red IR
7. Integración de cámaras y sistemas de seguridad
8. Tecnologías Inalámbricas
9. Sistemas de proximidad y control de acceso
10. Pasarelas a otras redes de gestión: Iluminación, Clima.
11. Sistemas de Interacción para personas con discapacidades o minusvalías. Parametrización de interfaces de control adaptado del entorno, avisos y vigilancia.

12. Otras tecnologías a considerar

UNIDAD FORMATIVA 3. DOCUMENTACIÓN, MANTENIMIENTO Y GESTIÓN DE INCIENCIAS EN UN PROYECTO DOMÓTICO.

UNIDAD DIDÁCTICA 1. DOCUMENTACIÓN DE UNA INSTALACIÓN DOMÓTICA/INMÓTICA.

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

UNIDAD DIDÁCTICA 2. MANTENIMIENTO DE UNA INSTALACIÓN DOMÓTICA/INMÓTICA.

1. Puesta a punto de la instalación y protocolo de pruebas.
2. Mantenimiento de un sistema domótico a Nivel Hardware
3. Mantenimiento de un sistema domótico a Nivel Software
4. Tele-mantenimiento (Programación y mantenimiento a distancia)
5. Mantenimiento de prevención de la instalación mediante gestión domótica.

UNIDAD DIDÁCTICA 3. GESTIÓN DE INCIDENCIAS EN UNA INSTALACIÓN DOMÓTICA/INMÓTICA.

1. Detección de fallos en un sistema domótico
2. Localización de problemática debida al hardware:
3. Fallo de Dispositivos o conexiones
4. Fallos en el medio de transmisión
5. Fallos originados por el entorno y la localización del sistema
6. Localización de problemática debida al software:
7. Fallos de comunicación y protocolo
8. Fallos de funcionalidad
9. Estados no evaluados previamente
10. Solución: Procedimientos y recomendaciones para reponer dispositivos (o añadirlos) en la instalación

11. Solución: Procedimientos y recomendaciones para actualizar, modificar software o firmware en la instalación

FICHA TÉCNICA 3 MF1220_3 Implantación y Mantenimiento de Sistemas de Control de Accesos y Presencia y de Videovigilancia (Online)

1. MÓDULO 1. IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

UNIDAD FORMATIVA 1. INSTALACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE VIDEO VIGILANCIA Y SEGURIDAD.

UNIDAD DIDÁCTICA 1. SISTEMAS DE VIDEOVIGILANCIA

1. Definición de sistemas de CCTV y video vigilancia
2. Aplicación de los sistemas de video a la seguridad
3. Identificación de los principales campos de aplicación mediante el estudio de casos reales
4. Descripción de la evolución de los sistemas de video vigilancia

UNIDAD DIDÁCTICA 2. VIDEO Y TRATAMIENTO DE LA IMAGEN

1. Definición de los conceptos de luz, imagen y video
2. Descripción de los tipos de lentes y sus características principales
3. Análisis de la señal de vídeo e imagen analógica
4. Formación, tratamiento y transmisión de la imagen analógica
5. Características y formatos de vídeo analógico
6. Ventajas e inconvenientes del vídeo analógico
7. Análisis de la señal de vídeo e imagen Digital
8. Formación, tratamiento y transmisión de la imagen digital
9. Características y formatos de vídeo analógico
10. Ventajas e inconvenientes del vídeo digital
11. Parámetros de evaluación de las señales de video

UNIDAD DIDÁCTICA 3. SISTEMAS DE VIDEO VIGILANCIA Y SEGURIDAD ANALÓGICOS

1. Hardware: cámaras y dispositivos de sistema
2. Soporte, cableado y topología del sistema analógico de vídeo vigilancia
3. Configuración, métodos de gestión y visualización en sistemas analógicos
4. Topología, escalabilidad e Infraestructura de un sistema analógico

5. Características del sistema analógico

UNIDAD DIDÁCTICA 4. SISTEMAS DE VÍDEO VIGILANCIA Y SEGURIDAD DIGITALES

1. Hardware: cámaras y dispositivos de sistema
2. Soporte, cableado, tecnologías de transporte y topología del sistema digital de vídeo vigilancia
3. Configuración, métodos de gestión y visualización en sistemas digitales
4. Topología, escalabilidad e Infraestructura de un sistema digital
5. Características del sistema digital y conectividad con otras redes
6. Integración analógica en el mundo digital: Sistemas mixtos

UNIDAD DIDÁCTICA 5. ALMACENAMIENTO DE LA INFORMACIÓN OBTENIDA

1. Sistemas de almacenamiento en formato analógico
2. Sistemas de almacenamiento formato digital
3. Dimensionado del sistema de almacenamiento en función de los requerimientos del proyecto
4. Protección y seguridad de los datos e información aportada por el sistema:
5. Protección mediante un sistema de alimentación ininterrumpida los dispositivos de toda la instalación de video vigilancia
6. Copias de seguridad y sistemas de prevención de pérdidas de datos
7. Redundancia
8. Acceso protegido y gestión de privilegios en los sistemas de videovigilancia
9. Autentificación de la información. Marca de Agua
10. Copias seguridad actualizadas de la información de control del sistema. Accesos, zonas de vigilancia, Bases de datos, horarios, etc.

UNIDAD DIDÁCTICA 6. FUNCIONALIDADES Y GESTIÓN DEL SISTEMA DE VIDEO VIGILANCIA

1. Métodos de Grabación
2. A demanda
3. Planificada
4. Continua
5. Por eventos
6. Detección de movimiento
7. Configuraciones de visualización
8. Búsqueda inteligente de eventos
9. Generación de eventos
10. Seguridad: Gestión de alertas y avisos; Interacción con otros sistemas y/o redes de

comunicación o CRA (Centrales receptoras de alarmas)
11. Análisis, proceso y obtención de información relevante: Video Inteligente: Video procesado por herramientas de software informático:
12. Conteo de personas
13. Reconocimiento Facial
14. Seguimiento de objetos y personas
15. Lector de Matriculas
16. Avisos sobre objetos que desaparecen / aparecen
17. Análisis de trayectorias y recorridos
18. Obtención de informes y estadísticas
19. Detección de situaciones anómalas
20. Procesado de Imagen
21. Otras

UNIDAD DIDÁCTICA 7. PLANIFICACIÓN DEL PROCESO DE ACOMETIDA E IMPLANTACIÓN DE UN PROYECTO DE VIDEO VIGILANCIA

1. Evaluación de las recomendaciones y puntos clave previos a acometer un proyecto de vídeo vigilancia
2. Restricciones de los sistemas y de funcionalidad
3. Limitaciones de los dispositivos de captación de vídeo, transmisión de vídeo, comunicación y almacenamiento.
4. Problemática del medio de comunicación (distancias, interferencias, atenuaciones, etc.)
5. Problemática debida al medio y la localización del sistema (entorno)
6. Protecciones de los aparatos (Ips)
7. Factor Humano
8. Evaluación de los niveles de riesgo y tipos de amenazas
9. Evaluación de las necesidades de vigilancia y nivel de protección
10. Análisis de la situación: ¿Qué hay que vigilar?
11. Planteamiento: ¿Cómo y cuándo vigilar? ¿Desde dónde vigilar? ¿Quién ha de vigilar?
12. Estructuración del sistema y búsqueda de la ubicación optima de los dispositivos
13. Planteamiento de las funcionalidades del sistema
14. Integración con otros sistemas y redes: reacciones y posibilidades ante una detección o evento
15. Criterios de selección del dispositivos
16. Interpretación y evaluación del proyecto y la infraestructura necesaria para acometerlo
17. Estimación de tiempos de ejecución, recursos y personal necesario
18. Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas)

19. Comprobación del cumplimiento de la Normativa y reglamentación sobre Seguridad Privada y Ley Orgánica de Protección de Datos
20. Configuración del sistema y puesta en marcha tanto del software como del hardware, según las especificaciones y funcionalidades requeridas.
21. Documentación generada o utilizada en el proceso:
22. Usada:
23. Generada

UNIDAD DIDÁCTICA 8. SIMULACIÓN DEL DESARROLLO DE UN PROYECTO DE VIDEOVIGILANCIA SIGUIENDO LAS PAUTAS QUE SE INDIQUEN

1. 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.
2. 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.
3. 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
4. Parametrización y ajuste del sistema de videovigilancia
5. 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.
6. Realización del informe de la puesta en marcha y la documentación necesaria

UNIDAD FORMATIVA 2. INSTALACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE CONTROL DE ACCESOS Y PRESENCIA.

UNIDAD DIDÁCTICA 1. SISTEMAS DE CONTROL DE ACCESO Y PRESENCIA

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

UNIDAD DIDÁCTICA 2. COMPONENTES Y CARACTERÍSTICAS DE LOS SISTEMAS Y DISPOSITIVOS QUE FORMAN EL CONTROL DE ACCESO Y PRESENCIA.

1. Sistemas mecánicos automatizados integrados en la gestión de accesos
2. Electro cerraduras

3. Puertas y Barreras
4. Torniquetes y Tornos
5. Rampas y Elevadores
6. Sistemas diseñados para minusválidos
7. Otros tipos de activaciones o eventos
8. Dispositivos, Sistemas y tecnologías de identificación / autentificación
9. Relojes de control y / o tarificación
10. Teclados: Códigos y contraseñas de acceso
11. Lectores de tarjeta
12. Lectores de proximidad
13. Sensores Biométricos e Identidad biométrica; Como identificar a través de rasgos y factores únicos en cada persona
14. Dispositivos, Software y datos de control del sistema
15. Hardware de control e integración de sistema
16. Conectividad y cableado. Infraestructura, funcionamiento y topología de los sistemas de control de acceso y presencia
17. Punto de gestión y monitorización del sistema:

UNIDAD DIDÁCTICA 3. FUNCIONALIDADES Y APLICACIONES DE LOS SISTEMAS DE CONTROL DE ACCESO Y PRESENCIA

1. 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.
2. Control de horarios y eficiencia en empresas o procesos productivos.
3. Tratamiento de datos:
4. Generación de estadísticas y datos de ocupación
5. Tarificación de servicios y tiempos
6. Sistemas de localización, control y detección de personas en un entorno cerrado; control de errantes no intrusivo
7. Sistemas de control médico, acceso a datos y posibilidad de actualización de información automatizado. (Aplicable o otros procesos similares)
8. Gestión de alarmas y eventos
9. Accesos no deseados
10. Alertas no permitidos o fuera de horario
11. Alarmas de averías o mal funcionamiento del sistema
12. Interacción con otros sistemas y/o redes de comunicación o CRA (Centrales receptoras de alarmas)

13. Soluciones de control logístico y de distribución
14. Soluciones de Gestión de Asistencia a Eventos

UNIDAD DIDÁCTICA 4. PROTECCIÓN Y SEGURIDAD DEL SISTEMA Y DE LOS DATOS E INFORMACIÓN APORTADA POR EL SISTEMA:

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

UNIDAD DIDÁCTICA 5. PROCESO DE ACOMETIDA E IMPLANTACIÓN DE UN PROYECTO DE CONTROL DE ACCESOS Y PRESENCIA

1. Evaluación de las recomendaciones y puntos clave previos a acometer un proyecto de control de accesos y presencia
2. Restricciones de los sistemas y de su funcionalidad
3. Problemática del medio de comunicación (número máximo de dispositivos, distancias, interferencias, atenuaciones, etc.)
4. Problemática debida al medio y la localización del sistema (entorno)
5. Protecciones de los aparatos (Ips)
6. Factor Humano
7. Evaluación de los niveles de riesgo y tipos de amenazas
8. Evaluación de las necesidades y definición del servicio y funcionalidades a implantar
9. Interpretación y evaluación del proyecto y la infraestructura necesaria para acometerlo
10. Estimación de tiempos de ejecución, recursos y personal necesario
11. Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas)
12. Análisis de la situación: ¿Qué accesos hay que controlar?
13. Planteamiento y planificación: ¿Cómo y cuándo se controlan? ¿Desde dónde controlar y gestionar el sistema?
14. Estructuración del sistema y búsqueda de la ubicación optima de los dispositivos
15. Planteamiento de las funcionalidades del sistema
16. Integración con otros sistemas y redes: Reacciones y posibilidades ante una detección o evento

17. Comprobación el cumplimiento de la normativa y reglamentación sobre seguridad privada y Ley Orgánica de Protección de Datos
18. Configuración del sistema y puesta en marcha tanto del software como del hardware, según las especificaciones y funcionalidades requeridas.
19. Documentación generada o utilizada en el proceso:
20. Usada:
21. Generada

UNIDAD DIDÁCTICA 6. SIMULACIÓN DEL DESARROLLO DE UN PROYECTO DE CONTROL DE ACCESOS Y PRESENCIA SIGUIENDO LAS PAUTAS QUE SE INDIQUEN

1. 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.
2. 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.
3. 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
4. Parametrización y ajuste del sistema de control de accesos
5. 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.
6. Realización del informe de la puesta en marcha y la documentación necesaria

UNIDAD FORMATIVA 3. MANTENIMIENTO Y GESTIÓN DE INCIDENCIAS EN PROYECTOS DE VIDEO VIGILANCIA, CONTROL DE ACCESOS Y PRESENCIA.

UNIDAD DIDÁCTICA 1. PROCESOS DE MANTENIMIENTO EN SISTEMAS DE VIDEOVIGILANCIA

1. Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento de los dispositivos hardware del sistema.
2. Mantenimiento de cámaras y dispositivos hardware de tratamiento de vídeo
3. Comprobación de dispositivos de interconexión, sujeción, cableado e infraestructura de monitorización y control
4. Mantenimiento de sistemas de almacenamiento
5. Mantenimiento de los Sistemas de protección y alimentación ininterrumpida o SAI.
6. 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
7. Comprobación del funcionamiento del software de gestión, visualización, grabación y tratamiento de datos del sistema de videovigilancia
8. Comprobación de la correcta parametrización a nivel software de los dispositivos del sistema: cámaras, servidores, comunicación, etc.
9. Actualización en caso necesario del software de gestión
10. Comprobación del sistema de copias de seguridad y el acceso a información del sistema.
11. Comprobación del sistema de seguridad, nivel de privilegios y protección del sistema
12. Actualización del firmware de los dispositivos que lo requieran
13. 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.
14. Mantenimiento del hardware y dispositivos físicos de comunicación o integración con otras redes:
15. Pruebas y protocolos de evaluación y correcto funcionamiento de la comunicación a nivel software
16. Actualizar el sistema para seguir cumpliendo con la normativa técnica y legal en el momento de realizar el mantenimiento en caso de necesitarla
17. Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de mantenimiento
18. 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.

UNIDAD DIDÁCTICA 2. INCIDENCIAS Y ALERTAS EN PROYECTOS DE VIDEO VIGILANCIA

1. Incidencias de fallos en hardware: Proceso de reinstalación de dispositivos averiados
2. Incidencias de fallos en Software: Proceso de reconfiguración / actualización / sustitución del software de gestión.
3. Tratamiento de errores o alertas de mal funcionamiento.
4. Sistemas y herramientas de detección de errores, tanto a nivel de hardware como software
5. Procesos de depuración y reconfiguración del sistema
6. Prueba y puesta en marcha de la nueva configuración del sistema
7. Incidencias de Modificación del entorno. Adaptación a las nuevas configuraciones.
8. Cambio de escenario a vigilar debido a muebles, árboles, arbustos u otros obstáculos físicos para el correcto funcionamiento del sistema.
9. Alteración de la estructura a vigilar. Procesos de reposicionamiento y nueva configuración del sistema
10. Gestión de cambios en la configuración requerida por la dirección del lugar

11. Avisos, Gestión y modificaciones en remoto del sistema de video vigilancia
12. Generación de la nueva documentación o actualización de la documentación ya existente tras las operaciones de gestión de incidencias
13. Actualización y mejora del estado del sistema de videovigilancia
14. Evaluación del estado del sistema
15. Propuestas de mejora del sistema
16. Aplicación de nuevas funcionalidades: Procesos para la actualización / ampliación / integración del sistema de video vigilancia

UNIDAD DIDÁCTICA 3. PROCESOS Y TAREAS DE MANTENIMIENTO EN SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA

1. Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento de los dispositivos hardware del sistema.
2. Mantenimiento mecánico de los dispositivos físicos de control de accesos: Barreras, puertas, tornos y resto de dispositivos mecánicos del sistema
3. Mantenimiento eléctrico y electrónico de las automatizaciones de control: Cerraduras, tarjetas y componentes electrónicos e informáticos del sistema
4. 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
5. Comprobación de Dispositivos de interconexión, sujeción, Cableado e infraestructura de monitorización, avisos y control
6. Mantenimiento de Soporte del sistema de Gestión y almacenamiento de datos
7. Mantenimiento de los Sistemas de protección y alimentación ininterrumpida o SAI.
8. 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
9. 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
10. Comprobación la correcta parametrización a nivel software de los dispositivos del sistema
11. Actualización en caso necesario del software de gestión
12. Comprobación del sistema de copias de seguridad y el acceso a información del sistema.
13. Comprobación del sistema de seguridad, nivel de privilegios y protección del sistema
14. Actualización del firmware de los dispositivos que lo requieran
15. Mantenimiento del hardware y dispositivos físicos de comunicación o integración con otras redes:
16. Pruebas y protocolos de evaluación y correcto funcionamiento de la comunicación a nivel

software

17. Actualizar el sistema para seguir cumpliendo con la normativa técnica y legal en el momento de realizar el mantenimiento en caso de necesitarla
18. Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de mantenimiento
19. 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.

UNIDAD DIDÁCTICA 4. GESTIÓN DE INCIDENCIAS Y ALERTAS

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