IFCT0510 – GESTIÓN DE SISTEMAS INFORMÁTICOS.

FECHA INICIO: 01/06/2016 **FECHA FIN**: 18/11/2016

HORAS: 500 (420 TEORÍA + 80 PRÁCTICAS) **HORARIO**: 9:00 – 14:00 (DE LUNES A VIERNES)

TEORÍA: FECHA INICIO: 01/06/2016 FECHA FIN: 25/10/2016

PRÁCTICAS: FECHA INICIO: 26/10/2016 FECHA FIN: 18/11/2016

PERIODO VACACIONAL: 29/07/2016 – 28/08/2016 (ambas fechas incluidas)

PLAZO ENTREGA SOLICITUD: Hasta el 23/05/2016 (inclusive)

DOCUMENTACIÓN A ENTREGAR: SOLICITUD (se entrega en el centro de formación)

COPIA DE: DNI, SS, TITULACIÓN, TARJETA DESEMPELO.

SESIÓN INFORMATIVA: 24/05/2016

REQUISITOS IMPRESCIDIBLES: Menor de 30 años.

Estar en posesión del Bachiller o equivalente

Estar Inscrito como demandantes de empleo en el SAE

COLECTIVOS PRIORITARIOS: Baja cualificación

Desempleados de larga duración

Personas que no hayan accedido a su primer empleo.

Personas procedentes del Plan Prepara

CONTENIDOS

MÓDULO	Nº HORAS	FECHA INCIO	FECHA FIN
MF0484: Administración hardware de un sistema informático	120	01/06/2016	04/07/2016
MF0485: Administración software de un sistema informático	210	05/07/2016	29/09/2016
MF0486: Seguridad en equipos informáticos	90	30/09/2016	25/10/2016
MP0398: Módulo de prácticas profesionales no laborales de Gestión de sistemas informáticos	80	26/10/2016	18/11/2016

COMPETENCIA GENERAL:

Configurar, administrar y mantener un sistema informático a nivel de hardware y software, garantizando la disponibilidad, óptimo rendimiento, funcionalidad e integridad de los servicios y recursos del sistema.

CONTENIDOS DE LA ACCIÓN FORMATIVA

Certificado de Profesionalidad denominado "GESTIÓN DE SISTEMAS INFORMÁTICOS".

Código: IFCT0510

Nivel de cualificación profesional: 3

Entorno Profesional:

Ámbito profesional:

Desarrolla su actividad profesional en empresas o entidades de naturaleza pública o privada de cualquier tamaño en el área de sistemas del departamento de informática.

Sectores productivos:

Se sitúa en todos los sectores del tejido empresarial dada su característica de transectorialidad que sobreviene de la necesidad de las organizaciones de tratar y administrar su información estén en el sector que estén. También está presente en los siguientes tipos de empresas:
Empresas o entidades de cualquier tamaño que utilizan sistemas informáticos para su gestión y que pueden estar enmarcadas en cualquier sector productivo.
Empresas dedicadas a la comercialización de equipos informáticos.
Empresas que prestan servicios de asistencia técnica informática.

Ocupaciones o puestos de trabajo relacionados:

2721.1018 Administrador de sistemas de redes
Administrador de sistemas.
Responsable de informática.

CONTENIDOS

MF0484_3 - ADMINISTRACIÓN HARDWARE DE UN SISTEMA INFORMÁTICO.

UF1891 - DIMENSIONAR, INSTALAR Y OPTIMIZAR EL HARDWARE

1. Clasificar e inventariar el hardware
   - → Identificar y clasificar el hardware:
     - * Conocer los distintos tipos de hardware según finalidad.
     - * Conocer la arquitectura de servidores y PCs.
     - * Diferenciar los componentes identificando sus funciones.
     - * Clasificar los componentes según características, utilidad, y propósito.
     - * Instalar y sustituir componentes en un sistema informáticos, atendiendo a la documentación del fabricante y a las normas de la organización.
   - → Establecer la conectividad del hardware:
     - * Diferenciar los diferentes buses de comunicación en un sistema informático.
     - * Distinguir los distintos tipos de conectividad con los dispositivos periféricos.
     - * Identificar los distintos tipos de conectividad y tecnologías de conectividad entre los elementos hardware que componen la arquitectura de una plataforma para la prestación de un servicio.
     - * Establecer la conectividad entre PCs y/o servidores.
     - * Conectar los servidores con equipos de almacenamiento externo.
     - * Diseñar la conexión con equipos de copia de seguridad.
     - * Establecer la conexión con Internet.
     - * Elegir e instalar el controlador de entrada/salida más adecuado según la finalidad perseguida.
   - → Documentar e inventariar el hardware:
     - * Enumerar los equipos detallando componentes, estado, y ubicación.
     - * Documentar las configuraciones y parametrizaciones.
     - * Documentar las conectividades.

- Etiquetar el hardware.

→ Mantener el inventario:
- Actualizarlo con las altas, bajas, y modificaciones.
- Auditar el inventario.

2. Monitorizar el rendimiento

→ Diseñar la monitorización:
- Distinguir los distintos tipos de monitorizaciones según su finalidad. Diseñar la monitorización externa para garantizar la disponibilidad del sistema y diseñar la monitorización para la gestión de capacidad del sistema.
- Seleccionar técnicas o herramientas en función de las características del hardware.
- Definir parámetros a monitorizar. Conocer los parámetros habituales a monitorizar.
- Monitorizar la CPU, RAM, y discos del sistema.
- Monitorizar la conectividad.
- Monitorizar los servicios.
- Seleccionar los elementos a monitorizar y los umbrales de aviso según los procedimientos definidos por la organización.
- Establecer las alertas: Configurar alertas ante la indisponibilidad de servicio y configurar alertas para garantizar la correcta gestión de capacidad según los procedimientos definidos en la organización.

→ Monitorizar el sistema:
- Obtener estadísticas de rendimiento.
- Interpretar correctamente los informes gráficos de uso.

→ Diagnosticar el estado del sistema:
- Analizar el rendimiento: Comparar los valores obtenidos con el histórico de uso del sistema y localizar los cuellos de botella del sistema.
- Proponer mejoras.
- Evaluar la viabilidad de sustitución o ampliación de los elementos hardware que causan los cuellos de botella, por otros de superior rendimiento que cumplan la misma función.
- Evaluar alternativas de diseño a la arquitectura que se adecuen mejor a las necesidades de rendimiento del sistema.
- Optimizar la parametrización para implementar un mejor rendimiento:
- Revisar la configuración de la BIOS del sistema.
- Revisar la documentación del fabricante en busca de nuevas versiones de firmware que obtengan mejor rendimiento.

3. Diseñar e implementar arquitecturas tolerantes a fallos

→ Instalar los elementos hardware del sistema atendiendo a las especificaciones del fabricante y a las normas de la organización.

→ Verificar el correcto funcionamiento del sistema tras su instalación.

→ Diseñar los puntos de tolerancia a fallos del sistema:
- Definir e implementar la tolerancia a fallos eléctricos.
- Definir e implementar la tolerancia a fallos de disco, y de conectividad.

→ Conocer los procedimientos de respaldo y de recuperación de fallos definidos en la empresa:
- Externalizar y salvaguardar las copias según los procedimientos vigentes en la organización.
- Facilitar a los técnicos de copias de seguridad los soportes que contiene las copias necesarias para la restauración del servicio.
- Instalar y configurar la arquitectura hardware necesaria para la instalación del sistema de copias de seguridad.

→ Conocer arquitecturas que permiten mayor tolerancia a fallos:
- Conocer el concepto de sistemas en cluster.
- Diseñar e implementar la arquitectura hardware necesaria para la instalación de un cluster. Implementar la arquitectura hardware necesaria para la instalación de un cluster de base de datos.
- Conocer el concepto de sistemas balanceados por red.

4. Diagnosticar y resolver las averías
   - → Consultar la documentación del fabricante y la documentación interna de la organización, así como al servicio de asistencia técnica del fabricante, o de terceros con los que la organización tenga contrato de mantenimiento, en busca del origen y resolución de incidentes.
   - → Utilizar las herramientas de diagnóstico y documentación facilitadas por el fabricante.
   - → Planificar y ejecutar la reparación acorde a la documentación del fabricante y a los procedimientos internos.
   - → Planificar y ejecutar la reparación garantizando la integridad de la información, y minimizando el impacto sobre la disponibilidad de servicio:
     - * Poner en marcha los mecanismos definidos en la organización para mantener el servicio mientras se procede la sustitución o reparación.
     - * Sustituir o reparar el componente averiado atendiendo a las especificaciones del fabricante.
     - * Verificar el correcto funcionamiento del sistema tras la sustitución de los componentes averiados.
     - * Restablecer la normal explotación del servicio.
   - → Conocer e interpretar adecuadamente los planes de recuperación de servicio existentes en la empresa.

UF1892 - GESTIONAR EL CRECIMIENTO Y LAS CONDICIONES AMBIENTALES

1. Gestionar el crecimiento
   - → Planificar las ampliaciones. Dimensionar los crecimientos futuros:
     - * Extrapolar de las mediciones de la plataforma en producción.
     - * Simular con modelos matemáticos las nuevas cargas previstas.
     - * Evaluar si las nuevas cargas previstas son asumibles en la plataforma actual.
   - → Analizar el mercado en busca de las soluciones hardware que ofrece:
     - * Conocer el catálogo de productos de los principales fabricantes.
     - * Seleccionar el producto más adecuado.
     - * Identificar correctamente los distintos tipos de hardware.
     - * Conocer las orientaciones de precios.
     - * Razonar la propuesta equilibrando la componente técnica y la económica.
   - → Localizar a los prescriptores de mercado:
     - * Utilizar los informes comparativos como apoyo a la elección de hardware.
     - * Utilizar los informes de tendencias como apoyo a la elección de hardware.
   - → Ejecutar las ampliaciones garantizando la mayor disponibilidad del servicio.

2. Establecer las condiciones ambientales adecuadas
   - → Conocer los factores ambientales que pueden afectar al funcionamiento de la instalación:
     - * Identificar los factores que afectan a los equipos informáticos.
     - * Identificar los factores que afectan a las comunicaciones.
   - → Interpretar adecuadamente las necesidades ambientales del hardware.
     - * Identificar los parámetros críticos ambientales para el correcto funcionamiento del hardware: Establecer mediciones de temperatura, humedad, y presión, y establecer mediciones de ruidos, vibraciones, y campos electromagnéticos.
     - * Revisar especificaciones de los fabricantes del hardware.
     - * Establecer rangos de uso de los parámetros para el equipamiento.
   - → Comprobar la calidad del suministro industrial:
     - * Comprobar la instalación eléctrica: Comprobar que la capacidad de la instalación eléctrica cumplen con los valores esperados de consumo y comprobar conexión del equipamiento a circuitos filtrados por SAIs.

        - Comprobar la instalación de refrigeración: Revisar las especificaciones del acondicionamiento de frío y comprobar que cumple con los requerimientos de refrigeración esperados en base a las especificaciones técnicas del equipamiento hardware.
    - → Diseñar la ubicación de los equipos en la sala:
        - Diseñar de la distribución.
        - Elegir el emplazamiento de los diferentes equipos hardware.

MF0485_3 - ADMINISTRACIÓN SOFTWARE DE UN SISTEMA INFORMÁTICO
UF1893 - INSTALACIÓN Y PARAMETRIZACIÓN DEL SOFTWARE

1. Software
    - → Conocer y comprender qué es el software, y para qué sirve.
    - → Distinguir software, de firmware, y de hardware.
    - → Identificar los diferentes tipos de software.

2. Sistemas Operativos
    - → Comprender la definición y utilidad de los sistemas operativos:
        - Enumerar las funciones de un sistema operativo.
        - Conocer la evolución histórica de los sistemas operativos.
        - Distinguir los diferentes componentes de un sistema operativo.
        - Comprender la gestión de procesos.
        - Distinguir los diferentes tipos de sistemas de archivos.
        - Conocer los sistemas de entrada/salida.
        - Conocer el uso de controladores para la gestión de hardware.
        - Distinguir los parámetros habituales a configurar y sus valores típicos.
        - Conocer los servicios habituales y su finalidad.
        - Conocer la utilidad de usuarios y grupos de usuarios, así como los de uso habitual.
    - → Identificar los distintos tipos de sistemas operativos, describiendo sus funciones y estructura.
    - → Clasificar los sistemas operativos:
        - Clasificar los sistemas operativos según propósito.
        - Clasificar los sistemas operativos según su grado de implantación.
        - Sistemas operativos monousuario y multiusuario.
        - Sistemas operativos monotarea y multitarea.
        - Sistemas operativos distribuidos.
        - Sistemas operativos en tiempo real.
    - → Conocer las políticas definidas en la organización, de aplicación en la instalación del sistema operativo.
    - → Instalar y parametrizar los sistemas operativos:
        - Realizar los preparativos previos a la instalación.
        - Recolectar los controladores necesarios.
        - Definir el tipo de sistema de archivo a utilizar, seleccionándolo de entre las posibles alternativas, en base a las necesidades del uso previsto.
        - Definir los valores de los parámetros habituales a configurar.
        - Instalar el sistema operativo, configurando el hardware con los controladores adecuados, que garanticen el correcto funcionamiento del sistema:
            - ✓ Instalar manualmente el sistema operativo.
            - ✓ Instalar desatendidamente el sistema operativo.
            - ✓ Instalar automáticamente el sistema operativo.

- ✓ Clonar servidores.
- ✓ Configurar la red.
- ✓ Comprobar la correcta instalación del sistema operativo mediante pruebas de arranque y parada, y herramientas de diagnóstico.
- ✓ Actualizar el sistema operativo.

→ Conocer y utilizar adecuadamente las herramientas de gestión del sistema operativo, de uso habitual:
- * Conocer y utilizar las herramientas de gestión de grupos y usuarios.
- * Conocer y utilizar correctamente las herramientas de gestión de permisos del sistema de archivos.
- * Conocer y utilizar correctamente las herramientas de configuración y diagnóstico de red.
- * Conocer y utilizar correctamente las herramientas de gestión de servicios.
- * Conocer y utilizar correctamente las herramientas de monitorización del sistemas facilitadas por el fabricante del sistema.

→ Securizar el sistema atendiendo a las normas definidas:
- * Establecer la configuración inicial de usuarios y grupos.
- * Configurar los permisos en el sistema de archivos.
- * Configurar los permisos en el registro de configuraciones.
- * Establecer los permisos en la configuración de red.
- * Revisar y desinstalar o deshabilitar los servicios innecesarios.

→ Documentar la instalación:
- * Registrar el proceso y las incidencias habidas, así como las medidas adoptadas para su resolución.
- * Detallar los valores de los parámetros establecidos.

3. Software de aplicación

→ Distinguir entre los distintos tipos de software de aplicación atendiendo a su uso:
- * Conocer los distintos paquetes ofimáticos de uso habitual.
- * Distinguir las distintas funcionalidades que son capaces de prestar las herramientas colaborativas.
- * Conocer la necesidad de servicio que cubre el software ERP.
- * Conocer la necesidad de servicio que cubre el software CRM.

→ Conocer las políticas definidas en la organización, de aplicación en la elección e instalación del software de aplicación:
- * Comprobar la autorización de la instalación.
- * Utilizar adecuadamente las listas de aplicaciones permitidas.
- * Registrar la instalación realizada.

→ Instalar el software de aplicación, atendiendo a las recomendaciones del fabricante, y a las normas de seguridad de la organización:
- * Comprobar los requisitos del software de manera previa a la instalación.
- * Seguir las instrucciones de instalación dadas por el fabricante.
- * Actualizar el software de aplicación.

→ Comprobar el correcto funcionamiento del software de aplicación.

→ Desplegar masiva y desatendidamente software de aplicación.

4. Automatizaciones

→ Conocer los diferentes lenguajes de programación de uso habitual para la automatización de tareas:
- * Distinguir el entorno nativo de cada lenguaje de programación.

→ Utilizar un editor adecuado para el desarrollo del código.

→ Desarrollar pequeños scripts para la ejecución de tareas de mantenimiento:

- Conocer los diferentes lenguajes de programación de uso más común utilizables en cada sistema operativo.
- Conocer los comandos y estructuras de los lenguajes de scripting.
- Utilizar adecuadamente la documentación de consulta de los lenguajes de scripting, para facilitar la correcta escritura del código.
- Programar scripts para la ejecución de tareas de mantenimiento.

→ Seleccionar el lenguaje de programación más adecuado en función de los requisitos de la tarea a automatizar y del sistema operativo sobre el que se deba ejecutar.

→ Configurar la ejecución automática de la tarea en el sistema operativo:
- Establecer el horario y frecuencia más adecuados.
- Configurar la ejecución en el sistema comprobando su correcta ejecución, y resultados.

→ Utilizar herramientas de automatización.

5. Inventario de sw

→ Seleccionar adecuadamente los parámetros a inventariar en un sistema.

→ Gestionar las licencias:
- Inventariar las licencias compradas.
- Inventariar las licencias instaladas.
- Realizar un plan de compra de licencias en base al crecimiento estimado y los modelos de licenciamiento del software utilizado.

→ Gestionar herramientas de inventariado:
- Utilizar adecuadamente herramientas de inventario para extraer informes de licencias en uso, y de licencias compradas.
- Mantener al día el inventario.
- Utilizar herramientas de inventariado automático.

→ Inventariar la configuración base y de aplicación.

→ Actualizar la lista de aplicaciones permitidas por usuario.

UF1894 - MANTENIMIENTO DEL SOFTWARE

1. Planes de mantenimiento

→ Conocer la utilidad y funciones de los planes de mantenimiento:
- Mantener actualizado el software.
- Gestionar el antivirus.
- Formar a los usuarios en las labores de mantenimiento que deben realizar.
- Optimizar el sistema de archivos.

→ Diseñar, desarrollar y documentar el plan de mantenimiento:
- Diseñar los mantenimientos proactivos.
- Documentar los mantenimientos reactivos.

→ Gestionar los problemas frecuentes:
- Localizar y documentar los problemas frecuentes.
- Resolver los casos de problemas frecuentes.
- Dotar a los usuarios de medios para solucionar por sus propios medios los problemas frecuentes.
- Atajar la causa raíz de los problemas frecuentes.

→ Utilizar el conocimiento adquirido con la experiencia:
- Consultar las bases de datos de conocimiento acorde con las normas establecidas en la organización.
- Actualizar las base de datos de conocimiento con nueva información derivada de las actividades de mantenimiento.

→ Atender al usuario:
- Registrar las solicitudes de los usuarios, estableciendo una correcta priorización en su resolución.
- Informar al usuario del estado de resolución de su solicitud y del tiempo estimado de resolución de la misma.

- Formar al usuario en los procedimientos y canales adecuados para la solicitud de servicio y notificación de incidente, así como en las posibles soluciones a aplicar ante la aparición de problemas frecuentes.

→ Actualizar el sistema, manteniéndolo al día en las versiones adecuadas a las funcionalidades requeridas por las necesidades, y a los requisitos de seguridad del sistema:
- Actualizar el sistema operativo.
- Actualizar las aplicaciones.
- Parchear el sistema operativo.
- Parchear las aplicaciones.

2. Optimización del uso de los recursos

→ Comprobar la adecuación del rendimiento del sistema a las necesidades de la organización:
- Seleccionar los parámetros a medir para comprobar el rendimiento del sistema.
- Establecer la monitorización necesaria para medir el rendimiento del sistema.
- Representar gráficamente el rendimiento del sistema, interpretándolo, y estableciendo la adecuación o no a las necesidades de la organización.
- Proponer las mejoras necesarias para el incremento del rendimiento.

→ Utilizar las herramientas de modelado para predecir el rendimiento del sistema en base a las previsiones de incremento de carga del sistema.

→ Realizar pruebas de carga para comprobar la escalabilidad del sistema y su adecuación a las necesidades presentes y futuras de la organización:
- Seleccionar las herramientas adecuadas para la realización de las pruebas de carga en función de los servicios a prestar.
- Diseñar e implementar el plan de pruebas de carga.
- Realizar las pruebas de carga sin provocar problemas de disponibilidad de servicio en el sistema en producción.
- Representar e interpretar el resultado de las pruebas de carga.

UF1895 - AUDITORÍAS Y CONTINUIDAD DE NEGOCIO

1. Copias de respaldo

→ Tipificar los datos según sus necesidades de copia.

→ Diferenciar los distintos tipos de copias, distinguiendo las diferencias entre copias completas, incrementales, y diferenciales, así como las ventajas e inconvenientes de cada una de ellas, y las combinaciones más habituales de las mismas.

→ Establecer correctamente los periodos de retención acordes con las normas de seguridad de la empresa, con las necesidades según el tipo de datos, y con la legislación vigente.

→ Dimensionar las copias de seguridad:
- Establecer el tamaño de copia completa acorde con los datos a copiar y la ocupación estimada en el dispositivo de copias.
- Establecer el tamaño de las copias en función del tiempo, acorde con la política de copias a utilizar.

→ Establecer la política de copias de la organización:
- Definir el plan de copias indicando cada tipo de copia a realizar, la hora de programación, la ventana de copia, el periodo de retención.
- Revisar la adecuación de la política de copias a las normas de la organización, así como a la legalidad vigente.

→ Proponer los dispositivos de copia y soportes más adecuados en base a las necesidades de la organización:
- Conocer las distintas alternativas posibles para los dispositivos de copia.
- Razonar la mejor adecuación de cada alternativa a las necesidades de la organización.

→ Realizar las copias de seguridad según los procedimientos y políticas vigentes en la organización:
- Implementar y configurar las copias de seguridad.
- Programar y ejecutar las copias de seguridad.

- Verificar las copias de seguridad mediante restauraciones, documentando los tiempos de restauración y el resultado obtenido.

→ Gestionar el ciclo de vida de los soportes:
- Salvaguardar los soportes de copia, manteniéndolos en condiciones óptimas para su conservación.
- Externalizar las copias.
- Destruir los soportes tras su ciclo de vida útil de manera acorde con las normas de seguridad de la empresa, garantizando la imposibilidad de extracción de información de los mismos.

→ Documentación de planes de recuperación:
- Diseñar los pasos a seguir para la completa restauración de un sistema en producción.
- Documentar las restauraciones a realizar para el restablecimiento de un sistema en producción, tras un problema mayor.

2. Legislación vigente
   → Conocer las Leyes vigentes relacionadas con el tratamiento de datos:
   - Legislación vigente en materia de protección de datos de carácter personal.
   - Legislación vigente en materia de comercio electrónico.
   - Legislación vigente en materia de protección de la propiedad intelectual.

   → Enumerar los puntos principales a tener en cuenta.

3. Alternativas a las copias.
   → Distinguir entre salvaguarda de datos, y disponibilidad del servicio.
   → Enumerar las alternativas para garantizar la disponibilidad del servicio:
   - Diseñar alternativas en cluster.
   - Diseñar alternativas basadas en almacenamiento externo.
   - Diseñar alternativas basadas en copias de imágenes.

   → Indicar ventajas e inconvenientes de las alternativas para garantizar la disponibilidad del servicio sobre las copias de seguridad.

4. Planes de auditoría.
   → Describir los objetivos de los planes de auditoría:
   - Distinguir entre las auditorías por su tipo y aplicación (de rendimiento, de seguridad, de mejora continua, de optimización de uso)

   → Describir el perfil del auditor.
   → Auditar el sistema:
   - Diseñar el plan de auditoría.
   - Utilizar herramientas de auditoría.
   - Documentar el resultado de la auditoría.

MF0486_3 - SEGURIDAD EN EQUIPOS INFORMÁTICOS

1. Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos
   → Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
   → Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
   → Salvaguardas y tecnologías de seguridad más habituales
   → La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

2. Análisis de impacto de negocio
   → Identificación de procesos de negocio soportados por sistemas de información.
   → Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio

→ Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad.

3. Gestión de riesgos
   → Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
   → Metodologías comúnmente aceptadas de identificación y análisis de riesgos
   → Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

4. Plan de implantación de seguridad
   → Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio
   → Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información.
   → Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas.

5. Protección de datos de carácter personal
   → Principios generales de protección de datos de carácter personal
   → Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
   → Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización.
   → Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

6. Seguridad física e industrial de los sistemas. Seguridad lógica de sistemas
   → Determinación de los perímetros de seguridad física
   → Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
   → Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
   → Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
   → Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
   → Elaboración de la normativa de seguridad física e industrial para la organización.
   → Sistemas de ficheros más frecuentemente utilizados
   → Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización.
   → Configuración de políticas y directivas del directorio de usuarios
   → Establecimiento de las listas de control de acceso (ACLs) a ficheros
   → Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
   → Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
   → Sistemas de autenticación de usuarios débiles, fuertes y biométricos
   → Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
   → Elaboración de la normativa de control de accesos a los sistemas informáticos

7. Identificación de servicios
   → Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información.
   → Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
   → Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

8. Robustecimiento de sistemas
   - → Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información.
   - → Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
   - → Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
   - → Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
   - → Actualización de parches de seguridad de los sistemas informáticos
   - → Protección de los sistemas de información frente a código malicioso
   - → Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
   - → Monitorización de la seguridad y el uso adecuado de los sistemas de información.

9. Implantación y configuración de cortafuegos
   - → Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
   - → Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
   - → Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
   - → Definición de reglas de corte en los cortafuegos
   - → Relación de los registros de auditoría del cortafuegos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
   - → Establecimiento de la monitorización y pruebas del cortafuegos

MP0398 - MÓDULO DE PRÁCTICAS PROFESIONALES NO LABORALES DE GESTIÓN DE SISTEMAS INFORMÁTICOS

1. Puesta en producción de nuevos sistemas
   - → Revisión de la documentación de instalación de sistemas y sugerir posibles mejoras sobre la misma.
   - → Instalación de servidores de manera acorde a las normas de la organización.
   - → Instalación de software de aplicación sobre los servidores.
   - → Desinstalación los servicios en desuso.
   - → Establecimiento la seguridad a nivel de servidor sobre los servidores instalados.
   - → Diseño y configurar la monitorización de los sistemas instalados.
   - → Configuración de la auditoría del sistema acorde a las normas de la organización.
   - → Inventario de los nuevos sistemas puestos en producción.
   - → Configuración de copias de seguridad de los sistemas instalados.

2. Monitorización y rendimiento de sistemas
   - → Revisión de la documentación de monitorización de rendimiento y capacidad de los sistemas en producción.
   - → Revisión de la documentación de monitorización de consumo eléctrico y medioambiental de los sistemas en producción.
   - → Revisión de la documentación de auditoría de los sistemas en producción.
   - → Comportamiento de los sistemas en producción en base a las cargas de trabajo futuras esperadas.

3. Atender a los usuarios
   - → Revisión de la documentación de soporte a usuarios corporativos.
   - → Atención a los usuarios corporativos.
   - → Mejoras a los procedimientos y documentación de atención a usuarios. Copias de seguridad y restauración de servicio

4. Integración y comunicación en el centro de trabajo
   - → Revisión de la documentación de copias de seguridad de la organización.
   - → Procedimientos de recuperación de servidores de producción sobre equipos de pruebas, y documentar los resultados, proponiendo mejoras sobre dichos procedimientos y/o sobre las políticas de copias.

5. 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 ambiente.