PROCEDIMIENTO Nº AB1/2024 PARA LA CONTRATACIÓN DE PLATAFORMA DE TELEFORMACIÓN CON SERVICIO DE ASISTENCIA Y CONTENIDOS FORMATIVOS DEL PROYECTO " COMPETENCIAS DIGITALES PARA LA CIUDADANÍA EN ESPACIOS CONESPECIALES DIFICULTADES DEMOGRÁFICAS

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Definidas en el cuadro resumen de contratación y en el Pliego de Cláusulas particulares y condiciones de la contratación las obligaciones del contratista y sus responsabilidades en la ejecución del contrato constituyen las especificaciones contenidas en este Pliego de prescripciones técnicas el detalle de las particularidades que habrán de regir el abastecimiento de los suministros objeto del procedimiento.

1. **Suministro de plataforma de teleformación y Servicio de asistencia técnica (LOTE 1)**

El proyecto consiste en formar en competencias digitales a un número mínimo de 7.608 ciudadanos a lo largo de 3 anualidades. En 2024 se formarán al menos 2662 personas, 3804 en el 2025 y 1142 en el 2026. La plataforma de teleformación que se utilice para impartir acciones formativas deberá alojar el material virtual de aprendizaje correspondiente, poseer capacidad suficiente para desarrollar el proceso de aprendizaje y gestionar y garantizar la formación del alumnado, permitiendo la interactividad y el trabajo cooperativo, y reunir los siguientes requisitos técnicos de infraestructura, software y servicios y funciones:

Infraestructura

I) Tener un rendimiento, entendido como número de alumnos/as que soporte la plataforma, velocidad de respuesta del servidor a los usuarios, y tiempo de carga de las páginas Web o de descarga de archivos, que permita:

a)Soportar un número de alumno/as equivalente al número total de participantes en las especialidades formativas que esté impartiendo la empresa adjudicataria, garantizando un hospedaje mínimo igual al total del alumnado de dichas especialidades, considerando que el número máximo de alumnos por tutor es de 80 y un número de usuarios concurrentes del 50% de ese alumnado.

b)Disponer de la capacidad de transferencia necesaria para que no se produzca efecto retardo en la comunicación audiovisual en tiempo real, debiendo tener el servidor en el que se aloja la plataforma un ancho de banda mínimo de 100 Mbs, suficiente en bajada y subida.

II) Estar en funcionamiento 24 horas al día, los 7 días de la semana.

III) El servidor/servidores deben cumplir con los requisitos establecidos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por lo que el responsable de dicha plataforma ha de identificar la localización física del servidor y el cumplimento de lo establecido sobre transferencias internacionales de datos

en los artículos 40 a 43 de la citada Ley Orgánica 3/2018, de 5 de diciembre, así como, en lo que resulte de aplicación, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas respecto del tratamiento de datos personales y la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

IV) Compatibilidad tecnológica y posibilidades de integración con cualquier sistema operativo, base de datos, navegador de Internet de los más usuales o servidor web, debiendo ser posible utilizar las funciones de la plataforma con complementos (plug-in) y visualizadores compatibles. Si se requiriese la instalación adicional de algún soporte para funcionalidades avanzadas, la plataforma debe facilitar el acceso al mismo sin coste.

V) Sistema de Backup

VI) Sistema de protección ante ataques DDoS

Software y servicios

I) Compatibilidad con el estándar SCORM y paquetes de contenidos IMS.

II) Niveles de accesibilidad e interactividad de los contenidos disponibles mediante tecnologías web que como mínimo cumplan las prioridades 1 y 2 de la Norma UNE 139803:2012 o posteriores actualizaciones, según lo estipulado en el capítulo III del Real Decreto 1494/2007, de 12 de noviembre.

III) Sustentar el material virtual de aprendizaje de la especialidad formativa que a través de ella se imparta.

IV) Disponibilidad de un servicio de atención a usuarios que dé soporte técnico y mantenga la infraestructura tecnológica y que, de forma estructurada y centralizada, atienda y resuelva las consultas e incidencias técnicas del alumnado. Las formas de establecer contacto con este servicio, que serán mediante teléfono y mensajería electrónica, tienen que estar disponibles para el alumnado desde el inicio hasta la finalización de la acción formativa, manteniendo un horario de funcionamiento de mañana y de tarde y un tiempo de demora en la respuesta no superior a 48 horas laborables.

V) Capacidad de personalización con la imagen institucional

VI) Con el objeto de gestionar, administrar, organizar, diseñar, impartir y evaluar acciones formativas a través de Internet, la plataforma de teleformación integrará las herramientas y recursos necesarios a tal fin, disponiendo, específicamente, de herramientas de:

a)Comunicación, que permitan que el alumnado pueda interaccionar a través del navegador con el tutor-formador, el sistema y con el resto del alumnado. Esta comunicación electrónica ha de llevarse a cabo mediante herramientas de comunicación síncronas (aula virtual, chat, etc.) y asíncronas (correo electrónico, foro, calendario, tablón de anuncios, avisos).

b) Será obligatorio que cada acción formativa en modalidad de teleformación disponga, como mínimo, de un servicio de mensajería, un foro y un chat así como un sistema para la realización de videoconferencias en tiempo real.

c) Colaboración, que permita tanto el trabajo cooperativo entre los miembros de un grupo, como la gestión de grupos. Mediante tales herramientas ha de ser posible realizar operaciones de alta, modificación o borrado de grupos de alumnos, así como creación de

«escenarios virtuales» para el trabajo cooperativo de los miembros de un grupo (directorios o «carpetas» para el intercambio de archivos, herramientas para la publicación de los contenidos, y foros o chats privados para los miembros de cada grupo).

d) Administración, que permitan la gestión de usuarios (altas, modificaciones, borrado, gestión de la lista de clase, definición, asignación y gestión de permisos, perfiles y roles, autenticación y asignación de niveles de seguridad) y la gestión de acciones formativas.

VII) Gestión de contenidos, que posibiliten el almacenamiento y la gestión de archivos (visualizar archivos, organizarlos en carpetas –directorios- y subcarpetas, copiar, pegar, eliminar, comprimir, descargar o cargar archivos), la publicación organizada y selectiva de los contenidos de dichos archivos, y la creación de contenidos.

VIII) Evaluación y control del progreso del alumnado, que permitan la creación, edición y realización de pruebas de evaluación y autoevaluación y de actividades y trabajos evaluables, su autocorrección o su corrección (con retroalimentación), la visualización de información estadística sobre los resultados y el progreso de cada alumno y la obtención de informes de seguimiento.

Además, se desarrollará para la plataforma escogida las siguientes bloques de información:

- Estadísticas de los mensajes de los tutores/docentes con: Nombre y apellidos del tutor, el nombre del foro en el que se ha mandado la información, el asunto, el mensaje y la fecha en la que se envió.
- Informe con nombre y apellidos de los alumnos/as, la acción (visto/actualizado/abandonado/aceptado/respondido/completado/finalizado…), el tipo de componente sobre el cual se ha realizado, el elemento y la fecha.
- Un indicador con las horas de dedicación del usuario (cada usuario solo puede ver las suyas)
- Un informe con las horas de dedicación de cada alumno/a, y la nota de la evaluación final.
- Un sistema de aviso por email que se pueda configurar para que automáticamente notifique cuando un usuario hace login u otra acción en la plataforma.
- Un informe descargable de todos los alumnos (ciudadanos) con la siguiente información:

o Identificador único de las personas inscritas. Como identificador único se usará el NIF.

o Localidad de residencia del ciudadano.

o Actividad formativa en la que ha participado (código correspondiente al listado de actividades formativas).

o Indicación de si la actividad formativa fue finalizada con éxito por el ciudadano.

o Edad o rango de edad a la que pertenece.

o Sexo

o Situación laboral (estudiante primaria, estudiante secundaria o ciclo formativo, estudiante

universitario, desempleado, empleado por cuenta propia, empleado por cuenta ajena, jubilado, otras).

o Datos de contacto (teléfono y correo electrónico)

- Un informe descargable del listado de actividades formativas realizadas, que contendrá la siguiente información.

o Código de la actividad formativa.

o Nombre de la actividad.

o Descripción y contenido detallado.

o Localidad de impartición.

o Duración en horas total

o Horas en la modalidad presencial.

o Horas en la modalidad online.

o Fecha de inicio.

o Fecha de fin.

o Formador o formadores que imparten la actividad

Funciones:

Como mínimo:

- Creación y gestión de cursos: se permitirá la creación y gestión de tantas ediciones/cursos como sean necesarios. Cada uno de ellos, entre otros elementos, contendrá:

  - Presentación (página que contendrá la presentación y objetivos)

  - Contenidos (página que dará acceso a los contenidos)

  - Actividades o materiales adicionales

  - Foros y Seguimiento

  - Herramienta de emailing/comunicación

  - Área de Administración: La gestión de la plataforma se realizará desde el área de administración de la herramienta, para cuyo manejo no será necesario ningún conocimiento técnico o tecnológico. Desde el área de administración se permitirá, entre otras acciones:

  - Creación y gestión de contenidos y recursos

  - Creación y gestión de ediciones

  - Creación y gestión de matriculaciones de usuarios y grupos en cursos (manual y masivamente)

  - Generación de informes de auditoría de uso

- Generar estadísticas con los datos evolutivos de la formación realizada por cada alumno
- Gestión y configuración de itinerarios formativos
- Gestión y configuración de proceso de evaluación
- Gestión y configuración de Certificados de cada curso
- Visibilidad y exportación de un índice detallado de contenidos
- Gestión de foros
- Posibilidad de tutorizar la formación
- Gestión de Inscripciones:
- Almacenará un registro de todas las inscripciones recibidas
- Permitirá filtrar por nombre y apellidos de la persona solicitante, fechas de inscripción, categorías, cursos y estado (acepta, acepta automáticamente, rechaza, pendiente de validar)
- Perfil supervisor de registros (departamentos)
- Notificación de inscripción al usuario
- Exportación de las solicitudes a Excel

Otras Funciones y servicios:

- Gestión de altas y bajas de usuarios en la plataforma y matriculaciones (Secretaría).
- Comunicaciones con alumnado.
- Apoyo a dinamización.
- Seguimiento en el desarrollo de la formación.
- Atención y resolución de incidencias y/o dudas (atención primer nivel a usuarios) Inmediata en el caso de L-V de 08:30 – 14:30 h. - 24 h. en todos los demás casos.
- Elaboración de Informes de seguimiento de alumnado, tutores e incidencias
- Elaboración Informe de Finalización.
- Asesoramiento en gestión de convocatorias e-learning y presenciales.

2. Suministro de contenidos formativos (LOTE 2)

El suministro consistirá en el diseño, y producción de contenidos elearning para cada una de las especialidades formativas que se detallan en los módulos que se indican con una duración por módulo de 7,5 horas:

ESPECIALIDAD FORMATIVA - POSICIONAMIENTO EN LA WEB PARA EL EMPRENDIMIENTO.

MÓDULO 1 - CÓMO POSICIONAR PÁGINAS WEB CUANDO SE EMPRENDE UN NEGOCIO

1.1. Posicionamiento en buscadores de empresas de nueva creación.

1.1.1. Buscadores y directorios.

1.1.2. Relevancia de los resultados.

1.1.3. Tráfico cualificado.

1.1.4. Técnicas penalizables de posicionamiento.

1.2. Palabras clave.

1.2.1. La importancia de las palabras clave.

1.2.2. Analizar el tráfico que recibe el sitio web.

1.3. ¿Dónde utilizar las palabras clave?

1.3.1. Dominio y URL.

1.3.2. El título de la página. Encabezados y texto de la página.

1.3.3. Las etiquetas meta.

MÓDULO 2 - ENLACES Y MARCADORES SOCIALES

2.1. Enlaces (I).

2.1.1. Enlaces internos.

2.1.2. Conseguir enlaces externos. Alta en directorios.

2.2. Enlaces (II).

2.2.1. Marcadores sociales. Intercambio de enlaces.

2.2.2. Enlaces que penalizan.

2.2.3. Mapa del sitio (Sitemap).

2.3. Contenidos difíciles de posicionar cuando se crea una empresa.

2.3.1. Imágenes.

2.3.2. Flash. Alternativas actuales

2.3.3. El archivo robots.txt .

MÓDULO 3 - EL EMPRENDEDOR COMO ANALISTA WEB: CÓMO DISEÑAR UNA WEB Y MEDIR EL TRÁFICO CON GOOGLE ANALYTICS

3.1. Diseño y Usabilidad de la página Web del nuevo negocio Online.

3.1.1. Pasos previos al diseño web: dominio, hosting, etc.

3.1.2. Cómo elegir un proveedor para un diseño web a medida.

3.1.3. Prácticos: Aplicaciones de software disponibles.

3.1.4. Caso real: Virtual Shop.

3.1.5. Estructura del negocio online: BackOffice y Frontoffice.

3.1.6. Caso Real: Concepción de un negocio online.

3.1.7. Caso práctico resuelto.

3.2. Gestión de Blog Corporativo.

3.2.1. Cómo adecuar los contenidos para fidelizar al cliente.

3.2.2. El Blog en la estrategia online: Facebook Connect, etc.

3.2.3. Cómo crear un blog con Blogger, paso a paso.

3.2.4. Cómo crear un blog con Wordpress, paso a paso.

3.2.5. Caso práctico resuelto.

MÓDULO 4- MARKETING 3.0

4.1. Marketing 3.0.

4.1.1. Value Management: Prepararse para el Marketing 3.0.

4.1.2. Co-Creation: El cliente como creador del producto.

4.1.3 Comunidades 3.0: Comunicación Cliente-Cliente.

4.1.4. Creación de campañas de Comunicación en la Web Semántica.

4.1.5. Ejemplo Real: Nuestra marca y su ADN social.

4.1.6. Ejercicio Práctico: Crear una estrategia de Marketing dinámica 3.0

ESPECIALIDAD FORMATIVA: SEGURIDAD INFORMÁTICA Y FIRMA DIGITAL

MÓDULO 1 - FIRMA ELECTRÓNICA / FIRMA DIGITAL

1. Introducción a la Firma Electrónica y Firma Digital

1.1 Definición de firma electrónica y firma digital.

1.2 Diferencias entre firma electrónica y firma digital.

1.3 Importancia y aplicaciones en la era digital.

1.1 Marco Legal y Normativo

1.1.1 Legislación internacional y nacional relacionada con la firma electrónica y firma digital.

1.1.2 Requisitos legales para la validez de una firma electrónica y firma digital.

1.2 Tecnologías y Métodos de Implementación

1.2.1 Tecnologías subyacentes en la firma electrónica y firma digital.

1.2.2 Métodos de implementación de firma electrónica y firma digital.

1.2.3 Certificados digitales y autoridades de certificación.

1.3 Seguridad y Confianza en la Firma Digital

1.3.1 Principios de seguridad en la firma digital.

1.3.2 Amenazas y riesgos asociados a la firma digital.

1.3.3 Estrategias para garantizar la confianza en la firma digital.

1.4 Aplicaciones y Casos de Uso

1.4.1 Uso de la firma electrónica y firma digital en transacciones financieras.

1.4.2 Firma digital en contratos y documentos legales.

1.4.3 Integración de la firma digital en procesos empresariales y administrativos.

1.5 Implementación Práctica

1.5.1 Configuración y uso de herramientas para la generación de firma digital.

1.5.2 Proceso de firma digital en documentos electrónicos.

1.5.3 Verificación de la autenticidad de una firma digital.

1.6 Consideraciones Éticas y Sociales

1.6.1 Impacto de la firma digital en la privacidad y seguridad de los datos.

1.6.2 Aspectos éticos de la firma electrónica y firma digital.

1.6.3 Implicaciones sociales de la adopción masiva de la firma digital.

1.7 Futuras Tendencias y Desarrollos

1.7.1 Avances tecnológicos en el campo de la firma electrónica y firma digital.

1.7.2 Tendencias emergentes en regulaciones y estándares de firma digital.

1.7.3 Posibles aplicaciones futuras y su impacto en la sociedad y los negocios.

1.8 Evaluación y Certificación

1.8.1 Evaluaciones prácticas y teóricas para medir el conocimiento adquirido.

1.8.2 Certificación de competencias en firma electrónica y firma digital.

1.9 Conclusiones y Recomendaciones

1.9.1 Resumen de los principales conceptos aprendidos.

1.9.2 Recomendaciones para la implementación segura y efectiva de la firma electrónica y firma digital.

1.9.3 Reflexión sobre el futuro de la firma digital en un mundo cada vez más digitalizado.

MÓDULO 2 -TIPOS DE CERTIFICADOS

2. Tipos de certificados:

2.1. Certificados de Servidor (SSL: Capa de zócalos seguro)

2.2. Microsoft Server Gated Cryptography Certificates (Certificados de CGC-una extensión del protocolo

SSL- ofrecida por Microsoft).

2.3. Certificados Canalizadores.

2.4. Certificados de Correo Electrónico.

2.5. Certificados de Valoración de páginas WEB.

2.6. Certificados de Sello, Fecha y Hora

MÓDULO 3 - SISTEMAS DE SEGURIDAD EN LA EMPRESA

3. Sistemas de seguridad en la empresa.

3.1. Sistemas pasivos y reactivos.

3.2. Suplantación o spoofing:

3.2.1. SET (Secure Electronic Transaction).

3.2.2. PGP (Enterprise Security).

3.2.3. SSL (Secure Socket Layout).

ESPECIALIDAD FORMATIVA: GESTION DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

MÓDULO 1 - INTRODUCCIÓN A LA SEGURIDAD

1. INTRODUCCIÓN A LA SEGURIDAD

1.1. Introducción a la seguridad de información.

1.2. Modelo de ciclo de vida de la seguridad de la información.

1.3. Confidencialidad, integridad y disponibilidad. Principios de protección de la seguridad de la información.

1.4. Políticas de seguridad.

1.5. Tácticas de ataque.

1.6. Concepto de hacking.

1.7. Árbol de ataque.

1.8. Lista de amenazas para la seguridad de la información.

1.9. Vulnerabilidades.

1.10. Vulnerabilidades en sistemas Windows.

1.11. Vulnerabilidades en aplicaciones multiplataforma.

1.12. Vulnerabilidades en sistemas Unix y Mac OS.

1.13. Buenas prácticas y salvaguardas para la seguridad de la red.

1.14. Recomendaciones para la seguridad de su red

MÓDULO 2 - POLÍTICAS DE SEGURIDAD

2.1. Introducción a las políticas de seguridad.

2.2. ¿Por qué son importantes las políticas?

2.3. Qué debe de contener una política de seguridad.

2.4. Lo que no debe contener una política de seguridad.

2.5. Cómo conformar una política de seguridad informática.

2.6. Hacer que se cumplan las decisiones sobre estrategia y políticas.

MÓDULO 3 - AUDITORIA Y NORMATIVA DE SEGURIDAD

3.1. Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información.

3.2. Ciclo del sistema de gestión de seguridad de la información.

3.3. Seguridad de la información. 3.4. Definiciones y clasificación de los activos.

3.5. Seguridad humana, seguridad física y del entorno.

3.6. Gestión de comunicaciones y operaciones.

3.7. Control de accesos.

3.8. Gestión de continuidad del negocio.

3.9. Conformidad y legalidad.

MÓDULO 4 - ESTRATEGIAS DE SEGURIDAD

4.1. Menor privilegio.

4.2. Defensa en profundidad.

4.3. Punto de choque.

4.4. El eslabón más débil.

4.5. Postura de fallo seguro.

4.6. Postura de negación establecida: lo que no está prohibido.

4.7. Postura de permiso establecido: lo que no está permitido.

4.8. Participación universal.

4.9. Diversificación de la defensa.

4.10. Simplicidad.

MÓDULO 5 - EXPLORACIÓN DE LAS REDES

5.1. Exploración de la red.

5.2. Inventario de una red. Herramientas del reconocimiento.

5.3. NMAP Y SCANLINE.

5.4. Reconocimiento. Limitar y explorar.

5.5. Reconocimiento. Exploración.

5.6. Reconocimiento. Enumerar.

MÓDULO 6 - ATAQUES REMOTOS Y LOCALES

6.1. Clasificación de los ataques.

6.2. Ataques remotos en UNIX.

6.3. Ataques remotos sobre servicios inseguros en UNIX.

6.4. Ataques locales en UNIX.

6.5. ¿Qué hacer si recibimos un ataque?

MÓDULO 7 - SEGURIDAD EN REDES INALÁMBRICAS

7.1. Introducción.

7.2. Introducción al estándar inalámbrico 802.11 – WIFI

7.3. Topologías.

7.4. Seguridad en redes Wireless. Redes abiertas.

7.5. WEP.

7.6. WEP. Ataques.

7.7. Otros mecanismos de cifrado.

MÓDULO 8 - CRIPTOGRAFÍA Y CRIPTOANÁLISIS

8.1. Criptografía y criptoanálisis: introducción y definición.

8.2. Cifrado y descifrado.

8.3. Ejemplo de cifrado: relleno de una sola vez y criptografía clásica.

8.4. Ejemplo de cifrado: criptografía moderna.

8.5. Comentarios sobre claves públicas y privadas: sesiones.

MÓDULO 9 - AUTENTICACIÓN

9.1. Validación de identificación en redes.

9.2. Validación de identificación en redes: métodos de autenticación.

9.3. Validación de identificación basada en clave secreta compartida: protocolo.

9.4. Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman.

9.5. Validación de identificación usando un centro de distribución de claves.

9.6. Protocolo de autenticación Kerberos.

9.7. Validación de identificación de clave pública.

9.8. Validación de identificación de clave pública: protocolo de interbloqueo.

ESPECIALIDAD FORMATIVA: INTERNET SEGURO

MÓDULO 1 - INTRODUCCIÓN Y ANTIVIRUS

1. INTRODUCCIÓN Y ANTIVIRUS

1.1. Introducción a la seguridad.

1.2. Introducción a la seguridad.

1.3. Antivirus. Definición de virus. Tipos de virus

1.4. Previo a instalar ningún programa.

1.5. Antivirus. Descarga e instalación.

1.6. Otros programas recomendados.

1.7. Herramientas de desinfección gratuitas.

1.8. Técnico. Ejemplo de infección por virus.

1.9. Anexo.

1.10. Referencias.

1.11. Tengo un mensaje de error ¿y ahora?

1.12. Monográficos.

MÓDULO 2 - ANTIVIRUS. CONFIGURACIÓN, UTILIZACIÓN

2.1. Test de conocimientos previos.

2.2. Antivirus. Configuración.

2.3. Antivirus. Utilización.

2.4. Antivirus. Actualización.

2.5. Troyanos.

2.6. Pantalla típica de un troyano cuando estamos a punto de infectarnos.

2.7. Esquema de seguridad.

2.8. Técnico. Detalles del virus Sasser.

2.9. Anexo.

2.10. Referencias.

MÓDULO 3 - CORTAFUEGOS

3.1. Test de conocimientos previos.

3.2. Cortafuegos. Definición.

3.3. Tipos de cortafuegos.

3.4. Concepto de puerto.

3.5. Tipos de cortafuegos.

3.6. Cortafuegos de Windows XP.

3.7. Cortafuegos de Windows 7.

3.8. Cortafuegos de Windows 8.

3.9. Limitaciones de los cortafuegos.

3.10. Descarga e instalación. Zonealarm.

3.11. Configuración.

3.12. Utilización.

3.13. Actualización.

3.14. Consola del sistema.

3.15. Otros programas recomendados.

3.16. Direcciones de comprobación en línea.

3.17. Esquema de seguridad.

3.18. Novedad. USB Firewall.

3.19. Técnico. Cómo funciona un IDS (sistema de detección de intrusos) Inalámbricas.

3.20. Anexo.

3.21. Referencias.

MÓDULO 4 - ANTIESPÍAS

4.1. Test de conocimientos previos.

4.2. Definición de módulo espía.

4.3. Tipos de espías.

4.4. Cookies.

4.5. SpyBot.

4.6. Malwarebytes.

4.7. Spywareblaster.

4.8. Descarga e instalación.

4.9. Técnico. Evidence Eliminator, amenaza para que lo compres.

4.10. Anexo.

4.11. Referencias.

4.12. Glosario.

MÓDULO 5 - ANTIESPÍAS. CONFIGURACIÓN, UTILIZACIÓN

5.1. Test de conocimientos previos.

5.2. Configuración.

5.3. Utilización.

5.4. Actualización.

5.5. Otros programas recomendados.

5.6. Direcciones de comprobación en línea.

5.7. Cómo eliminar los programas espía de un sistema (Pasos).

5.8. Esquema de seguridad.

5.9. Kaspersky admite que están saturados de peligros en la red.

5.10. "Apple está 10 años detrás de Microsoft en materia de seguridad informática".

5.11. Anexo.

5.12. Referencias

MÓDULO 6 - ACTUALIZACIÓN DEL SISTEMA OPERATIVO

6.1. Test de conocimientos previos.

6.2. WindowsUpdate.

6.3. Configuraciones de Windows Update.

6.4. Módulos espía en Windows XP.

6.5. SafeXP.

6.6. Objetos (o complementos) del Internet Explorer.

6.7. Navegadores alternativos.

6.8. Anexo.

6.9. Referencias.

MÓDULO 7 - NAVEGADOR SEGURO. CERTIFICADOS

7.1. Test de conocimientos previos.

7.2. Navegador seguro.

7.3. Certificados.

7.4. Anexo. Tarjetas criptográficas y Token USB.

7.5. Técnico. ¿Qué es un ataque de denegación de servicio (Ddos)?

7.6. Anexo.

7.7. Referencias.

7.8. Anexo. DNI electrónico (eDNI).

MÓDULO 8 - CORREO SEGURO

8.1. Test de conocimientos previos.

8.2. Correo seguro.

8.3. Correo anónimo.

8.4. Técnico. Correo anónimo.

8.5. Hushmail.

8.6. Esquema de seguridad.

8.7. Anexo.

8.8. Referencias.

MÓDULO 9 - SEGURIDAD EN LAS REDES P2P

9.1. Test de conocimientos previos.

9.2. Seguridad en las redes P2P.

9.3. Peerguardian.

9.4. Seguridad al contactar con el Proveedor de Internet.

9.5. Checkdialer.

9.6. Esquema de seguridad.

9.7. Técnico. Usuarios P2P prefieren anonimato a velocidad.

9.8. España se posiciona como uno de los países del mundo con más fraudes en Internet.

9.9. Esquema de funcionamiento de una red.

9.10. Anexo.

9.11. Referencias.

MÓDULO 10 - COMPROBAR SEGURIDAD

10.1. Test de conocimientos previos.

10.2. Microsoft Baseline Security Analyzer.

10.3. Comprobaciones on-line de seguridad y antivirus.

10.4. Técnico. Comprobar seguridad de un sistema Windows XP.

10.5. Anexo.

10.6. Referencias.

MÓDULO 11- VARIOS

11.1. Test de conocimientos previos.

11.2. Copias de seguridad.

11.3. Contraseñas.

11.4. Control remoto.

11.5. Mensajería electrónica.

11.6. Privacidad y anonimato.

11.7. Boletines electrónicos.

11.8. Listas de seguridad.

11.9. Compras a través de Internet.

11.10. Banca electrónica.

11.11. Enlaces y noticias sobre seguridad informática.

11.12. Anexo. Navegador Firefox.

11.13. Agenda de control.

11.14. Técnico. PandaLabs descubre un nuevo troyano Briz que permite el control remoto del ordenador y realizar estafas online.

11.15. Técnico. Seguridad en Linux.

11.16. Seguridad inalámbrica (Wifi).

11.17. Referencias.

ESPECIALIDAD FORMATIVA: CIBERSEGURIDAD PARA USUARIOS

MÓDULO 1 - INTRODUCCIÓN A LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN

1.1. Conceptos de seguridad en los sistemas.

1.2. Clasificación de las medidas de seguridad.

1.3. Requerimientos de seguridad en los sistemas de información.

1.3.1. Principales características.

1.3.2. Confidencialidad.

1.3.3. Integridad.

1.3.4. Disponibilidad.

1.3.5. Otras características.

1.3.6. Tipos de ataques.

MÓDULO 2 - CIBERSEGURIDAD

2.1. Concepto de ciberseguridad.

2.2. Amenazas más frecuentes a los sistemas de información.

2.3. Tecnologías de seguridad más habituales.

2.4. Gestión de la seguridad informática.

MÓDULO 3 - SOFTWARE DAÑINO

3.1. Conceptos sobre software dañino.

3.2. Clasificación del software dañino.

3.3. Amenazas persistentes y avanzadas.

3.4. Ingeniería social y redes sociales.

MÓDULO 4 - SEGURIDAD EN REDES INALÁMBRICAS

4.1. Seguridad en redes inalámbricas

MÓDULO 5 - HERRAMIENTAS DE SEGURIDAD

5.1. Medidas de protección.

5.2. Control de acceso de los usuarios al sistema operativo.

5.2.1. Permisos de los usuarios.

5.2.2. Registro de usuarios.

5.2.3. Autentificación de usuarios.

5.3. Gestión segura de comunicaciones, carpetas y otros recursos compartidos.

5.3.1. Gestión de carpetas compartidas en la red.

5.3.2. Tipos de accesos a carpetas compartidas.

5.3.3. Compartir impresoras.

5.4. Protección frente a código malicioso.

5.4.1. Antivirus.

5.4.2. Cortafuegos (firewall).

5.4.3. Antimalware.

ESPECIALIDAD FORMATIVA: MEDIOS ELECTRÓNICOS

MÓDULO 1 - INTRODUCCIÓN A GOOGLE DRIVE Y SUS HERRAMIENTAS COLABORATIVAS

1.1 Funcionalidades y ventajas de Google Drive.

1.2 Creación y configuración de una cuenta de Google Drive.

1.3 Navegación y organización de archivos en Google Drive.

1.4 Compartir archivos y carpetas de forma colaborativa.

1.5 Colaboración en tiempo real en documentos, hojas de cálculo y presentaciones.

1.6 Configuración de permisos de acceso y edición en Google Drive.

1.7 Gestión de versiones de documentos colaborativos.

MÓDULO 2 - GMAIL, MEET Y CALENDAR

2.1 Funcionalidades principales de Gmail y su integración con Google Drive.

2.2 Organización y gestión de correos electrónicos en Gmail.

2.3 Programación y gestión de reuniones virtuales con Google Meet.

2.4 Integración de Google Calendar con Gmail para la gestión eficiente de eventos y citas.

2.5 Configuración de recordatorios y notificaciones en Google Calendar.

2.6 Uso de la función de programación de envío en Gmail.

MÓDULO 3 - DOCUMENTOS

3.1 Creación, edición y formato de documentos de texto en Google Docs.

3.2 Herramientas de colaboración en tiempo real en Google Docs.

3.3 Uso de plantillas y complementos para documentos en Google Docs.

3.4 Comentarios y sugerencias colaborativas en documentos en Google Docs.

3.5 Configuración de permisos de visualización y edición en documentos compartidos en Google Docs.

3.6 Exportación e impresión de documentos desde Google Docs.

MÓDULO 4 - HOJAS DE CÁLCULO

4.1 Creación, edición y formato de hojas de cálculo en Google Sheets.

4.2 Funciones y fórmulas básicas en Google Sheets.

4.3 Gráficos y visualizaciones de datos en Google Sheets.

4.4 Colaboración en tiempo real en hojas de cálculo en Google Sheets.

4.5 Importación y exportación de datos en Google Sheets.

4.6 Configuración de permisos de acceso y edición en hojas de cálculo compartidas en Google Sheets.

MÓDULO 5 - PRESENTACIONES Y FORMULARIOS

5.1 Creación, edición y formato de presentaciones en Google Slides.

5.2 Incorporación de imágenes, videos y animaciones en presentaciones en Google Slides.

5.3 Diseño de diapositivas y transiciones en Google Slides.

5.4 Colaboración en tiempo real en presentaciones en Google Slides.

5.5 Creación y personalización de formularios en Google Forms.

5.6 Uso de formularios para la recopilación de datos y respuestas en Google Forms.

5.7 Análisis de respuestas y generación de informes en Google Forms

a) Contenido del suministro

El contratista deberá diseñar, y producir nuevos contenidos elearning para teleformación síncrona que sean susceptibles de impartirse también presencialmente para cada una de las especialidades formativas, los contenidos tienen que estar actualizados para el año 2024 y si hay apartados en los epígrafes de los contenidos que hagan referencia a datos obsoletos, deben reemplazarse por los equivalentes actuales.

b) Características:

Deben presentarse en formato SCORM 1.2/2004, en pdf y en el formato nativo exportable de la plataforma. Se debe crear un SCORM independiente por cada tema de cada una de las especialidades incorporando al menos una evaluación final.

Los SCORM deben contener todos los elementos/contenidos y no estar enlazados externamente para que sean reutilizables en el futuro sin depender de terceros.

Los tipos de contenidos que deben tener los SCORM serán:

- Textos

• Videos.

•Enlaces a webs (materiales complementarios)

•Grabación de audios

•Imágenes

•Juegos de aprendizaje.

Los SCORM deben enviar a la plataforma los estados “passed”, “completed”, “failed”, “incomplete”, “browsed”, “not attempted”, RW, para poder registrar como es el progreso del alumno. Además deberán registrar la última página por la que va el alumno/a, para que pueda retomar el SCORM en el punto donde lo dejó. Cada SCORM deberá notificar a la plataforma las calificaciones obtenidas en las pruebas de evaluación de cada tema.

Dentro de cada curso se permitirán los siguientes formatos:

•Vídeo: avi, asf, asx, mpg, mpeg, m1v, mpe, qt, aif, aifc, mov, wmv, mp4.

•Audio: wav, wma, wax, mp2, mp3, mpa, mid, rmi, au, snd.

•Documentos: htm, html, doc, xls, txt, pps, pdf, sdc, stc, sdd, sxi, sti, sdw, sxw, stw, pdf, doc, ppp.

•Recursos de la Web 2.0

•Acceso a enlaces externos (intranet).

•Paquete SCORM 1.2 y/o 2004

•Actividades de videoconferencia

Los SCORM deben presentar la misma interfaz de navegación y deben ser homogéneos para todas las especialidades formativas. Los contenidos formativos deberán quedar producidos en un alto nivel multimedia utilizando herramientas de autor tipo Articulate Storyline 360º, permitiendo generar contenidos Scorm de alto impacto a nivel diseño y teniendo la posibilidad de aplicar gran diversidad de recursos digitales.

c) Características del suministro:

La empresa deberá suministrar:

•Programación didáctica para cada especialidad formativa

•Planificación de la evaluación para cada especialidad formativa

•Sistemas y documentos de evaluación para cada especialidad formativa

•Fichas de las actividades a realizar para cada especialidad formativa

•Guía del alumno

•Guía del profesor

Se deben incorporar materiales adicionales al temario presentado en formato SCORM, por cada tema como mínimo debe presentarse: una copia en formato PDF de los contenidos, enlaces a páginas web relevantes, vídeos explicativos complementarios y una videoconferencia relativa a los contenidos.

Los contenidos deben estar completos y se ajustarán a los establecidos para las correspondientes especialidades formativas.

El tipo y complejidad de las actividades de aprendizaje y de las de evaluación se corresponderán con las correspondientes capacidades y criterios de evaluación y se ajustarán al nivel de cualificación de cada especialidad.

La forma en que esté estructurado el contenido deberá informar sistemáticamente de las dificultades y progresos de aprendizaje de cada alumno, permitiendo al tutor-formador guiar y ajustar este aprendizaje y al alumno tener feedback continuo acerca de su desempeño.

Además, cada especialidad formativa y sus módulos deberán contener:

- Paquete/s SCORM de los contenidos del curso, que incluirá el material virtual de aprendizaje desarrollado en formato multimedia (utilizando vídeo, gráficos o imágenes, animaciones, audio, simulaciones, biblioteca u otros), de manera que se mantenga una estructura y funcionalidad homogénea.
- Las actividades de aprendizaje que ha de llevar a cabo el alumnado a través de la plataforma de teleformación, indicando las herramientas que se utilizarán en su realización (foro, chat, biblioteca virtual, vídeos, correo electrónico u otros).
- Las actividades de evaluación, integradas en el desarrollo del contenido, que permitirán al alumnado conocer su propio progreso, incluyendo las autoevaluaciones incluidas en los SCORM.
- Un documento en PDF que contenga toda la información incluida en el paquete
- SCORM: textos, imágenes, enlaces, actividades, etc.
- Examen de evaluación final del curso
- Guía del alumno
- Guía del profesor

La cantidad de contenidos principales (SCORM) tienen que ser suficientes para que la dedicación del alumno/a sea como mínimo de las horas establecidas para cada módulo y especialidad formativa, siendo el resto de contenidos considerados complementarios.

Dentro del plazo de garantía, si con antelación al inicio de las especialidades formativas o durante la impartición de las mismos, los docentes o cualquier personal del equipo de Formación detecta, algún elemento o contenido desfasado, erróneo, desactualizado, presencia de legislación derogada o cambiada, en el plazo de 5 días hábiles, este deberá ser modificado y actualizado por la empresa.

La empresa deberá suministrar los contenidos que sean solicitados por los técnicos responsables de la plataforma virtual, según la programación que corresponda, con una antelación mínima de 30 días antes del comienzo del curso con la totalidad de los contenidos de los temas/ módulos y/o unidades formativas de acuerdo con lo establecido en los presentes pliegos.

.....

En Cáceres, a 16 de febrero de 2024.

D. Gabriel Álvarez Arroyo - Presidente

Cáceres

Firmado digitalmente por 11761635X GABRIEL ROMÁN ÁLVAREZ (R: Q1073001H)
Nombre de reconocimiento (DN): 2.5.4.13=Contrato privado: Fecha contrato: 07-06-2022/Fecha autorización: 07-06-2022, cn=11761635X GABRIEL ROMÁN ÁLVAREZ (R: Q1073001H), givenName=GABRIEL ROMÁN, sn=ÁLVAREZ ARROYO, serialNumber=IDCES-11761635X, 2.5.4.97=VATES-Q1073001H, ou=PRESIDENCIA, o=CÁMARA OFICIAL DE COMERCIO, INDUSTRIA Y SERVICIOS DE CÁCERES, c=ES
Fecha: 2024.02.15 09:44:35 +01'00'