MÓDULO:	**CURSO:**
Seguridad y Alta Disponibilidad	2º Administración de Sistemas Informáticos en Redes

RESULTADOS DE APRENDIZAJE	**CONTENIDOS MÍNIMOS**
RA-1: Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo. RA-2: Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema. RA-3: Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad. RA-4: Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna. RA-5: Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio. RA-6: Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba. RA-7: Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	• Adopción de pautas y prácticas de tratamiento seguro de la información. • Implantación de mecanismos de seguridad activa. • Implantación de técnicas de acceso remoto. Seguridad perimetral. • Instalación y configuración de cortafuegos. • Instalación y configuración de servidores proxy. • Implantación de soluciones de alta disponibilidad. • Reconocimiento de la legislación y normativa sobre seguridad y protección de datos.

EVALUACIÓN

Tomás Bevía, 1
41400 Écija (Sevilla)
Tlf.: 955879918
Fax: 955902822

Criterios de evaluación

1a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
1b) Se han descrito las diferencias entre seguridad física y lógica.
1c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
1d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
1e) Se han adoptado políticas de contraseñas.
1f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.
1g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
1h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.
1i) Se han identificado las fases del análisis forense ante ataques a un sistema.

2a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.
2b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.
2c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.
2d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.
2e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.
2f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.
2g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.
2h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.
2i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.

3a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.
3b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.
3c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.
3d) Se han configurado redes privadas virtuales mediante protocolos seguros a

Tomás Bevía, 1
41400 Écija (Sevilla)
Tlf.: 955879918
Fax: 955902822

distintos niveles.
3e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.
3f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.
3g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.

4a) Se han descrito las características, tipos y funciones de los cortafuegos.
4b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.
4c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.
4d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.
4e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.
4f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.
4g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.
4h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.

5a) Se han identificado los tipos de proxy, sus características y funciones principales.
5b) Se ha instalado y configurado un servidor proxy-cache.
5c) Se han configurado los métodos de autenticación en el proxy.
5d) Se ha configurado un proxy en modo transparente.
5e) Se ha utilizado el servidor proxy para establecer restricciones de acceso web.
5f) Se han solucionado problemas de acceso desde los clientes al proxy.
5g) Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas.
5h) Se ha configurado un servidor proxy en modo inverso.
5i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores proxy.

6a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.
6b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.
6c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.
6d) Se ha implantado un servidor redundante que garantice la continuidad de

Tomás Bevía, 1
41400 Écija (Sevilla)
Tlf.: 955879918
Fax: 955902822

servicios en casos de caída del servidor principal.
6e) Se ha implantado un balanceador de carga a la entrada de la red interna.
6f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.
6g) Se ha evaluado la utilidad de los sistemas de clusters para aumentar la fiabilidad y productividad del sistema.
6h) Se han analizado soluciones de futuro para un sistema con demanda creciente.
6i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.

7a) Se ha descrito la legislación sobre protección de datos de carácter personal.
7b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
7c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
7d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.
7e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
7f) Se han contrastado las normas sobre gestión de seguridad de la información.
7g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

Competencias personales y sociales

Con el objetivo de realizar la asignación de empresas al alumnado de forma objetiva, se valorarán las siguientes competencias personales y sociales:

- Realiza las tareas programadas en el tiempo establecido.
- Muestra iniciativa antes los problemas que se plantean y toma decisiones adecuadas.
- Cuida los recursos y evita riesgos medioambientales.
- Capacidad de innovación y creatividad.
- Sabe dialogar, negociar y trabajar cooperativamente.
- Muestra empatía, respeto y valora la diversidad de los compañeros.

También se tendrá en cuenta la asistencia y las calificaciones obtenidas en los distintos módulos del ciclo formativo

Instrumentos de evaluación

Con el objetivo de realizar la asignación de empresas al alumnado de forma objetiva, se valorarán las siguientes competencias personales y sociales:

- **Pruebas teóricas y prácticas (P)**: cuestionarios escritos y/o ejercicios

Tomás Bevía, 1
41400 Écija (Sevilla)
Tlf.: 955879918
Fax: 955902822

prácticos que se realizarán en clase. Se realizarán sin material de apoyo.

- **Tareas prácticas (TP)**: trabajos y proyectos de carácter práctico que se realizarán en el aula y/o en casa de forma individual o en grupo, en función de los objetivos y tipo de trabajo.
- **Presentaciones y exposiciones orales (EX)**: presentaciones visuales, exposición y defensa en público de la misma. Este tipo de trabajo se realizará de forma individual o en grupo, en función de los objetivos.
- **Observación en el aula (OA)**: trabajos, prácticas y pruebas, tanto individuales como en grupo, con la ayuda del material de apoyo necesario y que se presentarán con regularidad en horario de clase.
- **Observación en la Empresa (OE)**: actividades planteadas por el docente para que el alumnado las desarrolle en la empresa. Estas actividades serán supervisadas y evaluadas tanto por el tutor laboral como por el docente del módulo, quien será el que finalmente las califique.
- En el caso del alumnado que haya interrumpido el periodo de FFEOE, éste se incorporará a partir de ese momento a las clases ordinarias, aplicándose los mismos instrumentos y criterios de calificación especificados en el presente punto. En estos casos la empresa u organismo equiparado no llegará a evaluar ninguno de los RRAA y actividades impartidas en periodo de FFEOE.

Criterios de calificación del módulo

- La ponderación asignada a los diferentes resultados de aprendizaje que deben adquirir los alumnos en este módulo será: RA-1 10%, RA-2 22%, RA-3 19%, RA-4 12%, RA-5 12%, RA-6 19%, RA-7 6%
- Resultados de aprendizaje imprescindibles: RA-1, RA-2, RA-3, RA-4, RA-5, RA-6. Deberán tener una calificación igual o superior a cinco para la superación del módulo profesional.
- El RA-2 y el RA-6 se trabajará en la empresa y en el instituto.
- El alumnado, previamente a su incorporación a la FFEOE, deberá haber superado los Resultados de Aprendizaje correspondientes a Prevención de Riesgos Laborales presentes tanto en el módulo transversal de IPE II, como en aquellos módulos profesionales en los que la PRL esté incluida.

TRATAMIENTO DE LA RECUPERACIÓN Y MEJORA DE LA CALIFICACIÓN FINAL

- Para el alumnado que, pese a asistir regularmente a clase y participar en las actividades programadas, no consiga evaluación positiva del módulo en la primera evaluación final, se plantearán opciones para mejorar las competencias necesarias de manera que pueda seguir el proceso de evaluación continua. Para ello plantearemos prácticas y/o actividades de repaso y recuperación.

Tomás Bevía, 1
41400 Écija (Sevilla)
Tlf.: 955879918
Fax: 955902822

- Durante el periodo comprendido entre la primera evaluación final y la segunda evaluación final se realizarán actividades de refuerzo y mejora de las competencias, que permitan al alumno la superación de los módulos pendientes de evaluación positiva o, en su caso, mejorar las calificaciones obtenidas en los mismos.

PÉRDIDA DE EVALUACIÓN CONTINUA

Este Ciclo Formativo tiene carácter presencial, de manera que los alumnos y/o alumnas que no asistan a un 20% o más de las horas de este módulo, perderán el derecho de evaluación continua y tendrán que realizar una serie de pruebas objetivas conforme a los criterios de evaluación que estén asociados a los RA no superados.

MATERIAL NECESARIO

El alumno debe traer un bolígrafo, un cuaderno para tomar apuntes y, si así lo indica el profesor, el libro de texto oficial del módulo. Aunque no es obligatorio, también se recomienda disponer de una memoria USB para realizar copias de seguridad.

Tomás Bevía, 1
41400 Écija (Sevilla)
Tlf.: 955879918
Fax: 955902822