	PROGRAMACIÓN DIDÁCTICA **DEPARTAMENTO DE INFORMATICA**	**Curso:** **2020/21** **Revisión:**
Módulo: SEGURIDAD Y ALTA DISPONIBILIDAD **Ciclo: GRADO SUPERIOR EN ADMINISTRACION DE SISTEMAS INFORMATICOS EN RED**		

ÍNDICE:

Contenido

1.- CRITERIOS DE EVALUACION 2
2.- CRITERIOS DE CALIFICACIÓN 5
3.- RESULTADOS DE APRENDIZAJE MÍNIMOS EXIGIBLES PARA OBTENER LA EVALUACIÓN POSITIVA DEL MÓDULO. 6
4.- PLAN DE REFUERZO DE LOS CONTENIDOS QUE NO PUDIERON IMPARTIRSE EL CURSO PASADO. 9

Realizado por: JAVIER SORINAS	**Revisado por:**	**Aprobado por:**
Profesor del módulo	Equipo docente	Departamento de:
Fecha:	Fecha:	Fecha: *(La del acta de aprobación en el Dpto.)*

1.- CRITERIOS DE EVALUACION

Este módulo profesional contiene la formación necesaria para desempeñar las funciones de configurar componentes y servicios en red.
La formación del módulo contribuye a alcanzar **los siguientes objetivos generales,** cuya consecución se expresa en los siguientes **resultados de aprendizaje** y **Criterios de Evaluación** que se expresan en el siguiente cuadro.

RESULTADOS DE APRENDIZA.	CRITERIOS DE EVALUACION
1. Adopta pautas y prácticas tratamiento seguro de la informac reconociendo las vulnerabilidades un sistema informático y la necesi de asegurarlo.	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos. b) Se han descrito las diferencias entre seguridad física y lógica. c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen. d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos. e) Se han adoptado políticas de contraseñas. f) Se han valorado las ventajas que supone la utilización de sistemas biométricos. g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información. h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas. i) Se han identificado las fases del análisis forense ante ataques a un sistema.
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático. b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo. c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles. d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados. e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso. f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas. g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas. h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema. i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.

3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna. b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral. c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización. d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles. e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas. f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela. g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.
4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna..	a) Se han descrito las características, tipos y funciones de los cortafuegos. b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico. c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red. d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado. e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware. g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos. h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.
5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	a) Se han identificado los tipos de «proxy», sus características y funciones principales. b) Se ha instalado y configurado un servidor «proxy-cache». c) Se han configurado los métodos de autenticación en el «proxy». d) Se ha configurado un «proxy» en modo transparente. e) Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web. f) Se han solucionado problemas de acceso desde los clientes al «proxy». g) Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas. h) Se ha configurado un servidor «proxy» en modo inverso. i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».

6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad. b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema. c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad. d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal. e) Se ha implantado un balanceador de carga a la entrada de la red interna. f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos. g) Se ha evaluado la utilidad de los sistemas de «clusters» para aumentar la fiabilidad y productividad del sistema. h) Se han analizado soluciones de futuro para un sistema con demanda creciente. i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.
7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia. Criterios de evaluación:	a) Se ha descrito la legislación sobre protección de datos de carácter personal. b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada. c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos. d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen. e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico. f) Se han contrastado las normas sobre gestión de seguridad de la información. g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

NOTA: la inspección considera que no es necesario que aparezcan en la programación didáctica pues se recogen el BOA (currículo). Nosotros justificamos su aparición para que el profesorado lo tengan ya en este documento desde el principio, pues hay una gran rotación de profesorado y se pueda utilizar esta herramienta desde el inicio del curso y no tener que recurrir de inicio al título y currículo.

2.- CRITERIOS DE CALIFICACIÓN

RESULTADO DE APRENDIZAJE	CALIFICACIÓN
RA1- Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	15%
RA2 - Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	15%
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	15%
RA4 - Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	15%
RA5 - Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	15%
RA6 - Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	15%
RA7 - Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	10%

3.- RESULTADOS DE APRENDIZAJE MÍNIMOS EXIGIBLES PARA OBTENER LA EVALUACIÓN POSITIVA DEL MÓDULO.

RESULTADOS DE APRENDIZAJE.	CRITERIOS DE EVALUACIÓN.
RA1- Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos. **b) Se han descrito las diferencias entre seguridad física y lógica.** **c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.** d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos. e) Se han adoptado políticas de contraseñas. f) Se han valorado las ventajas que supone la utilización de sistemas biométricos. **g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.** **h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.** **i) Se han identificado las fases del análisis forense ante ataques a un sistema.**
RA2 - Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático. b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo. **c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.** **d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.** e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso. **f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas**. g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas. h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema. **i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.**
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna. **b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.** c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.

	d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles. e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas. f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela. g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.
RA4 - Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	**a) Se han descrito las características, tipos y funciones de los cortafuegos.** **b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.** c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red. **d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.** e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware. **g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.** h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.
RA5 - Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	**a) Se han identificado los tipos de «proxy», sus características y funciones principales.** **b) Se ha instalado y configurado un servidor «proxy-cache».** c) Se han configurado los métodos de autenticación en el «proxy». d) Se ha configurado un «proxy» en modo transparente. **e) Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.** f) Se han solucionado problemas de acceso desde los clientes al «proxy». g) Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas. h) Se ha configurado un servidor «proxy» en modo inverso. i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».
RA6 - Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	**a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.** b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema. c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad. **d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.** **e) Se ha implantado un balanceador de carga a la entrada de la red interna.**

	f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos. g) Se ha evaluado la utilidad de los sistemas de «clusters» para aumentar la fiabilidad y productividad del sistema. h) Se han analizado soluciones de futuro para un sistema con demanda creciente. i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.
RA7 - Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	**a) Se ha descrito la legislación sobre protección de datos de carácter personal.** **b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.** c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos. d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen. e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico. **f) Se han contrastado las normas sobre gestión de seguridad de la información.** g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

4.- PLAN DE REFUERZO DE LOS CONTENIDOS QUE NO PUDIERON IMPARTIRSE EL CURSO PASADO.

Se realiza un repaso a principio de curso para aclarar conceptos y se realizan ejercicios o ejemplos para ayudar a consolidar contenidos.