

GUÍA DIDÁCTICA FORMACIÓN ONLINE

Curso:SEGURIDAD EN REDES WAN E
INTERNET (ON LINE)
FTO19-0235-02

**Tutores de la edición de septiembre de 2019:
Daniel Díaz, Rafael Bravo, Gregorio Corral, Eugenio Rubio**

Leganés, a 19 de Julio de 2019

I.- Bienvenida y presentación de la actividad

Te damos la bienvenida al curso sobre Seguridad en redes WAN e Internet del Instituto Nacional de Administración Pública

La **meta de esta actividad** es transmitir la necesidad de considerar la seguridad en todos los aspectos de nuestra relación con las aplicaciones y servicios en redes de datos e Internet en las que desarrollamos buena parte de nuestro trabajo: a la hora de diseñar, implantar, gestionar y utilizar los diversos sistemas que nos brinda Internet.

El curso se compone de 6 *módulos*. Te invitamos a participar activamente en todos ellos de una manera sostenida en el tiempo.

II.- El INAP: misión, visión y valores

La **misión del INAP** es satisfacer las necesidades ciudadanas mediante su contribución al proceso de transformación de la Administración pública en una organización cada vez más democrática, inclusiva, diversa, sostenible, representativa y alineada con la sociedad a la que sirve. Para ello, lleva a cabo procesos de selección y atracción de talento valioso y plural (de altas capacidades), aprendizaje en valores, competencias y habilidades de los empleados públicos, y una permanente reflexión e investigación sobre los retos del Estado y sus Administraciones públicas.

Visión: El INAP tiene la vocación de ser un actor primordial en la adaptación de la Administración pública española a las demandas que plantea la sociedad actual; además quiere colaborar a que la Administración contribuya a la construcción de la sociedad del futuro. Para ello, alinea su actividad investigadora y formativa con los compromisos de la Agenda 2030 para el Desarrollo Sostenible y con las reflexiones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre las capacidades de los empleados públicos del futuro para afrontar los retos de servir y crear valor público para una sociedad plural, diversa, inclusiva, abierta, interdependiente y participativa.

El INAP propicia la extensión de **valores, principios y alianzas orientados al bien común**. Por ello, la actividad del INAP proyecta valores éticos que han de orientar la actividad pública: transparencia, igualdad efectiva, inclusión, diversidad, desarrollo sostenible, responsabilidad, representatividad, participación e integridad.

III.- Curso “Seguridad en redes WAN e Internet”

Objetivos de aprendizaje

La Meta de este curso es transmitir la necesidad de considerar la

seguridad en todos los aspectos de nuestra relación con las aplicaciones y servicios en redes de datos e Internet en las que desarrollamos buena parte de nuestro trabajo: a la hora de diseñar, implantar, gestionar y utilizar los diversos sistemas que nos brinda Internet.

Además pretende contribuir a crear un foro de discusión que genere lazos profesionales entre personas de las Administraciones Públicas que sigan el curso en materia de seguridad.

El curso comienza con la visión de la organización: políticas, normas y planes, hasta acabar en aspectos tan prácticos como los protocolos de seguridad y la configuración de cortafuegos.

Objetivos de aprendizaje:

Módulo 1: "Conceptos generales de seguridad informática"

- Saber explicar que la seguridad en redes no se debe plantear como una actuación aislada y puntual: cualquier actuación en seguridad debe responder a un planteamiento global acorde con una estrategia y definida en la Política de seguridad de la Organización.
- Proporcionar una aproximación general de los aspectos a contemplar en la seguridad en redes y en Internet en particular. Poder enumerar los servicios básicos de seguridad.

Módulo 2: "Criptografía"

- Proporcionar ciertas nociones básicas acerca de la criptografía, que permitirán comprender cómo funcionan algunos de los algoritmos criptográficos en los que se basan la mayoría de los protocolos, servicios y mecanismos de seguridad.
- Entender los principios básicos de la criptografía, y la diferencia entre los cifradores de flujo y de bloque y los simétricos y asimétricos.

Módulo 3: "Arquitectura de TCP/IP"

- Poder explicar de manera somera la organización en niveles de Internet, las funciones y dependencias de los distintos niveles.
- Entender como el nivel de red resuelve el direccionamiento, la interconexión y el encaminamiento global de datagramas.
- Tener nociones básicas sobre las funciones del protocolo de transporte y aplicación. Poder explicar la dependencia entre ellos y dónde requerimos distintas funciones de seguridad.

Módulo 4: "Servicio de seguridad en redes"

- Conocer y poder enumerar los tipos de autenticación criptográfica
- Conocer las características de las funciones de resumen de mensaje, las existentes y su aplicabilidad, y poder explicar las implicaciones de los avances del criptoanálisis en la aplicabilidad de las funciones de resumen de mensaje, concretamente dónde podemos seguir utilizando algoritmos supuestamente "rotos".
- Comprender el concepto de gestión de identidad: roles y nuevos servicios. Conocer y poder enumerar los sistemas de gestión de identidad más exitosos y sus implicaciones arquitecturales.

Módulo 5: "Seguridad en Internet"

- Explicar de manera somera los servicios y amenazas principales en Internet.
- Enumerar y dar algunos detalles acerca de los protocolos que nos permiten dotar de seguridad a dichos servicios.

Módulo 6: "Arquitecturas de seguridad y configuración de cortafuegos"

- Conocer las arquitecturas de seguridad más frecuentes en las redes

de las organizaciones. Ser capaces de fundamentar algunos cambios de una arquitectura concreta en lo tocante a la seguridad.
 - Ser capaces de configurar un cortafuegos para controlar el acceso a los servicios de **la organización y a Internet**.

Fechas y plataforma de impartición

Las fechas en que se discutirán los contenidos de los módulos en los foros son las siguientes:

- a) Conceptos generales de seguridad informática. Del 16/9 al 20/9.
- b) Criptografía. Del 23/9 al 27/9.
- c) Arquitectura de TCP/IP. Del 30/9 al 4/10.
- d) Servicio de seguridad en redes. Del 7/10 al 11/10.
- e) Seguridad en Internet. Del 14/10 al 18/10.
- f) Arquitecturas de seguridad y configuración de cortafuegos. Del 21/10 al 25/10.
- g) *Actividades de repaso y evaluación adicionales. Del 28/10 al 1/11.*

Cronograma del curso

Calendario de trabajo de todas las actividades, unidades o módulos que conforman el curso, así como las ventanas de fechas en que cada una de ellas estará disponible para el alumno.

Ver ejemplo:

1ª SEMANA				
16/9	17/9	18/9	19/9	20/9
* Foro de bienvenida y presentación de los alumnos				
* Manual Módulo 1				
*Foro 1				
			Cuestionario Módulo 1	
2ª SEMANA				
23/9	24/9	25/9	26/9	27/9
*Manual Módulo 2				
*Foro 2				
		Cuestionario Módulo 1		
			Cuestionario Módulo 2	

3ª SEMANA				
30/9	1/10	2/10	3/10	4/10
* Manual Módulo 3				
*Foro 3				
		Cuestionario Módulo 2		
			Cuestionario Módulo 3	
4ª SEMANA				
7/10	8/10	9/10	10/10	11/10
*Manual Módulo 4				
*Foro 4				
		Cuestionario Módulo 3		
			Cuestionario Módulo 4	
5ª SEMANA				
14/10	15/10	16/10	17/10	18/10
* Manual Módulo 5				
*Foro 5				
		Cuestionario Módulo 4		
			Cuestionario Módulo 5	
6ª SEMANA				
21/10	22/10	23/10	24/10	25/10
*Manual Módulo 6				
*Foro 6				
		Cuestionario Módulo 5		
			Cuestionario Módulo 6	
7ª SEMANA				
28/10	29/10	30/10	31/10	1/11
		Cuestionario Módulo 6		
			Cuestionario Global	Cuestionario Global

IMPORTANTE: todas las actividades precedidas con un * estarán accesibles para los alumnos desde su fecha de inicio marcada en el cronograma hasta la fecha de finalización del curso: 3 de noviembre.

Leyenda de fondos

COLOR SIGNIFICADO

	Fecha de inicio de la actividad o de accesibilidad al contenido. La hora de apertura serán las 08:00 CEST.
	Fecha de fin de la actividad o de accesibilidad al contenido. La hora de cierre serán las 23:59 CEST.
	Fecha de inicio y fin de la actividad o de accesibilidad al contenido.

Programa

De forma esquemática se deben indicar los diferentes módulos que componen el programa de la acción formativa, junto con el contenido de cada uno de los temas que los componen.

Módulos	Contenidos
I.-Conceptos generales de seguridad informática	Capítulo 1 INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN Capítulo 2 OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN Capítulo 3 MEDIDAS DE PROTECCIÓN Capítulo 4 PLANES DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Capítulo 5 POLÍTICAS DE SEGURIDAD Capítulo 6 INTRODUCCIÓN A LA SEGURIDAD EN REDES
II.- Criptografía	Capítulo 1 INTRODUCCIÓN A LA CRIPTOGRAFÍA Capítulo 2 MÉTODOS CRIPTOGRÁFICOS CLÁSICOS Capítulo 3 CRIPTOSISTEMAS SIMÉTRICOS Capítulo 4 CRIPTOSISTEMAS ASIMÉTRICOS
III.- Arquitectura de TCP/IP	Capítulo 1 SISTEMAS ABIERTOS Capítulo 2 NIVEL DE INTERNET Capítulo 3 DIRECCIONAMIENTO IP Capítulo 4 NIVEL DE TRANSPORTE Capítulo 5 NIVEL DE APLICACIÓN Capítulo 6 PROTOCOLOS, PUERTOS Y SOCKETS
IV.- Servicios de Seguridad en Redes	Capítulo 1 SERVICIOS Y MECANISMOS DE SEGURIDAD Capítulo 2 AUTENTICACIÓN CRIPTOGRÁFICA Capítulo 3 SISTEMAS DE GESTIÓN DE IDENTIDAD EN INTERNET
V.- Seguridad en Internet	Capítulo 1. INTRODUCCIÓN A LA SEGURIDAD EN INTERNET Capítulo 2. VIRUS EN INTERNET Capítulo 3. PROTOCOLOS DE SEGURIDAD
VI.- Arquitecturas de seguridad y configuración de cortafuegos	Capítulo 1 INTRODUCCIÓN A LOS CORTAFUEGOS Capítulo 2 ARQUITECTURAS DE LOS CORTAFUEGOS Capítulo 3 CONFIGURACIÓN DE CORTAFUEGOS

Metodología de aprendizaje

Cada módulo comienza con unos materiales generales del tema en pdf y la discusión se abre en el foro correspondiente. En el foro los profesores traen a consideración diversos materiales adicionales, noticias, herramientas y propuestas de actividades. **TODOS** los alumnos deben participar en la medida de sus conocimientos tanto para expresar dudas como para añadir otros puntos de vista o enlaces que enriquezcan la discusión, y también para enviar los resultados de las actividades propuestas. Dos días después de abrirse el foro los alumnos pueden realizar el cuestionario del tema hasta la fecha indicada en el cuestionario (normalmente una semana).

Sistema de evaluación del alumnado

En este curso pueden obtenerse dos calificaciones **APTO** o **NO APTO**.

Para **obtener de la calificación de APTO** se exige haber hecho aportaciones en un mínimo de dos foros y que la ponderación al 70% de los cuestionarios de evaluación con el 30% de la participación sea igual o superior a 5.

También se ofrece a los alumnos que hayan realizado al menos la mitad de los cuestionarios de evaluación realizar una evaluación de conjunto sobre todos los módulos, como alternativa a las evaluaciones individuales de los módulos.

Entendemos la participación en el foro como aportar algo, por supuesto la realización de una actividad es una aportación, pero también plantear una duda de forma razonada, aclarar la duda de otro compañero, explicar el punto de vista de uno sobre un tema, plantear una noticia o un hecho que ejemplifica algo relacionado con el tema, etc. Los mensajes del tipo “Estoy de acuerdo con el comentario anterior.” que no aportan un razonamiento explicado con las palabras de cada uno, se considerarán mensajes pero no aportaciones y no tendrán el mismo valor para medir la participación.

Obtención y envío del certificado del curso

Los alumnos que hayan superado las pruebas de evaluación establecidas para el curso obtendrán del INAP el certificado de aprovechamiento.

Este certificado les será enviado por correo electrónico a la cuenta que el alumno tenga dada de alta en el portal del alumno:

<http://www.inap.es/alumno>. Desde ese mismo portal también se puede acceder en cualquier momento a los certificados expedidos.

Este certificado les será enviado por correo electrónico a la cuenta que el alumno tenga dada de alta en el portal del alumno: <http://www.inap.es/alumno>. Desde ese mismo portal también se puede acceder en cualquier momento a los certificados expedidos.

Equipo docente

Relación de cada uno de los tutores y encargados de los diferentes módulos, una breve reseña sobre su cargo y responsabilidad, y el módulo o unidad que tutorizará:

Tutor	Cargo o puesto y responsabilidad	Unidad o Módulo a tutorizar
Daniel Díaz	Dr.Ing. De Telecomunicación	
Rafael Bravo	Ingeniero Informático	
Gregorio Corral	Ingeniero Informático	
Eugenio Drosdov	Graduado Ing. Telecomunicación	

Régimen académico

Los alumnos que no observen las reglas elementales de participación, respeto y consideración hacia profesores, compañeros o personal del INAP y, en general, que contravengan lo dispuesto en el Código Ético del INAP (que puede consultarse en <http://www.inap.es/conocenos>), podrán ser excluidos de las actividades formativas.

Exclusión en actividades formativas online

Los **alumnos que no se conecten** a la plataforma digital durante la primera semana sin previo aviso ni justificación, **serán excluidos de la actividad formativa** y sustituidos por otras personas que se encuentren en la lista de espera para poder participar en ella.

La falta de conexión durante la primera semana también podrá determinar la exclusión en selecciones posteriores.

Asimismo, podrán ser excluidos de actividades formativas online todos aquellos que incumplan reiteradamente el plan de trabajo establecido por los tutores o que no se conecten con regularidad a la plataforma.

Evaluación de la actividad por los participantes

Cada participante deberá valorar el curso cumplimentando un cuestionario de satisfacción que recibirá por correo electrónico durante el mismo. Una vez finalizada la actividad, tendrá que remitirlo al INAP antes de la fecha indicada.

Esta opinión es muy importante para el INAP, ya que nos permite aprender y mejorar.

Problemas o incidencias con la plataforma de formación

Antes de comenzar a realizar las distintas actividades de que consta el curso se debe de leer la guía de ayuda para el uso de la plataforma de formación con el objetivo de tener un conocimiento sobre sus principales funcionalidades, navegación, servicio de correo interno y otros aspectos relevantes.

En caso de incidencias relacionadas con el funcionamiento de la plataforma puedes ponerte en contacto con el CAU:

- 91 0780255: De lunes a viernes de 08'00 a 23'59 horas y sábados de 09'00 a 20'00 horas.
- cau@inap.es