

III. OTRAS DISPOSICIONES

MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

- 997** *Resolución de 7 de enero de 2011, del Instituto Nacional de Administración Pública, por la que se convocan acciones formativas en materia de seguridad de las tecnologías de la administración electrónica en colaboración con el Centro Criptológico Nacional.*

Entre las funciones asignadas al Instituto Nacional de Administración Pública, de acuerdo con el Real Decreto 1661/2000, de 29 de septiembre, por el que se aprueba el Estatuto del Instituto Nacional de Administración Pública, se encuentra la formación y el perfeccionamiento de los empleados públicos.

El Instituto Nacional de Administración Pública, en colaboración con el Centro Criptológico Nacional, convoca para el primer semestre del año 2011, nueve actividades formativas en materia de seguridad de las tecnologías de la administración electrónica en la modalidad presencial (Anexo I).

Quienes se encuentren afectados por una discapacidad, debidamente acreditada, cuyo grado de minusvalía sea igual o superior al 33% podrán hacer constar tal circunstancia en la solicitud, debiendo comunicar al Centro Criptológico Nacional, en caso de ser seleccionado, las adaptaciones necesarias para la realización del curso.

Igualmente, en aplicación del Real Decreto 2271/2004, de 3 de diciembre, se valorará como criterio de participación a quienes se encuentren afectados por una discapacidad cuyo grado de minusvalía sea igual o superior al 33%.

De conformidad con lo establecido en el Acuerdo de Formación para el Empleo de las Administraciones Públicas, de 22 de marzo de 2010, se fomentarán las medidas, en materia de formación, que tiendan a favorecer la conciliación de la vida familiar y laboral.

Adicionalmente, de conformidad con el artículo 60 de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, se otorgará preferencia, durante un año, a quienes se hayan incorporado al servicio activo procedentes del permiso de maternidad o paternidad, o hayan reingresado desde la situación de excedencia por razones de guarda legal y atención a personas mayores dependientes o personas con discapacidad.

Asimismo, el INAP se reservará al menos un cuarenta por ciento de las plazas para su adjudicación a mujeres que reúnan los requisitos establecidos, salvo que el número de solicitudes de mujeres sea insuficiente para cubrir este porcentaje.

Los empleados públicos podrán recibir y participar en cursos de formación durante los permisos de maternidad, paternidad, así como durante las excedencias por motivos familiares.

BASES

Primera. Objeto.—Mediante la presente resolución se convocan nueve actividades formativas en materia de seguridad de las tecnologías de la administración electrónica, las cuales se detallan en el Anexo I, y que se desarrollarán durante el primer semestre de 2011.

Segunda. Destinatarios.—Podrán solicitar dichas actividades formativas los empleados públicos de las Administraciones Públicas de los subgrupos A1, A2 y C1, y personal laboral equivalente, que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de sistemas de las tecnologías de la información y las comunicaciones, en la seguridad de los mismos, y según la materia, en entornos web y desarrolladores de aplicaciones web. El personal militar perteneciente al Ministerio de

Defensa deberá tramitar su solicitud a través de la convocatoria específica que realizará dicho Ministerio.

Tercera. *Selección.*—El número de alumnos admitidos no excederá, con carácter general, de treinta. La selección de los participantes la realizará el Centro Criptológico Nacional. En la selección se observarán los siguientes criterios: trayectoria profesional y curricular de los candidatos, adecuación del puesto desempeñado a los contenidos de la acción formativa, equilibrio entre organismos e instituciones, e interés objetivo de la organización administrativa en la participación del solicitante en el curso. Sólo se asignará un curso por año a cada solicitante. En caso de recibir varias solicitudes de un mismo organismo o institución se seleccionará al candidato con el perfil más ajustado al destinatario del curso.

Una vez efectuada la selección definitiva de participantes, el Centro Criptológico Nacional comunicará por correo electrónico a cada uno de los alumnos, su admisión, el aula y el horario en que tendrá lugar. Se exigirá a cada seleccionado como requisito para poder realizar el curso que conteste a este correo confirmando su asistencia.

La inasistencia, sin previo aviso o cumplida justificación de quienes hubiesen sido seleccionados para participar en el curso podrá determinar su exclusión en selecciones posteriores.

Cuarta. *Inscripción y plazo de presentación de solicitudes.*—Los interesados que cumplan con el perfil de destinatario descrito deberán inscribirse electrónicamente en la página web del INAP (www.inap.es).

El plazo de presentación de solicitudes electrónicas será de diez días naturales, durante 24 horas, contados a partir del día siguiente al de la publicación de la presente resolución en el Boletín Oficial del Estado.

Quinta. *Diplomas.*—Los participantes que acrediten un buen aprovechamiento de las enseñanzas impartidas recibirán el correspondiente diploma. Una inasistencia superior al diez por ciento de las horas lectivas programadas, sea cual sea la causa, imposibilitará la expedición del mismo.

Sexta. *Información adicional.*—Se podrá solicitar información adicional sobre esta convocatoria en los teléfonos: 91372.67.85/91372.53.77, así como a la dirección de correo electrónico formación.ccn@cni.es. Asimismo se podrán realizar consultas a través de la página web del Instituto Nacional de Administración Pública en Internet: www.inap.es

Madrid, 7 de enero de 2011.—El Director del Instituto Nacional de Administración Pública, Ángel Manuel Moreno Molina.

ANEXO I

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
FTS1109 1800001	VI CURSO BÁSICO STIC – INFRAESTRUCTU RA DE RED	Proporcionar a los participantes los conocimientos necesarios para que sean capaces de comprobar, con suficiente garantía, los aspectos de seguridad relativos a la infraestructura de red basada en elementos de comunicaciones (concentradores, enrutadores,...), dispositivos inalámbricos y redes privadas virtuales (VPN) introduciendo los conceptos de cortafuegos, sistemas de detección de intrusos (IDS) y dispositivos trampa (honeypots y honeynets).	<p>- Un conocimiento mínimo de sistemas Windows/Unix, así como conocimientos básicos de protocolos y equipamiento de red.</p> <p>- Se considerarán como prioridades para la selección al curso:</p> <ul style="list-style-type: none"> ▪ Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de las tecnologías de la información y comunicaciones (TIC). ▪ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el Centro Criptológico Nacional. ▪ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. <p>-Tener responsabilidades, a nivel técnico, en la implementación u operación de sistemas de las TIC o en la gestión de la seguridad de dichos sistemas por un período superior a 1 año.</p>	Dispositivos comunicaciones Dispositivos de filtrado Redes inalámbricas Redes privadas virtuales Seguridad perimetral	25h	Del 4 al 8 de abril
FTS1109 1700001	VI CURSO BÁSICO STIC – BASES DE DATOS	Proporcionar a los participantes los conocimientos necesarios para que sean capaces de comprobar, con suficiente garantía, los aspectos de seguridad relativos a la configuración segura de las bases de datos Oracle y MS SQL Server.	<p>- Un conocimiento mínimo a nivel administrativo de base de datos, así como conocimientos básicos de sistemas Windows/Unix y protocolos de red.</p> <p>-Se considerarán como prioridades para la selección al curso:</p> <ul style="list-style-type: none"> ▪ Actividad relacionada con la administración de bases de datos en sistemas de las tecnologías de la información y comunicaciones (TIC). ▪ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el Centro Criptológico Nacional. ▪ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. <p>- Tener responsabilidades, a nivel técnico, en la implementación u operación de sistemas de las TIC o en la gestión de la seguridad de dichos sistemas por un período superior a 1 año.</p>	Seguridad entornos SQL Server. Seguridad entornos Oracle.	25h	Del 11 al 15 de abril
FTS1109 2200001	VIII CURSO ACREDITACIÓN STIC – ENTORNOS WINDOWS	Proporcionar a los participantes los conocimientos necesarios para que sean capaces de comprobar, con suficiente garantía, los aspectos de seguridad de sistemas servidores Windows 2003, estaciones clientes con Windows XP, aplicaciones servidoras Internet Information Services (ISS) y servicios Exchange de Microsoft. Al tratarse de un curso de acreditación, se utilizará como marco de referencia la normativa recogida en la serie	<p>- Un conocimiento mínimo de sistemas Windows, así como conocimientos básicos de protocolos de red.</p> <p>- Se considerarán como prioridades para la selección al curso:</p> <ul style="list-style-type: none"> ▪ Haber realizado con anterioridad el Curso Básico STIC - Entornos Windows desarrollado por el Centro Criptológico Nacional (CCN). ▪ Actividad relacionada con la administración de sistemas de las tecnologías de la información y comunicaciones (TIC) bajo entornos Windows 2003/XP. ▪ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías 	Medidas técnicas STIC Seguridad sistemas operativos Seguridad servicios web Seguridad servicios de correo	25h	Del 28 de marzo al 1 de abril

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
		CCN-STIC implementando las configuraciones de seguridad definidas en las guías CCN-STIC-500 para entornos basados en tecnología Microsoft.	<p>de la Información y Comunicaciones (STIC) desarrollado por el CCN.</p> <ul style="list-style-type: none"> ▪ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. <p>- Tener responsabilidades, a nivel técnico, en la implementación u operación de sistemas de las TIC o en la gestión de la seguridad de dichos sistemas por un periodo superior a 1 año.</p>			
FTS1109 3100001	IV CURSO STIC – BÚSQUEDA DE EVIDENCIAS	Proporcionar a los participantes los conocimientos necesarios para que realizando un reconocimiento previo de un sistema de las TIC sean capaces de buscar y encontrar rastros y evidencias de un ataque o infección.	<p>- Un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.</p> <p>- Se considerarán como prioridades para la selección del curso:</p> <ul style="list-style-type: none"> ▪ Haber realizado con anterioridad el Curso Básico STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN). ▪ Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de las tecnologías de la información y comunicaciones (TIC). ▪ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN. ▪ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. <p>- Tener responsabilidades, a nivel técnico, en la implementación u operación de sistemas de las TIC o en la gestión de la seguridad de dichos sistemas por un periodo superior a 1 año.</p>	Metodología. Cómo y qué buscar. Estudio práctico. Lugares donde buscar datos. Análisis de ficheros.	25h	Del 25 al 29 de abril
FTS1109 3000001	VI CURSO STIC – INSPECCIONES DE SEGURIDAD	Proporcionar a los participantes los conocimientos y habilidades necesarias para que sean capaces de comprobar, con suficiente garantía, los aspectos de seguridad de redes, aplicaciones y dispositivos en cada organización concreta, así como verificar y corregir los procesos e implementaciones	<p>- Un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.</p> <p>- Se considerarán como prioridades para la selección del curso:</p> <ul style="list-style-type: none"> ▪ Poseer una habilitación de seguridad expedida por la Oficina Nacional de Seguridad (ONS) del Centro Nacional de Inteligencia. ▪ Actividad relacionada con la verificación de la seguridad asociada a sistemas de las tecnologías de la información y comunicaciones (TIC). ▪ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN. ▪ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. <p>- Tener responsabilidades, a nivel técnico, en la implementación u operación de sistemas de las TIC o en la gestión de la seguridad de dichos sistemas por un periodo superior a 1 año</p>	Herramientas de seguridad. Verificaciones de seguridad. Inspecciones STIC (Nivel 3).	25h	Del 9 al 13 de mayo
FTS1109 2500001	VI CURSO STIC - REDES INALÁMBRICAS	Proporcionar a los participantes los conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías	<p>- Un conocimiento mínimo de sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.</p> <p>- Se considerarán como prioridades para la selección al curso:</p>	Medidas técnicas Comunicación WMAN Comunicación WLAN Dispositivos WPAN	25h	Del 16 al 20 de mayo

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
		inalámbricas más adecuadas en cada organización concreta, y para implementar y utilizar de forma óptima cada una de las capacidades que éstas ofrecen para contribuir de forma eficiente al conjunto de la seguridad de la organización	<ul style="list-style-type: none"> ▪ Haber realizado con anterioridad el Curso Básico STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN). ▪ Actividad relacionada con la administración de la infraestructura de red asociada a Sistemas de las tecnologías de la información y comunicaciones (TIC). ▪ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN. ▪ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. <p>- Tener responsabilidades, a nivel técnico, en la implementación u operación de sistemas de las TIC o en la gestión de la seguridad de dichos sistemas por un período superior a 1 año.</p>			
FTS1109 2600001	VII CURSO STIC - CORTAFUEGOS	Proporcionar a los participantes los conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías de cortafuegos más adecuadas en cada organización concreta, y para implementar y utilizar de forma óptima cada una de las capacidades que éstos ofrecen para contribuir de forma eficiente al conjunto de la seguridad de la organización.	<p>- Un conocimiento mínimo de sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.</p> <p>- Se considerarán como prioridades para la selección al curso:</p> <ul style="list-style-type: none"> ▪ Haber realizado con anterioridad el Curso Básico STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN). ▪ Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de las tecnologías de la información y comunicaciones (TIC). ▪ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN. ▪ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. <p>- Tener responsabilidades, a nivel técnico, en la implementación u operación de sistemas de las TIC o en la gestión de la seguridad de dichos sistemas por un período superior a 1 año.</p>	Cortafuegos, protocolos y seguridad perimetral. NAT y reglas de filtrado. AAA y seguridad de contenidos. VPN y usuarios móviles. Enrutadores y cortafuegos a nivel sistema.	25h	Del 23 al 27 de mayo
FTS1109 2700001	VII CURSO STIC – DETECCIÓN DE INTRUSOS	Proporcionar a los participantes los conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías de detección de intrusiones más adecuadas en cada organización concreta, y para implementar y utilizar de forma óptima cada una de las capacidades que éstas ofrecen para contribuir de forma eficiente al conjunto de la seguridad de la organización.	<p>- Un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.</p> <p>- Se considerarán como prioridades para la selección al curso:</p> <ul style="list-style-type: none"> ▪ Haber realizado con anterioridad el Curso Básico STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN). ▪ Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de las tecnologías de la información y comunicaciones (TIC). ▪ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN. 	Conceptos de IDS y análisis de tráfico. Análisis de tráfico e IDS a nivel de red (NIDS). IDS a nivel sistema (HIDS). Análisis de registros y honeypots. Detección de ataques con infraestructura IDS combinada.	25h	Del 30 de mayo al 3 de junio

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
			<ul style="list-style-type: none"> ▪ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. - Tener responsabilidades, a nivel técnico, en la implementación u operación de sistemas de las TIC o en la gestión de la seguridad de dichos sistemas por un período superior a 1 año 			
FTS1109 3300001	II CURSO STIC – SEGURIDAD EN APLICACIONES WEB	Proporcionar a los participantes una visión detallada, actual y práctica de las amenazas y vulnerabilidades de seguridad que afectan a las infraestructuras, entornos y aplicaciones Web. Los diferentes módulos incluyen una descripción detallada de las vulnerabilidades estudiadas, técnicas de ataque, mecanismos de defensa y recomendaciones de seguridad, incluyendo numerosas demostraciones y ejercicios prácticos.	<ul style="list-style-type: none"> - Un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red. - Se considerarán como prioridades para la selección al curso: <ul style="list-style-type: none"> ▪ Haber realizado con anterioridad el Curso STIC – Inspecciones de Seguridad desarrollado por el Centro Criptológico Nacional (CCN). ▪ Haber realizado con anterioridad el Curso STIC – Cortafuegos desarrollado por el Centro Criptológico Nacional (CCN). ▪ Haber realizado con anterioridad el Curso STIC – Detección de Intrusos desarrollado por el Centro Criptológico Nacional (CCN). ▪ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN. ▪ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. - Tener responsabilidades, a nivel técnico, en la implementación u operación de sistemas de las TIC o en la gestión de la seguridad de dichos sistemas por un período superior a 1 año. 	Introducción a las amenazas en aplicaciones Web. Protocolos Web. Herramientas de análisis y manipulación Web. Ataques sobre entornos Web. Mecanismos de autenticación y autorización Web. Gestión de sesiones. Inyección SQL. Cross-Site Scripting (XSS). Cross-Site Request Forgery (CSRF).	25h	Del 6 al 10 de junio