

III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

6673 *Resolución de 6 de junio de 2013, del Instituto Nacional de Administración Pública, por la que se convocan acciones formativas en materia de seguridad de las tecnologías de la información y comunicaciones, en colaboración con el Centro Criptológico Nacional.*

Entre las funciones asignadas al Instituto Nacional de Administración Pública (INAP), de acuerdo con el Estatuto del Instituto Nacional de Administración Pública, aprobado por el Real Decreto 464/2011, de 1 de abril, se encuentra la formación y el perfeccionamiento de los empleados públicos.

Por ello, teniendo en cuenta las necesidades formativas de los empleados públicos para el adecuado ejercicio de sus funciones, esta Dirección adopta la siguiente resolución:

Primera. *Objeto.*

Mediante esta resolución se convocan actividades formativas en materia de seguridad de las tecnologías de la información y comunicaciones en la administración electrónica, según el programa y modalidad formativa que se describe en el anexo y que se desarrollarán durante el segundo semestre de 2013.

Segunda. *Destinatarios.*

Podrán solicitar el curso de especialidades criptológicas los empleados públicos pertenecientes a cuerpos y escalas de los subgrupos A1 y A2, y personal laboral equivalente, que presten sus servicios en las Administraciones públicas y tengan responsabilidad en la planificación, gestión, administración o mantenimiento de sistemas de las tecnologías de la información y las comunicaciones o en su seguridad.

Las demás actividades formativas podrán ser solicitadas por los empleados públicos de los subgrupos A1, A2 y C1, y equivalentes, que tengan responsabilidad, en el nivel técnico, en la planificación, gestión, administración o mantenimiento de sistemas de las tecnologías de la información y las comunicaciones o en su seguridad.

El personal militar perteneciente al Ministerio de Defensa deberá tramitar su solicitud a través de la convocatoria específica que realizará dicho ministerio.

Tercera. *Plazo de presentación de solicitudes.*

El plazo de presentación de solicitudes será de quince días contados a partir del día siguiente al de la publicación de esta resolución en el «Boletín Oficial del Estado».

Quienes deseen participar en los cursos convocados deberán solicitarlo mediante la cumplimentación del modelo de solicitud electrónica. Los candidatos deberán presentar la solicitud que figura en la página web del INAP (www.inap.es) entrando en «Aprendizaje» y, a continuación, seleccionando «Formación en administración electrónica», «Cursos en materia de seguridad TIC en colaboración con el CCN» y, finalmente, el apartado denominado «Inscripción electrónica». Una vez ejecutada la acción «Grabar solicitud», se les generará una copia del modelo de solicitud que deberán imprimir y pasar a la firma del superior jerárquico. Una vez firmada, deberán conservar la solicitud en su poder hasta que se les requiera su presentación.

Para cualquier incidencia técnica relacionada con la inscripción electrónica se podrá contactar con el INAP a través de la dirección de correo electrónico ft@inap.es

Cuarta. Selección.

1. El número de alumnos admitidos no excederá, con carácter general, de veinticuatro. 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. En el caso de recibir varias solicitudes de un mismo organismo o institución, se seleccionará al candidato con el perfil más ajustado al destinatario del curso.

2. Los empleados públicos podrán participar en cursos de formación durante los permisos por parto, adopción o acogimiento, así como durante la situación de excedencia por cuidado de familiares, según lo dispuesto en los artículos 49 y 89.4 de La Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.

3. De acuerdo 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 en la selección a quienes se hayan incorporado en el plazo de un año 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, con objeto de actualizar los conocimientos de los empleados públicos y empleadas públicas. Asimismo, se reservará al menos un 40 por ciento de las plazas en los cursos de formación para su adjudicación a mujeres que reúnan los requisitos establecidos, salvo que el número de solicitudes de mujeres sea insuficiente para cubrir este porcentaje.

4. En aplicación del Real Decreto 2271/2004, de 3 de diciembre, se valorará como criterio de selección a quienes se encuentren afectados por una discapacidad cuyo grado de minusvalía sea igual o superior al 33 por ciento. Las personas con discapacidad que soliciten el curso podrán hacer constar tal circunstancia en la inscripción, y podrán indicar, asimismo, las adaptaciones necesarias en el curso formativo, siempre y cuando hayan sido seleccionadas.

5. Una vez efectuada la selección definitiva de participantes, el Centro Criptológico Nacional comunicará por correo electrónico a cada uno de los alumnos seleccionados 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.

6. La inasistencia a los cursos presenciales, o falta de conexión a los cursos on line, sin previo aviso o cumplida justificación, de quienes hubiesen sido seleccionados para participar en el curso podrá determinar su exclusión en convocatorias posteriores.

Quinta. Modalidad formativa, lugar de celebración y calendario.

Las actividades formativas se realizarán en la modalidad y en las fechas detalladas en el anexo. En el caso de que resulte necesario realizar algún cambio en las fechas indicadas en la programación, será comunicado con antelación suficiente a los participantes en la actividad de que se trate. Para los cursos en la modalidad «on line», los alumnos deberán disponer de un equipo que tenga la configuración técnica necesaria en cada caso para la realización del curso.

El curso de gestión de seguridad de las tecnologías de la información y las comunicaciones e implantación del Esquema Nacional de Seguridad (Gestión STIC), en modalidad mixta, tendrá una fase on line y una presencial. La superación de la fase «on line» será requisito imprescindible para participar en la fase presencial. El curso de especialidades criptológicas, en modalidad mixta, constará de dos partes:

a) Parte I, con fase «on line» y presencial. Será imprescindible superar la prueba de evaluación de la fase «on line» para participar en la presencial.

b) Parte II, en modalidad presencial. Será requisito para participar haber superado la parte I.

Cualquier duda o problema técnico derivado del acceso a páginas web, o de la descarga o instalación de las aplicaciones requeridas para la realización del curso, deberá ser consultada con el administrador del sistema del equipo que esté utilizando.

La fase presencial de los cursos citados, así como las demás actividades formativas, se celebrarán en Madrid. La sede definitiva de desarrollo de las acciones se comunicará a los alumnos con antelación suficiente.

Sexta. *Configuración técnica mínima de los equipos para realizar la fase on line de los cursos en modalidad mixta.*

a) «Hardware»:

- 1.º Procesador 400 MHz.
- 2.º 128 megas de memoria RAM o superior.
- 3.º Tarjeta de sonido, altavoces o auriculares.

b) «Software»:

- 1.º Windows 2000, ME, XP, Vista, Windows 7.
- 2.º Internet Microsoft Explorer, versión 6.0 o superior, con máquina virtual Java SUN 1.4 o superior.
- 3.º Plug-in Macromedia Flash Player 6.
- 4.º Plug-in Macromedia Shockwave Player 8.5.
- 5.º Plug-in Real One Player.

En el caso de que el sistema operativo sea Windows NT, las versiones de los plug-in que se indican más arriba tendrán que ser las señaladas o inferiores.

c) Requisitos de conectividad:

Configuración de los servidores proxy/firewall de las redes corporativas en las que se encuentren los usuarios:

- 1.º Posibilidad de descargar ficheros con las extensiones dcr, swf, mp3, ra, rm desde el servidor de la empresa adjudicataria.
- 2.º Posibilidad de que los usuarios que no los tengan puedan descargar e instalar en sus equipos los plug-in enumerados en el párrafo anterior.

d) Otros requisitos:

- 1.º Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente.
- 2.º Tipo de conexión a Internet: banda ancha.

Séptima. *Diplomas.*

Los participantes que acrediten un buen aprovechamiento de las enseñanzas impartidas recibirán el correspondiente diploma. Una inasistencia o falta de conexión superior al diez por ciento de las horas lectivas programadas, aunque esté justificada, imposibilitará su expedición.

Octava. *Información adicional.*

Se podrá solicitar información adicional sobre esta convocatoria en la dirección de correo electrónico formacion.ccn@cni.es o a través del teléfono 91 372 67 85.

Madrid, 6 de junio de 2013.–El Director del Instituto Nacional de Administración Pública, Manuel Arenilla Sáez.

ANEXO

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0919	X CURSO DE GESTIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES-IMPLANTACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD	<p>Obtener los conocimientos necesarios para el análisis y gestión de riesgos de un sistema de las TIC. Como resultado de lo anterior, podrán redactar y aplicar los procedimientos y políticas de seguridad adecuados para proteger la información procesada, almacenada o transmitida por un sistema</p> <p>Familiarizar en el uso de la herramienta PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos) para ser capaces de realizar un análisis de riesgos formal siguiendo la metodología MAGERIT</p> <p>Proporcionar los conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías, estrategias y herramientas necesarias en cada organización concreta para verificar la seguridad de redes, aplicaciones y dispositivos, así como verificar y corregir los procesos e implementaciones</p> <p>Ofrecer la ayuda necesaria para poder implantar las medidas propuestas en el Esquema Nacional de Seguridad (ENS)</p>	<p>Se consideran como prioridades para la selección al curso:</p> <ul style="list-style-type: none"> • 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 • Tener responsabilidades, en el nivel directivo, 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 un año 	<p>Fase <i>on line</i>:</p> <ul style="list-style-type: none"> • Análisis y gestión de riesgos • Esquema Nacional de Seguridad <p>Fase presencial:</p> <ul style="list-style-type: none"> • Política STIC • Procedimientos STIC • Medidas técnicas STIC • Esquema Nacional de Seguridad • Análisis y gestión de riesgos • Inspecciones STIC 	<p>30 h <i>on line</i></p> <p>50 h presenciales</p>	<p>Fase <i>on line</i>: del 2 al 13 de septiembre</p> <p>Fase presencial: del 16 al 27 de septiembre</p>

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0920	XXIV CURSO DE ESPECIALIDADES CRIPTOLÓGICAS: Parte I - Fundamentos de criptología	Conocer los aspectos básicos necesarios para la elección adecuada de técnicas y parámetros criptológicos que se deben emplear en una red de cifra	Para participar en la fase presencial es imprescindible superar la fase <i>on line</i>	<p>Fase <i>online</i>:</p> <ul style="list-style-type: none"> • Principios digitales • Teoría de números <p>Fase presencial:</p> <ul style="list-style-type: none"> • Principios digitales • Teoría de números • Probabilidades • Criptografía clásica • <i>Tempest</i> • Teoría de la criptografía • Teoría de la criptofonía 	<p>125 h <i>on line</i></p> <p>50 h presenciales</p>	<p>Fase <i>on line</i>: del 2 de septiembre al 4 de octubre</p> <p>Fase presencial: del 7 al 18 de octubre</p>
	Parte II - Equipamiento criptológico	Proporcionar los conocimientos necesarios para administrar y gestionar redes de cifra con los cifradores adecuados y normativas adecuadas	Para participar es imprescindible haber superado la parte I	<ul style="list-style-type: none"> • Normativa y seguridad criptológica • Evaluación de equipos • Equipamiento criptológico • Interconexiones • Seguridad electrónica • Interoperabilidad 	25 h presenciales	Modalidad presencial: del 21 al 25 de octubre

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0925	VIII CURSO STIC – SEGURIDAD EN REDES INALÁMBRICAS	<p>Aportar conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías 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</p>	<ul style="list-style-type: none"> - Conocimiento mínimo en el nivel administrativo de sistemas <i>Linux</i> y <i>Windows</i>, así como conocimientos básicos de protocolos y equipamiento de red - Se consideran como prioridades para la selección al curso: <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 - Tener responsabilidades, en el 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 dos años 	<p>Medidas técnicas:</p> <ul style="list-style-type: none"> • Comunicación WMAN • Comunicación WLAN • Dispositivos WPAN 	25 h presenciales	Modalidad presencial: del 11 al 15 de noviembre

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0926	IX CURSO STIC - CORTAFUEGOS	<p>Impartir 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>	<ul style="list-style-type: none"> - Conocimiento mínimo en el nivel administrativo de sistemas <i>Linux</i> y <i>Windows</i>, así como conocimientos básicos de protocolos y equipamiento de red - Se consideran como prioridades para la selección al curso: <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 - Tener responsabilidades, en el 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 dos años 	<ul style="list-style-type: none"> • Cortafuegos, protocolos y seguridad perimetral • NAT y reglas de filtrado • AAA y seguridad de contenidos • VPN y usuarios móviles • Enrutadores y cortafuegos a nivel de sistema 	25 h presenciales	Modalidad presencial: del 18 al 22 de noviembre

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0927	IX CURSO STIC – DETECCIÓN DE INTRUSOS	Dotar de 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	<ul style="list-style-type: none"> - Conocimiento mínimo en el nivel administrativo de sistemas <i>Linux</i> y <i>Windows</i>, así como conocimientos básicos de protocolos y equipamiento de red - Se consideraran como prioridades para la selección al curso: <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 - Tener responsabilidades, en el 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 dos años 	<ul style="list-style-type: none"> • Conceptos de IDS y análisis de tráfico • Análisis de tráfico e IDS a nivel de Red (NIDS) • IDS a nivel de sistema (HIDS) • Análisis de registros y <i>honeypots</i> • Detección de ataques con infraestructura IDS combinada 	25 h presenciales	Modalidad presencial: del 25 al 29 de noviembre