

III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

- 592** *Resolución de 18 de enero de 2013, del Instituto Nacional de Administración Pública, por la que se convoca un curso de Seguridad de las Tecnologías de la Información y Comunicaciones en colaboración con el Centro Criptológico Nacional, en modalidad mixta.*

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

El INAP, en colaboración con el Centro Criptológico Nacional, convoca para el primer semestre del año 2013, un curso de Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC), cuya finalidad es proporcionar a los participantes los conocimientos y habilidades necesarias en la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.

Por ello, esta Dirección adopta la siguiente resolución:

Primera. *Objeto.*

Mediante esta resolución se convoca un curso de Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC), de 80 horas lectivas, 30 en modalidad on line y 50 en modalidad presencial, según el programa que se adjunta como anexo.

La superación de la fase on line será requisito imprescindible para participar en la fase presencial.

Segunda. *Lugar de celebración y calendario.*

La fase de formación on line se desarrollará del 18 de febrero al 1 de marzo de 2013, y la fase presencial, del 4 al 15 de marzo de 2013. La fase presencial del curso se celebrará en las instalaciones de la Escuela de Guerra del Ejército de Tierra, situadas en la c/ Santa Cruz de Marcenado, 25; 28015 Madrid.

Tercera. *Destinatarios.*

Podrán solicitar el curso los empleados públicos al servicio de las Administraciones públicas de los subgrupos A1, A2 o C1, y personal laboral equivalente, que tengan responsabilidades en la planificación, gestión o administración de los 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.

Cuarta. *Configuración técnica mínima de los equipos para realizar la fase on line.*

Para poder realizar la fase on line, los equipos deberán reunir los siguientes requisitos:

a) Hardware:

Procesador 40 MHz.

128 megas de memoria RAM o superior.

Tarjeta de sonido, altavoces o auriculares.

b) Software:

Windows 2000, ME, XP, Vista, Windows 7.

Internet Microsoft Explorer, versión 6.0 o superior, con máquina virtual Java SUN 1.4 o superior.

Plug-in Macromedia Flash Player 6.

Plug-in Macromedia Shockwave Player 8.5.

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 apartado previo.

d) Otros requisitos:

Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente.

Tipo de conexión a Internet: Banda ancha.

Quinta. *Selección.*

1. El número de alumnos admitidos no excederá de 30. 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, considerando prioritario encontrarse desarrollando actividades de planificación, gestión o administración de sistemas de las tecnologías de la información y las comunicaciones, o su seguridad; 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. 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 o falta de conexión, sin previo aviso o cumplida justificación, de quienes hubiesen sido seleccionados para participar en el curso podrá determinar su exclusión en selecciones posteriores.

Sexta. 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 15 días naturales, durante 24 horas, contados a partir del día siguiente al de la publicación de esta resolución en el «Boletín Oficial del Estado».

Para cualquier problema técnico relacionado con la inscripción electrónica se podrá contactar con el INAP a través de la dirección de correo electrónico ft@inap.es.

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, 18 de enero de 2013.–El Director del Instituto Nacional de Administración Pública, Manuel Arenilla Sáez.

ANEXO

Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (FTS-0914-01)

Materias	Programa	Breve descripción del contenido
Políticas STIC (Fase <i>on line</i>)	<ul style="list-style-type: none"> – Introducción a STIC. – Normativa de seguridad. – Políticas de seguridad. 	Orientaciones de seguridad. Conceptos y terminología STIC. Introducción a la criptología. Criptosistemas y modos de empleo de la cifra. Introducción a la criptofonía. Organización y gestión de seguridad. Política de seguridad de las TIC.
Procedimientos STIC (Fase <i>on line</i>)	<ul style="list-style-type: none"> – Procedimiento de acreditación. – Inspecciones STIC. – Gestión de incidentes. 	Acreditación de sistemas. Vulnerabilidades, amenazas y riesgos. Documentación de seguridad. Inspección STIC. Introducción a la amenaza TEMPEST. Gestión de incidentes de seguridad
Medidas técnicas STIC (Fase <i>on line</i>)	<ul style="list-style-type: none"> – Herramientas de seguridad. – Seguridad perimetral. – Redes inalámbricas. 	<i>Software</i> malicioso. Herramientas de seguridad. Seguridad perimetral. Interconexión de sistemas. Cortafuegos y sistemas de detección de intrusos. Seguridad inalámbrica.
Introducción a la criptología	<ul style="list-style-type: none"> – Criptografía clásica. – Criptosistemas modernos. – Teoría de la criptofonía 	Principios básicos de la criptología. Criptografía moderna. Criptografía de clave pública. Sistemas de criptofonía.
Introducción a la amenaza	<ul style="list-style-type: none"> – Vulnerabilidades y amenazas 	Vulnerabilidades y amenazas a los sistemas de información. Casos prácticos de ataque.

Materias	Programa	Breve descripción del contenido
Políticas STIC	<ul style="list-style-type: none"> - Introducción STIC. - Normativa de seguridad. - Políticas de seguridad. 	Esquema nacional de evaluación y certificación de la seguridad de las TIC. Esquema Nacional de Seguridad. Criterios de evaluación de la seguridad de las TIC Laboratorio de evaluación. Legislación nacional. Política de seguridad de las TIC en la Administración. Organización de seguridad de las TIC.
Procedimientos STIC	<ul style="list-style-type: none"> - Procedimiento de acreditación. - Análisis y gestión de riesgos. - Inspecciones STIC. - Gestión de incidentes. - Amenaza TEMPEST. 	Análisis y gestión de riesgos. MAGERIT y herramienta PILAR. Seguridad física, documental y del personal. Procedimiento de acreditación. Documentación de seguridad del sistema. Procedimiento de inspección STIC. Interconexión de sistemas. Gestión de incidentes. Evaluación TEMPEST.
Medidas técnicas STIC	<ul style="list-style-type: none"> - Herramientas de seguridad. - Equipamiento STIC. 	Dispositivos de protección de perímetro. Antivirus. Sistemas de protección de integridad. <i>Software</i> de cifrado. Herramientas de análisis de vulnerabilidades. Tarjetas inteligentes. Telefonía móvil. Seguridad inalámbrica. Infraestructura de clave pública (PKI).
Seguridad criptológica	<ul style="list-style-type: none"> - Seguridad criptológica. 	Coordinación criptológica. Tipos de cifradores. Equipamiento STIC para la Administración.
Grupo varios	<ul style="list-style-type: none"> - Inauguración y clausura. 	Inauguración. Juicio crítico y clausura.