

## III. OTRAS DISPOSICIONES

### MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

**5520** *Resolución de 13 de mayo de 2015, 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 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 viene colaborando desde hace años con el Centro Criptológico Nacional en la organización de actividades formativas para empleados públicos en materia de seguridad de las tecnologías de la información y comunicaciones, en el marco del convenio de colaboración suscrito entre la Secretaría de Estado de Administración Pública, el Centro Nacional de Inteligencia y el INAP, para impulsar la seguridad en el ámbito de la administración electrónica.

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:

Primero. *Objeto.*

Mediante esta resolución se convocan seis acciones 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 describen en el anexo, y que se desarrollarán durante el segundo semestre de 2015.

Segundo. *Destinatarios.*

Podrán solicitar el curso de especialidades criptológicas, y el de gestión de seguridad de las tecnologías de la información y del Esquema Nacional de Seguridad (Gestión STIC), los empleados públicos pertenecientes a cuerpos y escalas de los subgrupos A1 y A2, y el 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. Las demás actividades formativas podrán ser solicitadas por los empleados públicos de los subgrupos A1, A2 y C1, y el personal laboral equivalente, que tengan responsabilidades, 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.

Tercero. *Plazo de presentación de solicitudes.*

El plazo de presentación de solicitudes comenzará el día siguiente al de la publicación de esta resolución en el «Boletín Oficial del Estado» y finalizará el 16 de junio de 2015.

Quien desee participar en los cursos convocados deberá cumplimentar la correspondiente solicitud electrónica. El acceso a dicha solicitud se podrá realizar desde el catálogo de formación <http://buscadorcursos.inap.es/formacion-tic> donde se podrán localizar los cursos que se encuentran en período de inscripción. También podrá acceder entrando en <http://www.inap.es/cursos-de-seguridad-tic-en-colaboracion-con-el-ccn>.

Para realizar la inscripción será preciso contar con la autorización previa del superior jerárquico. A los efectos de formalizar dicha autorización, el sistema de inscripción le

permitirá imprimir la solicitud que, una vez firmada, deberá conservar en soporte papel y podrá ser requerida por el INAP en cualquier momento.

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](mailto:ft@inap.es).

#### Cuarto. *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 la falta de conexión a la parte «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.

#### Quinto. *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 resultara 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 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), y los cursos de acreditación en entornos Windows y de la herramienta PILAR, en modalidad

semipresencial, tendrán 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 constará de dos partes:

- a) Parte I, con fase a distancia y presencial. Será imprescindible superar la prueba de evaluación de la fase a distancia 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.

Sexto. *Configuración técnica mínima de los equipos para realizar la fase «on line».*

a) Hardware:

1. Procesador: 1,2 GHz.
2. 512 Mb de memoria RAM o superior.
3. Tarjeta de sonido, altavoces o auriculares.

b) Software:

1. «Windows Vista», «Windows 7» o «Windows 8».
2. «Microsoft Internet Explorer», versión 6.0 o superior, con máquina virtual «Java SUN» 1.4 o superior.
3. «Plug-in» «Macromedia Flash Player 6».
4. «Plug-in» «Macromedia Shockwave Player 8.5».
5. «Plug-in» «Real One Player».
6. 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. Posibilidad de descargar ficheros con las extensiones dcr, swf, mp3, ra, rm, desde el servidor de la empresa adjudicataria.
2. 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. Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente.
2. Tipo de conexión a Internet: Banda ancha.

Séptimo. *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.

Octavo. *Régimen académico.*

Los alumnos seleccionados 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 podrá consultarse en <http://www.inap.es/conocenos>) podrán ser excluidos de las actividades formativas.

Noveno. *Información adicional.*

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

Madrid, 13 de mayo de 2015.—El Director del Instituto Nacional de Administración Pública, Manuel Arenilla Sáez.

**ANEXO**

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0919	XII CURSO DE GESTIÓN DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES Y DEL ESQUEMA NACIONAL DE SEGURIDAD (GESTIÓN STIC)	<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 poder 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 la aplicación de 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"> <li>- Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el Centro Criptológico Nacional.</li> <li>- Haber realizado cursos relacionados con las tecnologías de la información o su seguridad.</li> <li>- 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 período superior a un año.</li> </ul>	<p>Fase <i>on line</i>:</p> <p>Curso de análisis y gestión de riesgos de los sistemas de información.</p> <p>Curso del Esquema Nacional de Seguridad.</p> <p>Fase presencial:</p> <p>Políticas STIC.</p> <p>Procedimientos STIC.</p> <p>Medidas técnicas STIC.</p> <p>Esquema Nacional de Seguridad.</p> <p>Análisis y gestión de riesgos.</p> <p>Inspecciones STIC.</p>	<p>30 h <i>on line</i>.</p> <p>50 h presenciales.</p>	<p>Fase <i>on line</i>:</p> <p>del 31 de agosto al 18 de septiembre.</p> <p>Fase presencial:</p> <p>del 21 de septiembre al 2 de octubre.</p>

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0920	XXVI 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 a distancia.	Fase a distancia: Principios digitales. Teoría de números. Fase presencial: Principios digitales. Teoría de números. Probabilidades. Criptografía clásica. <i>Tempest</i> . Teoría de la criptografía. Teoría de la criptofonía.	125 h a distancia. 50 h presenciales.	Fase a distancia: del 14 de septiembre al 16 de octubre. Fase presencial: del 19 al 30 de octubre.
	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.	Fase presencial: Normativa y seguridad criptológica. Evaluación de equipos. Equipamiento criptológico. Interconexiones. Seguridad electrónica. Interoperabilidad.	25 h presenciales.	Fase presencial: del 2 al 6 de noviembre.
0922	XII CURSO ACREDITACIÓN STIC – ENTORNOS WINDOWS	Proporcionar los conocimientos necesarios para comprobar, con suficiente garantía, los aspectos de seguridad de sistemas servidores <i>Windows Server 2008 R2</i> , estaciones clientes con <i>Windows 7</i> , aplicaciones servidoras <i>Internet Information Services (ISS)</i> y servicios <i>Exchange de Microsoft</i> .  Al tratarse de un curso de acreditación, se utilizará como marco de referencia la normativa recogida en la serie CCN-STIC implementando las configuraciones de seguridad definidas en las guías CCN-STIC-500 para entornos basados en tecnología <i>Microsoft</i> .	Un conocimiento mínimo de sistemas <i>Windows</i> , así como conocimientos básicos de protocolos de red.  Se considerarán como prioridades para la selección al curso:  - Haber realizado con anterioridad el Curso Básico STIC - Entornos <i>Windows</i> 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 <i>Windows 7/2008 Server</i> . - 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.	Fase <i>on line</i> : Curso básico de seguridad en entornos <i>Windows</i>  Fase presencial: Medidas técnicas STIC Seguridad sistemas operativos Seguridad servicios web Seguridad servicios de correo	15 h <i>on line</i> . 25 h presenciales.	Fase <i>on line</i> : del 21 de septiembre al 2 de octubre. Fase presencial: del 5 al 9 de octubre.

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0937	II CURSO DE ACTUALIZACIÓN DE CONOCIMIENTOS DE SEGURIDAD EN ENTORNOS WINDOWS (HERRAMIENTA CLARA)	Proporcionar los conocimientos necesarios sobre la evolución de la seguridad hacia la plataforma de Windows 7 y Windows Server 2008 R2 tomando como partida los conocimientos en infraestructuras Windows XP y Windows Server 2003.	Disponer de conocimientos de administración de sistemas Windows cliente y servidor.  Disponer conocimientos de redes (incluyendo TCP-IP) y conceptos básicos de seguridad.  Haber realizado con anterioridad el Curso Acreditación STIC - Entornos Windows desarrollado por el Centro Criptológico Nacional (CCN).	Modelo de seguridad de Windows XP y 2003 respecto a Windows 7 y 2008. Modelo de autorización y autenticación. Seguridad en el sistema de archivos. Subsistema de Red. Infraestructura de dominio. Administración basada en Powershell. Implementación de seguridad a través de las guías CCN-STIC. Herramienta CLARA.	16 h presenciales.	Modalidad presencial: del 13 al 15 de octubre.
0934	VI CURSO STIC – HERRAMIENTA PILAR	Proporcionar los conocimientos y habilidades necesarias para poder evaluar el estado de seguridad de un sistema, identificando y valorando sus activos y las amenazas que se ciernen sobre ellos, así como familiarizar a los asistentes con el uso de la herramienta PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos) para poder realizar un análisis de riesgos formal siguiendo la metodología MAGERIT.	Disponer de 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 del curso:  - Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN. - Haber realizado con anterioridad el Curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones (Gestión STIC) desarrollado por el CCN. - Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. - Estar desarrollando en su puesto de trabajo, actividades de planificación, gestión o implementación de sistemas de las tecnologías de la información y las comunicaciones, o la seguridad de los mismos, por un periodo superior a 1 año.	Fase on line: Análisis y gestión de riesgos. Introducción a la gestión del riesgo.  Fase presencial: Análisis de riesgos. Gestión del riesgo. Tratamiento de los riesgos.	10 h on line.  25 h presenciales.	Fase on line: del 2 al 13 de noviembre.  Fase presencial: del 16 al 20 de noviembre.

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0933	VII CURSO STIC – SEGURIDAD EN APLICACIONES WEB	Proporcionar 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.	<p>Disponer de un conocimiento mínimo de los sistemas <i>Linux</i> y <i>Windows</i>, 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"> <li>- Haber realizado con anterioridad el Curso STIC – Inspecciones de Seguridad desarrollado por el Centro Criptológico Nacional (CCN).</li> <li>- Haber realizado con anterioridad el Curso STIC – Cortafuegos desarrollado por el Centro Criptológico Nacional (CCN).</li> <li>- Haber realizado con anterioridad el Curso STIC – Detección de Intrusos desarrollado por el Centro Criptológico Nacional (CCN).</li> <li>- Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN.</li> <li>- Haber realizado cursos relacionados con las tecnologías de la información o su seguridad.</li> <li>- 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.</li> </ul>	<p>Introducción a las amenazas en aplicaciones Web.</p> <p>Protocolos Web.</p> <p>Herramientas de análisis y manipulación Web.</p> <p>Ataques sobre entornos Web.</p> <p>Mecanismos de autenticación y autorización Web.</p> <p>Gestión de sesiones.</p> <p>Inyección SQL.</p> <p>Cross-Site Scripting (XSS).</p> <p>Cross-Site Request Forgery (CSRF).</p>	25 h presenciales.	Modalidad presencial: del 23 al 27 de noviembre.