

III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

397 *Resolución de 11 de enero de 2017, 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 siete 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 primer semestre de 2017.

Segundo. *Destinatarios.*

Podrán solicitar el curso de especialidades criptológicas 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.

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 27 de enero de 2017.

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 que 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.

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 seguridad de las tecnologías de la información y comunicaciones (STIC), el curso de acreditación en entornos windows y el curso de especialidades criptológicas, 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:

- Parte I, con fase on line y presencial. Será imprescindible superar la prueba de evaluación de la fase a distancia para participar en la presencial.
- 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.º Procesador: 1,2 GHz.
- 2.º 1 Gb de memoria RAM o superior.
- 3.º Tarjeta de sonido, altavoces o auriculares.

b) Software:

- 1.º Windows vista, windows 7, windows 8 o windows 10.
- 2.º Microsoft internet explorer, versión 6.0 o superior, con máquina virtual Java SUN 1.4 o superior.
- 3.º Plug-in adobe flash player.
- 4.º En el caso de que el sistema operativo sea windows NT, las versiones de los plug-in que se indican anteriormente 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.

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 10 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 www.inap.es/conocenos) podrán ser excluidos de las actividades formativas.

Para el desarrollo de los procesos de aprendizaje, los alumnos contarán con el acceso gratuito a «Ágora» (<http://agora.edu.es/>), a La Administración al Día (<http://laadministracionaldia.inap.es>) y al Banco de Conocimiento (<http://bci.inap.es/>), así como a la Red Social Profesional (<https://social.inap.es/>).

Noveno. *Información adicional.*

Se podrá solicitar información adicional sobre esta convocatoria en la dirección de correo electrónico formacion.ccn@cni.es.

Madrid, 11 de enero de 2017.–El Director del Instituto Nacional de Administración Pública, Manuel Arenilla Sáez.

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0938	III CURSO STIC DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD (HERRAMIENTAS CCN-CERT)	Proporcionar los conocimientos necesarios para gestionar de manera adecuada los incidentes de seguridad TIC a los que se enfrenta una organización mediante la utilización de las herramientas del CCN-CERT	<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"> - 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 STIC – Inspecciones de Seguridad desarrollado por el Centro Criptológico Nacional (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 dos (2) años 	<p>Herramienta CARMEN:</p> <ul style="list-style-type: none"> Usuarios y roles Filtros básicos Uso de listas Indicadores de compromiso Análisis de movimiento externo (HTTP, DNS, SMTP) Análisis de movimiento lateral (NetBIOS) Analizadores e Indicadores Creación de <i>plugins</i> <p>Herramienta LUCIA:</p> <ul style="list-style-type: none"> Introducción a la herramienta Conceptos de RTIR Fujos de trabajo Sincronización de Instancias <p>Herramienta REYES:</p> <ul style="list-style-type: none"> Indicadores de compromiso Exportación de reglas SNORT, YARA, o IOCs de forma automática. Introducción de muestras de <i>malware</i> Automatización de tareas y procesos utilizando la API REST 	25 h presenciales	Modalidad presencial: del 13 al 17 de marzo

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0931	X CURSO STIC – BÚSQUEDA DE EVIDENCIAS	Proporcionar los conocimientos necesarios para que realizando un reconocimiento previo de un sistema de las TIC, adquirir la capacidad de buscar y encontrar rastros y evidencias de un ataque o infección	<p>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"> - 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, 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 dos (2) años 	<p>Metodología</p> <p>Cómo y qué buscar</p> <p>Estudio práctico</p> <p>Lugares donde buscar datos</p> <p>Análisis de ficheros</p>	25h presenciales	Modalidad presencial: del 27 al 31 de marzo

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0933	IX CURSO STIC – SEGURIDAD EN APLICACIONES WEB	<p>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>	<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"> - 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 un (1) año 	<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><i>Cross-Site Scripting (XSS)</i></p> <p><i>Cross-Site Request Forgery (CSRF)</i></p>	<p>25 h presenciales</p>	<p>Modalidad presencial:</p> <p>del 3 al 7 de abril</p>

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0922	XIV CURSO ACREDITACIÓN STIC – ENTORNOS WINDOWS (HERRAMIENTA CLARA)	<p>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>.</p> <p>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>.</p>	<p>Un conocimiento mínimo de sistemas <i>Windows</i>, 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"> - 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 un (1) año <p>Para participar en la fase presencial es imprescindible superar la fase a distancia</p>	<p>Fase <i>on line</i>:</p> <p>Curso básico de seguridad en entornos <i>Windows</i></p> <p>Fase presencial:</p> <p>Medidas técnicas STIC Seguridad sistemas operativos Seguridad servicios web Seguridad servicios de correo Herramienta CLARA</p>	<p>15 h <i>on line</i></p> <p>25 h presenciales</p>	<p>Fase <i>on line</i>: del 17 al 21 de abril</p> <p>Fase presencial: del 24 al 28 de abril</p>

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0936	VI CURSO STIC – SEGURIDAD EN DISPOSITIVOS MÓVILES	Proporcionar a los participantes los conocimientos y habilidades necesarias para conocer de manera detallada, actual y práctica las amenazas y vulnerabilidades de seguridad que afectan a los dispositivos móviles y sus comunicaciones	<p>Se supondrá, por parte de los solicitantes, un conocimiento mínimo a nivel administrativo de sistemas <i>Linux</i> y <i>Windows</i>, así como conocimientos básicos de sistemas de comunicaciones móviles</p> <p>Se considerarán como prioridades para la selección al curso, las siguientes:</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 (CCN) - Haber realizado cursos relacionados con las tecnologías de la información o su seguridad - Tener responsabilidades, a nivel directivo o 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 (2) años 	<p>Seguridad de las comunicaciones GSM, GPRS/EDGE, UMTS, LTE</p> <p>Dispositivos móviles</p> <p>Modelo y arquitectura de seguridad.</p> <p>Gestión local y empresarial de dispositivos móviles basados en <SO></p> <p>Cifrado de datos y gestión de certificados digitales y credenciales en <SO></p> <p>Comunicaciones USB</p> <p>Comunicaciones Bluetooth</p> <p>Comunicaciones Wi-Fi</p> <p>Comunicaciones GSM (2G) y UMTS (3G)</p> <p>Comunicaciones TCP/IP</p>	35 h presenciales	Modalidad presencial: del 4 al 12 de mayo

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0920	XXVIII 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	<p>Fase <i>on line</i>:</p> <p>Principios digitales Teoría de números</p> <p>Fase presencial:</p> <p>Principios digitales Teoría de números Probabilidades Criptografía clásica <i>Tempest</i> Teoría de la criptografía Teoría de la criptofonía</p>	<p>125 h <i>on line</i></p> <p>50 h presenciales</p>	<p>Fase <i>on line</i>:</p> <p>del 8 de mayo al 9 de junio</p> <p>Fase presencial: del 12 al 23 de junio</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 en la parte II es imprescindible haber superado la parte I.	<p>Fase presencial:</p> <p>Normativa y seguridad criptológica Evaluación de equipos Equipamiento criptológico Interconexiones Seguridad electrónica Interoperabilidad</p>	25 h presenciales	Fase presencial: del 26 al 30 de junio