



[INAP convoca acciones formativas en materia de seguridad de las tecnologías de la información y comunicaciones.](#)

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.

[Ver BOE](#)

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.

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.

Plazo de presentación de solicitudes.

El plazo de presentación de solicitudes comenzará el 14 de enero 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 <mailto:ft@inap.es>.

*Trabajando juntos. Decidimos todos
La dignidad no se negocia.*

ANEXO

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0914	XIV CURSO DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Proporcionar los conocimientos necesarios para conseguir una mentalización y concienciación adecuada en la seguridad de los Sistemas de las TIC y las amenazas y vulnerabilidades que representan las nuevas tecnologías	<p>Tener responsabilidades en la planificación, gestión o administración de los sistemas de las tecnologías de la información y las comunicaciones, o en su seguridad por un periodo superior a dos (2) años.</p> <p>Para participar en la fase presencial es imprescindible superar la fase a distancia</p>	<p>Fase <i>on line</i>:</p> <p>Curso de seguridad en tecnologías de la información y comunicaciones: Introducción a STIC Normativa de seguridad Políticas de seguridad Procedimiento de acreditación Inspecciones STIC Gestión de incidentes Herramientas de seguridad Seguridad perimetral Redes inalámbricas</p> <p>Fase presencial:</p> <p>Introducción a la criptología: Criptografía clásica Criptosistemas modernos Teoría de la criptofonía Introducción a la amenaza: Vulnerabilidades y amenazas Políticas STIC: Introducción STIC Normativa de seguridad Políticas de seguridad Procedimientos STIC: Procedimiento de acreditación. Análisis y gestión de riesgos Inspecciones STIC Gestión de incidentes Amenaza TEMPEST Medidas técnicas STIC: Herramientas de seguridad Equipamiento STIC Seguridad criptológica: Seguridad criptológica</p>	<p>30 h <i>on line</i></p> <p>50 h presenciales</p>	<p>Fase <i>on line</i>: del 13 al 24 de febrero</p> <p>Fase presencial: del 27 de febrero al 10 de marzo</p>

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 Flujos 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	<p>Modalidad presencial:</p> <p>del 13 al 17 de marzo</p>



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	<p>Modalidad presencial:</p> <p>del 27 al 31 de marzo</p>



CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0933	IX 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"> - 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</i> (XSS)</p> <p><i>Cross-Site Request Forgery</i> (CSRF)</p>	25 h presenciales	<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</i> de <i>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>:</p> <p>del 17 al 21 de abril</p> <p>Fase presencial:</p> <p>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 período 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	<p>Modalidad presencial:</p> <p>del 4 al 12 de mayo</p>



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	Fase <i>on line</i> : 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 <i>on line</i> 50 h presenciales	Fase <i>on line</i> : del 8 de mayo al 9 de junio Fase presencial: del 12 al 23 de junio
	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.	Fase presencial: Normativa y seguridad criptológica Evaluación de equipos Equipamiento criptológico Interconexiones Seguridad electrónica Interoperabilidad	25 h presenciales	Fase presencial: del 26 al 30 de junio