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	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. Para participar en la fase presencial es imprescindible superar la fase a distancia	Fase *on line*: 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 Fase presencial: 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	30 h *on line* 50 h presenciales	Fase *on line*: del 13 al 24 de febrero Fase presencial: del 27 de febrero al 10 de marzo

cve: BOE-A-2017-397
Verificable en http://www.boe.es

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	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 al 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 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	Herramienta CARMEN: 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 *plugins* Herramienta LUCIA: Introducción a la herramienta Conceptos de RTIR Flujos de trabajo Sincronización de Instancias Herramienta REYES: Indicadores de compromiso Exportación de reglas SNORT, YARA, o IOCs de forma automática. Introducción de muestras de *malware* Automatización de tareas y procesos utilizando la API REST	25 h presenciales	Modalidad presencial: del 13 al 17 de marzo

cve: BOE-A-2017-397
Verificable en http://www.boe.es

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	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 al curso: - 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	Metodología Cómo y qué buscar Estudio práctico Lugares donde buscar datos Análisis de ficheros	25h presenciales	Modalidad presencial: del 27 al 31 de marzo

cve: BOE-A-2017-397
Verificable en http://www.boe.es

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	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 al curso: - 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	Introducción a las amenazas en aplicaciones web Protocolos web Herramientas de análisis y manipulación web Ataques sobre entornos web Mecanismos de autenticación y autorización web Gestión de sesiones Inyección SQL *Cross-Site Scripting* (XSS) *Cross-Site Request Forgery* (CSRF)	25 h presenciales	Modalidad presencial: del 3 al 7 de abril

cve: BOE-A-2017-397
Verificable en http://www.boe.es

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0922	XIV CURSO ACREDITACIÓN STIC – ENTORNOS WINDOWS (HERRAMIENTA CLARA)	Proporcionar los conocimientos necesarios para comprobar, con suficiente garantía, los aspectos de seguridad de sistemas servidores *Windows Server* 2008 R2, estaciones clientes con *Windows* 7, aplicaciones servidoras *Internet Information Services* (ISS) y servicios *Exchange* de *Microsoft* 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 *Microsoft*	Un conocimiento mínimo de sistemas *Windows*, así como conocimientos básicos de protocolos de red Se considerarán como prioridades para la selección al curso: - Actividad relacionada con la administración de sistemas de las tecnologías de la información y comunicaciones (TIC) bajo entornos Windows 7/2008 Server - 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 Para participar en la fase presencial es imprescindible superar la fase a distancia	Fase *on line*: Curso básico de seguridad en entornos *Windows* Fase presencial: Medidas técnicas STIC Seguridad sistemas operativos Seguridad servicios web Seguridad servicios de correo Herramienta CLARA	15 h *on line* 25 h presenciales	Fase *on line*: del 17 al 21 de abril Fase presencial: del 24 al 28 de abril

cve: BOE-A-2017-397
Verificable en http://www.boe.es

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	Se supondrá, por parte de los solicitantes, un conocimiento mínimo a nivel administrativo de sistemas *Linux y Windows*, así como conocimientos básicos de sistemas de comunicaciones móviles Se considerarán como prioridades para la selección al curso, las siguientes: - 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	Seguridad de las comunicaciones GSM, GPRS/EDGE, UMTS, LTE Dispositivos móviles Modelo y arquitectura de seguridad. Gestión local y empresarial de dispositivos móviles basados en <SO> Cifrado de datos y gestión de certificados digitales y credenciales en <SO> Comunicaciones USB Comunicaciones Bluetooth Comunicaciones Wi-Fi Comunicaciones GSM (2G) y UMTS (3G) Comunicaciones TCP/IP	35 h presenciales	Modalidad presencial: del 4 al 12 de mayo

cve: BOE-A-2017-397
Verificable en http://www.boe.es

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 *on line*: Principios digitales Teoría de números Fase presencial: Principios digitales Teoría de números Probabilidades Criptografía clásica *Tempest* Teoría de la criptografía Teoría de la criptofonía	125 h *on line* 50 h presenciales	Fase *on line*: 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

http://www.boe.es
BOLETÍN OFICIAL DEL ESTADO
D. L.: M-1/1958 - ISSN: 0212-033X

cve: BOE-A-2017-397
Verificable en http://www.boe.es