III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

941 *Resolución de 28 de enero de 2016, 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 ocho 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 2016.

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.

El personal militar perteneciente al Ministerio de Defensa deberá tramitar su solicitud a través de la convocatoria específica que realizará dicho ministerio en «Boletín Oficial de Defensa». Con el fin de proceder a la expedición del certificado electrónico de superación del curso, es imprescindible que los solicitantes, una vez admitidos al curso, se inscriban también a través de la página web del INAP siguiendo las instrucciones descritas en el apartado tercero de esta convocatoria.

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 14 de febrero de 2016.

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.

cve: BOE-A-2016-941
Verificable en http://www.boe.es

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 especialidades criptológicas, el curso de seguridad en infraestructura de red y el curso de acreditación en entornos *Windows*, 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.

cve: BOE-A-2016-941
Verificable en http://www.boe.es

El curso de especialidades criptológicas constará de dos partes:

a) 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.
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, *Windows* 8 o *Windows* 10.
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.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 diez por ciento de las horas lectivas programadas, aunque esté justificada, imposibilitará su expedición.

cve: BOE-A-2016-941
Verificable en http://www.boe.es

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.

Noveno. *Información adicional.*

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

Madrid, 28 de enero de 2016.–El Director del Instituto Nacional de Administración Pública, Manuel Arenilla Sáez.

cve: BOE-A-2016-941
Verificable en http://www.boe.es

ANEXO

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0931	IX 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	25 h presenciales	Modalidad presencial: del 29 de febrero al 4 de marzo
0918	XI CURSO BÁSICO STIC – INFRAESTRUCTURA DE RED	Proporcionar los conocimientos necesarios para comprobar, con suficiente garantía, los aspectos de seguridad relativos a la infraestructura de red basada en elementos de comunicaciones (concentradores, enrutadores…), dispositivos inalámbricos y redes privadas virtuales (VPN) introduciendo los conceptos de cortafuegos, sistemas de detección de intrusos (IDS) y dispositivos trampa (*honeypots y honeynets*)	Un conocimiento mínimo de sistemas *Windows/Unix*, así como conocimientos básicos de protocolos y equipamiento de red Se considerarán como prioridades para la selección al curso: - 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 Centro Criptológico Nacional - 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 STIC de Infraestructura de Red Fase presencial: Dispositivos comunicaciones Dispositivos de filtrado Redes inalámbricas Redes privadas virtuales Seguridad perimetral	15 h *on line* 25 h presenciales	Fase *on line*: del 29 de febrero al 11 de marzo Fase presencial: del 14 al 18 de marzo

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0933	VIII 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 7 al 11 de marzo
0930	XI CURSO STIC – INSPECCIONES DE SEGURIDAD	Proporcionar los conocimientos y habilidades necesarias para comprobar, con suficiente garantía, los aspectos de seguridad de redes, aplicaciones y dispositivos en cada organización concreta, así como verificar y corregir los procesos e implementaciones	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: - Actividad relacionada con la verificación de la seguridad 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 período superior a dos (2) años	Herramientas de seguridad Verificaciones de seguridad Inspecciones STIC (Nivel 3)	25 h presenciales	Modalidad presencial: del 4 al 8 de abril

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0922	XIII 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 11 al 22 de abril Fase presencial: del 25 al 29 de abril
0917	XI CURSO BÁSICO STIC – BASES DE DATOS	Proporcionar los conocimientos necesarios para comprobar, con suficiente garantía, los aspectos de seguridad relativos a la configuración segura de las bases de datos *Oracle y MS SQL Server*	Un conocimiento mínimo a nivel administrativo de base de datos, así como conocimientos básicos de sistemas *Windows/Unix* y protocolos de red Se considerarán como prioridades para la selección al curso: - Actividad relacionada con la administración de bases de datos en 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 Centro Criptológico Nacional - 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	Seguridad entornos *SQL Server* Seguridad entornos *Oracle*	25h presenciales	Modalidad presencial: del 18 al 22 de abril

cve: BOE-A-2016-941
Verificable en http://www.boe.es

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0920	XXVII CURSO DE ESPECIALIDADES CRIPTOLÓGICAS: Parte I - Fundamentos de criptología Parte II - Equipamiento criptológico	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 25 de abril al 27 de mayo Fase presencial: del 30 de mayo al 10 de junio
		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 13 al 17 de junio

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0938	I 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 *plug-in* 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 9 al 13 de mayo

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