III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

6694 *Resolución de 12 de junio 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 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 2017.

Segundo. *Destinatarios.*

Podrán solicitar el curso de gestión de seguridad de las tecnologías de la información y del Esquema Nacional de Seguridad (Gestión STIC) los funcionarios 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 funcionarios pertenecientes a cuerpos y escalas de los subgrupos A1, A2 y C1, y el personal laboral equivalente, que tengan responsabilidades en la planificación, gestión, administración o mantenimiento de sistemas de las tecnologías de la información y las comunicaciones o en su seguridad.

Tercero. *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. 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.

El curso de gestión de seguridad de las tecnologías de la información y del Esquema Nacional de Seguridad (Gestión STIC), el curso STIC de detección de intrusos y el curso STIC de la Herramienta PILAR, en modalidad semipresencial, tendrán una fase on line y

cve: BOE-A-2017-6694
Verificable en http://www.boe.es

una presencial. La superación de la fase on line será requisito imprescindible para participar en la fase presencial.

La fase presencial de las actividades semipresenciales, así como los cursos en modalidad presencial, se celebrarán en Madrid. La sede definitiva de desarrollo de las acciones se comunicará a los alumnos con antelación suficiente.

Las actividades formativas podrán ser grabadas o retransmitidas en streaming, lo que se comunica a los efectos oportunos.

Cuarto. *Solicitudes.*

1. 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.

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 descargar la solicitud que, una vez firmada, deberá conservar 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.

2. El plazo de presentación de solicitudes comenzará el día siguiente al de la publicación de esta resolución en el «Boletín Oficial del Estado» y será de diez días hábiles.

Quinto. *Selección y admisión de alumnos.*

1. El número de alumnos admitidos no excederá, con carácter general, de veinticuatro. La selección de los participantes la realizará el Centro Criptológico Nacional. Además de los establecidos específicamente en el anexo para cada curso, en la selección se observarán los siguientes criterios: trayectoria profesional y curricular de los candidatos; vinculación entre el puesto desempeñado y 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 funcionarios 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 funcionarios 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 deberán hacer constar tal circunstancia en la inscripción, y en caso de ser seleccionadas, habrán de indicar las adaptaciones necesarias para la participación en la actividad formativa.

5. 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.

cve: BOE-A-2017-6694
Verificable en http://www.boe.es

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

Para la realización de la fase on line, los equipos deberán contar con la siguiente configuración mínima:

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. *Certificados.*

Los participantes que acrediten un buen aprovechamiento de las enseñanzas impartidas recibirán un correo electrónico indicándoles la dirección a la que podrán acceder para descargarse su certificado en soporte digital. 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 puede 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 puede solicitar información adicional sobre esta convocatoria en la dirección de correo electrónico formacion.ccn@cni.es.

Madrid, 12 de junio de 2017.–El Director del Instituto Nacional de Administración Pública, Manuel Arenilla Sáez.

cve: BOE-A-2017-6694
Verificable en http://www.boe.es

ANEXO

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0927	XIII CURSO STIC – DETECCIÓN DE INTRUSOS	Proporcionar a los participantes los conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías de detección de intrusiones más adecuadas en cada organización concreta, y para implementar y utilizar de forma óptima cada una de las capacidades que éstas ofrecen para contribuir de forma eficiente al conjunto de la seguridad de la organización	Conocimiento mínimo en el nivel administrativo de sistemas *Linux* y *Windows*, así como conocimientos básicos de protocolos y equipamiento de red Se consideran 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, en el 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 Para participar en la fase presencial es imprescindible superar la fase *on line*	Fase *on line*: Curso STIC de Detección de Intrusos Fase presencial: Conceptos de IDS y análisis de tráfico Análisis de tráfico e IDS a nivel de Red (NIDS) IDS a nivel de sistema (HIDS) Análisis de registros y *honeypots* Detección de ataques con infraestructura IDS combinada	15 h *on line* 25 h presenciales	Fase *on line*: del 4 al 8 de septiembre Fase presencial: del 11 al 15 de septiembre

cve: BOE-A-2017-6694
Verificable en http://www.boe.es

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0919	XIV CURSO DE GESTIÓN DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES Y DEL ESQUEMA NACIONAL DE SEGURIDAD (GESTIÓN STIC)	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 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 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 Ofrecer la ayuda necesaria para la aplicación de las medidas propuestas en el Esquema Nacional de Seguridad (ENS)	Se consideran 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 Centro Criptológico Nacional - Haber realizado cursos relacionados con las tecnologías de la información o su seguridad - 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	Fase *on line*: Curso de análisis y gestión de riesgos de los sistemas de información Curso del Esquema Nacional de Seguridad Fase presencial: Políticas STIC Procedimientos STIC Medidas técnicas STIC Esquema Nacional de Seguridad Análisis y gestión de riesgos Inspecciones STIC	30 h *on line* 50 h presenciales	Fase *on line*: Del 11 al 22 de septiembre Fase presencial: del 25 de septiembre al 6 de octubre

cve: BOE-A-2017-6694
Verificable en http://www.boe.es

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0925	XII CURSO STIC – SEGURIDAD EN REDES INALÁMBRICAS	Proporcionar a los participantes los conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías inalámbricas más adecuadas en cada organización concreta, y para implementar y utilizar de forma óptima cada una de las capacidades que éstas ofrecen para contribuir de forma eficiente al conjunto de la seguridad de la organización	Conocimiento mínimo en el nivel administrativo de sistemas *Linux* y *Windows,* así como conocimientos básicos de protocolos y equipamiento de red Se consideran 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, en el 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	Medidas técnicas: Comunicación WMAN Comunicación WLAN Dispositivos WPAN	25 h presenciales	Modalidad presencial: del 18 al 22 de septiembre

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0930	XII 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, en el 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)	25h presenciales	Modalidad presencial: del 23 al 27 de octubre

cve: BOE-A-2017-6694
Verificable en http://www.boe.es

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0934	VIII 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 el puesto de trabajo actividades de planificación, gestión o implementación de sistemas de las tecnologías de la información y las comunicaciones, o su seguridad, por un período 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 6 al 10 de noviembre Fase presencial: del 13 al 17 de noviembre

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0939	I CURSO STIC AVANZADO DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD	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 con anterioridad el curso de Gestión de Incidentes - 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 Casos prácticos de ataques complejos	25 h presenciales	Modalidad presencial: del 20 al 24 de noviembre

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

cve: BOE-A-2017-6694
Verificable en http://www.boe.es