III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

388 *Resolución de 9 de enero de 2018, del Instituto Nacional de Administración Pública, por la que se convocan acciones formativas en materia de seguridad de las tecnologías de la información y las 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 las 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, con el fin de continuar desarrollando las competencias de los empleados públicos implicados en la seguridad de las tecnologías de la información y las comunicaciones,

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 las comunicaciones que se desarrollarán durante el primer semestre de 2018, según el programa y modalidad formativa que se describen en el anexo.

Segundo. *Destinatarios.*

Estas actividades formativas podrán ser solicitadas por los empleados públicos 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, mantenimiento o seguridad de sistemas de las tecnologías de la información y las comunicaciones. En el anexo se detallan los requisitos específicos para cada acción formativa.

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 previstas, 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 de dicha actividad. 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 se esté utilizando.

El curso de seguridad de las tecnologías de la información y comunicaciones (STIC) y el curso de acreditación en entornos windows tendrán una fase on line y 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.

cve: BOE-A-2018-388
Verificable en http://www.boe.es

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 del INAP 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 tal efecto, la solicitud firmada deberá conservarse por las personas interesadas y 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 aplicación del Real Decreto 2271/2004, de 3 de diciembre, se valorará como criterio de selección el reconocimiento de un grado de discapacidad igual o superior al 33 por ciento. En el caso de recibir varias solicitudes de un mismo organismo o institución, se seleccionará al candidato con el perfil más ajustado al 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. Para que pueda ser convenientemente valorada, las personas con discapacidad que soliciten el curso deberán hacer constar tal circunstancia en la inscripción y, en el caso de ser seleccionadas, habrán de indicar las adaptaciones necesarias para la participación en la actividad formativa.

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.

cve: BOE-A-2018-388
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.

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 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 a través de la dirección de correo electrónico formacion.ccn@cni.es.

Madrid, 9 de enero de 2018.–El Director del Instituto Nacional de Administración Pública, Manuel Arenilla Sáez.

cve: BOE-A-2018-388
Verificable en http://www.boe.es

ANEXO

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0914	XV curso de seguridad de las tecnologías de la información y comunicaciones	Conocer las principales amenazas y vulnerabilidades y adquirir conocimientos para asegurar una adecuada seguridad de los Sistemas de las TIC.	Tener responsabilidades en la planificación, gestión, administración y/o seguridad de sistemas de las tecnologías de la información y las comunicaciones por un periodo superior a dos (2) años. Para participar en la fase presencial es imprescindible haber superado la fase on line.	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 12 al 23 de febrero. Fase presencial: Del 26 de febrero al 9 de marzo.

cve: BOE-A-2018-388
Verificable en http://www.boe.es

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0938	IV curso STIC de gestión de incidentes de ciberseguridad (herramientas CCN-CERT)	Adquirir conocimientos 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 de 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, 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.	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	Del 12 al 16 de marzo.
0931	XI curso STIC-búsqueda de evidencias	Adquirir la capacidad de realizar reconocimientos de sistemas de las TIC para identificar rastros y evidencias de ataques o infecciones.	Disponer de un conocimiento mínimo de los sistemas Linux y Windows, así como de 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, 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 periodo superior a dos (2) años.	Metodología. Cómo y qué buscar. Estudio práctico. Lugares donde buscar datos. Análisis de ficheros.	25 horas presenciales	Del 19 al 23 de marzo.

cve: BOE-A-2018-388
Verificable en http://www.boe.es

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0933	X curso STIC-seguridad en aplicaciones web	Adquirir una visión detallada, actual y práctica de las amenazas y vulnerabilidades de seguridad que afectan a las infraestructuras, entornos y aplicaciones web.	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, 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 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). Los diferentes módulos incluyen una descripción detallada de vulnerabilidades, técnicas de ataque, mecanismos de defensa y recomendaciones de seguridad, incluyendo numerosas demostraciones y ejercicios prácticos.	25 h presenciales	Del 9 al 13 de abril.
0922	XV curso acreditación STIC- entornos windows (herramienta CLARA)	Adquirir 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.	Disponer de un conocimiento mínimo de sistemas Windows, así como de 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, 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 un (1) año. Para participar en la fase presencial es imprescindible haber superado la fase on line.	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. 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.	15 h on line 25 h presenciales	Fase on line: Del 9 al 13 de abril. Fase presencial: Del 16 al 20 de abril.

cve: BOE-A-2018-388
Verificable en http://www.boe.es

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0936	VII curso STIC-seguridad en dispositivos móviles	Adquirir conocimientos y habilidades para reconocer y abordar de manera detallada, actual y práctica las amenazas y vulnerabilidades de seguridad que afectan a los dispositivos móviles y sus comunicaciones.	Disponer de un conocimiento mínimo a nivel administrativo de sistemas Linux y Windows, así como de 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, en el 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	Del 3 al 11 de mayo.
0938	V curso STIC de gestión de incidentes de ciberseguridad (herramientas CCN-CERT)	Adquirir conocimientos 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, 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.	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 EST.	25 h presenciales	Del 21 al 25 de mayo.

cve: BOE-A-2018-388
Verificable en http://www.boe.es