# III. OTRAS DISPOSICIONES

## MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

**898** *Resolución de 27 de enero de 2014, 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.

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:

Primera. *Objeto.*

Mediante esta resolución se convocan actividades 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 describe en los anexos y que se desarrollarán durante el primer semestre de 2014.

Segunda. *Destinatarios.*

Podrán solicitar dichas actividades formativas los empleados públicos pertenecientes a los cuerpos y escalas de los subgrupos A1, A2 y C1, y el personal laboral equivalente, que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de sistemas de las tecnologías de la información y las comunicaciones o en su seguridad y, según la materia, en entornos web y desarrollo de aplicaciones web.

El personal militar perteneciente al Ministerio de Defensa deberá tramitar su solicitud a través de la convocatoria específica que realizará dicho departamento.

Tercera. *Plazo de presentación de solicitudes.*

El plazo de presentación de solicitudes será de quince días naturales contados a partir del día siguiente al de la publicación de esta resolución en el «Boletín Oficial del Estado».

Quien desee participar en el curso convocado deberá solicitarlo mediante la cumplimentación del modelo de solicitud electrónica. Los candidatos deberán presentar la solicitud que figura en la página web del INAP (www.inap.es) entrando en «Aprendizaje» y, a continuación, seleccionando «Formación en administración electrónica», «Cursos en materia de seguridad TIC en colaboración con el CCN» y, finalmente, el apartado denominado «Inscripción electrónica». Una vez ejecutada la acción «Grabar solicitud», se generará una copia del modelo de solicitud que deberán imprimir y pasar a la firma del superior jerárquico. Una vez firmada, deberán conservar la solicitud en su poder hasta que se les requiera su presentación.

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.

Cuarta. *Selección.*

1. El número de alumnos admitidos no excederá, con carácter general, de veinte. 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;

cve: BOE-A-2014-898

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 falta de conexión a los cursos 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.

Quinta. *Modalidad formativa, lugar de celebración y calendario.*

Las actividades formativas en modalidad presencial se celebrarán en las fechas que se indican en el anexo. En el caso de que resulte 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 la 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 seguridad de las tecnologías de la información y las comunicaciones de la herramienta PILAR, impartido en modalidad mixta, tendrá 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 del curso citado, así como las demás actividades formativas, se celebrarán en Madrid. La sede definitiva de desarrollo de dichas actividades se comunicará a los alumnos con antelación suficiente.

Sexta. *Configuración técnica mínima de los equipos para realizar la fase on line del curso de seguridad de las tecnologías de la información y las comunicaciones de la herramienta PILAR.*

a) Hardware:

1.º Procesador 400 MHz.
2.º 128 Mb de memoria RAM o superior.
3.º Tarjeta de sonido, altavoces o auriculares.

cve: BOE-A-2014-898

b) Software:

1.º Windows 2000, ME, XP, Vista, Windows 7.
2.º Microsoft Internet Explorer, versión 6.0 o superior con máquina virtual Java SUN 1.4 o superior.
3.º Plug-in Macromedia Flash Player 6.
4.º Plug-in Macromedia Shockwave Player 8.5.
5.º Plug-in Real One Player.
6.º En el caso de que el sistema operativo sea Windows NT, las versiones indicadas de los plug-in 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 apartado previo.

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.

Séptima. *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.

Octava. *Información adicional.*

Se podrá solicitar información adicional sobre esta convocatoria en la dirección de correo electrónico formacion.ccn@cni.es o a través del teléfono 91 372 67 85.

Madrid, 27 de enero de 2014.–El Director del Instituto Nacional de Administración Pública, Manuel Arenilla Sáez.

cve: BOE-A-2014-898

## ANEXO

| CÓDIGO | DENOMINACIÓN | OBJETIVOS | REQUISITOS | PROGRAMA | DURACIÓN | FECHAS |
|---|---|---|---|---|---|---|
| 0918 | IX CURSO BÁSICO STIC – INFRAESTRUCTURA DE RED | Proporcionar a los participantes los conocimientos necesarios para que sean capaces de 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<br>- Se considerarán como prioridades para la selección al curso:<br>■ Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de las tecnologías de la información y comunicaciones (TIC)<br>■ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el Centro Criptológico Nacional<br>■ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad<br>-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 año | Dispositivos comunicaciones<br>Dispositivos de filtrado<br>Redes inalámbricas<br>Redes privadas virtuales<br>Seguridad perimetral | 25 h | Del 17 al 21 de marzo |
| 0936 | III CURSO STIC – SEGURIDAD EN DISPOSITIVOS MÓVILES | Proporcionar a los concurrentes 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 concurrentes, un conocimiento mínimo a nivel administrativo de sistemas *Linux y Windows*, así como conocimientos básicos de sistemas de comunicaciones móviles<br>- Se considerarán como prioridades para la selección al curso, las siguientes:<br>■ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el Centro Criptológico Nacional (CCN)<br>■ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad<br>- 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 un año. | Seguridad de las comunicaciones GSM, GPRS/EDGE, UMTS, LTE<br>Dispositivos móviles<br>Modelo y arquitectura de seguridad<br>Gestión local y empresarial de dispositivos móviles basados en <SO><br>Cifrado de datos y gestión de certificados digitales y credenciales en <SO><br>Comunicaciones USB<br>Comunicaciones *Bluetooth*<br>Comunicaciones *Wi-Fi*<br>Comunicaciones GSM (2G) y UMTS (3G)<br>Comunicaciones TCP/IP | 35 h | Del 24 de marzo al 1 de abril |
| 0922 | XI CURSO ACREDITACIÓN STIC – ENTORNOS WINDOWS | Proporcionar a los participantes los conocimientos necesarios para que sean capaces de comprobar, con suficiente garantía, los aspectos de seguridad de sistemas servidores *Windows 2003*, estaciones clientes con *Windows XP*, aplicaciones servidoras *Internet Information Services (ISS) y servicios Exchange de Microsoft*<br><br>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<br>- Se considerarán como prioridades para la selección al curso:<br>■ Haber realizado con anterioridad el Curso Básico STIC - Entornos *Windows* desarrollado por el Centro Criptológico Nacional (CCN)<br>■ Actividad relacionada con la administración de sistemas de las tecnologías de la información y comunicaciones (TIC) bajo entornos *Windows* 2003/XP<br>■ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN<br>■ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad<br>- 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 año | Medidas técnicas STIC<br>Seguridad sistemas operativos<br>Seguridad servicios web<br>Seguridad servicios de correo | 25 h | Del 7 al 11 de abril |

| CÓDIGO | DENOMINACIÓN | OBJETIVOS | REQUISITOS | PROGRAMA | DURACIÓN | FECHAS |
|---|---|---|---|---|---|---|
| 0931 | VII CURSO STIC – BÚSQUEDA DE EVIDENCIAS | Proporcionar a los participantes los conocimientos necesarios para que, tras realizar un reconocimiento previo de un sistema de las TIC, sean capaces 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<br>- Se considerarán como prioridades para la selección del curso:<br>■ Haber realizado con anterioridad el Curso Básico STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN)<br>■ Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de las tecnologías de la información y comunicaciones (TIC)<br>■ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN<br>■ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad<br>- 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 un año | Metodología<br><br>Cómo y qué buscar<br><br>Estudio práctico<br><br>Lugares donde buscar datos<br><br>Análisis de ficheros | 25 h | Del 21 al 25 de abril |
| 0933 | VI CURSO STIC – SEGURIDAD EN APLICACIONES WEB | Proporcionar a los participantes 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 | - Un conocimiento mínimo de los sistemas *Linux y Windows*, así como conocimientos básicos de protocolos y equipamiento de red<br><br>- Se considerarán como prioridades para la selección al curso:<br>■ Haber realizado con anterioridad el Curso STIC – Inspecciones de Seguridad desarrollado por el Centro Criptológico Nacional (CCN)<br>■ Haber realizado con anterioridad el Curso STIC – Cortafuegos desarrollado por el Centro Criptológico Nacional (CCN)<br>■ Haber realizado con anterioridad el Curso STIC – Detección de Intrusos desarrollado por el Centro Criptológico Nacional (CCN)<br>■ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN<br>■ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad<br><br>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 año | Introducción a las amenazas en aplicaciones web<br>Protocolos web<br>Herramientas de análisis y manipulación web<br>Ataques sobre entornos web<br>Mecanismos de autenticación y autorización web.<br>Gestión de sesiones<br>Inyección SQL<br>*Cross-Site Scripting* (XSS)<br>*Cross-Site Request Forgery* (CSRF) | 25 h | Del 5 al 9 de mayo |
| 0930 | IX CURSO STIC – INSPECCIONES DE SEGURIDAD | Proporcionar a los participantes los conocimientos y habilidades necesarias para que sean capaces de 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<br>- Se considerarán como prioridades para la selección del curso:<br>■ Actividad relacionada con la verificación de la seguridad asociada a sistemas de las tecnologías de la información y comunicaciones (TIC)<br>■ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN<br>■ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad<br>- 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 año | Herramientas de seguridad<br><br>Verificaciones de seguridad<br><br>Inspecciones STIC (Nivel 3) | 25 h | Del 19 al 23 de mayo |

| CÓDIGO | DENOMINACIÓN | OBJETIVOS | REQUISITOS | PROGRAMA | DURACIÓN | FECHAS |
|---|---|---|---|---|---|---|
| 0934 | V CURSO STIC – HERRAMIENTA PILAR | Proporcionar a los participantes 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 | - Un conocimiento mínimo de los sistemas *Linux y Windows*, así como conocimientos básicos de protocolos y equipamiento de red<br><br>- Se considerarán como prioridades para la selección del curso:<br>■ Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN<br>■ Haber realizado con anterioridad el Curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones (GSTIC) desarrollado por el CCN<br>■ Haber realizado cursos relacionados con las tecnologías de la información o su seguridad<br><br>- Estar desarrollando en su 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 periodo mínimo de un año | Fase *on line* (10 horas):<br>- Análisis y gestión de riesgos<br>- Introducción a la gestión del riesgo<br><br>Fase presencial (25 horas):<br>- Análisis de riesgos<br>- Gestión del riesgo<br>- Tratamiento de los riesgos | 35 h | Fase *on line:* del 26 al 30 de mayo<br><br>Fase presencial: del 2 al 6 de junio |



cve: BOE-A-2014-898