III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

1748 *Resolución de 7 de febrero de 2013, 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.*

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, en colaboración con el Centro Criptológico Nacional, convoca para el primer semestre del año 2013 ocho actividades formativas en materia de seguridad de las tecnologías de la información y comunicaciones en la administración electrónica, de las cuales una se impartirá en modalidad mixta, tal y como se detalla en los anexos.

Por ello, esta Dirección adopta la siguiente resolución:

Primera. *Objeto.*

Mediante la presente resolución se convocan actividades formativas en materia de seguridad de las tecnologías de la información y comunicaciones en la administración electrónica, según el programa previsto en los anexos, y que se desarrollarán durante el primer semestre de 2013. El curso de seguridad de las tecnologías de la información y comunicaciones de la herramienta PILAR (Proceso Informático y Lógico de Análisis de Riesgos) se celebrará en modalidad mixta.

Segunda. *Destinatarios.*

Podrán solicitar dichas actividades formativas los empleados públicos de las Administraciones públicas de los subgrupos A1, A2 y C1, y el personal laboral equivalente, que tengan responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de sistemas de las tecnologías de la información y las comunicaciones, 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 ministerio.

Tercera. *Lugar de celebración y calendario.*

El curso de seguridad de las tecnologías de la información y las comunicaciones de la herramienta PILAR, en modalidad mixta, tendrá una fase on line que se desarrollará del 27 al 31 de mayo de 2013, y una fase presencial, del 3 al 7 de junio de 2013. La superación de la fase on line será requisito imprescindible para participar en la fase presencial. Las actividades formativas en modalidad presencial se celebrarán en las fechas que se indican en el anexo I.

La fase presencial del citado curso, 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.

Cuarta. *Configuración técnica mínima de los equipos para realizar la fase on line del curso sobre la herramienta PILAR.*

a) Hardware:

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

cve: BOE-A-2013-1748

b) Software:

1.º Windows 2000, ME, XP, Vista, Windows 7.
2.º Internet Microsoft 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.

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 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.

Quinta. *Selección.*

1. El número de alumnos admitidos no excederá de 20. 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. En el curso sobre la herramienta PILAR, se considerará como prioridad para ser seleccionado:

a) 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 de su seguridad, por un periodo mínimo de un año.
b) Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el Centro Criptológico Nacional.
c) Haber realizado con anterioridad el Curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones (GSTIC) desarrollado por el Centro Criptológico Nacional.
d) Haber realizado cursos relacionados con las tecnologías de la información o su seguridad.

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

cve: BOE-A-2013-1748

discapacidad, con objeto de actualizar los conocimientos de los empleados públicos y empleadas públicas. Asimismo, se reservará al menos un 40 por 100 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 o falta de conexión, sin previo aviso o cumplida justificación de quienes hubiesen sido seleccionados para participar en el curso podrá determinar su exclusión en selecciones posteriores.

Sexta. *Inscripción y plazo de presentación de solicitudes.*

Los interesados que cumplan con el perfil de destinatario descrito deberán inscribirse electrónicamente en la página web del INAP (www.inap.es).

El plazo de presentación de solicitudes electrónicas será de 15 días naturales, durante 24 horas, contados a partir del día siguiente al de la publicación de esta resolución en el «Boletín Oficial del Estado».

Para cualquier problema técnico relacionado con la inscripción electrónica, se podrá contactar con el INAP a través de la dirección de correo electrónico ft@inap.es.

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, 7 de febrero de 2013.–El Director del Instituto Nacional de Administración Pública, Manuel Arenilla Sáez.

cve: BOE-A-2013-1748

ANEXO I

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0922	X 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*. 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: ▪ Haber realizado con anterioridad el Curso Básico STIC - Entornos *Windows*, desarrollado por el Centro Criptológico Nacional (CCN). ▪ Actividad relacionada con la administración de sistemas de las tecnologías de la información y comunicaciones (TIC) bajo entornos *Windows 2003/XP*. ▪ 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 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 Seguridad sistemas operativos Seguridad servicios web Seguridad servicios de correo	25 h	Del 1 al 5 de abril
0917	VIII CURSO BÁSICO STIC – BASES DE DATOS	Proporcionar a los participantes los conocimientos necesarios para que sean capaces de 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 (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 año.	Seguridad entornos *SQL Server*. Seguridad entornos *Oracle*.	25 h	Del 8 al 12 de abril
0918	VIII 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. - 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 (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 año.	Dispositivos comunicaciones Dispositivos de filtrado Redes inalámbricas Redes privadas virtuales Seguridad perimetral	25 h	Del 15 al19 de abril

cve: BOE-A-2013-1748

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0930	VIII 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. - Se considerarán como prioridades para la selección del 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 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 un año	Herramientas de seguridad. Verificaciones de seguridad. Inspecciones STIC (nivel 3).	25 h	Del 22 al 26 de abril
0933	V 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. - 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 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 un 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	Del 6 al 10 de mayo
0936	II 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 concurrentes, 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 un año.	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.	25 h	Del 20 al 24 de mayo

Código	Denominación	Objetivos	Requisitos	Programa	Duración	Fechas
0931	VI CURSO STIC – BÚSQUEDA DE EVIDENCIAS	Proporcionar a los participantes los conocimientos necesarios para que, realizando 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. - Se considerarán como prioridades para la selección del 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 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 periodo superior a un año.	Metodología. Cómo y qué buscar. Estudio práctico. Lugares donde buscar datos. Análisis de ficheros.	25 h	Del 10 al 14 de junio

ANEXO II

Código	Denominación	Objetivos	Modalidad y asisgnaturas	Contenido	Créditos		
					Total	Teoría	Práctica
0934	IV 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	▪ Fase *on line* (10 horas) - Análisis y gestión de riesgos - Introducción a la gestión del riesgo	▪ Análisis de riesgos (activos, amenazas, salvaguardas, indicadores de impacto). Calificación de los riesgos.	1	1	0
			▪ Fase presencial (25 horas) - Análisis de riesgos - Gestión del riesgo - Tratamiento de los riesgos	▪ Análisis de riesgos (activos, amenazas, salvaguardas, indicadores de impacto). Mitología. Herramientas. Ciclos de gestión de riesgos. Plan director. Costes. Métodos de aseguramiento. Herramienta PILAR	2,4	0,8	1,6
			▪ Grupo varios	▪ Inauguración. Juicio crítico y clausura	0,1	0,1	0

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