III. OTRAS DISPOSICIONES

MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

10337 *Resolución de 6 de junio de 2011, del Instituto Nacional de Administración Pública, por la que se convocan acciones formativas en materia de seguridad de las tecnologías de la administración electrónica en colaboración con el Centro Criptológico Nacional en modalidad presencial y mixta, para el segundo semestre de 2011.*

Entre las funciones asignadas al Instituto Nacional de Administración Pública, de acuerdo con el Real Decreto 464/2011, de 1 de abril, por el que se aprueba el Estatuto del Instituto Nacional de Administración Pública, se encuentra la formación y el perfeccionamiento de los empleados públicos.

El Instituto Nacional de Administración Pública, en colaboración con el Centro Criptológico Nacional, convoca para el segundo semestre del año 2011, tres actividades formativas en materia de seguridad de las tecnologías de la administración electrónica en la modalidad presencial y mixta (on line/presencial) (véase Anexo).

En aplicación del Real Decreto 2271/2004, de 3 de diciembre, se valorará como criterio de participación a quienes se encuentren afectados por una discapacidad cuyo grado de minusvalía sea igual o superior al 33%. Quienes se encuentren afectados por una discapacidad, debidamente acreditada, cuyo grado de minusvalía sea igual o superior al 33% podrán hacer constar tal circunstancia en la solicitud. En caso de ser seleccionado, podrán indicarse al Centro Criptológico Nacional las adaptaciones que consideren necesarias en el curso formativo en el momento de confirmación de su asistencia en el mismo.

De conformidad con lo establecido en el Acuerdo de Formación para el Empleo de las Administraciones Públicas, de 22 de marzo de 2010, se fomentarán las medidas, en materia de formación, que tiendan a favorecer la conciliación de la vida familiar y laboral.

Adicionalmente, de conformidad 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, durante un año, a quienes se hayan incorporado 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.

Finalmente, los empleados públicos podrán recibir y participar en cursos de formación durante los permisos de maternidad, paternidad, así como durante las excedencias por motivos familiares.

Bases

Primera. *Objeto*.–Mediante la presente Resolución se convocan tres actividades formativas en materia de seguridad de las tecnologías de la administración electrónica en la modalidad presencial y mixta (on line/presencial), cuyas materias se detallan en el Anexo.

En los cursos mixtos, para participar en la fase presencial, será condición imprescindible superar las pruebas correspondientes a la fase on-line.

Segunda. *Destinatarios*.–Podrán solicitar dichas actividades formativas, en el caso del curso de Especialidades Criptológicas, los funcionarios de los subgrupos A1 y A2, y personal laboral equivalente, que tenga responsabilidades en la planificación, gestión, administración o mantenimiento de los sistemas de las tecnologías de la información y las comunicaciones, o en la seguridad de los mismos. Para el resto de actividades formativas

cve: BOE-A-2011-10337

los funcionarios de los subgrupos A1, A2 y C1, y personal laboral equivalente, que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de los sistemas de las tecnologías de la información y comunicaciones, o en la seguridad de los mismos.

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

Tercera. *Configuración técnica de su equipo (en el caso de cursos que cuenten con modalidad de teleformación-on line).*–Se dispondrá de un equipo que tenga como mínimo la siguiente configuración:

Hardware:

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

Software:

Windows 2000, ME, XP, Vista, Windows 7.
Internet Microsoft Explorer, versión 6.0 o superior con máquina virtual Java SUN 1.4 o superior.
Plug-in Macromedia Flash Player 6.
Plug-in Macromedia Shockwave Player 8.5.
Plug-in Real One Player.
En el caso de que el sistema operativo sea Windows NT, las versiones de los pluggins que se indican más arriba tendrán que ser las señaladas o inferiores.

Requisitos de Conectividad:

Configuración de los servidores proxy/firewall de las redes corporativas en las que se encuentren los usuarios:

Posibilidad de descargar ficheros con las extensiones dcr, swf, mp3, ra, rm desde el servidor de la empresa adjudicataria.
Posibilidad de que los usuarios que no los tengan puedan descargar e instalar en sus equipos los plug-ins enumerados en el apartado previo.

Otros requisitos:

Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente.
Tipo de conexión a Internet: Banda ancha.

Cuarta. *Selección.*–El número de alumnos admitidos no excederá de cuarenta y cinco. La selección final de los participantes corresponde al 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 caso de recibir varias solicitudes de un mismo organismo o institución se seleccionará al candidato con el perfil más ajustado al destinatario del curso.

Una vez efectuada la selección definitiva de participantes, el Centro Criptológico Nacional comunicará por correo electrónico a cada uno de los alumnos, 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.

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.

cve: BOE-A-2011-10337

Quinta. *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) entrando en «Formación», seguidamente en «Formación en Administración Electrónica» y a continuación seleccionando «Cursos de Seguridad TIC en colaboración con el CCN». En este apartado estará publicada la información relativa a cada una de las actividades formativas con la opción «Presentación de solicitud telemática», ejecutando la opción «Inscripción». Una vez cumplimentado el modelo de solicitud deberá ejecutarse la opción «Grabar y enviar» para completar la transmisión de datos telemática. Se generará una copia del modelo de solicitud que deberá imprimir y pasar a la firma del superior jerárquico, la cual deberá conservar en su poder.

Para cualquier incidencia o duda en la inscripción debe dirigirse al correo electrónico ft@inap.es.

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

Sexta. *Diplomas.*–Los participantes que acrediten un buen aprovechamiento de las enseñanzas impartidas recibirán el correspondiente diploma. Una inasistencia superior al diez por ciento de las horas presenciales lectivas, así como la falta de seguimiento continuo en la plataforma on line, sea cual sea la causa, imposibilitará la expedición del mismo.

Séptima. *Información adicional.*–Se podrá solicitar información adicional sobre esta convocatoria en los teléfonos: 91372.67.85/91372.53.77, así como a la dirección de correo electrónico formacion.ccn@cni.es.

Madrid, 6 de junio de 2011.–El Director del Instituto Nacional de Administración Pública, Ángel Manuel Moreno Molina.

cve: BOE-A-2011-10337

ANEXO

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
FTS110932 00001	IV CURSO COMMON CRITERIA	Proporcionar a los participantes los conocimientos necesarios de la normativa Common Criteria en la que se basa la actividad central del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC que constituye el Centro Criptológico Nacional según el RD 421/2004	-Haber realizado con anterioridad los siguientes cursos: ■ Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el Centro Criptológico Nacional. ■ Gestión de la Seguridad de las Tecnologías de la Información y Comunicaciones desarrollado por el Centro Criptológico Naconal. ■ Cursos relacionados con las tecnologías de la información o su seguridad. -Tener responsabilidades, a nivel funcional, 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.	Modelo general Especificación de Protection Profile (PP) y Security Target (ST) Requisitos funcionales de seguridad Requisitos de garantía de seguridad Metodología de desarrollo de Protection Profile (PP) y Security Target (ST) CC como herramienta de adquisiciones	25h	Del 12 al 16 de septiembre
FTS110934 00001	II 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 e identificando y valorando las amenazas que se ciernen sobre ellos. Familiarizar a los participantes con el uso de la herramienta PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos) siendo capaces de realizar un análisis de riesgos formal siguiendo la metodología MAGERIT.	Se consideran 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. - 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. - Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. - Tener responsabilidades, a 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 dos (2) años. Es imprescindible superar las pruebas de conocimientos adquiridos de la fase on line para poder realizar la fase presencial. Durante la fase presencial del curso, los participantes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el	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	Curso mixto: on line y presencial 10h 25h	 Del 26 al 30 de septiembre Del 3 al 7 de octubre

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
			curso como “APTO”. En caso de no superar el mínimo exigido, el alumno será considerado “NO APTO” suponiendo la baja en el curso. Al finalizar el curso, los participantes que lo hayan superado con aprovechamiento obtendrán un Certificado firmado por el Secretario de Estado Director del Centro Nacional de Inteligencia y por el Director del Instituto Nacional de Administración Pública como garantía de la superación del curso.			
FTS11092000001	XXIII CURSO DE ESPECIALIDADES CRIPTOLÓGICAS: Fase I - Fundamentos de criptología Fase II - Equipamiento criptológico	**Fase I:** -Proporcionar a los participantes los conocimientos básicos necesarios para la elección adecuada de técnicas y parámetros criptológicos a emplear en una red de cifra. **Fase II:** -Proporcionar a los participantes los conocimientos necesarios para Administrar y gestionar redes de cifra con los cifradores adecuados y normativas adecuadas.	El curso se desarrollará en dos fases: • Fase I: mixta, con una parte on line y otra presencial. • Fase II: presencial. Será condición imprescindible para realizar las distintas fases y partes del curso, superar las pruebas correspondientes, en las que se valorarán los conocimientos adquiridos en cada una. **Fase I**: el examen de la parte on line (fase I) consistirá en la contestación de un total de 30 preguntas teóricas de tipo test en formato escrito con cuatro respuestas posibles (una única verdadera) no restando puntos las mal contestadas y versarán sobre las materias estudiadas en la fase a on line. Cada pregunta tendrá el mismo valor, siendo la nota obtenida función de las preguntas acertadas respecto al número total de formuladas. Será necesario concluir esta prueba, por lo menos, con un mínimo exigido de cinco (5) puntos. La nota final del curso será de "APTO/NO APTO" cuyo resultado se considerará sólo para el acceso a la parte presencial (fase I) que se inicia posteriormente. En esta parte presencial (fase I), el alumno tendrá que superar una prueba sobre el contenido del curso. Las preguntas serán teóricas tipo test en formato escrito con cuatro respuestas	**Fase I: mixta (200 horas)** Parte on line (150 horas) Principios digitales. Teoría de números. Parte presencial (50 horas) Principios digitales. Teoría de números. Probabilidades. Criptografía clásica. Tempest. Teoría de la Criptografía. Teoría de la Criptofonía. **Fase II: presencial (25 horas)** Normativa y seguridad criptológica. Evaluación de equipos. Equipamiento criptológico. Interconexiones. Seguridad electrónica. Interoperabilidad.	225 horas	Fase I Parte on line: Del 2 de septiembre al 14 de octubre Parte presencial: del 17 al 28 de octubre Fase II presencial: Del 14 al 18 de noviembre

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
			posibles (una única verdadera) no restando puntos las mal contestadas. Cada pregunta tendrá el mismo valor, siendo la nota obtenida función de las preguntas acertadas respecto al número total de formuladas. Será necesario concluir esta prueba, por lo menos, con un mínimo exigido de cinco (5) puntos. En caso de no superar el mínimo exigido, el alumno deberá realizar una recuperación. La no superación de esta última supondrá la baja en el curso. Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el acta de finalización del curso. La **Fase II** se desarrollará en modalidad presencial, con lo cual los asistentes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerado como "APTO/NO APTO" según los mínimos exigidos. Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el acta de finalización del curso. Al finalizar el curso, los participantes que hayan superado las dos fases del curso, obtendrán un certificado firmado por el Secretario de Estado Director del Centro Nacional de Inteligencia y por el Director del Instituto Nacional de Administración Pública.			

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