III. OTRAS DISPOSICIONES

MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

10336 *Resolución de 6 de junio de 2011, del Instituto Nacional de Administración Pública, por la que se convoca curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones - Implantación del Esquema Nacional de Seguridad-, en colaboración con el Centro Criptológico Nacional en modalidad mixta.*

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, un curso de gestión de seguridad de las tecnologías de la información y las comunicaciones, cuya finalidad es proporcionar a los participantes los conocimientos necesarios para el análisis y gestión de riesgos de un sistema de las tecnologías de la información y las comunicaciones, así como proporcionar la ayuda necesaria para poder implantar las medidas propuestas en el Esquema Nacional de Seguridad. Esta actividad formativa de modalidad mixta contendrá una fase inicial de teleformación (on line).

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, podrá 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 curso GSTIC (FTS 110919)

Primera. *Objeto*.–Mediante la presente Resolución se convoca un curso de gestión de seguridad de las tecnologías de la información y las comunicaciones -implantación del Esquema Nacional de Seguridad- en la modalidad de teleformación (on line) y presencial, cuyas materias se detallan en anexo a esta Resolución.

La fase de teleformación (on line) se desarrollará del 5 al 16 de septiembre, y la fase presencial, del 19 al 30 de septiembre. El lugar de desarrollo de la fase presencial del curso será en la sede del Centro Superior de Estudios de la Defensa Nacional (CESEDEN), paseo de la Castellana, 61, Madrid (28071).

cve: BOE-A-2011-10336

Segunda. *Programa formativo*.

Fase de teleformación (on-line) (30horas):

Análisis y gestión de riesgos.
Esquema Nacional de Seguridad.

Fase presencial (50horas):

Política STIC.
Procedimientos STIC.
Medidas técnicas STIC.
Esquema Nacional de Seguridad.
Análisis y gestión de riesgos.
Inspecciones STIC.

Para participar en la fase presencial, será condición imprescindible superar las pruebas correspondientes a la fase on-line.

Tercera. *Destinatarios*.–Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los subgrupos A1 y A2, y personal laboral equivalente, que tenga responsabilidades en la planificación, gestión o administración de los sistemas de las tecnologías de la información y las 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.

Se considerarán como prioridades para la selección al curso las siguientes:

1. Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el Centro Criptológico Nacional.
2. Haber realizado cursos relacionados con las tecnologías de la información o su seguridad.
3. Tener responsabilidades 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.

Cuarta. *Configuración técnica de su equipo.*–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:

cve: BOE-A-2011-10336

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.

Quinta. *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.

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) 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 al curso 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 relacionada con el proceso de inscripción debe escribirse 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».

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 presenciales lectivas programadas, sea cual sea la causa, imposibilitará la expedición del mismo.

Octava. *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-2011-10336

ANEXO

Curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones Implantación del Esquema Nacional de Seguridad

(FTS-0919-01)

Denominación de materias	Asignaturas que componen la materia	Créditos			Contenidos
		Total	Teoría	Práct	
Política STIC.	Introducción a STIC. Normativa de seguridad. Política de seguridad.	0,6	0,6	0	Orientaciones de seguridad. Conceptos y terminología STIC. Introducción a la Criptología. Criptosistemas y modos de empleo de la cifra. Introducción a la criptofonía. Organización y Gestión de Seguridad. Política de Seguridad de las TIC.
Procedimientos STIC.	Procedimiento de acreditación. Inspecciones STIC. Gestión de incidentes.	0,5	0,5	0	Acreditación de sistemas. Vulnerabilidades, amenazas y riesgos. Documentación de seguridad. Inspección STIC. Amenaza TEMPEST y TRANSEC. Gestión de Incidentes de seguridad
Medidas técnicas STIC.	Herramientas de seguridad. Seguridad perimetral. Redes Inalámbricas.	0,5	0,5	0	Software malicioso. Herramientas de Seguridad. Seguridad perimetral. Interconexión de sistemas. Cortafuegos y Sistemas de detección de intrusos. Seguridad inalámbrica.
Esquema Nacional de Seguridad.	Introducción y categorización del ENS Auditoría y organización de seguridad en el ENS Evaluación y certificación. Normativa de seguridad.	2,8	2,8	0	Esquema Nacional de Seguridad. Procedimiento de auditoría y acreditación. Organización de Seguridad. Documentación de Seguridad. Gestión de incidentes de seguridad.
Análisis y gestión de riesgos.	Análisis y gestión de riesgos. Metodología MAGERIT. Herramienta PILAR.	2,2	1	1,2	Introducción al análisis y gestión de riesgos. Activos. Amenazas, impacto y riesgo. Instalación Herramienta PILAR. Salvaguardas y evaluaciones. Generación de documentación de seguridad. Ejemplos prácticos.
Inspecciones STIC.	Interconexión en el ENS Inspecciones STIC. Seguridad en entornos Web e inalámbricos	0,8	0,8	0	Introducción a las Inspecciones STIC. Herramientas y verificaciones de seguridad. Seguridad en los Sistemas y Dispositivos. Seguridad en aplicaciones Web. El factor humano. Casos de estudio.
Grupo varios.	Inauguración y clausura.	0,6	0,6	0	Examen previo. Inauguración. Juicio crítico y clausura.

cve: BOE-A-2011-10336