III. OTRAS DISPOSICIONES

MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

996 *Resolución de 7 de enero de 2011, del Instituto Nacional de Administración Pública, por la que se convoca curso de Seguridad de las Tecnologías de la Información y Comunicaciones en colaboración con el Centro Criptológico Nacional en modalidad mixta (blended learning).*

Entre las funciones asignadas al Instituto Nacional de Administración Pública, de acuerdo con el Real Decreto 1661/2000, de 29 de septiembre, 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 primer semestre del año 2011, un curso de seguridad de las tecnologías de la información y las comunicaciones cuya finalidad es proporcionar a los participantes los conocimientos necesarios en la seguridad de los sistemas de las tecnologías de la información y las comunicaciones. Esta actividad formativa de modalidad mixta contendrá una fase inicial de teleformación (formación on line).

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 debiendo comunicar al Centro Criptológico Nacional, en caso de ser seleccionado, las adaptaciones necesarias para la realización del curso.

Igualmente, 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%.

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 que, en materia de formación, 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.

Asimismo, se reservará al menos un cuarenta por cierto de las plazas para su adjudicación a mujeres que reúnan los requisitos establecidos, salvo que el número de solicitudes de mujeres sea insuficiente para cubrir este porcentaje.

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 STIC (FTS 110914)

Primera. *Objeto.*–Mediante la presente resolución se convoca un curso de seguridad de las tecnologías de la información y las comunicaciones en la modalidad mixta (blended learning) cuyas materias se detallan en el anexo I.

La fase a distancia (on line) se desarrollará del 28 de febrero al 11 de marzo, y la fase presencial, del 14 al 25 de marzo. 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-2011-996

Segunda. *Programa formativo.*–Fase de teleformación (on-line) (30 horas):

Políticas STIC.
Procedimientos STIC.
Medidas Técnicas STIC.

Fase presencial (50 horas):

Introducción a la Criptología.
Introducción a la Amenaza.
Políticas STIC.
Procedimientos STIC.
Medidas Técnicas STIC.
Seguridad Criptológica.

La superación de la parte on line será requisito imprescindible para participar en la fase presencial.

Tercera. *Destinatarios.*–Podrán solicitar el curso los empleados públicos al servicio de las Administraciones Públicas de los subgrupos A1, A2 y C1, 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 considerará como prioridad para ser seleccionado el estar desarrollando en su puesto de trabajo, actividades de planificación, gestión o administración de sistemas de las tecnologías de la información y las comunicaciones, o la seguridad de los mismos, por un periodo mínimo de un año.

Cuarta. *Configuración técnica mínima de los equipos.*

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.

cve: BOE-A-2011-996

Quinta. *Selección*.–El número de alumnos admitidos no excederá de treinta. 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 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).

El plazo de presentación de solicitudes electrónicas será de diez 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 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 formación.ccn@cni.es. Asimismo se podrán realizar consultas a través de la página web del Instituto Nacional de Administración Pública en Internet: www.inap.es

Madrid, 7 de enero de 2011.–El Director del Instituto Nacional de Administración Pública, Ángel Manuel Moreno Molina.

cve: BOE-A-2011-996

ANEXO I

Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (FTS 110914)

Materias	Programa	Breve descripción del contenido
Políticas STIC (Fase on-line).	– Introducción a STIC. – Normativa de Seguridad. – Políticas de Seguridad.	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 (Fase on-line).	– Procedimiento de acreditación. – Inspecciones STIC. – Gestión de incidentes.	Acreditación de sistemas. Vulnerabilidades, amenazas y riesgos. Documentación de seguridad. Inspección STIC. Introducción a la amenaza TEMPEST. Gestión de incidentes de Seguridad
Medidastécnicas STIC (Fase on-line).	– Herramientas de Seguridad. – Seguridad Perimetral. – Redes Inalámbricas.	Software malicioso. Herramientas de seguridad. Seguridad perimetral. Interconexión de sistemas. Cortafuegos y sistemas de detección de intrusos. Seguridad inalámbrica.
Introducción a la criptología.	– Criptografía clásica. – Criptosistemas modernos. – Teoría de la criptofonía.	Principios Básicos de la criptología. Criptografía moderna. Criptografía de clave pública. Sistemas de criptofonía.
Introducción a la amenaza.	– Vulnerabilidades y amenazas.	Vulnerabilidades y amenazas a los sistemas de información. Casos prácticos de ataque.
Políticas STIC.	– Introducción STIC. – Normativa de Seguridad. – Políticas de Seguridad.	Esquema Nacional de Evaluación y Certificación de la Seguridad de las T.I.C. Esquema Nacional de Seguridad. Criterios de evaluación de la seguridad de las T.I.C Laboratorio de evaluación. Legislación Nacional. Política de seguridad de las TIC en la Administración. Organización de seguridad de las TIC
Procedimientos STIC.	– Procedimiento de acreditación. – Análisis y gestión de riesgos. – Inspecciones STIC. – Gestión de incidentes. – Amenaza TEMPEST.	Análisis y gestión de riesgos. MAGERIT y Herramienta PILAR. Seguridad física, documental y del personal. Procedimiento de acreditación. Documentación de seguridad del sistema. Procedimiento de inspección STIC. Interconexión de sistemas. Gestión de incidentes. Evaluación TEMPEST.
Medidastécnicas STIC.	– Herramientas de seguridad. – Equipamiento STIC.	Dispositivos de protección de perímetro. Antivirus. Sistemas de protección de integridad. Software de cifrado. Herramientas de análisis de vulnerabilidades. Tarjetas inteligentes. Telefonía móvil. Seguridad inalámbrica. Infraestructura de clave pública (PKI).
Seguridad criptológica.	– Seguridad criptológica.	Coordinación criptológica. Tipos de cifradores. Equipamiento STIC para la Administración.
Grupo varios.	– Inauguración y clausura.	Inauguración. Juicio crítico y clausura.

cve: BOE-A-2011-996