III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

8959 *Resolución de 28 de junio de 2012, del Instituto Nacional de Administración Pública, por la que se convoca curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones e 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 (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 segundo semestre del año 2012 un curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)-Implantación del Esquema Nacional de Seguridad, cuya finalidad es proporcionar a los participantes los conocimientos y habilidades necesarias para el análisis y gestión de riesgos de los sistemas de las tecnologías de la información y las comunicaciones, 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 que sean capaces de realizar un análisis de riesgos formal siguiendo la metodología MAGERIT y proporcionar la ayuda necesaria para poder implantar las medidas propuestas en el Esquema Nacional de Seguridad (ENS). Esta actividad formativa de modalidad mixta contendrá una fase inicial de formación 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 por ciento, quienes podrán hacer constar tal circunstancia en la solicitud y podrán indicar, asimismo, las adaptaciones necesarias en el curso formativo, siempre y cuando sean admitidos.

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 40 por ciento 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

Primera. *Objeto.*

Mediante esta resolución se convoca un curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)-Implantación del Esquema Nacional de Seguridad, en modalidad mixta, cuyas materias se detallan en el anexo.

La fase de formación on line se desarrollará del 3 al 14 de septiembre de 2012, y la fase presencial, del 17 al 28 de septiembre de 2012, esta última en la sede del Centro

cve: BOE-A-2012-8959

Superior de Estudios de la Defensa Nacional (CESEDEN), situada en el paseo de la Castellana, 61, 28071 Madrid.

Segunda. *Programa formativo.*

a) Fase on line (30 horas):

– Análisis y gestión de riesgos.
– Introducción a la gestión del riesgo.

b) Fase presencial (50 horas):

– Análisis de riesgos.
– Gestión del riesgo.
– Tratamiento de los riesgos.

La superación de la fase 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 o C1, y el personal laboral equivalente, que tengan responsabilidades en la planificación, gestión o implementación de los sistemas de las tecnologías de la información y las comunicaciones, o en su seguridad. 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:

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 la seguridad de aquellos, 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.

Cuarta. *Configuración técnica mínima de los equipos.*

a) Hardware:

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

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.

cve: BOE-A-2012-8959

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.*

El número de alumnos admitidos no excederá de 30. 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 quince 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, sea cual sea la causa, 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. Asimismo, se podrán realizar consultas a través de la página web del INAP en internet: www.inap.es.

Madrid, 28 de junio de 2012.–El Director del Instituto Nacional de Administración Pública, Manuel Arenilla Sáez.

cve: BOE-A-2012-8959

ANEXO

Curso «Gestión STIC-Implantación del Esquema Nacional de Seguridad»

Denominación de materias	Asignaturas que componen la materia	Créditos TOT	Créditos TEO	Créditos PRA	Breve descripción del contenido
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-2012-8959