III. OTRAS DISPOSICIONES

MINISTERIO DE LA PRESIDENCIA

9964 *Resolución de 1 de junio de 2009, 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 en sus distintas modalidades en colaboración con el Centro Criptológico Nacional.*

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.

La oferta de «Actividades Formativas INAP. 2009» publicada en la página web del Instituto Nacional de Administración Pública (www.inap.map.es) prevé, para el segundo semestre, la organización de una serie de actividades formativas agrupadas en varias áreas de conocimiento, según los diversos perfiles profesionales cuya finalidad es la formación continua y la actualización permanente de los conocimientos y las capacidades profesionales de los empleados públicos.

El Instituto Nacional de Administración Pública, en colaboración con el Centro Criptológico Nacional, prevé un total de 7 actividades formativas en el segundo semestre de 2009 en materia de seguridad de las tecnologías de la información y comunicaciones. Las actividades formativas serán presenciales, y según se detalle en el anexo, algunos contendrán una fase previa por correspondencia.

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 IV Acuerdo de Formación Continua en las Administraciones Públicas, de 21 de septiembre de 2005, 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 comunes

1. *Solicitudes*

a) Los candidatos deberán presentar la solicitud que figura en la página web del INAP (www.inap.map.es) entrando en «Formación» y a continuación seleccionando, según la actividad formativa que soliciten:

Formación en Tecnologías de la Información y las Comunicaciones donde aparecerá el listado de cursos y un apartado denominado «Presentación de solicitudes» para la preinscripción.

cve: BOE-A-2009-9964

b) Quienes deseen participar en los cursos, detallados en el anexo, deberán solicitarlo mediante la cumplimentación del modelo de solicitud telemática, y sólo en los casos en los que se solicite se aportará la documentación adicional exigida en su caso.

Cumplimentado el modelo de solicitud deberán ejecutar la opción «grabar y enviar» para completar la transmisión de datos telemática.

Se les generará una copia del modelo de solicitud que deberán imprimir y pasar a la firma del superior jerárquico, la cual deberán conservar en su poder hasta que se les solicite su presentación.

Los empleados públicos cuyas unidades de formación no se encuentren en el listado desplegable del modelo de solicitud del INAP, deberán ponerse en contacto con el Instituto a través del correo electrónico ft@inap.map.es.

c) Los datos de las solicitudes telemáticas serán enviados al Centro Criptológico Nacional, quien realizará la selección de alumnos de cada curso, debiendo asegurarse de que todas ellas cumplen con los requisitos exigidos para cada una de las acciones formativas.

El plazo de presentación de solicitudes telemáticas a que se refiere la presente base 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».

2. *Destinatarios*

Podrán participar en los cursos de formación en materia de seguridad de las tecnologías de la información y comunicaciones, detallados en el anexo, los empleados públicos de las Administraciones Públicas cuyo perfil se adecúe al descrito en el apartado de destinatarios.

3. *Selección*

a) El número de alumnos admitidos por curso presencial no excederá, con carácter general, de treinta.

b) La selección 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. Sólo se asignará un curso por año a cada solicitante. 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.

c) La inasistencia, sin previo aviso o cumplida justificación, de quienes hubiesen sido seleccionados para participar en las actividades formativas podrá determinar su exclusión en selecciones posteriores.

d) Una vez efectuada la selección definitiva de participantes, el Centro Criptológico Nacional comunicará por correo electrónico a cada uno de los alumnos, su admisión a cada acción formativa, 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.

4. *Modalidad formativa y calendario*

Las actividades formativas de cada materia se realizarán en la modalidad y en las fechas detalladas en el anexo. En caso de modificar las fechas indicadas en la programación será comunicado con antelación suficiente a los participantes.

cve: BOE-A-2009-9964

5. *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 programadas, sea cual sea la causa, imposibilitará la expedición del mismo.

6. Información adicional en la página web del INAP http://www.inap.map.es, así como en el correo electrónico formación.ccn@cni.es y en los teléfonos: 913726785 -913725377.

Madrid, 1 de junio de 2009.–La Directora del Instituto Nacional de Administración Pública, Pilar Arranz Notario.

cve: BOE-A-2009-9964

ANEXO

Código	Denominación	Objetivos	Destinatarios	Requisitos	Programa	Duración	Fechas
				CURSOS STIC			
FTS09-0919-01	VI Curso de Gestión STIC (Fase inicial a distancia y fase presencial)	Proporcionar a los concurrentes los conocimientos necesarios para el análisis y gestión de riesgos de un Sistema de las TIC. Como resultado de lo anterior, podrán redactar y aplicar los procedimientos y políticas de seguridad adecuados para proteger la información procesada, almacenada o transmitida por un Sistema.	Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los subgrupos A1 y A2 que tenga responsabilidades, a nivel directivo, en la planificación, gestión, administración o mantenimiento de los Sistemas de las Tecnologías de la Información y Comunicaciones (TIC), o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.	El desarrollo del curso en dos fases (a distancia y presencial) hace que sea condición imprescindible para participar en la fase de presencial, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase a distancia. El examen de la fase a distancia consistirá en la contestación de un total de 50 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 distancia.	Fase a distancia: ■ Introducción a STIC ■ Normativa de Seguridad ■ Política de Seguridad ■ Procedimiento de Acreditación ■ Inspecciones STIC ■ Gestión de Incidentes ■ Herramientas de Seguridad ■ Seguridad Perimetral ■ Redes Inalámbricas Fase presencial: ■ Evaluación y Certificación. ■ Normativa de Seguridad ■ Análisis y Gestión de Riesgos. ■ Metodología MAGERIT ■ Herramienta PILAR ■ Inspecciones STIC ■ Evaluación TEMPEST ■ Herramientas de Seguridad. ■ Verificaciones de Seguridad	145	Fase a distancia: del 21 de septiembre al 16 de octubre Fase presencial: 19 al 30 de octubre
FTS09-0920-01	XXI Curso de Especialidades Criptológicas (CEC) (Fase a distancia inicial y fase presencial)	La finalidad del "XXI Curso de Especialidades Criptológicas" es proporcionar a los concurrentes los conocimientos necesarios para el empleo de técnicas criptológicas y la dirección de una red de cifra.	Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los subgrupos A1 y A2 que tenga responsabilidades, a nivel directivo, en la planificación, gestión, administración o mantenimiento de los Sistemas de las tecnologías de la información y comunicaciones (TIC), o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.	El desarrollo del curso en dos fases (a distancia y presencial) hace que sea condición imprescindible para participar en la fase de presencial, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase a distancia. El examen de la fase a distancia consistirá en la contestación de un total de 75 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 distancia. En la fase presencial, el alumno tendrá que superar una prueba por cada una de las materias que componen el contenido del curso. Las preguntas serán teóricas en formato escrito, siendo con cuatro respuestas posibles (una única verdadera) las de tipo test, no restando puntos las mal contestadas. Será necesario concluir cada una de las evaluaciones, por lo menos, con el mínimo exigido siendo el resultado de las mismas ponderado por el número de créditos de que consta cada materia. En caso de no superar el mínimo exigido, el alumno deberá realizar una evaluación de recuperación que en el caso de no superar supondrá la baja en el curso. El mínimo exigido en cada materia será de cinco (5), en el caso de preguntas tipo test, cada una de ellas tendrá el mismo valor, siendo la nota obtenida función de las preguntas acertadas respecto al número total de formuladas.	Fase a distancia: ■ Principios Digitales ■ Teoría de Números ■ Probabilidades ■ Criptografía Clásica ■ Teoría de la Criptografía ■ Teoría de la Criptofonía ■ Seguridad Electrónica Fase presencial: ■ Principios Digitales ■ Teoría de Números ■ Probabilidades ■ Criptografía Clásica ■ Teoría de la Criptografía ■ Teoría de la Criptofonía ■ Seguridad Electrónica	340	Fase a distancia: del 31 de agosto al 6 de noviembre Fase presencial: del 10 de noviembre al 4 de diciembre

Código	Denominación	Objetivos	Destinatarios	Requisitos	Programa	Duración	Fechas
FTS09-0925-01	IV Curso STIC - Redes Inalámbricas	La finalidad del "IV Curso STIC - Redes Inalámbricas" es proporcionar a los participantes los conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías inalámbricas más adecuadas en cada Organización concreta, y para implementar y utilizar de forma óptima cada una de las capacidades que éstas ofrecen para contribuir de forma eficiente al conjunto de la seguridad de la organización.	Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos/subgrupos A1, A2 y C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las Tecnologías de la Información y Comunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.	Se partirá de un conocimiento mínimo de los participantes a nivel administrativo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red. Las prioridades en la selección serán: ▪ Haber realizado con anterioridad el Curso de Acreditación STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN). ▪ 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 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 dos (2) años.	Medidas técnicas: ▪ Comunicación WMAN ▪ Comunicación WLAN ▪ Dispositivos WPAN	25	Del 31 de agosto al 4 de septiembre
FTS09-0926-01	V Curso STIC - Cortafuegos	La finalidad del "V Curso STIC - Cortafuegos" es proporcionar a los concurrentes los conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías de cortafuegos más adecuadas en cada Organización concreta, y para implementar y utilizar de forma óptima cada una de las capacidades que éstos ofrecen para contribuir de forma eficiente al conjunto de la seguridad de la organización.	Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos/subgrupos A1, A2 y C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las Tecnologías de la Información y Comunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.	Se partirá de un conocimiento mínimo de los participantes a nivel administrativo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red. Las prioridades en la selección serán: ▪ Haber realizado con anterioridad el Curso de Acreditación STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN). ▪ 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 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 dos (2) años.	▪ Cortafuegos, Protocolos y Seguridad Perimetral ▪ NAT y Reglas de Filtrado ▪ AAA y Seguridad de Contenidos ▪ VPN y Usuarios Móviles ▪ Enrutadores y Cortafuegos a nivel Sistema	25	Del 7 al 11 de septiembre

Código	Denominación	Objetivos	Destinatarios	Requisitos	Programa	Duración	Fechas
FTS09-0927-01	V Curso STIC - Detección de Intrusos	La finalidad del "V Curso STIC - Detección de Intrusos" es proporcionar a los concurrentes los conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías de detección de intrusiones más adecuadas en cada Organización concreta, y para implementar y utilizar de forma óptima cada una de las capacidades que éstas ofrecen para contribuir de forma eficiente al conjunto de la seguridad de la organización.	Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos/subgrupos A1, A2 y C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las Tecnologías de la Información y Comunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.	Se partirá de un conocimiento mínimo de los participantes a nivel administrativo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red. Las prioridades en la selección serán: ▪ Haber realizado con anterioridad el Curso de Acreditación STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN). ▪ 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 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 dos (2) años.	▪ Conceptos de IDS y Análisis de Tráfico ▪ Análisis de Tráfico e IDS a nivel de Red (NIDS) ▪ IDS a nivel Sistema (HIDS). ▪ Análisis de Registros y Honeypots ▪ Detección de Ataques con Infraestructura IDS Combinada	25	Del 14 al 18 de septiembre
FTS09-0930-01	IV Curso STIC - Inspecciones de Seguridad	La finalidad del "IV Curso STIC - Inspecciones de Seguridad" es proporcionar a los concurrentes los conocimientos y habilidades necesarias para que sean capaces de comprobar, con una garantía suficiente, los aspectos de seguridad de redes, aplicaciones y dispositivos en cada organización concreta, así como verificar y corregir los procesos e implementaciones	Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos/subgrupos A1, A2 y C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.	Se partirá de un conocimiento mínimo de los participantes a nivel administrativo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red. Las prioridades en la selección serán: ▪ Poseer una habilitación de seguridad expedida por la Oficina Nacional de Seguridad (ONS) del Centro Nacional de Inteligencia. ▪ Haber realizado con anterioridad el Curso STIC - Verificaciones de Seguridad desarrollado por el Centro Criptológico Nacional (CCN). ▪ Haber realizado con anterioridad el Curso STIC - Herramientas de Seguridad desarrollado por el Centro Criptológico Nacional (CCN). ▪ 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 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 dos (2) años.	▪ Herramientas de Seguridad ▪ Verificaciones de Seguridad ▪ Inspecciones STIC (Nivel 3)	25	Del 2 al 25 de septiembre

Código	Denominación	Objetivos	Destinatarios	Requisitos	Programa	Duración	Fechas
FTS09-0931-01	II Curso STIC - Búsqueda de Evidencias y Control de Integridad	La finalidad del "II Curso STIC - Búsqueda de Evidencias y Control de Integridad" es proporcionar a los concurrentes 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	Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A, B o C que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica	Se partirá de un conocimiento mínimo de los participantes a nivel administrativo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red. Las prioridades para la selección serán: ▪ Haber realizado con anterioridad el Curso de Acreditación STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN). ▪ 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 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 dos (2) años.	▪ Metodología ▪ Cómo y qué buscar ▪ Estudio práctico ▪ Lugares donde buscar datos ▪ Análisis de ficheros	25	Del 28 de septiembre al 2 de octubre