mediante dictamen técnico con clave EL010-04, y la entidad colaboradora Bureau Veritas, por certificado, han hecho constar respectivamente que el tipo o modelo presentado cumple todas las especificaciones actualmente establecidas por Orden de 28 de julio de 1980 sobre exigencias técnicas de los paneles solares,

Esta Dirección General, de acuerdo con lo establecido en la referida disposición ha resuelto certificar el citado producto, con la contraseña de certificación NPS-0705, y con fecha de caducidad el día 9 de febrero de 2008, definiendo como características técnicas del modelo o tipo certificado las que se indican a continuación, debiendo el interesado presentar, en su caso, el certificado de conformidad de la producción antes del 9 de febrero de 2008.

Esta certificación se efectúa en relación con la disposición que se cita y por tanto el producto deberá cumplir cualquier otro Reglamento o disposición que le sea aplicable.

El incumplimiento de cualquiera de las condiciones fundamentales en las que se basa la concesión de esta certificación dará lugar a la suspensión cautelar automática de la misma, independientemente de su posterior anulación, en su caso, y sin perjuicio de las responsabilidades legales que de ello pudieran derivarse.

Contra esta Resolución, que pone fin a la vía administrativa, cabe interponer, potestativamente, el recurso de reposición en el plazo de un mes contado desde el día siguiente al de notificación de esta Resolución, ante el Secretario General de Energía, previo al contencioso-administrativo, conforme a lo previsto en el artículo 116.1 de la Ley 4/1999 de 14 de enero, que modifica la Ley 30/1992 de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Marca: «Solel». Modelo: Sunmax.

Caracteristicas:

Material absorbente: Lámina de cobre.
Tratamiento superficial: Superficie selectiva.
Superficie de apertura: 5,96 m^2.
Superficie de absorbente: 5,98 m^2.

Lo que se comunica a los efectos oportunos.
Madrid, 9 de febrero de 2005.–El Director General, Jorge Sanz Oliva.

3486 *RESOLUCIÓN de 14 de febrero de 2005, de la Dirección General de Política Energética y Minas, por la que se certifica un colector plano, marca «Rand», modelo RAL 1 S, fabricado por Metal & Enameling Industries, Ltd.*

Recibida en la Dirección General de Política Energética y Minas la solicitud presentada por Metal & Enameling Industries, Ltd. con domicilio social en 17 Shenkar St. P.O.B. 3294, Petah-Tikva, 49130 Israel, para la certificación de un colector plano, fabricado por Metal & Enameling Industries, Ltd, en su instalación industrial ubicada en Israel.

Resultando que por el interesado se ha presentado el dictamen técnico emitido por el laboratorio de captadores solares del Centro Nacional de Energías Renovables, con clave n.º 30.0019.0-1.

Habiendo presentado certificado en el que la entidad Standars Institution of Israel confirma que la empresa fabricante cumple los requisitos de la norma ISO 9001.

Resultando que se ha presentado certificado expedido por la Entidad Nacional de Acreditación (ENAC) en el que se considera que los certificados emitidos por la entidad Standars Institution of Israel aportan el mismo nivel de confianza que los emitidos por entidades de certificación acreditadas por ENAC.

Por todo lo anterior se ha hecho constar que el tipo o modelo presentado cumple todas las especificaciones actualmente establecidas por Orden de 28 de julio de 1980 sobre exigencias técnicas de los paneles solares,

Esta Dirección General, de acuerdo con lo establecido en la referida disposición ha resuelto certificar el citado producto, con la contraseña de certificación NPS-0805, y con fecha de caducidad el día 14 de febrero de 2008 , definiendo como características técnicas del modelo o tipo certificado las que se indican a continuación, debiendo el interesado presentar, en su caso, el certificado de conformidad de la producción antes del 14 de febrero de 2008.

Esta certificación se efectúa en relación con la disposición que se cita y por tanto el producto deberá cumplir cualquier otro Reglamento o disposición que le sea aplicable.

El incumplimiento de cualquiera de las condiciones fundamentales en las que se basa la concesión de esta certificación dará lugar a la suspensión cautelar automática de la misma, independientemente de su posterior anulación, en su caso, y sin perjuicio de las responsabilidades legales que de ello pudieran derivarse.

Contra esta Resolución, que pone fin a la vía administrativa, cabe interponer, potestativamente, el recurso de reposición en el plazo de un mes contado desde el día siguiente al de notificación de esta Resolución, ante el Secretario General de Energía, previo al contencioso-administrativo, conforme a lo previsto en el artículo 116.1 de la Ley 4/1999 de 14 de enero, que modifica la Ley 30/1992 de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Marca: «Rand».
Modelo: RAL 1 S.

Características:

Material absorbente: Cobre.
Tratamiento superficial: Cromo negro selectivo.
Superficie de apertura: 2,00 m^2.
Superficie de absorbente: 1,97 m^2.

Lo que se comunica a los efectos oportunos.
Madrid, 14 de febrero de 2005.–El Director General, Jorge Sanz Oliva.

MINISTERIO DE ADMINISTRACIONES PÚBLICAS

3487 *RESOLUCIÓN de 17 de febrero de 2005, del Instituto Nacional de Administración Pública, por la que, en colaboración con el Centro Criptológico Nacional del Centro Nacional de Inteligencia, se convocan actividades formativas sobre seguridad de las tecnologías de la información y las comunicaciones.*

La Ley 11/2002, en su artículo 4.ºe), asigna al Centro Nacional de Inteligencia las funciones de «coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro».

Basándose en ello, el Instituto Nacional de Administración Pública convoca, en colaboración con el Centro Criptológico Nacional, y dentro del Plan Interadministrativo de formación en tecnologías de la información y las comunicaciones para el año 2005, las acciones formativas en materia de seguridad de las tecnologías de la información y las comunicaciones que se detallan en el Anexo I y que se desarrollarán de acuerdo con las siguientes bases.

Primera. *Alcance.*–Mediante la presente Resolución se convocan las siguientes acciones formativas:

1. Cursos Básicos STIC:

STIC0914-01 «Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)».

2. Cursos Intermedios STIC:

STIC0915-xx «Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones» (2 ediciones).
STIC0916-xx «Acreditación STIC–Entornos Windows» (2 ediciones).
STIC0917-xx «Acreditación STIC–Entornos Unix» (2 ediciones).
STIC0918-xx «Acreditación STIC–Infraestructura de Red» (2 ediciones).

3. Cursos de Especialización STIC:

STIC0919-01 «STIC–Cortafuegos».
STIC0920-01 «STIC–Detección de Intrusos».

El contenido, programación, número de plazas disponibles, requisitos de participación, lugar de impartición y otras características de cada acción formativa se detallan en el Anexo I.

Debe señalarse que, en cuanto a la organización de los cursos, todos ellos siguen una estructura similar: existe una primera fase a distancia en la que los alumnos deben familiarizarse con una serie de conceptos previos; a continuación deben superar un examen que acredite la adquisición

de tales conocimientos; y, seguidamente, los alumnos que hayan superado el examen asisten a la fase presencial del curso.

Segunda. *Destinatarios.*–Podrá solicitar estos cursos el personal al servicio de las Administraciones Públicas que tenga responsabilidades en la planificación, gestión, administración o mantenimiento de los sistemas de información y telecomunicaciones, o con la seguridad de los mismos.

No obstante lo anterior, en la descripción del Anexo I correspondiente a cada una de las acciones formativas se proporciona información acerca de sus destinatarios, así como, en su caso, de la existencia de posibles requisitos previos.

Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.

Tercera. *Solicitudes.*–Cada Unidad de Tecnologías de la Información y las Comunicaciones (Unidad TIC) de la Administración seleccionará y priorizará las solicitudes de participación del personal adscrito a dicha Unidad. A estos efectos, la Unidad solicitante deberá asegurarse de que los aspirantes que propone cumplen los requisitos que se exigen para cada uno de los cursos.

Las solicitudes deberán ser remitidas por el responsable de la Unidad TIC con rango de Subdirector General o asimilado (o, en su caso, por su superior jerárquico), utilizando para ello el procedimiento descrito en la base cuarta.

Cuarta. *Tramitación de las solicitudes.*

1. Para solicitar la participación en los distintos cursos deberá utilizarse la aplicación STIC05-CNI que, al igual que la presente Resolución, está disponible para su descarga en la página web del INAP (http://www.inap.map.es/inapweb/fortic.htm).

El fichero de solicitudes generado con dicha aplicación deberá remitirse por correo electrónico a la dirección cesfp.tic@inap.map.es, o en soporte magnético a la dirección postal siguiente: INAP, Formación en Tecnologías de la Información y las Comunicaciones, c./ Atocha, 106, 28012-Madrid.

2. La aplicación permite solicitar una relación priorizada de, como máximo, cinco inscripciones para cada acción formativa. Se pueden generar las solicitudes para la participación en un solo curso o en varios. Cada nuevo envío actualiza los datos remitidos anteriormente, por lo que siempre se utilizará la última información enviada por cada unidad antes de la finalización del plazo de solicitud.

La unidad solicitante deberá asegurarse de que los aspirantes que propone cumplen los requisitos que se exigen para cada uno de los cursos.

3. Excepcionalmente, en caso de que la Unidad solicitante no pudiera utilizar dicha aplicación, podrá remitir la solicitud a la dirección postal indicada anteriormente, mecanografiando o cumplimentando en forma manuscrita los datos necesarios en una copia del modelo de formulario del Anexo II.

4. El plazo para la aceptación de las peticiones de cursos finalizará, con carácter general, quince días naturales antes del inicio de cada acción formativa, salvo que se indique expresamente un plazo distinto en la información correspondiente a cada curso concreto.

5. Además de la información sobre los distintos cursos que se incluye en el Anexo I de la presente convocatoria, en la dirección web mencionada anteriormente se dispone de un catálogo de cursos con información actualizada acerca de los mismos. Asimismo, la aplicación de base de datos STIC05-CNI también incorpora un catálogo detallado.

6. Los posibles cambios que se puedan haber producido en las acciones formativas (calendario, horario, lugar de impartición, etc.) desde la fecha de esta convocatoria hasta la de finalización del plazo de solicitud, serán comunicados en la notificación de admisión de aspirantes a que se refiere el siguiente punto.

7. Efectuada la selección definitiva de los aspirantes, se notificará la relación de alumnos admitidos en cada acción formativa al responsable de la Unidad TIC que tramitó la solicitud.

Si la Unidad solicitante necesita hacer modificaciones sobre la relación de alumnos admitidos, además de comunicarlas por fax al nº 912739245, deberán realizarse también en la aplicación de base de datos utilizada para la propuesta inicial, debiendo enviarse nuevamente por correo electrónico o por diskette el fichero generado.

En relación con las modificaciones previas a la comunicación de aspirantes admitidos, dado que para proceder a la selección de participantes se utilizará el último envío del fichero de solicitudes remitido antes de finalizar el plazo de admisión, es posible realizar cuantas modificaciones sean necesarias antes de que finalice dicho plazo sin necesidad de la comunicación por fax a que se refiere el párrafo anterior (la modificación sólo debe enviarse por fax –además de enviar de nuevo la base de datos modificada– cuando ya se hayan comunicado los alumnos admitidos a la Unidad solicitante).

Cada Unidad solicitante deberá comunicar a los aspirantes admitidos su inclusión en el curso y asegurarse de su asistencia a la acción formativa. A estos efectos, es fundamental que las unidades comuniquen a los interesados su admisión en el curso de que se trate, así como los restantes datos que acompañan a la notificación de admisión.

Quinta. *Certificado de asistencia.*–Al finalizar cada uno de los cursos, los concurrentes que lo hayan superado con aprovechamiento obtendrán un Certificado rubricado por el Secretario de Estado Director del Centro Nacional de Inteligencia y por el Director General del Instituto Nacional de Administración Pública, como garantía de la superación del curso. Los certificados también se remitirán al Registro Central de Personal para su inscripción y demás efectos oportunos.

Sexta. *Información adicional.*–Se podrá solicitar información adicional sobre esta convocatoria dirigiéndose a:

Instituto Nacional de Administración Pública	Centro Criptológico Nacional
c/ Atocha, 106–28012 Madrid.	Avda. del Padre Huidobro, Km. 8,5, 28023 Madrid.
Fax: 912739245.	Fax: 913725808.
e-mail: cesfp.tic@inap.map.es	e-mail : CentroCriptologicoNacional@oc.mde.es

Asimismo, también se puede consultar la página de información del INAP en Internet: http://www.inap.map.es/inapweb/fortic.htm.

Madrid, 17 de febrero de 2005.–El Director, Francisco Ramos Fernández-Torrecilla.

ANEXO 1

STIC0914-01 «Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)»

Finalidad: La finalidad del curso STIC0914-01 «Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)» es proporcionar a los concurrentes los conocimientos necesarios para conseguir una mentalización y concienciación adecuada en la seguridad de los sistemas de información y las amenazas y vulnerabilidades que representan las nuevas tecnologías.

Créditos/horas del plan de estudios: La distribución de las 100 horas de la fase a distancia del curso (10 créditos) es la siguiente:

Teoría: 10 créditos/100 horas.

La distribución de las 55 horas de la fase de presente del curso (5,5 créditos) es la siguiente:

Teoría: 4,8 créditos/48 horas.
Práctica: 0,7 créditos/7 horas.

Normas y certificado de superación: Al desarrollarse el presente Curso en dos fases (a distancia y presente) será condición imprescindible para ser nombrado concurrente a la fase de presente, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase a distancia.

El examen previo 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.

En la fase de presente, el alumno tendrá que superar una prueba por el conjunto de las materias que componen el contenido del curso. Las preguntas serán 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 caso de no superar el mínimo exigido, el alumno deberá realizar una evaluación de recuperación que, si tampoco la supera, supondrá la consideración de No Apto y la baja en el Curso.

La nota final del curso se corresponderá con la calificación obtenida en la fase de presente, siendo la nota de la fase a distancia considerada sólo para el acceso a la fase que se inicia posteriormente.

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 concurrentes que lo hayan superado con aprovechamiento obtendrán un Certificado rubricado por el Secretario de Estado Director del Centro Nacional de Inteligencia y por el Director General del INAP, como garantía de la superación del curso. Los certificados también se remitirán al Registro Central de Personal para su inscripción y demás efectos oportunos.

Calendario:

STIC0914-01:

Fase a distancia: 14 de marzo–7 de abril de 2005.

Fase de presente: 8–22 de abril de 2005 (de 9.00 a 14.00 horas).
El día 8 de abril, examen previo de la parte A distancia.

La admisión de solicitudes para este curso finalizará el día 7 de marzo de 2005.

Destinatarios: Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A o B que tenga responsabilidades en la planificación, gestión, administración o mantenimiento de los sistemas de información y telecomunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.

Se considerará como prioridad para la selección de concurrentes al curso el estar desarrollando, en su actual destino, actividades de planificación, gestión, administración o mantenimiento de Sistemas de Información y Telecomunicaciones, o la seguridad de los mismos, por un período superior a dos años.

Número de plazas convocadas en cada edición: 20.

Materias y asignaturas: A continuación se detallan las materias y asignaturas en las que se distribuye el curso con expresión de contenidos y asignación de horas lectivas.

Denominación de materias	Asignaturas que componen la materia	Créditos			Breve descripción del contenido
		TOT	TEO	PRA	
Políticas STIC (fase a distancia).	Introducción a STIC. Normativa de Seguridad. Políticas de Seguridad.	5,0	5,0	0	Conceptos y Terminología STIC. Evaluación, Certificación y Acreditación. Esquemas de Certificación. Normativas y Estándares de Seguridad. Políticas de Seguridad de las TIC.
Procedimientos STIC (fase a distancia).	Análisis y Gestión de Riesgos. Análisis de Vulnerabilidades. Procedimiento de Acreditación. Gestión de Incidentes. Planes de Contingencia. Amenaza TEMPEST.	5,0	5,0	0	Vulnerabilidades y Amenazas a los Sistemas de Información. Documentación de Seguridad. Evaluación STIC. Amenaza TEMPEST y TRANSEC.
Introducción a la Criptología.	Criptografía Clásica. Teoría de la Criptografía. Teoría de la Criptofonía.	0,4	0,4	0	Principios Básicos de la Criptología. Criptografía Moderna. Criptografía de Clave Pública. Sistemas de Criptofonía.
Introducción a los Sistemas de Información y Telecomunicaciones.	Servicios de Telecomunicaciones.	0,5	0,5	0	Generalidades. Redes y Servicios de Telecomunicaciones. Protocolos. Mecanismos de Seguridad. Servicios de INTERNET.
Políticas STIC.	Introducción STIC. Normativa de Seguridad. Políticas de Seguridad.	1,0	1,0	0	Conceptos y Terminología STIC. Evaluación, Certificación y Acreditación. Esquemas de Certificación. Normativas y Estándares de Seguridad. Políticas de Seguridad de las TIC.
Procedimientos STIC.	Análisis y Gestión de Riesgos. Análisis de Vulnerabilidades. Procedimiento de Acreditación. Gestión de Incidentes. Planes de Contingencia. Amenaza TEMPEST.	1,4	0,9	0,5	Vulnerabilidades y Amenazas a los Sistemas de Información. Documentación de Seguridad. Evaluación STIC. Amenaza TEMPEST y TRANSEC. Caso Práctico de Ataque.
Medidas Técnicas STIC.	Herramientas de Seguridad. Equipamiento STIC.	1,4	1,4	0	Dispositivos de Protección de Perímetro. Antivirus. Detección de Intrusos (IDS). Infraestructura de Clave Pública (PKI). Equipamiento STIC para la Administración.
Seguridad Criptológica.	Seguridad Criptológica.	0,4	0,2	0,2	Proceso de Evaluación. Tipos de Cifradores. Equipamiento Criptológico.

Lugar de impartición: El lugar de desarrollo del curso es la sede institucional del Centro Nacional de Inteligencia, Avda. del Padre Huidobro Km. 8,5 28023 Madrid.

STIC0915-xx «Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones» (2 ediciones)

Finalidad: La finalidad del curso STIC0915-xx «Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones» (2 ediciones) consiste en proporcionar a los concurrentes los conocimientos necesarios para la valoración y gestión de riesgos de un Sistema de Información y Telecomunicaciones (CIS). 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 CIS contra la pérdida de la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios sistemas.

Los asistentes seleccionados se familiarizarán 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 y, además, serán capaces de dirigir una evaluación de seguridad sobre un CIS.

Créditos/horas del plan de estudios: La distribución de las 100 horas de la fase a distancia del curso (10 créditos) es la siguiente:

Teoría: 10 créditos/100 horas.

La distribución de las 55 horas de la fase de presente del curso (5,5 créditos) es la siguiente:

Teoría: 3,5 créditos/35 horas.
Práctica: 2 créditos/20 horas.

Normas y certificado de superación: Al desarrollarse el presente Curso en dos fases (a distancia y presente) será condición imprescindible para ser nombrado concurrente a la fase de presente, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase a distancia.

El examen previo 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.

En la fase de presente, el alumno tendrá que realizar una serie de prácticas que permitirán valorar si ha obtenido los conocimientos adecuados para superar el Curso y ser considerado como Apto. En caso de no superar el mínimo exigido, el alumno será considerado No Apto suponiendo la baja en el Curso.

La nota final del curso se corresponderá con la calificación obtenida en la fase de presente, siendo la nota de la fase a distancia considerada sólo para el acceso a la fase que se inicia posteriormente.

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 concurrentes que lo hayan superado con aprovechamiento obtendrán un Certificado rubricado por el Secretario de Estado Director del Centro Nacional de Inteligencia y por el Director General del INAP, como garantía de la superación del curso. Los certificados también se remitirán al Registro Central de Personal para su inscripción y demás efectos oportunos.

Calendario:

STIC0915-01:

Fase a distancia: 19 septiembre–13 octubre de 2005.
Fase de presente: 14–28 de octubre de 2005 (de 9.00 a 14.00 horas).
El día 14 de octubre, examen previo de la parte a distancia.

STIC0915-02:

Fase a distancia: 17 octubre–10 noviembre de 2005.
Fase de presente: 11–25 de noviembre de 2005 (de 9.00 a 14.00 horas).
El día 11 de noviembre, examen previo de la parte a distancia.

Destinatarios: Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A o B que tenga responsabilidades, a nivel directivo, en la planificación, gestión, administración o mantenimiento de los sistemas de información y telecomunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.

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

Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por este Centro.

Haber realizado cursos relacionados con las tecnologías de la información o su seguridad.

Tener responsabilidades en la implementación u operación de sistemas de información y telecomunicaciones, a nivel directivo, o en la gestión de la seguridad de dichos sistemas por un período superior a dos años.

Número de plazas convocadas en cada edición: 8.

Materias y asignaturas: A continuación se detallan las materias y asignaturas en las que se distribuye el curso con expresión de contenidos y asignación de horas lectivas.

Denominación de materias	Asignaturas que componen la materia	Créditos			Breve descripción del contenido
		TOT	TEO	PRA	
Políticas STIC (fase a distancia) .	Introducción a STIC. Normativa de Seguridad. Políticas de Seguridad.	5,0	5,0	0	Conceptos y Terminología STIC. Evaluación, Certificación y Acreditación. Esquemas de Certificación. Normativas y Estándares de Seguridad. Políticas de Seguridad de las TIC.
Procedimientos STIC (fase a distancia).	Análisis y Gestión de Riesgos. Análisis de Vulnerabilidades. Procedimiento de Acreditación. Gestión de Incidentes. Planes de Contingencia. Amenaza TEMPEST.	5,0	5,0	0	Vulnerabilidades y Amenazas a los Sistemas de Información. Documentación de Seguridad. Evaluación STIC. Amenaza TEMPEST y TRANSEC.
Políticas STIC.	Normativa de Seguridad.	0,3	0,3	0	Políticas de Seguridad de las TIC.
Procedimientos STIC.	Análisis y Gestión de Riesgos. Análisis de Vulnerabilidades. Procedimiento de Acreditación. Gestión de Incidentes. Planes de Contingencia.	3,5	2,0	1,5	Vulnerabilidades y Amenazas a los Sistemas de Información. Familiarización con Herramienta PILAR. Documentación de Seguridad. Gestión de Incidentes. Evaluación STIC.
Medidas Técnicas STIC.	Herramientas de Seguridad. Equipamiento STIC.	1,3	0,8	0,5	Dispositivos de Protección de Perímetro. Antivirus. Detección de Intrusos (IDS). Equipamiento STIC para la Administración.

Lugar de impartición: El lugar de desarrollo del curso es la sede institucional del Centro Nacional de Inteligencia, Avda. del Padre Huidobro, Km. 8,5, 28023 Madrid.

STIC0916-xx «Acreditación STIC–Entornos Windows» (2 ediciones)

Finalidad: La finalidad del curso STIC0916-xx «Acreditación STIC–Entornos Windows» (2 ediciones) es proporcionar a los concurrentes los conocimientos necesarios para que sean capaces de comprobar, con una garantía suficiente, los aspectos de seguridad de sistemas servidores Windows 2000 y de estaciones clientes profesionales Windows XP, servicios Internet Information Services y Exchange 2000 de Microsoft.

Créditos/horas del plan de estudios: La distribución de las 100 horas de la fase a distancia del curso (10 créditos) es la siguiente:

Teoría: 10 créditos/100 horas.

La distribución de las 30 horas de la fase de presente del curso (3 créditos) es la siguiente:

Teoría: 1 créditos/10 horas.
Práctica: 2 créditos/20 horas.

Normas y certificado de superación: Al desarrollarse el presente Curso en dos fases (a distancia y presente) será condición imprescindible para ser nombrado concurrente a la fase de presente, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase a distancia y la familiarización con entornos basados en sistemas operativos Windows.

El examen previo consistirá en una prueba práctica de conocimiento de entornos Windows y 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.

En la fase de presente, el alumno tendrá que realizar una serie de prácticas que permitirán valorar si ha obtenido los conocimientos adecuados para superar el Curso y ser considerado como Apto. En caso de no superar el mínimo exigido, el alumno será considerado No Apto suponiendo la baja en el Curso.

La nota final del curso se corresponderá con la calificación obtenida en la fase de presente, siendo la nota de la fase a distancia considerada sólo para el acceso a la fase que se inicia posteriormente.

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 concurrentes que lo hayan superado con aprovechamiento obtendrán un Certificado rubricado por el Secretario de Estado Director del Centro Nacional de Inteligencia y por el Director General del INAP, como garantía de la superación del curso. Los certificados también se remitirán al Registro Central de Personal para su inscripción y demás efectos oportunos.

Calendario:

STIC0916-01:

Fase a distancia: 14–31 marzo de 2005.
Fase de presente: 1–8 de abril de 2005 (de 9.00 a 14.00 horas).
El día 1 de abril, examen previo de la parte a distancia.

La admisión de solicitudes para este curso finalizará el día 7 de marzo de 2005.

STIC0916-02:

Fase a distancia: 18 abril–12 mayo de 2005.
Fase de presente: 13–20 de mayo de 2005 (de 9.00 a 14.00 horas).
El día 13 de mayo, examen previo de la parte a distancia.

Destinatarios: 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 información y/o telecomunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.

Se supondrá un conocimiento mínimo a nivel administrativo de sistemas Windows, así como conocimientos básicos de protocolos de red considerándose como prioridades para la selección de concurrentes al curso, las siguientes:

Actividad relacionada con la administración de sistemas de información y telecomunicaciones bajo entorno Windows NT/2000/XP.

Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por este Centro.

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 información y telecomunicaciones o en la gestión de la seguridad de dichos sistemas por un período superior a dos años.

Número de plazas convocadas en cada edición: 7.

Materias y asignaturas: A continuación se detallan las materias y asignaturas en las que se distribuye el Curso con expresión de contenidos y asignación de horas lectivas.

Denominación de materias	Asignaturas que componen la materia	Créditos			Breve descripción del contenido
		TOT	TEO	PRA	
Políticas STIC (fase a distancia).	Introducción a STIC. Normativa de Seguridad. Políticas de Seguridad.	5,0	5,0	0	Conceptos y Terminología STIC. Evaluación, Certificación y Acreditación. Esquemas de Certificación. Normativas y Estándares de Seguridad. Políticas de Seguridad de las TIC.
Procedimientos STIC (fase a distancia).	Análisis y Gestión de Riesgos. Análisis de Vulnerabilidades. Procedimiento de Acreditación. Gestión de Incidentes. Planes de Contingencia. Amenaza TEMPEST.	5,0	5,0	0	Vulnerabilidades y Amenazas a los Sistemas de Información. Documentación de Seguridad. Evaluación STIC. Amenaza TEMPEST y TRANSEC.
Políticas STIC.	Normativa de Seguridad.	0,3	0,3	0	Políticas de Seguridad de las TIC.
Medidas Técnicas STIC.	Seguridad en Sistemas Operativos. Seguridad en Servicios de Correo. Seguridad en Servicios Web.	2,5	0,7	1,8	Servidores Windows. Clientes Windows. Servicios de Correo Electrónico (Exchange 2000) y Servicios Web (Internet Information Server).

Lugar de impartición: El lugar de desarrollo del curso es la sede del Instituto Nacional de Administración Pública (INAP), c/. Atocha, 106, 28012 Madrid.

STIC0917-xx «Acreditación STIC–Entornos Unix» (2 ediciones)

Finalidad: La finalidad del curso STIC0917-xx «Acreditación STIC–Entornos Unix» (2 ediciones) es proporcionar a los concurrentes los conocimientos necesarios para que sean capaces de comprobar, con una garantía suficiente, los aspectos de seguridad de los sistemas operativos Unix (centrado en Sun Solaris), servicios Apache y Sendmail.

Créditos/horas del plan de estudios: La distribución de las 100 horas de la fase a distancia del curso (10 créditos) es la siguiente:

Teoría: 10 créditos/100 horas.

La distribución de las 30 horas de la fase de presente del curso (3 créditos) es la siguiente:

Teoría: 1 créditos/10 horas.
Práctica: 2 créditos/20 horas.

Normas y certificado de superación: Al desarrollarse el presente Curso en dos fases (a distancia y presente) será condición imprescindible para ser nombrado concurrente a la fase de presente, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase a distancia y la familiarización con entornos basados en sistemas operativos Unix.

El examen previo consistirá en una prueba práctica de conocimiento de entornos Unix y 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.

En la fase de presente, el alumno tendrá que realizar una serie de prácticas que permitirán valorar si ha obtenido los conocimientos adecuados para superar el Curso y ser considerado como Apto. En caso de no superar el mínimo exigido, el alumno será considerado No Apto suponiendo la baja en el Curso.

La nota final del curso se corresponderá con la calificación obtenida en la fase de presente, siendo la nota de la fase a distancia considerada sólo para el acceso a la fase que se inicia posteriormente.

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 concurrentes que lo hayan superado con aprovechamiento obtendrán un Certificado rubricado por el Secretario de Estado Director del Centro Nacional de Inteligencia y por el Director General del INAP, como garantía de la superación del curso. Los certificados también se remitirán al Registro Central de Personal para su inscripción y demás efectos oportunos.

Calendario:

STIC0917-01:

Fase a distancia: 2–26 mayo de 2005.
Fase de presente: 27 mayo–3 de junio de 2005 (de 9.00 a 14.00 horas).
El día 3 de junio, examen previo de la parte a distancia.

STIC0917-02:

Fase a distancia: 8 agosto–1 septiembre de 2005.
Fase de presente: 2–12 de septiembre de 2005 (de 9.00 a 14.00 horas).
El día 2 de septiembre, examen previo de la parte a distancia.

Destinatarios: 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 información y/o telecomunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.

Se supondrá un conocimiento mínimo a nivel administrativo de sistemas Unix, así como conocimientos básicos de protocolos de red considerándose como prioridades para la selección de concurrentes al curso, las siguientes:

Actividad relacionada con la administración de sistemas de información y telecomunicaciones bajo entorno Unix.

Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por este Centro.

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 información y telecomunicaciones o en la gestión de la seguridad de dichos sistemas por un período superior a dos años.

Número de plazas convocadas en cada edición: 3.

Materias y asignaturas: A continuación se detallan las materias y asignaturas en las que se distribuye el Curso con expresión de contenidos y asignación de horas lectivas.

Denominación de materias	Asignaturas que componen la materia	Créditos			Breve descripciónde contenido
		TOT	TEO	PRA	
Políticas STIC (fase a distancia).	Introducción a STIC. Normativa de Seguridad. Políticas de Seguridad.	5,0	5,0	0	Conceptos y Terminología STIC. Evaluación, Certificación y Acreditación. Esquemas de Certificación. Normativas y Estándares de Seguridad. Políticas de Seguridad de las TIC.
Procedimientos STIC (fase a distancia).	Análisis y Gestión de Riesgos. Análisis de Vulnerabilidades. Procedimiento de Acreditación. Gestión de Incidentes. Planes de Contingencia. Amenaza TEMPEST.	5,0	5,0	0	Vulnerabilidades y Amenazas a los Sistemas de Información. Documentación de Seguridad. Evaluación STIC. Amenaza TEMPEST y TRANSEC.
Políticas STIC.	Normativa de Seguridad.	0,3	0,3	0	Políticas de Seguridad de las TIC.

Denominación de materias	Asignaturas que componen la materia	Créditos			Breve descripcióndel contenido
		TOT	TEO	PRA	
Medidas Técnicas STIC.	Seguridad en Sistemas Operativos. Seguridad en Servicios de Correo. Seguridad en Servicios Web.	2,5	0,7	1,8	Servidores Unix-Solaris. Servicios de Correo Electrónico (Sendmail) y Servicios Web (Apache).

Lugar de impartición: El lugar de desarrollo del curso es la sede del Instituto Nacional de Administración Pública (INAP), c/. Atocha, 106, 28012 Madrid.

STIC0918-xx «Acreditación STIC–Infraestructura de Red» (2 ediciones)

Finalidad: La finalidad del curso STIC0918-xx «Acreditación STIC–Infraestructura de Red» (2 ediciones) es proporcionar a los concurrentes los conocimientos necesarios para que sean capaces de comprobar, con una garantía suficiente, los aspectos de seguridad relativos a la infraestructura de red (Dispositivos de Comunicaciones, Redes Privadas Virtuales, Detección de Intrusos, Honeypots, etc…).

Créditos/horas del plan de estudios: La distribución de las 100 horas de la fase a distancia del curso (10 créditos) es la siguiente:

Teoría: 10 créditos/100 horas

La distribución de las 30 horas de la fase de presente del curso (3 créditos) es la siguiente:

Teoría: 1 créditos/10 horas.
Práctica: 2 créditos/20 horas.

Normas y certificado de superación: Al desarrollarse el presente Curso en dos fases (a distancia y presente) será condición imprescindible para ser nombrado concurrente a la fase de presente, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase a distancia y la familiarización con entornos basados en sistemas operativos Windows y Unix.

El examen previo consistirá en una prueba práctica de conocimiento de entornos Windows/Unix y 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.

En la fase de presente, el alumno tendrá que realizar una serie de prácticas que permitirán valorar si ha obtenido los conocimientos adecuados para superar el Curso y ser considerado como Apto. En caso de no superar el mínimo exigido, el alumno será considerado No Apto suponiendo la baja en el Curso.

La nota final del curso se corresponderá con la calificación obtenida en la fase de presente, siendo la nota de la fase a distancia considerada sólo para el acceso a la fase que se inicia posteriormente.

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 concurrentes que lo hayan superado con aprovechamiento obtendrán un Certificado rubricado por el Secretario de Estado Director del Centro Nacional de Inteligencia y por el Director General del INAP, como garantía de la superación del curso. Los certificados también se remitirán al Registro Central de Personal para su inscripción y demás efectos oportunos.

Calendario: STIC0918-01:

Fase a distancia: 16 mayo–9 junio de 2005.
Fase de presente: 10–17 de junio de 2005 (de 9.00 a 14.00 horas).
El día 10 de junio, examen previo de la parte a distancia.

STIC0918-02:

Fase a distancia: 30 mayo–23 junio de 2005.
Fase de presente: 24 junio–1 de julio de 2005 (de 9.00 a 14.00 horas).
El día 24 de junio, examen previo de la parte a distancia.

Destinatarios: 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 información y/o telecomunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.

Se supondrá un conocimiento mínimo a nivel administrativo de Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red considerándose como prioridades para la selección de concurrentes al curso, las siguientes:

Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de información y telecomunicaciones.

Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por este Centro.

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 información y telecomunicaciones o en la gestión de la seguridad de dichos sistemas por un período superior a dos años.

Número de plazas convocadas en cada edición: 7.

Materias y asignaturas: A continuación se detallan las materias y asignaturas en las que se distribuye el Curso con expresión de contenidos y asignación de horas lectivas.

Denominación de materias	Asignaturas que componen la materia	Créditos			Breve descripción del contenido
		TOT	TEO	PRA	
Políticas STIC (fase a distancia).	Introducción a STIC. Normativa de Seguridad. Políticas de Seguridad.	5,0	5,0	0	Conceptos y Terminología STIC. Evaluación, Certificación y Acreditación. Esquemas de Certificación. Normativas y Estándares de Seguridad. Políticas de Seguridad de las TIC.
Procedimientos STIC (fase a distancia).	Análisis y Gestión de Riesgos. Análisis de Vulnerabilidades. Procedimiento de Acreditación. Gestión de Incidentes. Planes de Contingencia. Amenaza TEMPEST.	5,0	5,0	0	Vulnerabilidades y Amenazas a los Sistemas de Información. Documentación de Seguridad. Evaluación STIC. Amenaza TEMPEST y TRANSEC.
Políticas STIC.	Normativa de Seguridad.	0,3	0,3	0	Políticas de Seguridad de las TIC.
Medidas Técnicas STIC.	Dispositivos de Comunicaciones. Dispositivos de Filtrado. Acceso Remoto. Detección de Intrusos	2,5	0,7	1,8	Dispositivos de Comunicaciones (Switch y Routers). Dispositivos de Filtrado. Redes Privadas Virtuales. Servidores Centrales de Autenticación. Detección de Intrusos. Honeypots-Honeynets.

Lugar de impartición: El lugar de desarrollo del curso es la sede del Instituto Nacional de Administración Pública (INAP), c/. Atocha, 106, 28012 Madrid.

STIC0919-01 «STIC–Cortafuegos»

Finalidad: La finalidad del curso STIC0919-01 «STIC–Cortafuegos» es que los concurrentes se familiaricen con los distintos tipos de tecnologías de cortafuegos, con sus usos, y con el papel que pueden jugar tanto dentro de la seguridad perimetral de la organización como de una estrategia global de seguridad en profundidad.

Créditos/horas del plan de estudios: La distribución de las 100 horas de la fase a distancia del curso (10 créditos) es la siguiente:

Teoría: 10 créditos/100 horas.

La distribución de las 30 horas de la fase de presente del curso (3 créditos) es la siguiente:

Teoría: 1 créditos/10 horas.
Práctica: 2 créditos/20 horas.

Normas y certificado de superación: Al desarrollarse el presente Curso en dos fases (a distancia y presente) será condición imprescindible para ser nombrado concurrente a la fase de presente, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase a distancia y la familiarización con entornos basados en sistemas operativos Windows y Unix.

El examen previo consistirá en una prueba práctica de conocimiento de entornos Windows/Unix y 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.

En la fase de presente, el alumno tendrá que realizar una serie de prácticas que permitirán valorar si ha obtenido los conocimientos adecuados para superar el Curso y ser considerado como Apto. En caso de no superar el mínimo exigido, el alumno será considerado No Apto suponiendo la baja en el Curso.

La nota final del curso se corresponderá con la calificación obtenida en la fase de presente, siendo la nota de la fase a distancia considerada sólo para el acceso a la fase que se inicia posteriormente.

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 concurrentes que lo hayan superado con aprovechamiento obtendrán un Certificado rubricado por el Secretario de Estado Director del Centro Nacional de Inteligencia y por el Director General del INAP, como garantía de la superación del curso. Los certificados también se remitirán al Registro Central de Personal para su inscripción y demás efectos oportunos.

Calendario:

STIC0919-01:

Fase a distancia: 22 agosto–15 septiembre de 2005.

Fase de presente: 16–23 de septiembre de 2005 (de 9.00 a 14.00 horas).

El día 16 de septiembre, examen previo de la parte a distancia.

Destinatarios: 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 información y/o telecomunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.

Se supondrá un conocimiento mínimo a nivel administrativo de Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red considerándose como prioridades para la selección de concurrentes al curso, las siguientes:

Haber realizado con anterioridad el Curso de Acreditación STIC–Infraestructura de Red desarrollado por este Centro.

Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de información y telecomunicaciones.

Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por este Centro.

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 información y telecomunicaciones o en la gestión de la seguridad de dichos sistemas por un período superior a dos años.

Número de plazas convocadas en cada edición: 7.

Materias y asignaturas: A continuación se detallan las materias y asignaturas en las que se distribuye el Curso con expresión de contenidos y asignación de horas lectivas.

Denominación de materias	Asignaturas que componen la materia	Créditos			Breve descripción del contenido
		TOT	TEO	PRA	
Políticas STIC (fase a distancia).	Introducción a STIC. Normativa de Seguridad. Políticas de Seguridad.	5,0	5,0	0	Conceptos y Terminología STIC. Evaluación, Certificación y Acreditación. Esquemas de Certificación. Normativas y Estándares de Seguridad. Políticas de Seguridad de las TIC.
Procedimientos STIC (fase a distancia).	Análisis y Gestión de Riesgos. Análisis de Vulnerabilidades. Procedimiento de Acreditación. Gestión de Incidentes. Planes de Contingencia. Amenaza TEMPEST.	5,0	5,0	0	Vulnerabilidades y Amenazas a los Sistemas de Información. Documentación de Seguridad. Evaluación STIC. Amenaza TEMPEST y TRANSEC.
Políticas STIC.	Normativa de Seguridad.	0,3	0,3	0	Políticas de Seguridad de las TIC.
Medidas Técnicas STIC.	Protección Perimetral. Configuración de DPP. A uditoría. Respuesta Activa.	2,5	0,7	1,8	Dispositivos de Comunicaciones (Switch y Routers), Cortafuegos Personales, Cortafuegos a Nivel de Red, Caso Práctico de Ataque y Respuesta.

Lugar de impartición: El lugar de desarrollo del curso es la sede del Instituto Nacional de Administración Pública (INAP), c/. Atocha, 106. 28012 Madrid.

STIC0920-01 «STIC–Detección DE Intrusos»

Finalidad: La finalidad del curso STIC0920-01 «STIC–Detección de Intrusos» es que los concurrentes se familiaricen con los distintos tipos de tecnologías de detección de intrusos, con sus usos, y con el papel que pueden jugar tanto dentro de la seguridad perimetral de la organización como de una estrategia global de seguridad en profundidad.

Créditos/horas del plan de estudios: La distribución de las 100 horas de la fase a distancia del curso (10 créditos) es la siguiente:

Teoría: 10 créditos/100 horas.

La distribución de las 30 horas de la fase de presente del curso (3 créditos) es la siguiente:

Teoría: 1 créditos/10 horas.
Práctica: 2 créditos/20 horas.

Normas y certificado de superación: Al desarrollarse el presente Curso en dos fases (a distancia y presente) será condición imprescindible para ser nombrado concurrente a la fase de presente, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase a distancia y la familiarización con entornos basados en sistemas operativos Windows y Unix.

El examen previo consistirá en una prueba práctica de conocimiento de entornos Windows/Unix y 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.

En la fase de presente, el alumno tendrá que realizar una serie de prácticas que permitirán valorar si ha obtenido los conocimientos adecuados para superar el Curso y ser considerado como Apto. En caso de no superar el mínimo exigido, el alumno será considerado No Apto suponiendo la baja en el Curso.

La nota final del curso se corresponderá con la calificación obtenida en la fase de presente, siendo la nota de la fase a distancia considerada sólo para el acceso a la fase que se inicia posteriormente.

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 concurrentes que lo hayan superado con aprovechamiento obtendrán un Certificado rubricado por el Secretario de Estado Director del Centro Nacional de Inteligencia y por el Director General del INAP, como garantía de la superación del curso. Los certificados también se remitirán al Registro Central de Personal para su inscripción y demás efectos oportunos.

Calendario:

STIC0920-01:

Fase a distancia: 5–29 septiembre de 2005.
Fase de presente: 30 septiembre–7 de octubre de 2005 (de 9.00 a 14.00 horas).
El día 30 de septiembre, examen previo de la parte a distancia.

Destinatarios: 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 información y/o telecomunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.

Se supondrá un conocimiento mínimo a nivel administrativo de Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red considerándose como prioridades para la selección de concurrentes al curso, las siguientes:

Haber realizado con anterioridad el Curso de Acreditación STIC–Infraestructura de Red desarrollado por este Centro.

Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de información y telecomunicaciones.

Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por este Centro.

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 información y telecomunicaciones o en la gestión de la seguridad de dichos sistemas por un período superior a dos años.

Número de plazas convocadas en cada edición: 7

Materias y asignaturas: A continuación se detallan las materias y asignaturas en las que se distribuye el Curso con expresión de contenidos y asignación de horas lectivas.

Denominación de materias	Asignaturas que componen la materia	Créditos			Breve descripción del contenido
		TOT	TEO	PRA	
Políticas STIC (fase a distancia).	Introducción a STIC. Normativa de Seguridad. Políticas de Seguridad.	5,0	5,0	0	Conceptos y Terminología STIC. Evaluación, Certificación y Acreditación. Esquemas de Certificación. Normativas y Estándares de Seguridad. Políticas de Seguridad de las TIC.
Procedimientos STIC (fase a distancia).	Análisis y Gestión de Riesgos. Análisis de Vulnerabilidades. Procedimiento de Acreditación. Gestión de Incidentes. Planes de Contingencia. Amenaza TEMPEST.	5,0	5,0	0	Vulnerabilidades y Amenazas a los Sistemas de Información. Documentación de Seguridad. Evaluación STIC. Amenaza TEMPEST y TRANSEC.
Políticas STIC.	Normativa de Seguridad.	0,3	0,3	0	Políticas de Seguridad de las TIC.
Medidas Técnicas STIC.	Arquitectura IDS. Análisis de Tráfico de Red. Configuración de IDS. Proceso de Análisis de Firmas IDS.	2,5	0,7	1,8	Dispositivos de Comunicaciones (Switch y Routers). IDS en Host. IDS en Red. Análisis de Tráfico de Red. Caso Práctico de Ataque y Respuesta.

Lugar de impartición: El lugar de desarrollo del curso es la sede del Instituto Nacional de Administración Pública (INAP), c/. Atocha, 106, 28012 Madrid.

ANEXO II
RELACIÓN PRIORIZADA DE SOLICITUDES DE PARTICIPACIÓN EN CURSOS TIC

DENOMINACIÓN DEL CURSO:

CÓDIGO/REFª DEL CURSO: **CALENDARIO:**

UNIDAD SOLICITANTE:
CENTRO DIRECTIVO:
MINISTERIO/ORGANISMO:
Dirección:
Localidad: **CP:**
Provincia:
Teléfono: **Fax:**
E-mail:

	Fecha y firma:
Fecha:	
Firmado por:	
Cargo:	

RELACIÓN PRIORIZADA DE ASPIRANTES A PARTICIPAR EN EL CURSO					
DNI	**Apellidos**	**Nombre**	**Sexo**	**Tipo-Grupo**	**Correo electrónico**

Sus datos personales serán incorporados a un fichero automatizado, siendo tratados de forma totalmente confidencial (Ley 15/99) y únicamente podrán ser utilizados para el estricto cumplimiento de las funciones derivadas de las actividades de formación. Entre ellas se incluye la cesión de los mismos a profesores y alumnos del curso con idéntica finalidad. También podrán ser utilizados para el envío de publicidad sobre acciones formativas del INAP.
Pueden ejercitar los derechos de acceso, rectificación, oposición y cancelación en cualquier momento, dirigiéndose por escrito al INAP, Secretaría General, c./ Atocha, 106 - 28012 Madrid.