

### III. OTRAS DISPOSICIONES

## MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

**12615** *Resolución de 26 de noviembre de 2014, 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 colaboración con el Centro Criptológico Nacional.*

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 viene colaborando desde hace años con el Centro Criptológico Nacional en la organización de actividades formativas para empleados públicos en materia de seguridad de las tecnologías de la información y comunicaciones, en el marco del convenio de colaboración suscrito entre la Secretaría de Estado de Administración Pública, el Centro Nacional de Inteligencia y el INAP, para impulsar la seguridad en el ámbito de la administración electrónica.

Por ello, teniendo en cuenta las necesidades formativas de los empleados públicos para el adecuado ejercicio de sus funciones, esta Dirección adopta la siguiente resolución:

Primera. *Objeto.*

Mediante esta resolución se convocan nueve acciones formativas en materia de seguridad de las tecnologías de la información y comunicaciones en la administración electrónica, según el programa y modalidad formativa que se describen en el anexo, y que se desarrollarán durante el primer semestre de 2015.

Segunda. *Destinatarios.*

Podrán solicitar el curso de seguridad de las tecnologías de información y comunicaciones (STIC) los empleados públicos pertenecientes a cuerpos y escalas de los subgrupos A1 y A2, y el personal laboral equivalente, que tengan responsabilidades en la planificación, gestión o administración de los sistemas de las tecnologías de la información y las comunicaciones o en su seguridad. Las demás actividades formativas podrán ser solicitadas por los empleados públicos de los subgrupos A1, A2 y C1, y el personal laboral equivalente, que tengan responsabilidades, en el nivel técnico, en la planificación, gestión, administración o mantenimiento de 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.

Tercera. *Plazo de presentación de solicitudes.*

El plazo de presentación de solicitudes comenzará el día siguiente al de la publicación de esta resolución en el «Boletín Oficial del Estado» y finalizará el 16 de enero de 2015.

Quien desee participar en los cursos convocados deberá cumplimentar la correspondiente solicitud electrónica. El acceso a dicha solicitud se podrá realizar desde el catálogo de formación (<http://www.inap.es/catalogo-de-formacion>) donde se podrán localizar los cursos que se encuentran en periodo de inscripción. También podrá acceder a través del enlace <http://www.inap.es/cursos-de-seguridad-tic-en-colaboracion-con-el-ccn>, donde podrá seleccionar el curso deseado y acceder a «Inscripción electrónica». Ejecutada la acción «Grabar solicitud», se le generará una copia del modelo de solicitud que deberá imprimir y pasar a la firma del superior jerárquico. Una vez firmada, deberá conservar la solicitud en su poder hasta que se le requiera su presentación.

Para cualquier incidencia técnica relacionada con la inscripción electrónica, se podrá contactar con el INAP a través de la dirección de correo electrónico [ft@inap.es](mailto:ft@inap.es).

Cuarta. *Selección.*

1. El número de alumnos admitidos no excederá, con carácter general, de veinticuatro. 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 el caso de recibir varias solicitudes de un mismo organismo o institución, se seleccionará al candidato con el perfil más ajustado al destinatario del curso.

2. Los empleados públicos podrán participar en cursos de formación durante los permisos por parto, adopción o acogimiento, así como durante la situación de excedencia por cuidado de familiares, según lo dispuesto en los artículos 49 y 89.4 de La Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.

3. De acuerdo 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 en la selección a quienes se hayan incorporado en el plazo de un año 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, con objeto de actualizar los conocimientos de los empleados públicos y empleadas públicas. Asimismo, se reservará al menos un 40 por ciento de las plazas en los cursos de formación para su adjudicación a mujeres que reúnan los requisitos establecidos, salvo que el número de solicitudes de mujeres sea insuficiente para cubrir este porcentaje.

4. En aplicación del Real Decreto 2271/2004, de 3 de diciembre, se valorará como criterio de selección a quienes se encuentren afectados por una discapacidad cuyo grado de minusvalía sea igual o superior al 33 por ciento. Las personas con discapacidad que soliciten el curso podrán hacer constar tal circunstancia en la inscripción, y podrán indicar, asimismo, las adaptaciones necesarias en el curso formativo, siempre y cuando hayan sido seleccionadas.

5. Una vez efectuada la selección definitiva de participantes, el Centro Criptológico Nacional comunicará por correo electrónico a cada uno de los alumnos seleccionados 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.

6. La inasistencia a los cursos presenciales, o la falta de conexión a la parte *on line*, sin previo aviso o cumplida justificación, de quienes hubiesen sido seleccionados para participar en el curso podrá determinar su exclusión en convocatorias posteriores.

Quinta. *Modalidad formativa, lugar de celebración y calendario.*

Las actividades formativas se realizarán en la modalidad y en las fechas detalladas en el anexo. En el caso de que resultara necesario realizar algún cambio en las fechas indicadas en la programación, será comunicado con antelación suficiente a los participantes en la actividad de que se trate. Para los cursos en modalidad *on line*, los alumnos deberán disponer de un equipo que tenga la configuración técnica necesaria en cada caso para la realización del curso.

El curso de seguridad de las tecnologías de la información y las comunicaciones (STIC) y los cursos STIC de infraestructura de red, y de detección de intrusos, en modalidad semipresencial, tendrán una fase *on line* y una presencial. La superación de la fase *on line* será requisito imprescindible para participar en la fase presencial.

Cualquier duda o problema técnico derivado del acceso a páginas web, o de la descarga o instalación de las aplicaciones requeridas para la realización del curso, deberá ser consultada con el administrador del sistema del equipo que se esté utilizando.

La fase presencial de los cursos citados, así como las demás actividades formativas, se celebrarán en Madrid. La sede definitiva de desarrollo de las acciones se comunicará a los alumnos con antelación suficiente.

Sexta. *Configuración técnica mínima de los equipos para realizar la fase on line.*

a) *Hardware:*

- 1.º Procesador: 1,2 GHz.
- 2.º 512 MB de memoria RAM o superior.
- 3.º Tarjeta de sonido, altavoces o auriculares.

b) *Software:*

- 1.º *Windows 2000, ME, Vista, Windows 7 o Windows 8.*
- 2.º *Microsoft Internet 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.*
- 6.º 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.

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 párrafo anterior.

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.

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, aunque esté justificada, imposibilitará su expedición.

Octava. *Régimen académico.*

Los alumnos seleccionados que no observen las reglas elementales de participación, respeto y consideración hacia profesores, compañeros o personal del INAP y, en general, que contravengan lo dispuesto en el Código Ético del INAP (que podrá consultarse en [www.inap.es/conocenos](http://www.inap.es/conocenos)) podrán ser excluidos de las actividades formativas.

Novena. *Información adicional.*

Se podrá solicitar información adicional sobre esta convocatoria en la dirección de correo electrónico [formacion.ccn@cni.es](mailto:formacion.ccn@cni.es) o a través del teléfono 91 372 67 85.

Madrid, 26 de noviembre de 2014.—El Director del Instituto Nacional de Administración Pública, P. S. (Real Decreto 464/2011, de 1 de abril), el Gerente del Instituto Nacional de Administración Pública, Enrique Silvestre Catalán.

**ANEXO**

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0914	XII CURSO DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Proporcionar a los participantes los conocimientos necesarios para conseguir una mentalización y concienciación adecuada en la seguridad de los sistemas de las TIC y las amenazas y vulnerabilidades que representan las nuevas tecnologías	<ul style="list-style-type: none"> <li>- Tener responsabilidades en la planificación, gestión o administración de los sistemas de las tecnologías de la información y las comunicaciones, o en su seguridad, por un periodo superior a dos años</li> <li>- Para participar en la fase presencial es imprescindible superar la fase <i>on line</i></li> </ul>	<p>Fase <i>on line</i>:</p> <p>Curso de seguridad en tecnologías de la información y comunicaciones:</p> <p>Introducción a STIC                      Normativa de seguridad                      Políticas de seguridad                      Procedimiento de acreditación                      Inspecciones STIC                      Gestión de incidentes                      Herramientas de seguridad                      Seguridad perimetral                      Redes inalámbricas</p> <p>Fase presencial:</p> <p>Introducción a la criptología:                      Criptografía clásica                      Criptosistemas modernos                      Teoría de la criptofonía</p> <p>Introducción a la amenaza:                      Vulnerabilidades y amenazas</p> <p>Políticas STIC:                      Introducción STIC                      Normativa de seguridad                      Políticas de seguridad</p> <p>Procedimientos STIC:                      Procedimiento de acreditación                      Análisis y gestión de riesgos                      Inspecciones STIC                      Gestión de incidentes                      Amenaza TEMPEST</p> <p>Medidas técnicas STIC:                      Herramientas de seguridad                      Equipamiento STIC</p> <p>Seguridad criptológica:                      Seguridad criptológica</p>	30 h <i>on line</i>	<p>Fase <i>on line</i>:</p> <p>Del 16 al 27 de febrero</p> <p>Fase presencial:                      Del 2 al 13 de marzo</p>

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0917	X CURSO BÁSICO STIC - BASES DE DATOS	Proporcionar a los participantes los conocimientos necesarios para que sean capaces de comprobar, con suficiente garantía, los aspectos de seguridad relativos a la configuración segura de las bases de datos <i>Oracle</i> y <i>MS SQL Server</i>	Un conocimiento mínimo a nivel administrativo de base de datos, así como conocimientos básicos de sistemas <i>Windows/Unix</i> y protocolos de red Se considerarán como prioridades para la selección al curso: - Actividad relacionada con la administración de bases de datos en 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 Centro Criptológico Nacional - 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 un año	Seguridad entornos <i>SQL Server</i> Seguridad entornos <i>Oracle</i>	25 h presenciales	Modalidad presencial: del 23 al 27 de marzo
0918	X CURSO BÁSICO STIC - INFRA-ESTRUCTURA DE RED	Proporcionar a los participantes los conocimientos necesarios para que sean capaces de comprobar, con suficiente garantía, los aspectos de seguridad relativos a la infraestructura de red basada en elementos de comunicaciones (concentradores, enrutadores...), dispositivos inalámbricos y redes privadas virtuales (VPN) introduciendo los conceptos de cortafuegos, sistemas de detección de intrusos (IDS) y dispositivos trampa ( <i>honeypots</i> y <i>honeynets</i> )	Un conocimiento mínimo de sistemas <i>Windows/Unix</i> , así como conocimientos básicos de protocolos y equipamiento de red Se considerarán como prioridades para la selección al curso: - 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 Centro Criptológico Nacional. - 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 un año.  Para participar en la fase presencial es imprescindible superar la fase <i>on line</i>	Fase <i>on line</i> : Curso Básico STIC de Infraestructura de Red  Fase presencial: Dispositivos comunicaciones Dispositivos de filtrado Redes inalámbricas Redes privadas virtuales Seguridad perimetral	15 h <i>on line</i>  25 h presenciales	Fase <i>on line</i> : del 16 al 27 de marzo  Fase presencial: del 6 al 10 de abril

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0930	X CURSO STIC - INSPECCIONES DE SEGURIDAD	Proporcionar a los participantes los conocimientos y habilidades necesarias para que sean capaces de comprobar, con suficiente garantía, los aspectos de seguridad de redes, aplicaciones y dispositivos en cada organización concreta, así como verificar y corregir los procesos e implementaciones	Un conocimiento mínimo de los sistemas <i>Linux</i> y <i>Windows</i> , así como conocimientos básicos de protocolos y equipamiento de red Se considerarán como prioridades para la selección al curso: - 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 periodo superior a dos años	Herramientas de seguridad Verificaciones de seguridad Inspecciones STIC (nivel 3)	25 h presenciales	Modalidad presencial: del 13 al 17 de abril
0936	IV CURSO STIC - SEGURIDAD EN DISPOSITIVOS MÓVILES	Proporcionar a los participantes los conocimientos y habilidades necesarias para conocer de manera detallada, actual y práctica las amenazas y vulnerabilidades de seguridad que afectan a los dispositivos móviles y sus comunicaciones	Se supondrá, por parte de los concurrentes, un conocimiento mínimo a nivel administrativo de sistemas <i>Linux</i> y <i>Windows</i> , así como conocimientos básicos de sistemas de comunicaciones móviles Se considerarán como prioridades para la selección al curso, las siguientes: - Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el Centro Criptológico Nacional (CCN) - Haber realizado cursos relacionados con las tecnologías de la información o su seguridad - Tener responsabilidades, a nivel directivo o 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 años	Seguridad de las comunicaciones GSM, GPRS/EDGE, UMTS, LTE Dispositivos móviles Modelo y arquitectura de seguridad Gestión local y empresarial de dispositivos móviles basados en <SO> Cifrado de datos y gestión de certificados digitales y credenciales en <SO> Comunicaciones USB Comunicaciones <i>Bluetooth</i> Comunicaciones <i>Wi-Fi</i> Comunicaciones GSM (2G) y UMTS (3G) Comunicaciones TCP/IP	35 h presenciales	Modalidad presencial: del 20 al 28 de abril
0931	VIII CURSO STIC - BÚSQUEDA DE EVIDENCIAS	Proporcionar a los participantes 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	Un conocimiento mínimo de los sistemas <i>Linux</i> y <i>Windows</i> , así como conocimientos básicos de protocolos y equipamiento de red Se considerarán como prioridades para la selección al curso: - Haber realizado con anterioridad el Curso Básico STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN)	Metodología Cómo y qué buscar Estudio práctico Lugares donde buscar datos Análisis de ficheros	25 h presenciales	Modalidad presencial: del 4 al 8 de mayo

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0925	X CURSO STIC - SEGURIDAD EN REDES INALÁMBRICAS	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	<ul style="list-style-type: none"> <li>- Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de las tecnologías de la información y comunicaciones (TIC)</li> <li>- Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN</li> <li>- Haber realizado cursos relacionados con las tecnologías de la información o su seguridad</li> <li>- 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 años</li> </ul> <p>Conocimiento mínimo en el nivel administrativo de sistemas <i>Linux</i> y <i>Windows</i>, así como conocimientos básicos de protocolos y equipamiento de red.</p> <p>Se consideraran como prioridades para la selección al curso:</p> <ul style="list-style-type: none"> <li>- Haber realizado con anterioridad el Curso Básico STIC - Infraestructura de Red, desarrollado por el Centro Criptológico Nacional (CCN)</li> <li>- Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de las tecnologías de la información y comunicaciones (TIC)</li> <li>- Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC), desarrollado por el CCN</li> <li>- Haber realizado cursos relacionados con las tecnologías de la información o su seguridad</li> <li>- 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 años</li> </ul>	<p>Medidas técnicas:</p> <ul style="list-style-type: none"> <li>Comunicación WMAN</li> <li>Comunicación WLAN</li> <li>Dispositivos WPAN</li> </ul>	25 h presenciales	Modalidad presencial: del 18 al 22 de mayo
0926	XI CURSO STIC - CORTAFUEGOS	Proporcionar a los participantes 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	<p>Conocimiento mínimo en el nivel administrativo de sistemas <i>Linux</i> y <i>Windows</i>, así como conocimientos básicos de protocolos y equipamiento de red</p> <p>Se consideraran como prioridades para la selección al curso:</p> <ul style="list-style-type: none"> <li>- Haber realizado con anterioridad el Curso Básico STIC - Infraestructura de Red, desarrollado por el Centro Criptológico Nacional (CCN)</li> <li>- Actividad relacionada con la administración de la infraestructura de red asociada a sistemas</li> </ul>	<ul style="list-style-type: none"> <li>Cortafuegos, protocolos y seguridad perimetral</li> <li>NAT y reglas de filtrado</li> <li>AAA y seguridad de contenidos</li> <li>VPN y usuarios móviles</li> <li>Enrutadores y cortafuegos a nivel de sistema</li> </ul>	25 h presenciales	Modalidad presencial: del 25 al 29 de mayo

CÓDIGO	DENOMINACIÓN	OBJETIVOS	REQUISITOS	PROGRAMA	DURACIÓN	FECHAS
0927	XI CURSO STIC - DETECCIÓN DE INTRUSOS	Proporcionar a los participantes 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	<p>de las tecnologías de la información y comunicaciones (TIC)</p> <ul style="list-style-type: none"> <li>- Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC), desarrollado por el CCN</li> <li>- Haber realizado cursos relacionados con las tecnologías de la información o su seguridad</li> <li>- 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 años</li> </ul> <p>Conocimiento mínimo en el nivel administrativo de sistemas <i>Linux</i> y <i>Windows</i>, así como conocimientos básicos de protocolos y equipamiento de red</p> <p>Se consideraran como prioridades para la selección al curso:</p> <ul style="list-style-type: none"> <li>- Haber realizado con anterioridad el Curso Básico STIC - Infraestructura de Red, desarrollado por el Centro Criptológico Nacional (CCN)</li> <li>- Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de las tecnologías de la información y comunicaciones (TIC)</li> <li>- Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC), desarrollado por el CCN</li> <li>- Haber realizado cursos relacionados con las tecnologías de la información o su seguridad</li> <li>- 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 años</li> </ul> <p>Para participar en la fase presencial es imprescindible superar la fase <i>on line</i></p>	<p>Fase <i>on line</i>:</p> <p>Curso STIC de Detección de Intrusos</p> <p>Fase presencial:</p> <p>Conceptos de IDS y análisis de tráfico</p> <p>Análisis de tráfico e IDS a nivel de Red (NIDS)</p> <p>IDS a nivel de sistema (HIDS)</p> <p>Análisis de registros y <i>honeypots</i></p> <p>Detección de ataques con infraestructura IDS combinada</p>	<p>15 h <i>on line</i></p> <p>25 h presenciales</p>	<p>Fase <i>on line</i>: del 25 de mayo al 5 de junio</p> <p>Fase presencial: del 8 al 12 de junio</p>