



Resolución de la directora general del Instituto Nacional de Administración Pública por la que se convocan acciones formativas en materia de seguridad de las tecnologías de la información y la comunicación en colaboración con el Centro Criptológico Nacional.

El Instituto Nacional de Administración Pública (INAP) de acuerdo con su Estatuto, aprobado por el Real Decreto 464/2011, de 1 de abril, tiene entre sus funciones la formación de las empleadas y empleados públicos.

El INAP y el Centro Criptológico Nacional del Centro Nacional de Inteligencia (CNI-CCN) formalizaron en el mes de agosto de 2020 un convenio de colaboración para la organización de actividades formativas para las empleadas y empleados públicos en materia de seguridad de las tecnologías de la información y la comunicación. Como resultado de este convenio se han formado un total 1.454 personas en las convocatorias anteriores.

El INAP, mediante la mejora de las competencias profesionales de las empleadas y empleados públicos, quiere ser un actor central en la transformación de la Administración pública que ayude a construir la sociedad española del futuro. Ese objetivo es buena muestra de su compromiso, junto con el CCN, de fortalecer las competencias en ciberseguridad como uno de los desafíos más importantes de la era digital. Incluyendo el nuevo Esquema Nacional de Seguridad como estándar de referencia y herramienta de prevención frente a los riesgos y amenazas de los sistemas informáticos.

Y que el presente no hace más que confirmar la importancia de la sensibilización y la formación en materia de seguridad TIC. Por eso, la alianza INAP-CCN quiere contribuir mediante la formación a que el ser humano sea, como se suele afirmar, el eslabón menos débil de la cadena de la seguridad tecnológica. Las amenazas están por muchas partes: el trabajo en remoto o las infraestructuras de red, mediante programas maliciosos, ransomware o incluso las llamadas “amenazas persistentes avanzadas”. Pues bien, mediante una metodología principalmente en línea tutorizada, cerca de 240 empleados y empleadas públicas de perfil TIC saldrán más capacitados para detectar y afrontar este tipo de amenazas que rondan las administraciones públicas y les impiden a menudo realizar su función correctamente, con la consiguiente pérdida de valor.

Esta convocatoria se enmarca en el Plan de Formación del INAP para 2022, publicado el 16 de diciembre de 2021 ([acceso a publicación](#)), y estableció las condiciones generales de las acciones formativas para este año.

En virtud de lo anterior, resuelvo:

Primero. *Objeto.*

Mediante esta resolución se convocan las diez acciones formativas en materia de seguridad de las tecnologías de la información y las comunicaciones (STIC) incluidas en el anexo, que se desarrollarán durante el segundo semestre del año 2022.

La información publicada en el anexo se puede ampliar en la ficha descriptiva de cada actividad formativa disponible en la página web del INAP (<https://buscadorcursos.inap.es/>). En ella se detallan los objetivos, los contenidos, el horario, el lugar de celebración, así como otra información de interés relativa al desarrollo de cada actividad.



Segundo. *Destinatarios, condiciones de admisión y criterios de selección.*

Es requisito común para participar en las actividades convocadas en la presente resolución tener la condición de empleado público y prestar servicios a través de una relación de carácter funcional, laboral o estatutario en cualquiera de las Administraciones públicas.

Estas actividades formativas podrán ser solicitadas por el personal funcionario de los subgrupos A1, A2, B y C1, y por el personal laboral equivalente, que tengan responsabilidades en la planificación, gestión, administración, mantenimiento o seguridad de sistemas de las tecnologías de la información y las comunicaciones.

En el anexo se detallan los requisitos específicos de participación en cada acción formativa.

El número de participantes admitidos por actividad formativa no excederá, con carácter general, de 24. La selección de los participantes la realizará el Centro Criptológico Nacional (CCN) en colaboración con el INAP.

Además de los establecidos específicamente en el anexo para cada actividad formativa, en la selección se observarán los siguientes criterios:

- Candidatos pertenecientes a organismos que tengan suscritos servicios de ciberseguridad con el CCN;
- La vinculación entre el puesto desempeñado y los contenidos de la acción formativa;
- El equilibrio entre organismos e instituciones, e interés objetivo de la organización administrativa en la participación del solicitante en la actividad formativa debidamente justificada por el responsable del departamento ministerial u organismo.

Se podrá participar en las actividades 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 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre.

En aplicación del Real Decreto 2271/2004, de 3 de diciembre, se valorará como criterio de selección el reconocimiento de un grado de discapacidad igual o superior al 33 por ciento. En el caso de recibir varias solicitudes de un mismo organismo o institución, se seleccionará al candidato con el perfil más ajustado a los contenidos de la actividad formativa. Las personas con discapacidad que soliciten participar en una actividad podrán hacer constar tal circunstancia en la inscripción, y, en tal caso, deberán indicar las adaptaciones que necesitarían para poder desarrollarla.

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.

Una vez efectuada la selección definitiva de participantes, el CCN se comunicará por correo electrónico con quienes hayan sido admitidos, que deberán confirmar su participación en la actividad formativa cumplimentando un formulario electrónico en los plazos indicados en él. Los solicitantes no admitidos recibirán igualmente un correo electrónico para comunicarles esta circunstancia.

Tercero. *Modalidad 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 previstas, será comunicado con antelación suficiente a los participantes en la actividad de que se trate. Para todas las actividades formativas, los participantes deberán disponer de un equipo que tenga la configuración técnica necesaria en cada caso para la realización de dicha actividad (ver apartado cuarto). Cualquier duda o problema técnico derivado del acceso a páginas web, o de la descarga o instalación de las aplicaciones requeridas para la realización de la acción formativa, deberá ser consultada con el administrador del sistema del equipo que se esté utilizando.

Las siguientes actividades formativas tendrán una primera fase en línea asíncrona, cuya superación será requisito imprescindible para participar en la segunda fase síncrona:

- VII Curso STIC – cibervigilancia;
- VI y VII Curso del Esquema Nacional de Seguridad;
- IX Curso STIC – seguridad en infraestructuras de red;
- XVIII Curso de gestión de seguridad de los Sistemas de Información y Comunicación (Gestión STIC);

La información de las actividades formativas que cuentan con sesiones síncronas obligatorias programadas, se encuentra detallada en la ficha descriptiva de cada una de ellas.

Las sesiones síncronas podrán ser grabadas, lo que se comunica a los efectos oportunos.

Cuarto. *Configuración técnica mínima de los equipos.*

Las actividades que dispongan de fase en línea asíncrona previa, requerirán un equipo con la siguiente configuración mínima:

- a) Hardware:
 1. 2 Gb de memoria RAM o superior.
 2. Tarjeta de sonido, altavoces o auriculares.



b) Software:

1. Windows 8 o superior, Mac OS X 10.10.5 o superior, Ubuntu 16.04 o superior.
2. Última versión disponible de alguno de los siguientes navegadores de Internet: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome o Apple Safari.
3. Permitir ventanas emergentes en el navegador para el sitio web desde el que se desarrolla el curso.

c) Requisitos de conectividad. Configuración de los servidores proxy/firewall de las redes corporativas en las que se encuentren los usuarios:

1. Posibilidad de descargar ficheros con la extensión PDF.
2. Posibilidad de que los usuarios que no lo tengan puedan descargar e instalar en sus equipos el software enumerado en el párrafo anterior.

d) Otros requisitos:

1. Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente.
2. Tipo de conexión a Internet: banda ancha.

Para la realización de la fase en línea síncrona o presencial, los equipos deberán contar con la siguiente configuración recomendada mínima. Los detalles de configuración específicos para cada curso se comunicarán en el momento de la selección:

a) Hardware:

1. Procesador Intel i5 o superior.
2. 8 Gb de memoria RAM o superior.
3. 100 Gb de espacio disponible en disco.
4. Tener habilitada virtualización en BIOS.

b) Software:

1. Microsoft Windows 8/10/11 (64 bits).
2. Última versión de los navegadores Mozilla Firefox o Google Chrome
3. Entorno de virtualización en el que poder ejecutar las máquinas virtuales a utilizar durante el curso.

c) Requisitos de conectividad. Configuración de los servidores proxy/firewall de las redes corporativas en las que se encuentren los usuarios:

1. Posibilidad de descargar ficheros con la extensión PDF.
2. Posibilidad de que los usuarios que no lo tengan puedan descargar e instalar en sus equipos el software enumerado en el párrafo anterior.

d) Otros requisitos:

1. Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente.



2. Tipo de conexión a Internet: banda ancha.

Quinto. *Solicitudes.*

Quien desee participar en las actividades formativas convocadas deberá cumplimentar la correspondiente solicitud electrónica. El acceso a dicha solicitud se podrá realizar desde el catálogo de formación del INAP <https://buscadorcursos.inap.es/>, donde se podrán localizar las actividades formativas que se encuentran en periodo de inscripción.

Para realizar la inscripción será preciso contar con la autorización previa del superior jerárquico. Para formalizar dicha autorización, el sistema de inscripción le permitirá descargar la solicitud, que deberá conservar, ya que podrá ser requerida por el INAP en cualquier momento.

El plazo de presentación de solicitudes comenzará a las 12:00h del día 20 de junio de 2022 y finalizará a las 23:59h del día 4 de julio de 2022 (UTC+2).

En caso de incidencias en la realización de la solicitud electrónica, pueden ponerse en contacto con el Centro de Atención al Usuario (CAU):

- Correo electrónico: cau@inap.es
- Teléfono de contacto: 910616892.
- Horario de atención de lunes a viernes a 8:00 a 20:00 horas.

Sexto. *Información adicional.*

A través del [espacio del alumnado](#) del portal web del INAP se puede acceder a toda la información y servicios electrónicos que el INAP pone a disposición de los participantes, incluida la relacionada con las preguntas más frecuentes que se plantean al realizar la inscripción. Asimismo, mediante certificado electrónico será posible gestionar en el [Portal del Alumnado](#) los datos personales y las solicitudes, así como consultar el expediente de las actividades formativas realizadas en este Instituto.

Para el desarrollo de los procesos de aprendizaje, el alumnado contará con el acceso gratuito a “[Ágora](#)” a [La Administración al Día](#) y al [Banco de Conocimiento](#), así como a la [Red Social Profesional](#) del INAP.

Se puede solicitar información adicional sobre esta convocatoria enviando un mensaje a soporte_formacion@ccn.cni.es.

Firmado electrónicamente.- La Directora del Instituto Nacional de Administración Pública, Consuelo Sánchez Naranjo.

ANEXO

CÓDIGO	DENOMINACIÓN	REQUISITOS	CRITERIOS ESPECÍFICOS DE SELECCIÓN	MODALIDAD	DURACIÓN	FECHAS
0957	II CURSO STIC AMAZON WEB SERVICES (AWS) EN EL ENS	Disponer de un conocimiento mínimo de comunicaciones y seguridad de las Tecnologías de la Información y Comunicación. Un aprovechamiento óptimo de la formación se conseguirá si se cuenta además con conocimientos o experiencia previa con el Esquema Nacional de Seguridad y con entornos de nube pública.	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 con anterioridad el Curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones (Gestión STIC) desarrollado por el Centro Criptológico Nacional. Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. Tener responsabilidades en la implementación, gestión u operación de sistemas de las TIC o en la gestión de la seguridad de dichos sistemas por un período superior a un (1) año.	En línea tutorizada	Síncrona: 20h.	Del 5 al 8 de septiembre
0944	VII CURSO STIC - CIBERVIGILANCIA	Disponer de un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.	Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicación (STIC) desarrollado por el Centro Criptológico Nacional (CCN). 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. Para participar en la fase presencial es imprescindible superar la fase en línea.	En línea tutorizada	Fase asíncrona: 25h. Fase síncrona: 25h.	Del 5 al 9 de septiembre Del 12 al 16 de septiembre

CÓDIGO	DENOMINACIÓN	REQUISITOS	CRITERIOS ESPECÍFICOS DE SELECCIÓN	MODALIDAD	DURACIÓN	FECHAS
0945	VI CURSO STIC - ESQUEMA NACIONAL DE SEGURIDAD	Disponer de un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.	Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicación (STIC) desarrollado por el Centro Criptológico Nacional (CCN). Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. Tener responsabilidades, en el nivel directivo, 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 (1) año. Para participar en la fase presencial es imprescindible superar la fase en línea.	Mixta: en línea tutorizada + presencial	Fase asíncrona: 40h. Fase presencial: 20h.	Del 12 al 26 de septiembre Del 27 al 30 de septiembre
0939	VI CURSO AVANZADO STIC DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD	Disponer de un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.	Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicación (STIC) desarrollado por el CCN. Haber realizado con anterioridad el Curso STIC de Gestión de incidentes de ciberseguridad (Herramientas CCN-CERT). 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.	En línea tutorizada	Síncrona: 25h.	Del 19 al 23 de septiembre

CÓDIGO	DENOMINACIÓN	REQUISITOS	CRITERIOS ESPECÍFICOS DE SELECCIÓN	MODALIDAD	DURACIÓN	FECHAS
0945	VII CURSO STIC - ESQUEMA NACIONAL DE SEGURIDAD	Disponer de un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.	Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicación (STIC) desarrollado por el Centro Criptológico Nacional (CCN). Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. Tener responsabilidades, en el nivel directivo, 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 (1) año. Para participar en la fase presencial es imprescindible superar la fase en línea.	En línea tutorizada	Fase asíncrona: 40h. Fase síncrona: 20h.	Del 26 de septiembre al 7 de octubre Del 10 al 11 y del 13 al 14 de octubre
0955	I CURSO STIC - DESARROLLO SEGURO	Disponer de un conocimiento mínimo en lenguajes de programación y seguridad, así como conocimientos o experiencia previa en el área de desarrollo de software y conocimientos técnicos en JAVA.	Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicación (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 técnico, en el desarrollo de software por un período superior a un (1) año.	En línea tutorizada	Síncrona: 25h.	Del 3 al 7 de octubre

CÓDIGO	DENOMINACIÓN	REQUISITOS	CRITERIOS ESPECÍFICOS DE SELECCIÓN	MODALIDAD	DURACIÓN	FECHAS
0940	IX CURSO STIC – SEGURIDAD EN INFRAESTRUCTURAS DE RED	Disponer de un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.	<p>Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicación (STIC) desarrollado por el Centro Criptológico Nacional (CCN).</p> <p>Haber realizado cursos relacionados con las tecnologías de la información o su seguridad.</p> <p>Actividad relacionada con la administración de la infraestructura de red asociada a sistemas de las tecnologías de la información y comunicaciones (TIC).</p> <p>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 (1) año.</p> <p>Para participar en la fase presencial es imprescindible superar la fase en línea.</p>	En línea tutorizada	<p>Fase asíncrona: 15h.</p> <p>Fase síncrona: 25h.</p>	<p>Del 10 al 21 de octubre</p> <p>Del 24 al 28 de octubre</p>
0952	II CURSO STIC DE CIBERINTELIGENCIA	Disponer de un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.	<p>Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicación (STIC) desarrollado por el CCN.</p> <p>Haber realizado con anterioridad el Curso STIC de Gestión de incidentes de ciberseguridad (Herramientas CCN-CERT).</p> <p>Haber realizado cursos relacionados con las tecnologías de la información o su seguridad.</p> <p>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.</p>	En línea tutorizada	Síncrona: 25h.	Del 17 al 21 de octubre

CÓDIGO	DENOMINACIÓN	REQUISITOS	CRITERIOS ESPECÍFICOS DE SELECCIÓN	MODALIDAD	DURACIÓN	FECHAS
0919	XVIII CURSO DE GESTIÓN DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y DEL ESQUEMA NACIONAL DE SEGURIDAD (GESTIÓN STIC)	Disponer de un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.	Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicación (STIC) desarrollado por el Centro Criptológico Nacional (CCN). Haber realizado cursos relacionados con las tecnologías de la información o su seguridad. Tener responsabilidades, en el nivel directivo, 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 (1) año.	Mixta: en línea tutorizada + presencial	Fase asíncrona: 30h. Fase presencial: 25h. Fase síncrona: 25h.	Del 31 de octubre al 11 de noviembre Del 14 al 18 de noviembre, de 9:00 a 14:00 horas Del 21 al 25 de noviembre, de 9:00 a 14:00 horas
0954	III CURSO STIC DE TRAZABILIDAD DEL DATO	Disponer de un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red.	Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicación (STIC) desarrollado por el CCN. Haber realizado con anterioridad el Curso STIC de Gestión de incidentes de ciberseguridad (Herramientas CCN-CERT). 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.	En línea tutorizada	Síncrona: 15h.	Del 2 al 4 de noviembre