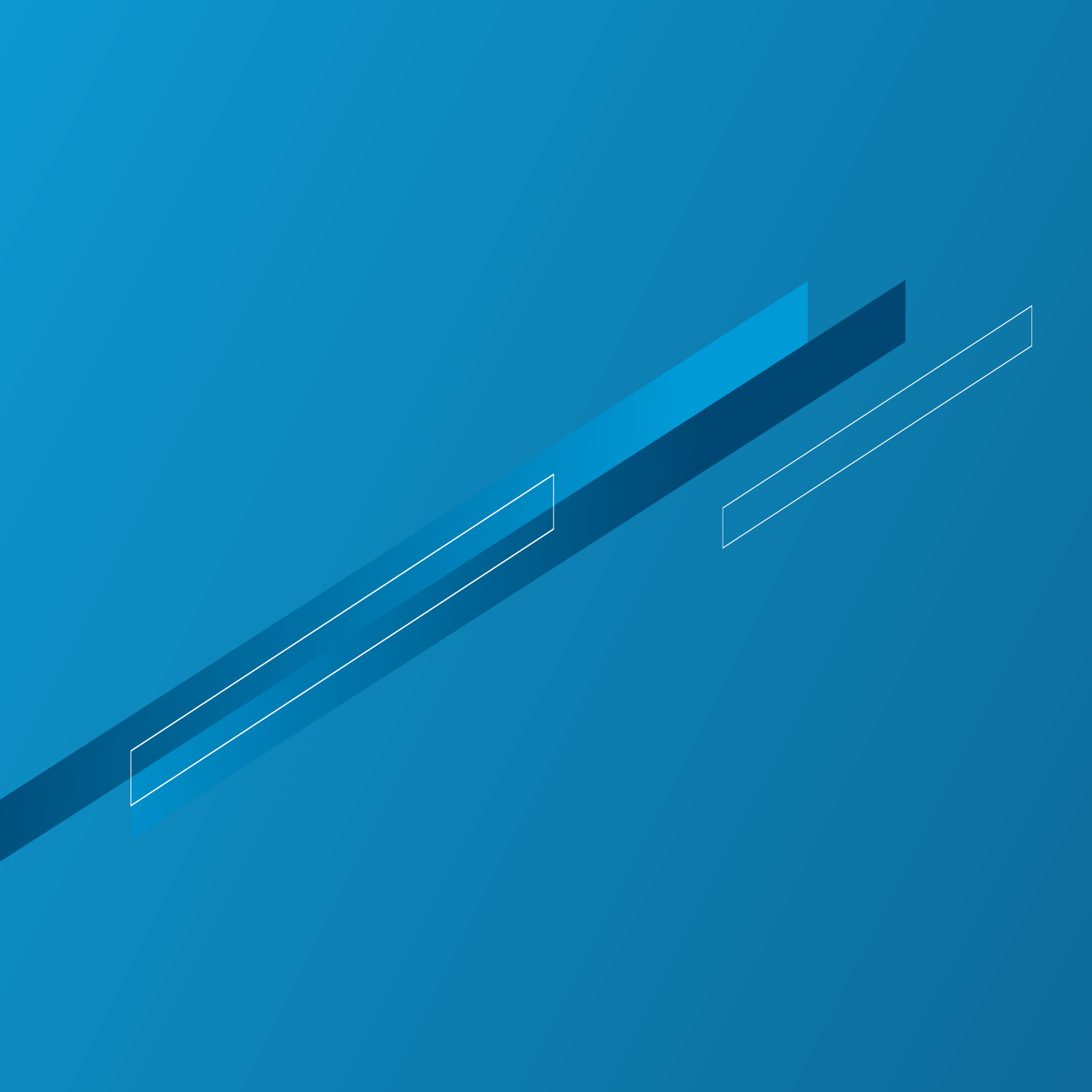
Plan de Formación 2020

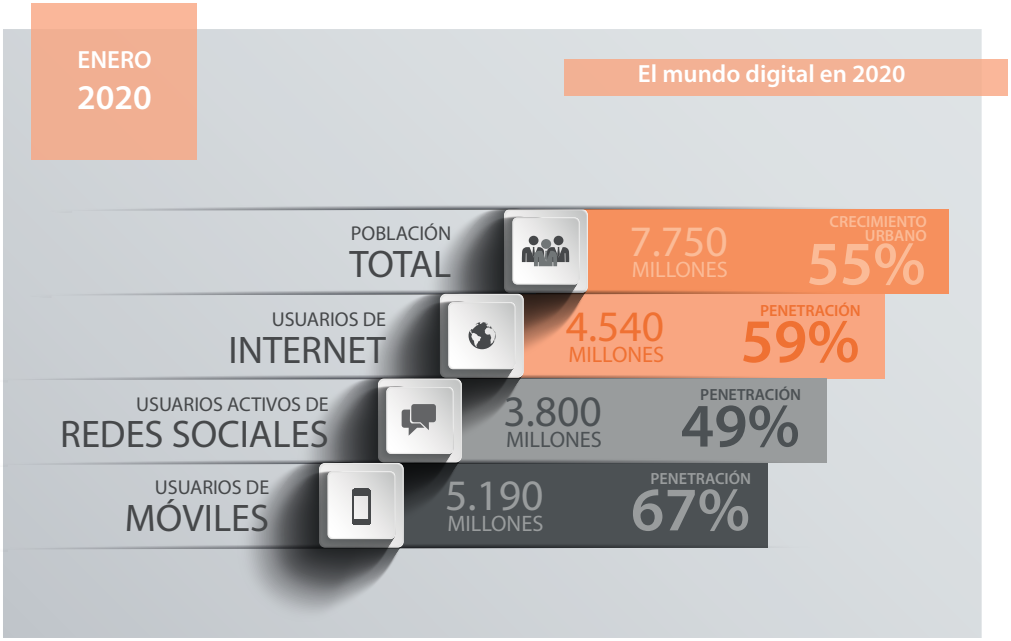
Centro Criptológico Nacional

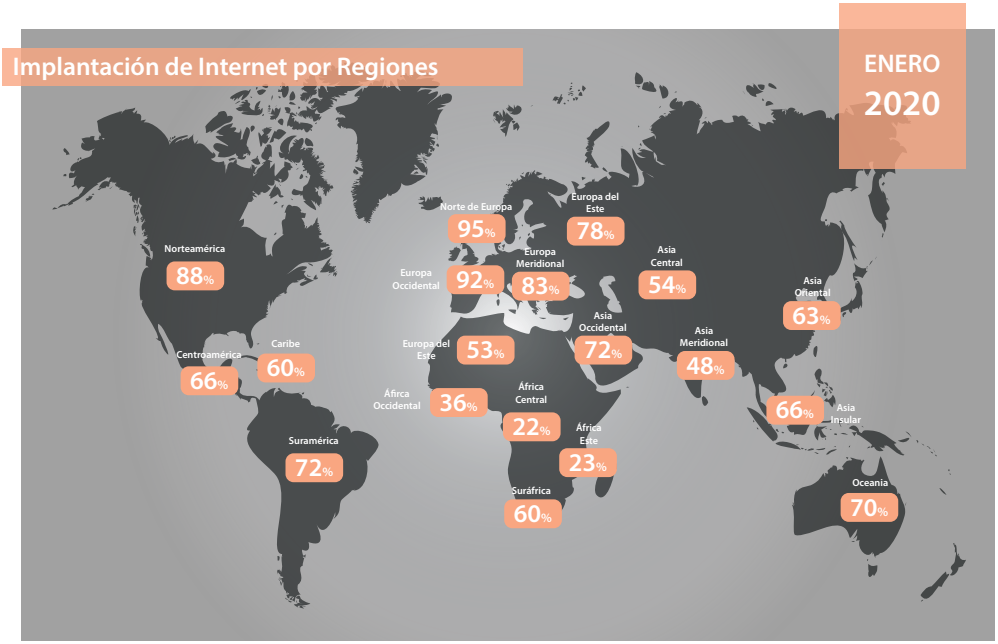


Índice

1. Necesidad formativa y nuevos retos

La evolución de las nuevas tecnologías, especialmente las relacionadas con la información y la comunicación, y el uso generalizado de internet ha propiciado el desarrollo de un nuevo escenario: el ciberespacio, cuya protección ante posibles amenazas y agresiones resulta imprescindible.





Para lograr un ciberespacio seguro, en el que los riesgos puedan mitigarse hasta un margen asumible, es fundamental concienciar y sensibilizar a la sociedad; pues solo a través de una capacitación continua se pueden prevenir y tratar de manera oportuna los incidentes de ciberseguridad.

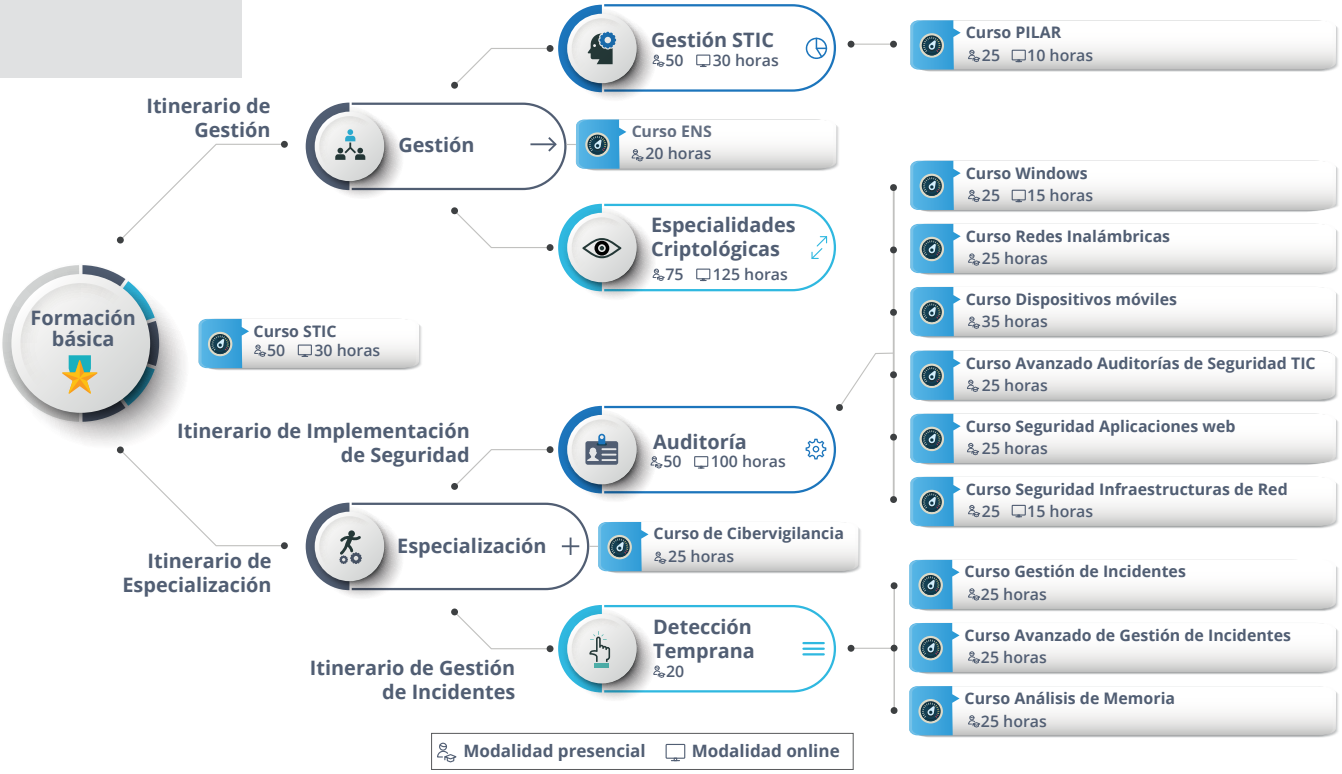
Ante la necesidad de fomentar y desarrollar perfiles profesionales cualificados para el sector público, el **Centro Criptológico Nacional (CCN)** ofrece un amplio programa de cursos formativos, adaptado a las necesidades planteadas por su comunidad de referencia. Este Plan de Formación, con un diseño curricular flexible, se ha ido transformando a medida que lo han hecho las tecnologías, adaptándose así al nuevo escenario que presenta el ciberespacio.

La oferta formativa del Centro Criptológico Nacional se ha elaborado para dar una respuesta eficaz a los retos del siglo XXI. Ante la necesidad de que esta respuesta sea global, el CCN pone a disposición del sector público, del sector privado e, incluso, de otros Estados, su conocimiento y experiencia en la formación de personal en el ámbito de la ciberseguridad.

Además, como garantía de superación de la formación realizada, el CCN otorga a los concurrentes que la hayan superado con aprovechamiento, un **Certificado** que especifica las materias y créditos asociados.

2. Formación curricular

El Plan de Formación del Centro Criptológico Nacional se ha diseñado atendiendo a la necesidad de capacitar, tanto presencialmente como a distancia, a profesionales cualificados que disponen de distinto perfil y nivel de formación. Por este motivo, se ha establecido una **formación BÁSICA** que, a través del curso STIC, introduce al alumno en el ámbito de la Seguridad de las Tecnologías de la Información y la Comunicación.



Completada la formación básica, el profesional que desee perfeccionar sus conocimientos puede elegir entre dos itinerarios: **gestión** y **especialización**. El primero, dispone a su vez de dos ramas: **gestión STIC** y la rama de **Especialidades Criptológicas**.

Por su parte, el itinerario de especialización, dirigido a personal más técnico, cuenta con el módulo de **Auditoría** y con el de **Gestión de Incidentes**, cada uno de ellos compuesto por un conjunto de cursos que permiten al alumno especializarse en la materia.

Finalidad

La finalidad del **"Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)"** es proporcionar a los asistentes los conocimientos necesarios para conseguir una concienciación adecuada en la seguridad de los Sistemas de las TIC y las amenazas y vulnerabilidades que representan las nuevas tecnologías.

Créditos / Horas del Plan de Estudios

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

- Teoría: 3 créditos / 30 horas

La distribución de las 50 horas de la fase presencial del curso (5 créditos) es la siguiente:

- Teoría: 4,5 créditos / 45 horas
- Práctica: 0,5 créditos / 5 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en dos fases (on-line y presencial) será condición imprescindible para participar en la fase presencial, superar las pruebas correspondientes a los exámenes previstos durante la fase on-line en los que se valoran los conocimientos adquiridos en dicha fase.

La nota final del curso será de "APTO", siendo la nota de la fase on-line considerada sólo para el acceso a la fase presencial que se inicia posteriormente.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Se considerará como prioridad para la selección de participantes al curso el estar desarrollando, en su actual destino, actividades de planificación, gestión o administración de Sistemas de las TIC, o la Seguridad de los mismos, por un período superior a un (1) año.

Requisitos técnicos mínimos de los equipos

Se dispondrá de un equipo que tenga una configuración mínima de:

Hardware:

- Procesador 1,3Ghz. 2GB de memoria RAM o superior.

Software:

- Windows 8 o superior, Mac OS X 10.10.5 o superior, Ubuntu 16.04 o superior.
- Última versión disponible de alguno de los siguientes navegadores: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome o Apple Safari (el navegador Microsoft Edge no es compatible con la plataforma online).

• Plug-in Adobe Flash Player correctamente instalado y configurado en el navegador que se esté utilizando.

• Será necesario configurar correctamente el navegador para que permita ventanas emergentes del sitio https://www.ccn-cert.cni.es

Requisitos de conectividad:

• Conexión a Internet de banda ancha (equivalente a un ADSL doméstico).

• Posibilidad de descargar ficheros con la extensión PDF desde el servidor donde esté alojado el curso.

• Posibilidad de que los usuarios que lo requieran, puedan descargar e instalar en sus equipos el software enumerado anteriormente.

Otros requisitos:

• Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente. El tipo de la conexión a Internet deberá ser banda ancha (equivalente a un ADSL doméstico).

Acceso al curso (Fase On-line)

Para poder participar en la fase on-line, será necesario que el alumno sea usuario registrado del portal CCN-CERT (https://www.ccn-cert.cni.es), donde está ubicada la plataforma de e-learning. En el proceso de registro se establece un nombre de usuario y una clave de acceso al Portal para su conexión. Con antelación a la celebración del curso, a través de correo electrónico, se facilitará a los alumnos los datos y las instrucciones de acceso a la fase on-line. El alumno tendrá que tener en cuenta los siguientes requisitos:

• La cuenta de correo empleada para la comunicación entre el tutor y los alumnos puede ser una personal o de trabajo, pero tendrá que coincidir con la indicada en la solicitud telemática.

• Es preciso que la cuenta de correo esté operativa y sea de uso frecuente.

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.	3,8	3,8	0	Orientaciones de Seguridad. Conceptos y Terminología STIC. Introducción a la Criptología. Criptosistemas y Modos de Empleo de la Cifra. Introducción a la Criptofonía. Organización y Gestión de Seguridad. Política de Seguridad de las TIC.

Procedimientos STIC (Fase a Distancia)	- Procedimiento de Acreditación. - Inspecciones STIC. - Gestión de Incidentes.	3,1	3,1	0	Acreditación de Sistemas. Vulnerabilidades, Amenazas y Riesgos. Documentación de Seguridad. Inspección STIC. Amenaza TEMPEST y TRANSEC. Gestión de Incidentes de Seguridad.
Medidas Técnicas STIC (Fase a Distancia)	- Herramientas de Seguridad. - Seguridad Perimetral. - Redes Inalámbricas.	4,6	4,6	0	Software Malicioso. Herramientas de Seguridad. Seguridad perimetral. Interconexión de Sistemas. Cortafuegos y Sistemas de Detección de Intrusos. Seguridad Inalámbrica.
Introducción a la Criptología	- Criptografía Clásica. - Criptosistemas Modernos. - Teoría de la Criptofonía	0,7	0,7	0	Principios Básicos de la Criptología. Criptografía Moderna. Criptografía de Clave Pública. Sistemas de Criptofonía.
Introducción a la Amenaza	- Vulnerabilidades y Amenazas	0,4	0,1	0,3	Vulnerabilidades y Amenazas a los Sistemas de Información. Amenaza TEMPEST. Caso Práctico de Ataque.
Políticas STIC	- Introducción STIC. - Normativa de Seguridad. - Políticas de Seguridad.	0,7	0,7	0	Esquema Nacional de Evaluación y Certificación de la Seguridad de las T.I. Criterios de Evaluación de la Seguridad de las T.I. Laboratorio de Evaluación. Legislación Nacional. Política de Seguridad de las TIC en la Administración. Organización de Seguridad de las TIC
Procedimientos STIC	- Procedimiento de Acreditación. - Análisis y Gestión de Riesgos. - Inspecciones STIC. - Gestión de Incidentes. - Amenaza TEMPEST.	0,9	0,9	0	Análisis y Gestión de Riesgos. MAGERIT y Herramienta PILAR. Seguridad Física, Documental y del Personal. Procedimiento de Acreditación. Documentación de Seguridad del Sistema. Procedimiento de Inspección STIC. Interconexión de Sistemas. Gestión de Incidentes. Evaluación TEMPEST.
Medidas Técnicas STIC	- Herramientas de Seguridad. - Equipamiento STIC.	1,4	1,2	0,2	Dispositivos de Protección de Perímetro. Antivirus. Sistemas de Protección de Integridad. Software de Cifrado. Herramientas de Análisis de Vulnerabilidades. Tarjetas Inteligentes. Telefonía Móvil. Seguridad Inalámbrica. Infraestructura de Clave Pública (PKI).
Seguridad Criptológica	- Seguridad Criptológica.	0,3	0,3	0	Coordinación Criptológica. Tipos de Cifradores. Equipamiento STIC para la Administración.
Grupo Varios	- Inauguración y Clausura.	0,6	0,6	0	Examen Previo. Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso de Gestión de Seguridad de las Tecnologías de la Información y Comunicaciones y del Esquema Nacional de Seguridad (Gestión STIC)"** consiste en:

- Proporcionar los conocimientos necesarios para el análisis y gestión de riesgos de un Sistema de las TIC. Como resultado de lo anterior, podrán redactar y aplicar los procedimientos y políticas de seguridad adecuados para proteger la información procesada, almacenada o transmitida por un Sistema.
- Familiarizar a los asistentes 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.
- Proporcionar los conocimientos y habilidades necesarias para poder decidir cuáles son las tecnologías, estrategias y herramientas necesarias en cada Organización concreta para verificar la seguridad de redes, aplicaciones y dispositivos así como verificar y corregir los procesos e implementaciones.
- Proporcionar la ayuda necesaria para poder implantar las medidas propuestas en el **Esquema Nacional de Seguridad (ENS)**.

Créditos / Horas del Plan de Estudios

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

- Teoría: 3 créditos / 30 horas

La distribución de las 50 horas de la fase presencial del curso (5 créditos) es la siguiente:

- Teoría: 3 créditos / 30 horas
- Práctica: 2 créditos / 20 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en dos fases (on-line y presencial) será condición imprescindible para participar en la fase presencial, superar las pruebas correspondientes a los exámenes previstos durante la fase on-line en los que se valoran los conocimientos adquiridos en dicha fase.

La nota final del curso será de "APTO", siendo la nota de la fase on-line considerada sólo para el acceso a la fase presencial que se inicia posteriormente.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1 o A2 que tenga responsabilidades a nivel directivo, o en la planificación, gestión o administración de los Sistemas de las tecnologías de la información y comunicaciones (TIC), o con la seguridad de los mismos.

Se consideran 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.
- 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 período superior a un (1) año.

Requisitos técnicos mínimos de los equipos

Se dispondrá de un equipo que tenga una configuración mínima de:

Hardware:

- Procesador 1,3Ghz. 2GB de memoria RAM o superior.

Software:

- Windows 8 o superior, Mac OS X 10.10.5 o superior, Ubuntu 16.04 o superior.
- Última versión disponible de alguno de los siguientes navegadores: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome o Apple Safari (el navegador Microsoft Edge no es compatible con la plataforma online).
- Plug-in Adobe Flash Player correctamente instalado y configurado en el navegador que se esté utilizando.
- Será necesario configurar correctamente el navegador para que permita ventanas emergentes del sitio https://www.ccn-cert.cni.es

Requisitos de conectividad:

- Conexión a Internet de banda ancha (equivalente a un ADSL doméstico).
- Posibilidad de descargar ficheros con la extensión PDF desde el servidor donde esté alojado el curso.
- Posibilidad de que los usuarios que lo requieran, puedan descargar e instalar en sus equipos el software enumerado anteriormente.

Otros requisitos:

- Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente. El tipo de la conexión a Internet deberá ser banda ancha (equivalente a un ADSL doméstico).

Acceso al curso (Fase On-line)

Para poder participar en la fase on-line, será necesario que el alumno sea usuario registrado del portal CCN-CERT (https://www.ccn-cert.cni.es), donde está ubicada la plataforma de e-learning. En el proceso de registro se establece un nombre de usuario y una clave de acceso al Portal para su conexión. Con antelación a la celebración del curso, a través de correo electrónico, se facilitará a los alumnos los datos y las instrucciones de acceso a la fase on-line. El alumno tendrá que tener en cuenta los siguientes requisitos:

- La cuenta de correo empleada para la comunicación entre el tutor y los alumnos puede ser una personal o de trabajo, pero tendrá que coincidir con la indicada en la solicitud telemática.

• Es preciso que la cuenta de correo esté operativa y sea de uso frecuente.

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	- Introducción a STIC. - Normativa de Seguridad. - Políticas de Seguridad.	0,6	0,6	0	Orientaciones de Seguridad. Conceptos y Terminología STIC. Introducción a la Criptología. Criptosistemas y Modos de Empleo de la Cifra. Introducción a la Criptofonía. Organización y Gestión de Seguridad. Política de Seguridad de las TIC.
Procedimientos STIC	- Procedimiento de Acreditación. - Inspecciones STIC. - Gestión de Incidentes.	0,5	0,5	0	Acreditación de Sistemas. Vulnerabilidades, Amenazas y Riesgos. Documentación de Seguridad. Inspección STIC. Amenaza TEMPEST y TRANSEC. Gestión de Incidentes de Seguridad.
Medidas Técnicas STIC	- Herramientas de Seguridad. - Seguridad Perimetral. - Redes Inalámbricas.	0,5	0,5	0	Software Malicioso. Herramientas de Seguridad. Seguridad perimetral. Interconexión de Sistemas. Cortafuegos y Sistemas de Detección de Intrusos. Seguridad Inalámbrica.
Esquema Nacional de Seguridad	- Introducción y Categorización del ENS - Auditoría y Organización de Seguridad en el ENS - Evaluación y Certificación. - Normativa de Seguridad.	2,8	2,8	0	Esquema Nacional de Seguridad. Procedimiento de Auditoría y Acreditación. Organización de Seguridad. Documentación de Seguridad. Gestión de Incidentes de Seguridad.
Análisis y Gestión de Riesgos	- Análisis y Gestión de Riesgos. - Metodología MAGERIT. - Herramienta PILAR.	2,2	1	1,2	Introducción al Análisis y Gestión de Riesgos. Activos. Amenazas, Impacto y Riesgo. Instalación Herramienta PILAR. Salvaguardas y Evaluaciones. Generación de Documentación de Seguridad. Ejemplos prácticos.
Inspecciones STIC	- Interconexión en el ENS - Inspecciones STIC. - Seguridad en entornos Web e Inalámbricos	0,8	0,8	0	Introducción a las Inspecciones STIC. Herramientas y Verificaciones de Seguridad. Seguridad en los Sistemas y Dispositivos. Seguridad en Aplicaciones Web. El Factor Humano. Casos de Estudio.
Grupo Varios	- Inauguración y Clausura.	0,6	0,6	0	Examen Previo. Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC – Herramienta PILAR"** es proporcionar los conocimientos y habilidades necesarias para poder evaluar el estado de seguridad de un sistema, identificando y valorando sus activos e identificando y valorando las amenazas que se ciernen sobre ellos.

Familiarizar a los concurrentes 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.

Créditos / Horas del Plan de Estudios

La distribución de las 10 horas de la fase on-line del curso (1 crédito) es la siguiente:

- Teoría: 1 crédito / 10 horas

La distribución de las 25 horas de la fase presencial del curso (2,5 créditos) es la siguiente:

- Teoría: 1 crédito / 10 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en dos fases (on-line y presencial) será condición imprescindible para participar en la fase presencial, superar las pruebas correspondientes a los exámenes previstos durante la fase on-line en los que se valoran los conocimientos adquiridos en dicha fase.

Durante la fase presencial del curso, los participantes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2 o C1 que tenga responsabilidades que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de los Sistemas de las tecnologías de la información y comunicaciones (TIC), o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica.

Se consideran 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.
- Haber realizado con anterioridad el Curso de Gestión 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 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 dos (2) años.

Requisitos técnicos mínimos de los equipos

Se dispondrá de un equipo que tenga una configuración mínima de:

Hardware:

• Procesador 1,3Ghz. 2GB de memoria RAM o superior.

Software:

• Windows 8 o superior, Mac OS X 10.10.5 o superior, Ubuntu 16.04 o superior.

• Última versión disponible de alguno de los siguientes navegadores: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome o Apple Safari (el navegador Microsoft Edge no es compatible con la plataforma online).

• Plug-in Adobe Flash Player correctamente instalado y configurado en el navegador que se esté utilizando.

• Será necesario configurar correctamente el navegador para que permita ventanas emergentes del sitio https://www.ccn-cert.cni.es

Requisitos de conectividad:

• Conexión a Internet de banda ancha (equivalente a un ADSL doméstico).

• Posibilidad de descargar ficheros con la extensión PDF desde el servidor donde esté alojado el curso.

• Posibilidad de que los usuarios que lo requieran, puedan descargar e instalar en sus equipos el software enumerado anteriormente.

Otros requisitos:

• Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente. El tipo de la conexión a Internet deberá ser banda ancha (equivalente a un ADSL doméstico).

Acceso al curso (Fase On-line)

A través de correo electrónico se facilitara a cada alumno seleccionado la dirección de la plataforma e-learning, un nombre de usuario y una clave de acceso al curso para su conexión. Estos datos se enviarán con antelación a la celebración del mismo para que se familiarice con la metodología y con la plataforma. El alumno tendrá que tener en cuenta lo siguientes requisitos:

• La cuenta de correo empleada para la comunicación entre el tutor y los alumnos puede ser una personal o de trabajo, pero tendrá que coincidir con la indicada en la solicitud telemática.

• Es preciso que la cuenta de correo esté operativa y sea de uso frecuente.

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	
Análisis y Gestión de Riesgos (fase on-line)	- Análisis de Riesgos. - Introducción a la Gestión del Riesgo.	1	1	0	Análisis de Riesgos (activos, amenazas, salvaguardas, indicadores de impacto). Calificación de los Riesgos.
Medidas Técnicas STIC	- Análisis de Riesgos. - Gestión del Riesgo. - Tratamiento de los Riesgos.	2,4	0,8	1,6	Análisis de Riesgos (activos, amenazas, salvaguardas, indicadores de impacto). Mitología. Herramientas. Ciclos de Gestión de Riesgos. Plan director. Costes. Métodos de aseguramiento. Herramienta PILAR
Grupo Varios	- Inauguración y Clausura.	0,1	0,1	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso de Especialidades Criptológicas"** es proporcionar a los asistentes los conocimientos básicos necesarios para:

- la elección adecuada de técnicas y parámetros criptológicos a emplear en una red de cifra.

La finalidad del **"Curso de Especialidades Criptológicas: Fase II - Equipamiento Criptológico"** es proporcionar a los asistentes los conocimientos necesarios para administrar y gestionar redes de cifra con los cifradores adecuados y normativas adecuadas.

Créditos / Horas del Plan de Estudios - Fase On-line

La distribución de las 125 horas de la fase on-line del curso (12,5 créditos) es la siguiente:

- Teoría: 12,5 créditos / 125 horas

Créditos / Horas del Plan de Estudios - Fase Presencial

La distribución de las 75 horas de la fase presencial del curso (7,5 créditos) es la siguiente:

- Teoría: 6,7 créditos / 67 horas
- Práctica: 0,8 créditos / 8 horas

Normas y Certificado de superación

Al desarrollarse el Curso en dos fases (on-line y presencial) será condición imprescindible para ser nombrado asistente de la fase presencial, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase on-line.

El examen previo consistirá en la contestación de un total de 30 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. Cada pregunta tendrá el mismo valor, siendo la nota obtenida función de las preguntas acertadas respecto al número total de formuladas. Será necesario concluir esta prueba, por lo menos, con un mínimo exigido de cinco (5) puntos.

La nota final del curso será de "APTO", siendo la nota de la fase a distancia considerada sólo para el acceso a la fase que se inicia posteriormente.

Durante la **fase presencial**, el alumno tendrá que superar otra prueba sobre el contenido del curso. Las preguntas serán teóricas tipo test en formato escrito con cuatro respuestas posibles (una única verdadera) no restando puntos las mal contestadas. Cada pregunta tendrá el mismo valor, siendo la nota obtenida función de las preguntas acertadas respecto al número total de formuladas. Será necesario concluir esta prueba, por lo menos, con un mínimo exigido de cinco (5) puntos. En caso de no superar el mínimo exigido, el alumno deberá realizar una evaluación de recuperación que en el caso de no superar supondrá la baja en el Curso.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los subgrupos A1 o A2 que tenga responsabilidades en la planificación, gestión, administración o mantenimiento de los Sistemas de las tecnologías de la información y comunicaciones (TIC), o con la seguridad de los mismos.

Se consideran como prioridades para la selección al curso, las siguientes:

- Estar desarrollando, en su actual destino, actividades de planificación, gestión, administración o mantenimiento de Sistemas de las TIC, o la seguridad de los mismos, por un período superior a dos (2) años.

Requisitos técnicos mínimos de los equipos

Se dispondrá de un equipo que tenga una configuración mínima de:

Hardware:

- Procesador 1,3Ghz. 2GB de memoria RAM o superior.

Software:

- Windows 8 o superior, Mac OS X 10.10.5 o superior, Ubuntu 16.04 o superior.
- Última versión disponible de alguno de los siguientes navegadores: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome o Apple Safari (el navegador Microsoft Edge no es compatible con la plataforma online).
- Plug-in Adobe Flash Player correctamente instalado y configurado en el navegador que se esté utilizando.
- Será necesario configurar correctamente el navegador para que permita ventanas emergentes del sitio https://www.ccn-cert.cni.es

Requisitos de conectividad:

- Conexión a Internet de banda ancha (equivalente a un ADSL doméstico).
- Posibilidad de descargar ficheros con la extensión PDF desde el servidor donde esté alojado el curso.
- Posibilidad de que los usuarios que lo requieran, puedan descargar e instalar en sus equipos el software enumerado anteriormente.

Otros requisitos:

- Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente. El tipo de la conexión a Internet deberá ser banda ancha (equivalente a un ADSL doméstico).

Acceso al curso (Fase On-line)

Para poder participar en la fase on-line, será necesario que el alumno sea usuario registrado del portal CCN-CERT (https://www.ccn-cert.cni.es), donde está ubicada la plataforma de e-learning. En el proceso de registro se establece un nombre

de usuario y una clave de acceso al Portal para su conexión. Con antelación a la celebración del curso, a través de correo electrónico, se facilitará a los alumnos los datos y las instrucciones de acceso a la fase on-line. El alumno tendrá que tener en cuenta lo siguientes requisitos:

- La cuenta de correo empleada para la comunicación entre el tutor y los alumnos puede ser una personal o de trabajo, pero tendrá que coincidir con la indicada en la solicitud telemática.
- Es preciso que la cuenta de correo esté operativa y sea de uso frecuente.

Materias y asignaturas - Fase On-line

A continuación se detallan las materias y asignaturas en las que se distribuye la primera fase del 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	
Principios Digitales (Fase online)	- Principios Digitales	4,5	4,5	0	Números utilizados en Electrónica Digital. Códigos Binarios. Puertas Lógicas Básicas: AND, OR, NOT. Simplificación de Circuitos: Diagramas. Estructuras básicas: Flips-Flops. Contadores. Registros de Desplazamiento. Tipos de circuitos.
Teoría de Números (Fase online)	- Teoría de Números	4,5	4,5	0	Bases numéricas. Divisibilidad. Aritmética Modular. Grupos. Anillos y Cuerpos. Anillos de Polinomios.
Criptografía Clásica (Fase online)	- Criptografía Clásica	3,5	3,4	0,1	Principios básicos de la criptografía. Procedimientos manuales de cifra. Criptógrafos mecánicos.

Materias y asignaturas - Fase Presencial

A continuación se detallan las materias y asignaturas en las que se distribuye la segunda parte del 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	
Teoría de la Criptografía	- Teoría de la Criptografía	5,3	5	0,3	Criptografía moderna. Cifrado en serie. Cifrado en bloque. Funciones resumen. Criptografía de clave pública. Criptografía con curvas elípticas. Firma digital. Protocolos criptográficos. Criptografía cuántica y postcuántica. Blockchain. Infraestructura de Clave Pública. Ataques por canal lateral. Aplicaciones de la criptografía. Nuevas líneas.

Tempest	- Tempest	0,3	0,3	0	Fenómeno Tempest, Amenaza Tempest, Contramedidas. Caso práctico.
Normativa y Seguridad cripto	- Normativa Criptológica. - Políticas de Seguridad Criptológica.	0,2	0,2	0	Uso de Cifradores Certificados, Procedimientos de Empleo, Colocación de Etiquetas de Seguridad, Gestión de claves, Incidentes de Seguridad. Coditos Seguros de Verificación (CSV) Criptografía de empleo en el ENS Amenazas, medidas de seguridad y actuación.
Evaluación de Equipos	- Evaluación FIPS140. - Evaluación Common Criteria. - Evaluación LINCE. - Evaluación Criptológica. - Evaluación TEMPEST.	0,4	0,4	0	Evaluación de la seguridad de los Equipos: Evaluación FIPS 2-140, Evaluación Common Criteria, Evaluación LINCE, Evaluación Criptológica, Evaluación TEMPEST y zoning. Aprobación y cualificación.
Equipamiento criptológico y de seguridad TIC	- Equipos de cifra - Productos de seguridad TIC	0,5	0,4	0,1	Cifradores Nacionales de Datos, IP, Voz. Equipamiento Criptológico OTAN y UE. Productos de seguridad TIC CPSTIC
Interconexiones	- Interconexión de sistemas	0,1	0,1	0	Interconexión de sistemas con distinta clasificación.
Grupo Varios	- Inauguración y Clausura.	0,7	0,5	0,2	Examen Previo. Inauguración. Examen Final. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC - Cibervigilancia"** es proporcionar a los asistentes los conocimientos necesarios para comprender y definir necesidades de información en cada paso del espectro de obtención de información en Fuentes Abiertas (OSINT), particularizando el enfoque OSINT en su aplicación al desarrollo de labores de Cibervigilancia.

El programa tiene el formato de curso autocontenido con el propósito de aportar a los asistentes una visión general práctica de conocimientos y procedimientos OSINT para desarrollar labores de Cibervigilancia, de manera que los asistentes tengan acceso a un conjunto útil de técnicas y metodologías mínimas para comenzar a realizar tareas específicas, una especie de caja de herramientas para la Cibervigilancia OSINT.

En ese contexto, el curso ha sido diseñado para combinar metodología con tecnología dentro de un proceso de investigación OSINT; desarrollar la capacidad de definir utilidades tácticas

para acortar procesos de búsqueda, rastreo de elementos informativos de interés, y monitorización de escenarios digitales específicos; la adquisición de nuevos hábitos en la web de uso avanzado de búsquedas en medios sociales; la sistematización de procedimientos para el análisis y evaluación de escenarios e identidades digitales a partir de la información obtenida; así como la aproximación práctica a la investigación y la elaboración de informes de cibervigilancia.

La filosofía de transmisión de conocimientos, en cuanto a procedimientos, técnicas y tecnologías estudiados, en la que se inscribe el curso es la propia de la Ciberseguridad Preventiva y la Ciberdefensa Pasiva.

Créditos / Horas del Plan de Estudios

La distribución de las 25 horas de la fase presencial del curso (2,5 créditos) es la siguiente:

- Teoría: 0,7 créditos / 7 horas
- Práctica: 1,8 créditos / 18 horas

Normas y Certificado de superación

La formación se desarrollará en modalidad en línea por lo que los participantes deberán conectarse a la emisión de las clases en directo durante los cinco días de curso. Durante las sesiones se realizarán una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

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 asistentes que lo hayan superado con aprovechamiento obtendrán un Certificado como garantía de la superación del mismo.

Destinatarios

Podrán solicitar el curso los empleados públicos de los subgrupos A1, A2 y C1, y el personal laboral equivalente, que tengan responsabilidades en la planificación, gestión, administración o seguridad de sistemas de las tecnologías de la información y las comunicaciones y que, asimismo, necesite para su puesto de trabajo llevar a cabo tareas de cibervigilancia, investigación y elaboración de informes relacionados con la detección de amenazas en redes sociales.

Se supondrá, por parte de los asistentes, un conocimiento mínimo de los sistemas *Linux* y *Windows*, así como conocimientos básicos de protocolos y equipamiento de red.

Se utilizarán medios comerciales (COTS) al alcance de cualquier usuario de Internet que hagan que las comunicaciones y actividades puedan pasar desapercibidas dentro del tráfico habitual de un usuario en la Red, evitando el señalamiento de la actividad a realizar.

Requisitos técnicos mínimos de los equipos

Se dispondrá de un equipo que tenga una configuración mínima de:

Hardware:

- 8 GB de memoria RAM o superior.

Software:

- Windows 7 o superior.
- Entorno de virtualización en el que poder ejecutar las máquinas virtuales a utilizar durante el curso (VMware Player o Virtualbox).

Requisitos de conectividad:

- Necesidad de disponer de un acceso a Internet de banda ancha para el desarrollo de las prácticas previstas.

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	
Medidas Técnicas STIC	- Conceptos generales y metodología OSINT - Obtención OSINT - Redes Sociales - Cibervigilancia - Anonimización - Herramientas - Elaboración de Informes	2,3	0.5	2,8	Introducción. Conceptos generales del entorno de trabajo. Metodología OSINT. Obtención OSINT: Búsquedas. Redes Sociales. Cibervigilancia: Definición y Objetivos. Ciberprotección y Anonimización en cibervigilancia. Arquitectura de Redes Sociales. APIs de las Redes Sociales. Google Dorks. Herramientas libres para monitorizar e investigar. Aproximación práctica al trazado de un contenido. Aproximación práctica al perfilado de una identidad digital. Identificación de Bots en Redes Sociales. Elaboración de informes de cibervigilancia. Organización de una unidad de cibervigilancia. Casos de uso. Observatorio Digital: ELISA.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso Básico de Auditorías de Seguridad TIC"** es proporcionar a los asistentes los conocimientos y habilidades necesarias para que sean capaces de comprobar y auditar, con una garantía suficiente, los aspectos de seguridad de sistemas TIC en cada organización concreta, así como verificar y corregir los procesos e implementaciones.

Créditos / Horas del Plan de Estudios

La distribución de las 50 horas de la fase presencial del curso (5 créditos) es la siguiente:

- Teoría: 3,5 créditos / 35 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

El curso se desarrollará de forma presencial con lo cual, los concurrentes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2 o C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos.

Se supondrá, por parte de los asistentes, un conocimiento mínimo de los sistemas *Linux* y *Windows*, así como conocimientos básicos de protocolos y equipamiento de red, considerándose 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.
- 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.

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	
Medidas Técnicas STIC	- Auditorías de Seguridad TIC. - Metodología de Auditorías - Inspección ENS - Inspección STIC	4,8	3,3	1,5	Introducción a Auditorías.Guía CCN-STIC 303. Metodología de Auditorías. Cumplimiento de aspectos Organizativos. Inspección ENS de Nivel 3. Inspección STIC. Inspección Técnica de Caja Negra Nivel 5. Inspección Técnica de Aplicación Niveles 4 y 5. Soluciones CCN. Inspecciones STIC: Casos de Estudio. Modelos de Informe. Informe Ejecutivo.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso Avanzado de Auditorías de Seguridad TIC"** es proporcionar a los asistentes los conocimientos y habilidades necesarias para que sean capaces de comprobar e inspeccionar con un mayor nivel de especialización aplicaciones e infraestructuras donde sea necesario llegar a conocer la superficie de exposición a vulnerabilidades y las amenazas existentes mediante pruebas de seguridad de Caja Blanca y de Caja Negra.

Créditos / Horas del Plan de Estudios

La distribución de las 25 horas de la fase presencial del curso (2,5 créditos) es la siguiente:

- Teoría: 1 crédito / 10 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

El curso se desarrollará de forma presencial con lo cual, los concurrentes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2 o C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos.

Se supondrá, por parte de los asistentes, un conocimiento mínimo de los sistemas *Linux* y *Windows*, así como conocimientos básicos de protocolos y equipamiento de red, considerándose como prioridades para la selección al curso, las siguientes:

- Haber realizado con anterioridad el Curso Básico de Auditorías de Seguridad TIC.
- 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.

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	
Medidas Técnicas STIC	- Pentesting: Redes y Servicios Externos - Auditoría de Servicios Web - Auditoría de Sistemas	2,3	0.8	1,5	Pentesting. Técnicas de Footprinting. Técnicas de Fingerprinting. Análisis de Vulnerabilidades. Ataques contra Servicios Web. Análisis de Servidores. Análisis de la Seguridad de Sistemas. Ataques a Infraestructuras. Exploits. Explotación de Vulnerabilidades con Metasploit Framework.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso Acreditación STIC - Entornos Windows"** es proporcionar a los participantes los conocimientos necesarios para que sean capaces de comprobar, con una garantía suficiente, los aspectos de seguridad de sistemas servidores y de estaciones clientes profesionales con Windows. También se mostrará la implantación segura de servicios Web (IIS) y servicios de Correo Electrónico (MS Exchange).

Al tratarse de un curso de acreditación, se utilizará como marco de referencia la normativa recogida en la serie CCN-STIC implementando las configuraciones de seguridad definidas en las guías CCN-STIC-500 para entornos basados en tecnología Microsoft.

Créditos / Horas del Plan de Estudios

La distribución de las 15 horas de la fase on-line del curso (1,5 créditos) es la siguiente:

- Teoría: 1,5 créditos / 15 horas

La distribución de las 25 horas de la fase presencial del curso (2,5 créditos) es la siguiente:

- Teoría: 1 crédito / 10 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en dos fases (on-line y presencial) será condición imprescindible para ser nombrado asistente a la fase presencial, superar las pruebas correspondientes a la fase on-line en las que se valoran los conocimientos adquiridos en dicha fase.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2 o C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos. Para el personal militar, el Ministerio de Defensa hará una convocatoria específica. Se supondrá, por parte de los asistentes, un conocimiento mínimo a nivel administrativo de sistemas Windows, así como conocimientos básicos de protocolos de red considerándose como prioridades para la selección al curso, las siguientes:

- Haber realizado con anterioridad el Curso Básico STIC - Entornos Windows desarrollado por el Centro Criptológico Nacional (CCN).
- Actividad relacionada con la administración de Sistemas de las tecnologías de la información y comunicaciones (TIC) bajo entornos Windows.
- Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN.

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

• Tener responsabilidades, a nivel técnico, en la implementación u operación de Sistemas de las TIC o en la gestión de la seguridad de dichos Sistemas por un período superior a dos (2) años.

Requisitos técnicos

Se dispondrá de un equipo que tenga una configuración mínima de:

Hardware:

• Procesador 1,3Ghz. 2GB de memoria RAM o superior.

Software:

• Windows 8 o superior, Mac OS X 10.10.5 o superior, Ubuntu 16.04 o superior.

• Última versión disponible de alguno de los siguientes navegadores: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome o Apple Safari (el navegador Microsoft Edge no es compatible con la plataforma online).

• Plug-in Adobe Flash Player correctamente instalado y configurado en el navegador que se esté utilizando.

• Será necesario configurar correctamente el navegador para que permita ventanas emergentes del sitio https://www.ccn-cert.cni.es.

Requisitos de conectividad:

• Conexión a Internet de banda ancha (equivalente a un ADSL doméstico).

• Posibilidad de descargar ficheros con la extensión PDF desde el servidor donde esté alojado el curso.

• Posibilidad de que los usuarios que lo requieran, puedan descargar e instalar en sus equipos el software enumerado anteriormente.

Otros requisitos:

• Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente. El tipo de la conexión a Internet deberá ser banda ancha (equivalente a un ADSL doméstico).

Acceso al curso (Fase On-line)

Para poder participar en la fase on-line, será necesario que el alumno sea usuario registrado del portal CCN-CERT (https://www.ccn-cert.cni.es), donde está ubicada la plataforma de e-learning. En el proceso de registro se establece un nombre de usuario y una clave de acceso al Portal para su conexión. Con antelación a la celebración del curso, a través de correo electrónico, se facilitará a los alumnos los datos y las instrucciones de acceso a la fase on-line. El alumno tendrá que tener en cuenta lo siguientes requisitos:

• La cuenta de correo empleada para la comunicación entre el tutor y los alumnos puede ser una personal o de trabajo, pero tendrá que coincidir con la indicada en la solicitud telemática.

• Es preciso que la cuenta de correo esté operativa y sea de uso frecuente.

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	
Curso Básico STIC Seguridad en Entornos Windows (Fase Online)	- Sistemas Operativos. - Administración y seguridad. - Directorio Activo y políticas.	1,5	1,5	0	Introducción a la gestión del S.O. Windows Server y clientes Windows. Administración básica. Seguridad del sistema local. Directorio Activo. Políticas de grupo. Guías CCN-STIC asociadas.
Medidas Técnicas STIC	- Seguridad Sistemas Operativos. - Seguridad Servicios Web. - Seguridad Servicios de Correo.	2,3	0,8	1,5	Servidores Windows (Introducción al Directorio Activo. Controlador de Dominio. Servidores Miembro. Configuraciones de Seguridad). Windows (Plantillas de Seguridad. Equipo Miembro de Dominio. Equipo Cliente Independiente). Internet Information Services (Seguridad en ISS. Plantillas de Seguridad. Servidor ISS Miembro de Dominio. Servidor ISS Independiente). Exchange (Seguridad en Exchange. Plantillas de Seguridad. Servidor Exchange Miembro de Dominio. Servidor Exchange Independiente).
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC - Redes Inalámbricas"** es proporcionar a los asistentes 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.

Créditos / Horas del Plan de Estudios

La distribución de las 25 horas de la fase presencial del curso (2,5 créditos) es la siguiente:

- Teoría: 1 crédito / 10 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

El curso se desarrollará de forma presencial con lo cual, los concurrentes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal con responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos.

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

- Haber realizado con anterioridad el Curso Básico STIC - Infraestructura de Red desarrollado por el Centro Criptológico Nacional (CCN).
- Actividad relacionada con la administración de la infraestructura de red asociada a Sistemas de las tecnologías de la información y comunicaciones (TIC).
- Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN.
- Haber realizado cursos relacionados con las tecnologías de la información o su seguridad.
- Tener responsabilidades, a nivel técnico, en la implementación u operación de Sistemas de las TIC o en la gestión de la seguridad de dichos Sistemas por un período superior a dos (2) años.

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	
Medidas Técnicas STIC	- Comunicación WMAN. - Comunicación WLAN. - Dispositivos WPAN.	2,4	0,9	1,5	Comunicación entre Sedes (WMAN). Tecnología pre-WIMAX. Autenticación mediante Certificados Digitales. Cifrado de Comunicaciones. Uso de VLAN. Comunicaciones dentro de las Sedes (WLAN). Red Inalámbrica para Acceso Interno. Red Inalámbrica para Clientes Itinerantes. Distribución de Puntos de Acceso. Protocolo 802.1X. Ataques Clásicos a Redes Inalámbricas. Dispositivos Móviles Personales (WPAN). Red de Área Personal Bluetooth. Casos de Estudio.
Grupo Varios	- Inauguración y Clausura.	0,1	0,1	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC - Seguridad en Comunicaciones y Dispositivos Móviles"** es proporcionar a los asistentes una visión detallada, actual y práctica de las amenazas y vulnerabilidades de seguridad que afectan a los dispositivos móviles y sus comunicaciones. Los diferentes módulos incluyen una descripción detallada de las vulnerabilidades estudiadas, técnicas de ataque, mecanismos de defensa y recomendaciones de seguridad, incluyendo numerosas demostraciones prácticas.

En la primera parte del curso se estudiarán las vulnerabilidades asociadas a los protocolos de comunicaciones de voz y datos 2G y 3G; mientras que la segunda parte del curso se centra en los elementos técnicos y los mecanismos de seguridad de las principales plataformas móviles (Microsoft Windows Phone, Android y Apple iOS).

Adicionalmente, el curso ofrece un análisis detallado de las soluciones de gestión empresarial de dispositivos móviles (MDM, *Mobile Device Management*) comparando los diferentes modelos de gestión existentes, sus características de seguridad, y las principales capacidades y funcionalidades que ofrecen.

Créditos / Horas del Plan de Estudios

La distribución de las 35 horas de la fase presencial del curso (3,5 créditos) es la siguiente:

- Teoría: 1,5 créditos / 15 horas
- Práctica: 2 créditos / 20 horas

Normas y Certificado de superación

El curso se desarrollará de forma presencial con lo cual, los asistentes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2 o C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos.

Se supondrá, por parte de los participantes, un conocimiento mínimo a nivel administrativo de sistemas *Linux* y *Windows*, así como conocimientos básicos de sistemas de comunicaciones móviles. Se consideran 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.
- 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 período superior a un (1) año.

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	
Medidas Técnicas STIC	- 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 Bluetooth. - Comunicaciones Wi-Fi. - Comunicaciones GSM (2G) y UMTS (3G) - Comunicaciones TCP/IP.	3,4	1,4	2	Arquitectura GSM, GPRS/EDGE, UMTS, LTE. Actualización del sistema operativo. Modelo y arquitectura de seguridad. Gestión local y empresarial de dispositivos móviles basados en <SO>. Políticas, perfiles, roles y configuraciones de seguridad. Acceso físico al dispositivo móvil. Cifrado de datos en <SO>. Gestión de certificados digitales y credenciales en <SO>. Eliminación de datos del dispositivo móvil. Configuración por defecto del dispositivo móvil. Comunicaciones USB. Comunicaciones Bluetooth. Comunicaciones Wi-Fi. Comunicaciones GSM (2G) y UMTS (3G): mensajes de texto (SMS), voz y datos. Comunicaciones TCP/IP. SSL/TLS. IPv6. VPNs. Copia de seguridad de datos en la plataforma móvil. Instalación y eliminación de aplicaciones en <SO>. Aplicaciones disponibles por defecto en <SO>. Navegación web. Correo electrónico (e-mail). Redes sociales. Aplicaciones de terceros: Mercado de aplicaciones
Grupo Varios	- Inauguración y Clausura.	0,1	0,1	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC – Seguridad en Aplicaciones Web"** es proporcionar a los participantes una visión detallada, actual y práctica de las amenazas y vulnerabilidades de seguridad que afectan a las infraestructuras, entornos y aplicaciones Web. Los diferentes módulos incluyen una descripción detallada de las vulnerabilidades estudiadas, técnicas de ataque, mecanismos de defensa y recomendaciones de seguridad, incluyendo numerosas demostraciones y ejercicios prácticos.

Se utilizará como marco de referencia la normativa recogida en la serie CCN-STIC implementando las configuraciones de seguridad definidas en la guía CCN-STIC-412, requisitos de seguridad de entornos y aplicaciones Web.

Créditos / Horas del Plan de Estudios

La distribución de las 25 horas de la fase presencial del curso (2,5 créditos) es la siguiente:

- Teoría: 1 crédito / 10 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

El curso se desarrollará de forma presencial con lo cual, los asistentes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2 o C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de sistemas y redes, entornos Web y desarrolladores de aplicaciones Web.

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

- Haber realizado con anterioridad el Curso STIC – Inspecciones de Seguridad desarrollado por el Centro Criptológico Nacional (CCN).
- Haber realizado con anterioridad el Curso STIC – Cortafuegos desarrollado por el Centro Criptológico Nacional (CCN).
- Haber realizado con anterioridad el Curso STIC – Detección de Intrusos desarrollado por el Centro Criptológico Nacional (CCN).
- Haber realizado con anterioridad el Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) desarrollado por el CCN.

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

• Tener responsabilidades, a nivel técnico, en la implementación u operación de Sistemas de las TIC o en la gestión de la seguridad de dichos Sistemas por un período superior a dos (2) años.

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	
Medidas Técnicas STIC	- Introducción a las amenazas en aplicaciones Web. - Protocolos Web. - Herramientas de análisis y manipulación Web. - Ataques sobre entornos Web. - Mecanismos de Autenticación y Autorización Web. - Gestión de Sesiones. - Inyección SQL. - Cross-Site Scripting (XSS) - Cross-Site Request Forgery (CSRF).	2,4	0,9	1,5	Arquitecturas de aplicaciones Web. Metodología de análisis de seguridad de Aplicaciones Web. Web Application Firewalls. Protocolos HTTP/ HTML7SSL/TLS. Reconocimiento del entorno Web. Vulnerabilidades de la plataforma Web. Herramientas de ataque Web. Proxies de manipulación Web. Desplazamiento por los directorios. Inyección de código y contenidos. Autenticación Web (básica, certificados) y Autorización Web. Gestión de identificadotes y token de sesión. Cookies. Tipos de inyección (SQL, LDAP). Tipos de XSS. Evasión de la detección de XSS. Ataque CSRF. Recomendaciones de Seguridad
Grupo Varios	- Inauguración y Clausura.	0,1	0,1	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC – Seguridad en Infraestructuras de Red"** es conocer las principales amenazas que afectan a las infraestructuras y equipamiento que soportan nuestras redes de comunicaciones, así como conocer y aplicar las medidas decuadas para garantizar su seguridad.

Créditos / Horas del Plan de Estudios

La distribución de las 15 horas de la fase on-line del curso (1,5 créditos) es la siguiente:

- Teoría: 1,5 créditos / 15 horas

La distribución de las 25 horas de la fase presencial del curso (2,5 créditos) es la siguiente:

- Teoría: 1 crédito / 10 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en dos fases (on-line y presencial) será condición imprescindible para participar en la fase presencial, superar las pruebas correspondientes a los exámenes previstos durante la fase on-line en los que se valoran los conocimientos adquiridos en dicha fase.

La nota final del curso será de "APTO", siendo la nota de la fase on-line considerada sólo para el acceso a la fase presencial que se inicia posteriormente.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2 o C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos.

Se supondrá, por parte de los participantes, un conocimiento mínimo de sistemas operativos, así como conocimientos básicos de protocolos y equipamiento de red considerándose como prioridades para la selección al curso, las siguientes:

- 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 (1) año.

Requisitos técnicos

Se dispondrá de un equipo que tenga una configuración mínima de:

Hardware:

- Procesador 1,3Ghz. 2GB de memoria RAM o superior.

Software:

- Windows 8 o superior, Mac OS X 10.10.5 o superior, Ubuntu 16.04 o superior.
- Última versión disponible de alguno de los siguientes navegadores: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome o Apple Safari (el navegador Microsoft Edge no es compatible con la plataforma online).
- Plug-in Adobe Flash Player correctamente instalado y configurado en el navegador que se esté utilizando.
- Será necesario configurar correctamente el navegador para que permita ventanas emergentes del sitio https://www.ccn-cert.cni.es.

Requisitos de conectividad:

- Conexión a Internet de banda ancha (equivalente a un ADSL doméstico).
- Posibilidad de descargar ficheros con la extensión PDF desde el servidor donde esté alojado el curso.
- Posibilidad de que los usuarios que lo requieran, puedan descargar e instalar en sus equipos el software enumerado anteriormente.

Otros requisitos:

- Es preciso tener una cuenta de correo electrónico operativa y de uso frecuente. El tipo de la conexión a Internet deberá ser banda ancha (equivalente a un ADSL doméstico).

Acceso al curso (Fase On-line)

Para poder participar en la fase on-line, será necesario que el alumno sea usuario registrado del portal CCN-CERT (https://www.ccn-cert.cni.es), donde está ubicada la plataforma de e-learning. En el proceso de registro se establece un nombre de usuario y una clave de acceso al Portal para su conexión. Con antelación a la celebración del curso, a través de correo electrónico, se facilitará a los alumnos los datos y las instrucciones de acceso a la fase on-line. El alumno tendrá que tener en cuenta lo siguientes requisitos:

- La cuenta de correo empleada para la comunicación entre el tutor y los alumnos puede ser una personal o de trabajo, pero tendrá que coincidir con la indicada en la solicitud telemática.
- Es preciso que la cuenta de correo esté operativa y sea de uso frecuente.

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	
Medidas Técnicas STIC (Fase a Distancia)	- Curso STIC Seguridad Infraestructura de Red	1,5	1,5	0	Redes de ordenadores. Internet.Aplicaciones. Protocolos de transporte. Redes IP. Direcciones y prefijos. Routers. Reenvío de datagramas. Protocolo IP e ICMP. NAT. Encaminamiento en redes IP. Encaminamiento estático. Protocolos de encaminamiento dinámico. OSPF. BGP. Redes de área local (LAN). Conmutadores/Switches Ethernet.Algoritmo de aprendizaje. VLANes. Encaminamiento en redes LAN: STP. Nociones básicas de configuración de equipos de red.
Medidas Técnicas STIC	- Introducción a la seguridad en infraestructuras de red - Seguridad en redes de área local. - Identificación, autenticación y control de acceso. Redes privadas virtuales. - Seguridad en redes IP. - Auditorias de seguridad de equipos.	2,3	0,8	1,5	Tipos de amenazas. Políticas de seguridad. Responsabilidades. Anatomía de un ataque. Conceptos básicos de seguridad. Uso de la criptografía para la protección. Confidencialidad e integridad. Cifrado. Certificados. Seguridad en el acceso a la gestión de equipos de red. Concepto de "Hardening" de equipos. Actualización segura de software. Agregación de logs. Amenazas y ataques a switches. Falsification de ARP. DHCP starvation/spoofing. Encaminamiento en LAN: ataques al protocolo Spanning Tree. Medidas de seguridad para mitigar los ataques. Mecanismos básicos de identificación y autenticación. Control de accesos. Autenticación centralizada de usuarios. RADIUS. Sistemas de control de acceso a redes. Redes Privadas Virtuales. Amenazas y ataques a routers. Falsificación de direcciones IP. Ataques de denegación de servicio. Seguridad en protocolos de encaminamiento: autenticación. Contramedidas: Unicast Reverse Path Forwarding, listas de acceso, monitorización de flujos: NetFlow/sflow. Técnicas de encaminamiento para mitigar ataques DoS. Herramienta ROCIO.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC – de Gestión de Incidentes de Ciberseguridad" e**s proporcionar a los asistentes los conocimientos necesarios para gestionar de manera adecuada los incidentes de seguridad TIC a los que se enfrenta una organización mediante la utilización de las herramientas del CCN-CERT.

Créditos / Horas del Plan de Estudios

La distribución de las 25 horas de la fase presencial del curso (2,5 créditos) es la siguiente:

- Teoría: 1 crédito / 10 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

El curso se desarrollará de forma presencial con lo cual, los concurrentes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2 o C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos.

Se supondrá, por parte de los asistentes, un conocimiento mínimo de los sistemas *Linux* y *Windows*, así como conocimientos básicos de protocolos y equipamiento de red, considerándose 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.
- Haber realizado con anterioridad el Curso STIC –Inspecciones de Seguridad 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 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.

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	
Medidas Técnicas STIC	- Herramienta CARMEN - Herramienta LUCIA - Herramienta REYES	2,3	0,8	1,5	Herramienta CARMEN: Usuarios y roles, filtros básicos, uso de listas, indicadores de compromiso, análisis de movimiento externo (HTTP, DNS, SMTP), análisis de movimiento lateral (NetBIOS), analizadores e indicadores, creación de plugins. Herramienta LUCIA: Introducción a la herramienta, conceptos de RTIR, flujos de trabajo, sincronización de instancias. Herramienta REYES: Indicadores de compromiso, exportación de reglas SNORT, YARA o IOCs, introducción de muestras de malware, automatización de tareas y procesos utilizando la API REST.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC - Avanzado de Gestión de Incidentes de Ciberseguridad"** es proporcionar a los asistentes los conocimientos necesarios que posibiliten el desempeño de un equipo de analistas de seguridad en el proceso de investigación de incidentes complejos mediante la utilización de soluciones propias del CCN-CERT en la adquisición, procesamiento y análisis de tráfico de red.

Créditos / Horas del Plan de Estudios

La distribución de las 25 horas de la fase presencial del curso (2,5 créditos) es la siguiente:

- Teoría: 1 crédito / 10 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

El curso se desarrollará de forma presencial con lo cual, los participantes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2 o C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos.

Se supondrá, por parte de los asistentes, un conocimiento mínimo de los sistemas Linux y Windows, así como conocimientos básicos de protocolos y equipamiento de red, considerándose como prioridades para la selección al curso, las siguientes:

- Haber realizado con anterioridad el Curso (STIC) - Gestión de Incidentes de Ciberseguridad desarrollado por el Centro Criptológico Nacional.
- 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 con anterioridad el Curso STIC - Inspecciones de Seguridad 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 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.

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	
Medidas Técnicas STIC	- Herramienta CARMEN - Herramienta LUCIA - Herramienta REYES	2,3	0,8	1,5	Herramienta REYES: Introducción y conceptos. Integración con otras soluciones del CCN-CERT y sus posibilidades. Herramienta CLAUDIA: Introducción y conceptos. Integración con la herramienta CARMEN. Herramienta CARMEN: usuarios y roles, filtros básicos, uso de listas, indicadores de compromiso, análisis de movimiento externo (HTTP, DNS, SMTP), análisis de movimiento lateral (NetBIOS), analizadores e indicadores, creación de plugins. Casos prácticos: Identificación y detección de amenazas, utilización de herramientas de apoyo, detección de anomalías para la creación de IOC, búsqueda de APT, análisis de volcado de memoria.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC de Análisis de Memoria"** es proporcionar a los asistentes los conocimientos y habilidades necesarias para realizar, con una garantía suficiente, investigación de incidentes de seguridad mediante el empleo de técnicas de análisis forense de memoria.

Créditos / Horas del Plan de Estudios

La distribución de las 25 horas de la fase presencial del curso (2,5 créditos) es la siguiente:

- Teoría: 1 crédito / 10 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

El curso se desarrollará de forma presencial con lo cual, los participantes tendrán que realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

Destinatarios

Podrá solicitar este curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2 o C1 que tenga responsabilidades, a nivel técnico, en la planificación, gestión, administración o mantenimiento de Sistemas de las tecnologías de la información y comunicaciones, o con la seguridad de los mismos.

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

- 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.

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	
Medidas Técnicas STIC	- Análisis Forense en Sistemas Windows - Introducción a Windows Internals - Forensics en Sistemas Windows - Ring 3 - Forensics en Sistemas Windows - Ring 0 - Forensics en otras fuentes y reto final	2,3	0,8	1,5	Introducción a Memory Forensics. Arquitecturas Windows. Volatility. Adquisición de memoria RAM. Metodologías de análisis. Análisis de Memoria Desestructurada. Process Internals. Volatility listing modules. Pool memory. Conexiones de red. Inyección de código. User Artifacts en memoria. Kernel Objects. Otros bloques de memoria en Windows. Reto CTF de Atenea.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

3. Formación *online*

El portal del Centro Critpológico Nacional (www.ccn.cni.es) permite a los usuarios la realización de distintos cursos a través de esta plataforma.

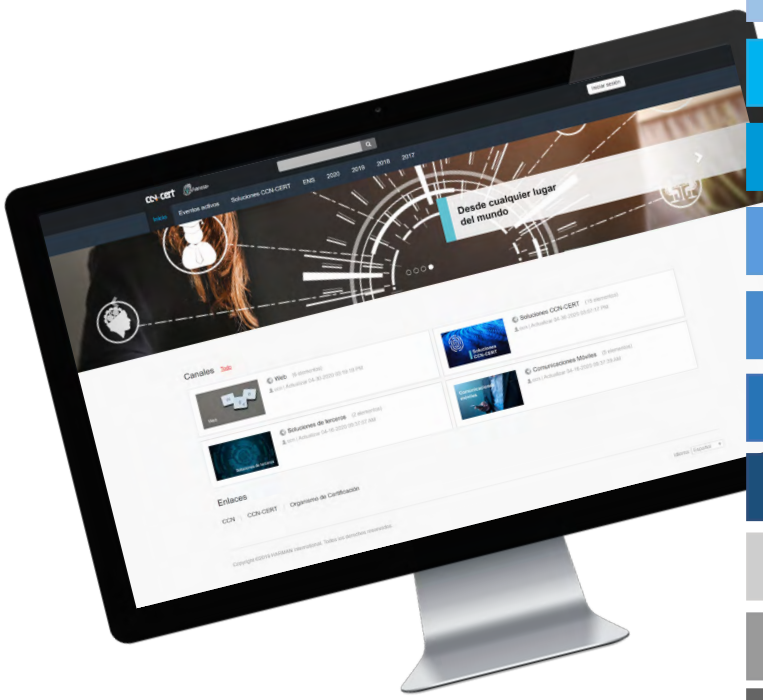
Se emplea una metodología docente 100% online, tanto en los contenidos de los temarios, como en los exámenes que se realizan una vez finalizado el curso.

- Curso básico de Ciberseguridad
- Curso básico de fundamentos Linux
- Curso INES
- Curso Seguridad en entornos Windows
- Análisis y Gestión de Riesgos de los Sistemas de Información
- Curso del Esquema Nacional de Seguridad
- Curso de Seguridad de las Tecnologías de la Información y las Comunicaciones

4. Formación a distancia y en *streaming*

Vanesa es una solución del CCN-CERT para la retransmisión en *streaming* de sesiones formativas en directo. La plataforma permite la asistencia de cientos de personas desde cualquier lugar del mundo.

Además, como valor añadido y para lograr una amplia difusión del contenido emitido, Vanesa conserva las grabaciones y el material empleado, permitiendo así su posterior visionado.



- Web
- Soluciones CCN-CERT
- Soluciones de terceros
- Comunicaciones Móviles
- Correo electrónico
- ENS
- Forense
- Dispositivos móviles
- Switches-Aruba
- Windows
- EXOS-Sistema operativo
- Jornadas

5. ATENEA Escuela

Atenea Escuela es una plataforma de desafíos de seguridad informática, compuesta por diferentes retos guiados y material formativo de apoyo, que tiene por objeto fomentar el aprendizaje de los usuarios menos entendidos o no expertos en el campo de la ciberseguridad.

Ha sido desarrollada por el CCN-CERT, como parte de la plataforma Atenea, con la convicción de que a través de los desafíos se puede incentivar el aprendizaje.

6. Publicaciones

Consciente de los posibles riesgos que pueden afectar a la seguridad de las Tecnologías de la Información y la Comunicación, el Centro Criptológico Nacional elabora, de manera periódica, **informes de Buenas Prácticas** con el objetivo de orientar al usuario en el empleo seguro de las nuevas tecnologías.

Estos informes, accesibles para cualquier usuario desde el portal del CCN-CERT (www.ccn-cert.cni.es), analizan las vulnerabilidades o amenazas existentes, ofrecen las pautas para mitigar o evitar que el incidente afecte a aquellos que emplean las tecnologías objeto del informe y, por último, recoge en un decálogo las recomendaciones de seguridad que se han de implementar para evitar las consecuencias derivadas de dichas amenazas o vulnerabilidades.

1. **BP/1** – Principios Ciberseguridad
2. **BP/2** – Correo electrónico
3. **BP/3** – Dispositivos móviles
4. **BP/4** – Ransomware
5. **BP/5** – Internet de las Cosas (IoT)
6. **BP/6** – Navegadores web
7. **BP/7** – Implementación HTTPS
8. **BP/8** – Redes Sociales
9. **BP/9** – Protección DoS Cortafuegos
10. **BP/10** – Recomendaciones CDN
11. **BP/11** – Recomendaciones redes WIFI corporativas
12. **BP/12** – Cryptojacking
13. **BP/13** – Desinformación en el Ciberespacio
14. **BP/14** – Declaración de Aplicabilidad ENS
15. **BP/15** – Buenas Prácticas en Virtualización
16. **BP/16** – Recomendaciones de seguridad de Adobe Acrobat Reader DC
17. **BP/17** – Recomendaciones de Seguridad de Mozilla Firefox
18. **BP/18** – Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es