Centro Criptológico Nacional

Oferta Formativa 2022

ángeles

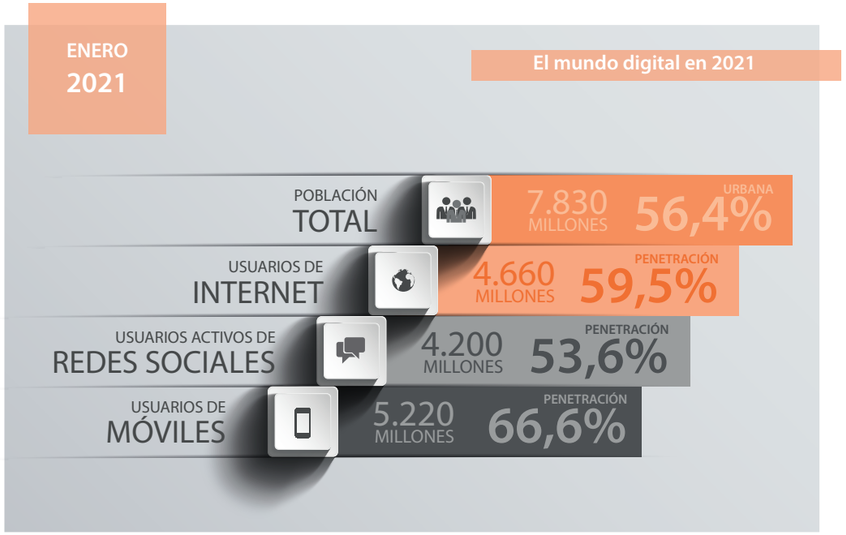
Formación, capacitación y talento en ciberseguridad

Índice

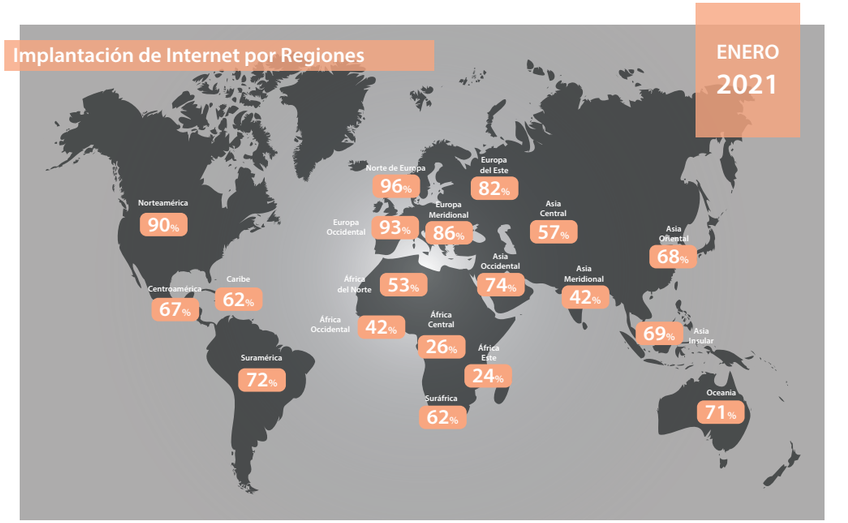
Necesidad formativa y nuevos retos	4
Formación curricular	6
Formación online	60
Formación a distancia y streaming	61
ATENEA Escuela	62
ELENA. Simulador de Técnicas de Vigilancia	63
Publicaciones	64

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.



Fuente: Digital 2021 Global Overview Report (We Are Social)



Fuente: Digital 2021 Global Overview Report (We Are Social)

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)** ha desarrollado la **plataforma Ángeles** de formación y cultura de ciberseguridad. En ella se puede encontrar todos los recursos desarrollados por el CCN, tanto de formación, como de concienciación y sensibilización en la materia.

Ángeles recoge cursos formativos en ciberseguridad, presenciales y online, adaptados al perfil del usuario y su nivel de formación. Dichos cursos se estructuran en este **Plan de Formación**, que 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.

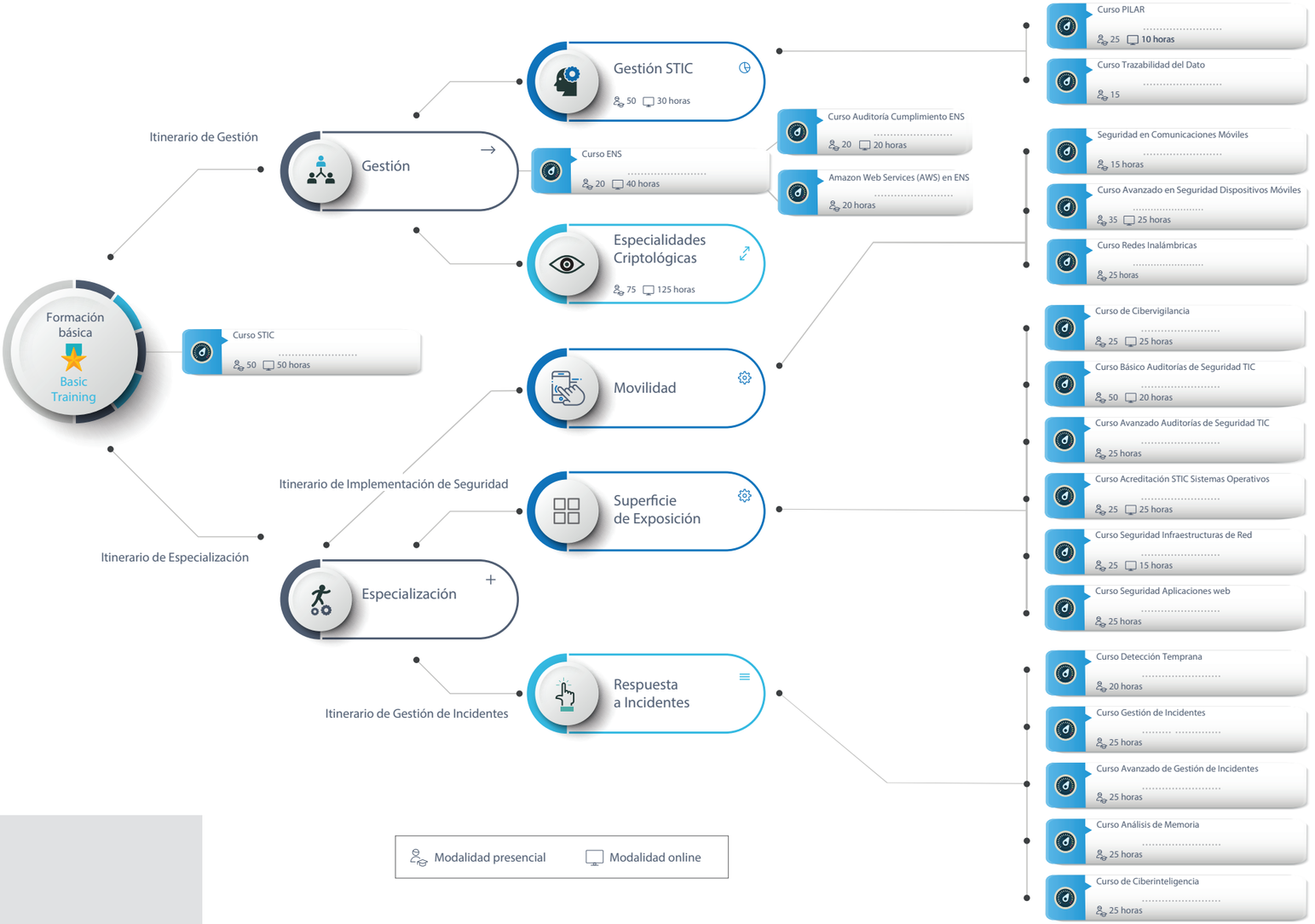
Además, como garantía de superación de la formación realizada, el CCN otorga a los concurrentes que la hayan superado con aprovechamiento, un **Certificado** que especifica las materias y créditos asociados.

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 50 horas de la fase asíncrona del curso (5 créditos) es la siguiente:

- Teoría: 5 créditos / 50 horas

La distribución de las 50 horas de la fase síncrona 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 (asíncrona y síncrona) será condición imprescindible para participar en la fase síncrona, superar las pruebas correspondientes a los exámenes previstos durante la fase asíncrona 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 asíncrona considerada sólo para el acceso a la fase síncrona 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

Podrán solicitar el curso los empleados públicos de los subgrupos A1, A2, B y C1, y el personal laboral equivalente, que tengan 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 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.

Acceso al curso (Fase asíncrona)

Para poder participar en la fase asíncrona, será necesario que el alumno sea usuario registrado del portal ÁNGELES (https://angeles-privado.ccn-cert.cni.es/), donde está ubicada la plataforma de e-learning. El alumno deberá 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 para la fase síncrona.

Denominación de Materias	Asignaturas que componen la Materia	CRÉDITOS			Breve Descripción del Contenido
		TOT	TEO	PRA	
Curso Básico de Ciberseguridad (Fase a Distancia)	- Introducción a ciberseguridad. - Amenazas. - Políticas de Seguridad.	2,0	2,0	0	Introducción. Tipos de amenazas. La Internet profunda (Deep Web). Aplicaciones. Navegación segura y correo electrónico. Virtualización. Seguridad en Dispositivos móviles y Redes inalámbricas. Mensajería instantánea y Redes Sociales. IoT. Política de Seguridad.
Curso de Seguridad de las Tecnologías de la Información y la Comunicación (Fase a Distancia)	- Introducción a STIC. - Normativa de Seguridad. - Políticas de Seguridad. Procedimiento de Acreditación. - Inspecciones STIC. - Gestión de Incidentes. Herramientas de Seguridad. - Seguridad Perimetral. - Redes Inalámbricas.	3,0	3,0	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. Acreditación de Sistemas. Vulnerabilidades, Amenazas y Riesgos. Documentación de Seguridad. Inspección STIC. Amenaza TEMPEST y TRANSEC. Gestión de Incidentes de Seguridad. Software Malicioso. Herramientas de Seguridad. Seguridad perimetral. Interconexión de Sistemas. Cortafuegos y Sistemas de Detección de Intrusos. Seguridad Inalámbrica.
Introducción: Aproximación a la ciberseguridad	- Aproximación a la ciberseguridad. - ENS-RGPD.	0,4	0,4	0	Aproximación española a la ciberseguridad. ENS: actualización, situación, modificaciones. ENS-RGPD.
ENS: Entorno de validación, Plan de adecuación	- ENS: Entorno de validación. Plan de adecuación. - Análisis de Riesgos.	0,3	0,2	0,1	Entorno de Validación del ENS (EVENS). Plan de Adecuación. Análisis de Riesgos. Declaración de Aplicabilidad. Casos de estudio.
Seguridad Criptológica	- Coordinación Criptológica. Seguridad Criptológica.	0,2	0,2	0	Coordinación Criptológica. Seguridad Criptológica. Equipamiento STIC.
Políticas STIC	- Introducción a STIC. - Normativa de Seguridad. - Políticas de Seguridad.	0,4	0,4	0	Estrategias de ciberseguridad. Legislación Nacional. 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. 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.	1,3	1,1	0,2	Análisis y Gestión de Riesgos. MAGERIT y Herramienta PILAR. Seguridad Física, Documental y del Personal. Perfiles de cumplimiento. Entorno de superficie de exposición. Evaluación continua de la seguridad. Procedimiento de Inspección STIC. Interconexión de Sistemas. Gestión de Incidentes. Amenaza TEMPEST.
Medidas Técnicas STIC	- Herramientas de Seguridad. - Equipamiento STIC.	2,0	2,0	0	Soluciones de auditoría. Seguridad Inalámbrica. Análisis de código dañino. Seguridad Web. Cibervigilancia. Seguridad Endpoints. Seguridad Móvil.
Grupo Varios	- Inauguración y Clausura.	0,4	0,2	0,2	Examen. Inauguración. Juicio Crítico y Clausura.

Modalidad: En línea tutorizada

- Fase asíncrona: 50h.
- Fase síncrona: 50h.

Finalidad

La finalidad del **"Curso del Esquema Nacional de Seguridad (ENS)"** es proporcionar a los asistentes los conocimientos necesarios para implantar el ENS y su aportación para mitigar las amenazas actuales.

- Adquirir los conocimientos y familiarizarse con las actividades necesarias para realizar el Plan de Adecuación al ENS en una organización; profundizar en los roles y comités necesarios para una gobernanza adecuada partiendo de una valoración de activos esenciales y la categorización de los sistemas de información que los soportan.
- Implantación del ENS, partiendo de un Plan de Adecuación previo; comprender cada una de las medidas de seguridad del ENS en función de la categoría del sistema y cómo deben ser implementadas; así como comprender la importancia de la subcontratación en el sector público.
- Comprender los conceptos esenciales de las auditorías y conocer el Esquema de Certificación del ENS y las diferentes herramientas que el CCN pone a disposición de las organizaciones para facilitar el cumplimiento del ENS.

Créditos / Horas del Plan de Estudios

La distribución de las 40 horas de la fase asíncrona del curso (4 créditos) es la siguiente:

- Teoría: 2,8 créditos / 28 horas
- Práctica: 1,2 créditos / 12 horas

La distribución de las 20 horas de la fase síncrona del curso (2 créditos) es la siguiente:

- Teoría: 1,6 créditos / 16 horas
- Práctica: 0,4 créditos / 4 horas

Normas y Certificado de superación

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

La fase síncrona se desarrollará en modalidad en línea por lo que los participantes deberán conectarse a la emisión de las clases en directo durante los cuatro (4) 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.

La nota final del curso será de "APTO", siendo la nota de la fase asíncrona considerada sólo para el acceso a la fase síncrona 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

Podrán solicitar el curso los empleados públicos de los subgrupos A1, A2, B 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 relacionadas con la adecuación al Esquema Nacional de Seguridad de su organización.

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.

Acceso al curso (Fase asíncrona)

Para poder participar en la fase asíncrona, será necesario que el alumno sea usuario registrado del portal ÁNGELES (https://angeles-privado.ccn-cert.cni.es/), donde está ubicada la plataforma de e-learning. El alumno deberá 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.

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			Contenido
		TOT	TEO	PRA	
Aproximación práctica al Esquema Nacional de Seguridad (Fase a Distancia)	- Introducción al ENS. - Plan de Adecuación al ENS. - Implementación de Medidas de Seguridad (I y II). - Contratación en el Sector Público. - Comparativas ENS – ISO 27001. - Auditorías y Certificación en el ENS.	4,0	2,8	1,2	Introducción al ENS. Justificación jurídica y normativa. Administración electrónica y seguridad. Fases de cumplimiento. Gestión del riesgo. Estructura de un Sistema de Gestión. Plan de Adecuación. Introducción al Anexo II. Niveles de madurez. Marco Organizativo. Marco operacional. Medidas de protección. Medidas compensatorias. Proveedores. Cadena de suministro. Soluciones On-Premise. Contratación en el Sector Público. ENS – ISO 27001. Certificación del ENS. Seguimiento y mejora de un SGSI. Auditorías.
Esquema Nacional de Seguridad	- Conceptos generales. Marco jurídico. Fases de cumplimiento. - Plan de adecuación. - Roles y responsabilidades. - Categorización de Sistemas. Gestión de riesgos. - Implantación del ENS. Medidas de Seguridad. - Cadena de suministro. - Auditorías y Cumplimiento. - Herramientas CCN.	1,8	1,4	0,4	Introducción al ENS: situación actual, principios básicos y requisitos mínimos, seguridad gestionada. Activos y activos esenciales. Ámbito de aplicación. Marco jurídico y normativas: diferencia entre normas jurídicas y estándares. Las ITS de seguridad. Fases de cumplimiento del ENS: Ciclo Deming y sus fases. Plan de adecuación. Implantación del plan. La mejora continua. Comités, roles y responsabilidades. Política de Seguridad de la información. Identificación y valoración de los activos esenciales. Valoración y categorización de Sistemas: dimensiones de seguridad, niveles de valoración, criterios de valoración. Dependencias entre activos. Análisis y Gestión de Riesgos, metodología MAGERIT, Herramienta PILAR. Implantación del ENS y el plan de mejora de la seguridad. Las medidas de seguridad del ENS y perfiles de cumplimiento. La cadena de suministro y la subcontratación en el sector público: armonización de medidas de seguridad. Auditorías y evidencia de cumplimiento del ENS: introducción, auditorías técnicas y de gestión. Declaración y Certificación de conformidad. Proceso de certificación. El Plan de Acciones Correctivas (PAC). Herramientas CCN para facilitar el cumplimiento del ENS.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Modalidad: En línea tutorizada

- Fase asíncrona: 40h.
- Fase síncrona: 20h.

Finalidad

La finalidad del **"Curso de Auditorías de Cumplimiento en el ENS"** es proporcionar a los asistentes los conocimientos y habilidades necesarias para la realización de las Auditorías de Certificación del ENS, conforme lo dispone la Resolución, de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, en todas las fases del proceso auditor: estudio documental previo, auditoría en modo remoto/in situ y redacción del Informe de Auditoría.

Créditos / Horas del Plan de Estudios

La distribución de las 20 horas de la fase asíncrona del curso (2 créditos) es la siguiente:

- Teoría: 2 créditos / 20 horas

La distribución de las 20 horas de la fase síncrona del curso (2 créditos) es la siguiente:

- Teoría: 0,5 créditos / 5 horas
- Práctica: 1,5 créditos / 15 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en dos (2) fases (asíncrona y síncrona) será condición imprescindible para participar en la fase síncrona, superar las pruebas correspondientes a los exámenes previstos durante la fase asíncrona en los que se valoran los conocimientos adquiridos en dicha fase.

La fase síncrona se desarrollará en modalidad en línea por lo que los participantes deberán conectarse a la emisión de las clases en directo durante los cuatro (4) 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.

La nota final del curso será de "APTO", siendo la nota de la fase asíncrona considerada sólo para el acceso a la fase síncrona 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

Podrán solicitar el curso los empleados públicos de los subgrupos A1, A2, B 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 relacionadas con la adecuación al Esquema Nacional de Seguridad de su organización.

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.

Acceso al curso (Fase asíncrona)

Para poder participar en la fase asíncrona, será necesario que el alumno sea usuario registrado del portal ÁNGELES (https://angeles-privado.ccn-cert.cni.es/), donde está ubicada la plataforma de e-learning. El alumno deberá 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			Contenido
		TOT	TEO	PRA	
Curso de Auditorías en el ENS (Fase a distancia asíncrona)	- Auditorías en los Sistemas de Información. - Conceptos generales de Auditoría y Certificación del ENS. Desarrollo y ejecución de una auditoría.	2,0	2,0	0	Definición de Auditoría. Criterios de auditoría. Definiciones previas. Principios esenciales. Programa de auditoría. Implementación. Definición de objetivos, alcance y criterios. Gestión de resultados. Alcance. Competencia técnica. Recursos de la Entidad Certificadora. Tiempo de auditoría. Hallazgos de Auditoría. Certificación en remoto. Servicios compartidos. Distintivo de conformidad. Certificación en situaciones excepcionales. Obligaciones de las Entidades. Aprobación provisional de conformidad. Alcance y objeto. Equipo auditor. Planificación. Evidencias. Elaboración y presentación de los hallazgos. Presentación del informe. Dictamen final.
Medidas Técnicas STIC	- Auditorías de cumplimiento en el ENS. Metodología de Auditorías. - Plan de Auditoría. - Evaluación del Plan de Adecuación. Evaluación de la Implantación. Informe de auditoría. Plan de acciones correctivas	1,8	0,3	1,5	Introducción. Conceptos básicos y proceso de adecuación al ENS. Planificación del proceso de auditoría. Evaluación del Plan de Adecuación: categorización, declaración de aplicabilidad y política de seguridad. Análisis de riesgos. Evaluación de la implantación: marco operacional, medidas de protección. Informe de auditoría y plan de acciones correctivas. Requisitos mínimos y composición de OAT. Soluciones CCN-CERT (INES-AMPARO-PILAR)
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC – Amazon Web Services (AWS) en el ENS"** es proporcionar a los asistentes los conocimientos necesarios para comprender y definir las medidas y configuraciones necesarias en entornos de nube pública en Amazon Web Services (AWS) para la correcta aplicación de las exigencias del Esquema Nacional de Seguridad

El programa tiene el formato de curso autocontenido con el propósito de aportar a los asistentes una visión general práctica de conocimientos y operación de entornos AWS centrándose en los servicios de Amazon Web Services orientados a seguridad.

En ese contexto, el curso ha sido diseñado para combinar metodología con tecnología dentro de un proceso despliegue y operación de entornos cloud. Se dedica gran parte del contenido a introducir AWS y sus servicios principales de modo que incluso participantes en la formación sin experiencia previa en AWS puedan entender los fundamentos del mismo.

Créditos / Horas del Plan de Estudios

La distribución de las 20 horas de la fase síncrona del curso (2 créditos) es la siguiente:

- Teoría: 1,5 créditos / 15 horas
- Práctica: 0,5 créditos / 5 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en modalidad síncrona será obligatoria la asistencia o conexión a todas las sesiones programadas, así como realizar una serie de prácticas que permitirán valorar si se 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 el curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2, B 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 seguridad y cumplimiento normativo del Esquema Nacional de Seguridad.

Se supondrá, por parte de los asistentes, un conocimiento mínimo de comunicaciones y seguridad. 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.

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.

Materias y asignaturas

A continuación, se detallan las materias y asignaturas en las que se distribuye el curso con expresión de contenidos.

Denominación de Materias	Asignaturas que componen la Materia	CRÉDITOS			Breve Descripción del Contenido
		TOT	TEO	PRA	
Amazon Web Services (AWS) en el ENS	- Introducción a ENS. - Introducción a AWS - Guías de configuración segura. - Controles de seguridad. - Protección de Información y Servicios.	1,8	1,3	0,5	Introducción a ENS. Modelo de responsabilidad compartida. Introducción a AWS. Guías de configuración segura. Laboratorio Prowler. Seguridad en la nube de AWS. AWS IAM. Amazon EC2. Amazon VPC. Contenedores en AWS. Serverless y AWS Lambda. Almacenamiento en AWS. Bases de datos en AWS. Cifrado en AWS. Monitorización de los recursos en AWS. Explotación - Inventario y protección de claves. KMS y ENS. Controles de seguridad en AWS. Detección de amenazas y vulnerabilidades. Protección de la información. Protección de los servicios.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Modalidad: En línea tutorizada

- Fase síncrona: 20 h.

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 asíncrona del curso (3 créditos) es la siguiente:

- Teoría: 3 créditos / 30 horas

La distribución de las 50 horas de la fase síncrona 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 (asíncrona y síncrona) será condición imprescindible para participar en la fase síncrona, superar las pruebas correspondientes a los exámenes previstos durante la fase asíncrona 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 asíncrona considerada sólo para el acceso a la fase síncrona 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.

Acceso al curso (Fase asíncrona)

Para poder participar en la fase asíncrona, será necesario que el alumno sea usuario registrado del portal ÁNGELES (https://angeles-privado.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 asíncrona. 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 asíncrona del curso (1 crédito) es la siguiente:

- Teoría: 1 crédito / 10 horas

La distribución de las 25 horas de la fase síncrona 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 (asíncrona y síncrona) será condición imprescindible para participar en la fase síncrona, superar las pruebas correspondientes a los exámenes previstos durante la fase asíncrona en los que se valoran los conocimientos adquiridos en dicha fase.

Durante la fase síncrona 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.

Acceso al curso (Fase asíncrona)

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 asíncrona)	- 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 STIC – Trazabilidad del dato"** es proporcionar a los asistentes los conocimientos necesarios para gestionar la documentación sensible y confidencial de la organización a través de un enfoque de seguridad centrada en los datos, de forma que pueda estar protegida y bajo control en cualquier ubicación, además de obtener una completa auditoría de accesos sobre la misma.

Créditos / Horas del Plan de Estudios - Fase síncrona

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

• Teoría: 1 créditos / 10 horas

• Práctica: 0,5 créditos / 5 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en modalidad síncrona será obligatoria la asistencia a todas las sesiones programadas, así como 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, B 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 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	
Trazabilidad del dato	- Actores y tipos de ataque de fugas de información. - Tecnologías de prevención frente a fugas de información. - Sistemas de seguridad centrados en los datos. - Clasificación y trazabilidad de la información. - Modelos de seguridad Zero-Trust y SASE. - Herramienta CARLA. - Casos prácticos de protección centrada en los datos y trazabilidad.	1,5	0,9	0,9	Introducción a un enfoque de seguridad centrado en los datos. Vectores de ataque sobre la información sensible y tipología de fugas de información. El modelo de seguridad Zero-Trust y SASE y su relación con la seguridad centrada en los datos. Casos de uso y beneficios de una solución de protección, control y trazabilidad del dato. Herramienta CARLA: Protección, Control y Trazabilidad del dato. Sesiones prácticas de trazabilidad y control de documentación sensible
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 asíncrona

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

- Teoría: 12,5 créditos / 125 horas

Créditos / Horas del Plan de Estudios - Fase síncrona

La distribución de las 75 horas de la fase síncrona 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 (asíncrona y síncrona) será condición imprescindible para ser nombrado asistente de la fase síncrona, superar las pruebas correspondientes al examen previo en el que se valoran los conocimientos adquiridos en la fase asíncrona.

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 síncrona**, 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.

Acceso al curso (Fase asíncrona)

Para poder participar en la fase asíncrona, será necesario que el alumno sea usuario registrado del portal ÁNGELES (https://angeles-privado.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 asíncrona. 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 asíncrona

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 síncrona

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 – Seguridad en Comunicaciones Móviles"** es proporcionar a los asistentes una visión detallada y actualizada de las amenazas y vulnerabilidades de seguridad que se ciernen sobre las comunicaciones móviles. El curso describe con detalle los ataques conocidos contra las diferentes generaciones de protocolos de comunicaciones móviles, introduciendo en cada caso los conceptos básicos de arquitectura y seguridad mínimos necesarios para que el alumno llegue a entender completamente el funcionamiento de cada ataque, con diferentes ejemplos prácticos y videos demostrativos.

Durante el curso se estudiarán las vulnerabilidades asociadas a las diferentes generaciones de los protocolos de red y datos: 2G, 3G, 4G y 5G.

Créditos / Horas del Plan de Estudios

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

- Teoría: 1,3 créditos / 13 horas
- Práctica: 0,2 créditos / 2 horas

Normas y Certificado de superación

La formación se desarrollará en modalidad presencial, con asistencia obligatoria a las sesiones o en modalidad en línea, en la que los participantes deberán conectarse a la emisión de las clases en directo durante los cuatro 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, a nivel técnico, 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 relacionadas con entornos de gestión de comunicaciones móviles, de seguridad de la información y auditorías de seguridad.

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.

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	
Seguridad en Comunicaciones Móviles	- Introducción a las comunicaciones móviles - Seguridad en comunicaciones 2G - Seguridad en comunicaciones 3G - Seguridad en comunicaciones 4G - Seguridad en comunicaciones 5G - Conclusiones finales	1,4	1,2	0,2	Introducción a las comunicaciones móviles. Seguridad en comunicaciones 2G: Voz y SMS en el interfaz de radio. Voz y SMS en la red core. GPRS/EDGE en el interfaz de radio. GPRS/EDGE en la red core. Seguridad en comunicaciones 3G: Introducción a 3G. Análisis de seguridad de la interfaz de radio. Análisis de seguridad de la red core. Contramedidas. Seguridad en comunicaciones 4G: Introducción a 4G. Implementación de llamadas de voz y SMS. Conceptos de seguridad. Ataques contra 4G. Conclusiones. Seguridad en comunicaciones 5G: Introducción. Conceptos de seguridad. Ataques contra 5G. Conclusiones. Conclusiones finales.
Grupo Varios	- Inauguración y Clausura.	0,1	0,1	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso Avanzado STIC - Dispositivos Móviles"** es proporcionar a los asistentes los conocimientos necesarios, mediante un acercamiento teórico y práctico a las plataformas mayoritariamente implantadas (Android e iOS), para conocer y analizar las amenazas existentes en los dispositivos móviles para así poder mitigarlas.

Una vez finalizado el curso, los participantes deberán conocer los desafíos y oportunidades que suponen estas plataformas, cuáles son sus debilidades y de qué manera se pueden acometer implementaciones seguras de estos dispositivos en sus respectivas organizaciones mediante un análisis de ambas plataformas, interacción con aplicaciones, los diferentes acercamientos a su arquitectura de seguridad, las amenazas más comunes y una introducción al análisis forense de estos dispositivos.

Créditos / Horas del Plan de Estudios

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

- Teoría: 2,3 créditos / 23 horas
- Práctica: 0,2 créditos / 2 horas

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

- Teoría: 1,0 créditos / 10 horas
- Práctica: 2,5 créditos / 25 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en dos (2) fases (asíncrona y síncrona) será condición imprescindible para participar en la fase síncrona, superar las pruebas correspondientes a los exámenes previstos durante la fase asíncrona en los que se valoran los conocimientos adquiridos en dicha fase.

La fase síncrona se desarrollará en modalidad en línea por lo que los participantes deberán conectarse a la emisión de las clases en directo durante los siete (7) 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.

La nota final del curso será de "APTO", siendo la nota de la fase asíncrona considerada sólo para el acceso a la fase síncrona 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

Podrán solicitar el curso los empleados públicos de los subgrupos A1, A2, B 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 la comunicación y que, asimismo, necesite para su puesto de trabajo llevar a cabo tareas relacionadas con la adecuación al Esquema Nacional de Seguridad de su organización.

Se supondrá, por parte de los asistentes, un conocimiento mínimo de los sistemas Linux y Windows y conocimientos de protocolos y equipamiento de red. Asimismo, será necesario disponer de conocimientos avanzados en manejo de entornos de virtualización y conocimientos medios de Shell Scripting y Java, 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 un (1) año.

Acceso al curso (Fase asíncrona)

Para poder participar en la fase asíncrona, será necesario que el alumno sea usuario registrado del portal ÁNGELES (https://angeles-privado.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 asíncrona. El alumno deberá 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	
Introducción a la seguridad en dispositivos móviles (Fase a distancia)	- Introducción. Android, iOS y otros sistemas operativos. Buenas prácticas. Acceso físico. Comunicaciones USB. Configuración por defecto. Cifrado del dispositivo.	1,0	0,8	0,2	Introducción a la seguridad en dispositivos móviles. Seguridad y acceso físico. Comunicaciones y amenazas en la actualidad.
Seguridad en dispositivos móviles (Fase a distancia)	- Pantalla de bloqueo. Actualización del Sistema Operativo y aplicaciones. Cifrado del dispositivo. Copias de seguridad. Capacidades de comunicación inalámbricas. Aplicaciones móviles.	1,5	1,5	0	Recomendaciones y buenas prácticas en el uso de dispositivos móviles. Describir las mejores prácticas. Protección y uso lo más seguro posible de los dispositivos móviles. Configuración y utilización de los mecanismos de protección existentes en la actualidad.
Seguridad en dispositivos móviles	- Problemas y oportunidades. Análisis de plataforma de dispositivo móvil. Interacción de aplicaciones móviles. Modelo y arquitectura de seguridad. Análisis de dispositivos móviles. Desbloqueo, rooteo y jailbreak. Arquitectura de almacenamiento y sistema de archivos. Aplicaciones ofuscadas de ingeniería inversa. Análisis de aplicaciones estáticas. Análisis de aplicaciones Android. Localización geográfica y spoofing. USB, Bluetooth, WiFi y NFC. Ataques y amenazas malware. Introducción al análisis forense del dispositivo móvil.	3,3	0,8	2,5	Implementación segura de dispositivos móviles. Debilidades en dispositivos móviles. Explotación de debilidades. Modelos de gestión de permisos en iOS y Android. Debilidades de firma de código en Android. Ejecución de aplicaciones. Últimas mejoras de seguridad en Android e iOS. Interacción de aplicaciones Android e iOS. Protección de aplicación mediante permisos y firmas. Modelo y arquitectura de seguridad. Laboratorio: uso de emuladores, análisis e interactuación con Android Debug Bridge, interacción vía Activity Manager. iOS Jailbreak. Unlocked Bootloaders. Exploits para Android. Arquitectura de almacenamiento de datos y sistema de archivos. Estructura del sistema de archivos. Decodificación de datos. Laboratorio: Aplicaciones ofuscadas de ingeniería inversa. Laboratorio: Análisis de aplicaciones estáticas. Laboratorio: Análisis de aplicaciones Android. Localización geográfica y Spoofing. Comunicaciones USB, Bluetooth, WiFi y NFC. Laboratorio: Manipulación de red. Laboratorio: Ataques SSL/TLS. Laboratorio: Ataques Web. Laboratorio: RAT. Amenazas malware. Introducción al análisis forense del dispositivo móvil. Conclusiones y referencias.
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 síncrona 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 síncrona 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 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	- 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 - 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 asíncrona del curso (2,5 créditos) es la siguiente:

- Teoría: 2,3 créditos / 23 horas
- Práctica: 0,2 créditos / 2 horas

La distribución de las 25 horas de la fase síncrona 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

Al desarrollarse el presente Curso en dos (2) fases (asíncrona y síncrona) será condición imprescindible para participar en la fase síncrona, superar las pruebas correspondientes a los exámenes previstos durante la fase asíncrona en los que se valoran los conocimientos adquiridos en dicha fase.

La fase síncrona se desarrollará en modalidad en línea por lo que los participantes deberán conectarse a la emisión de las clases en directo durante los cinco (5) 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.

La nota final del curso será de "APTO", siendo la nota de la fase asíncrona considerada sólo para el acceso a la fase síncrona 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

Podrán solicitar el curso los empleados públicos de los subgrupos A1, A2, B 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, 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 un (1) año.

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.

Acceso al curso (Fase asíncrona)

Para poder participar en la fase asíncrona, será necesario que el alumno sea usuario registrado del portal ÁNGELES (https://angeles-privado.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 asíncrona. El alumno deberá 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	
Introducción a la cibervigilancia (Fase a distancia)	- Introducción a la cibervigilancia. Técnicas de obtención en fuentes abiertas y social media. Gestión de aplicaciones para generar ciberinteligencia.	1,0	0,8	0,2	Introducción a la cibervigilancia. Técnicas de obtención en fuentes abiertas y social media. Gestión de aplicaciones para generación de inteligencia de fuentes abiertas.
Gestión de cibercrisis (Fase a distancia)	- Introducción. ¿Qué es una crisis? Definición y gestión de cibercrisis. Buenas prácticas en la gestión de cibercrisis. Casos de estudio. Resumen de recomendaciones.	1,5	1,5	0	Buenas prácticas en la gestión de crisis de ciberseguridad. Definición de crisis. Definición de cibercrisis. Gestión de cibercrisis. Buenas prácticas en la gestión de cibercrisis.
Cibervigilancia	- Conceptos generales y metodología OSINT. Obtención OSINT. Redes Sociales. Cibervigilancia. Anonimización. Herramientas asociadas. Elaboración de Informes.	2,3	0,5	1,8	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.
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 20 horas de la fase asíncrona del curso (2 créditos) es la siguiente:

- Teoría: 2,0 créditos / 20 horas

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

- Teoría: 2,6 créditos / 26 horas
- Práctica: 2,4 créditos / 24 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en dos (2) fases (asíncrona y síncrona) será condición imprescindible para participar en la fase síncrona, superar las pruebas correspondientes a los exámenes previstos durante la fase asíncrona en los que se valoran los conocimientos adquiridos en dicha fase.

La fase síncrona se desarrollará en modalidad en línea por lo que los participantes deberán conectarse a la emisión de las clases en directo durante los diez (10) 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.

La nota final del curso será de "APTO", siendo la nota de la fase asíncrona considerada sólo para el acceso a la fase síncrona 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, B 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 un (1) año.

Acceso al curso (Fase asíncrona)

Para poder participar en la fase asíncrona, será necesario que el alumno sea usuario registrado del portal ÁNGELES (https://angeles-privado.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 asíncrona. El alumno deberá 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	
Curso de Auditorías en el ENS (Fase a distancia asíncrona)	- Auditorías en los Sistemas de Información. - Conceptos generales de Auditoría y Certificación del ENS. - Desarrollo y ejecución de una auditoría.	2,0	2,0	0	Definición de Auditoría. Criterios de auditoría. Definiciones previas. Principios esenciales. Programa de auditoría. Implementación. Definición de objetivos, alcance y criterios. Gestión de resultados. Alcance. Competencia técnica. Recursos de la Entidad Certificadora. Tiempo de auditoría. Hallazgos de Auditoría. Certificación en remoto. Servicios compartidos. Distintivo de conformidad. Certificación en situaciones excepcionales. Obligaciones de las Entidades. Aprobación provisional de conformidad. Alcance y objeto. Equipo auditor. Planificación. Evidencias. Elaboración y presentación de los hallazgos. Presentación del informe. Dictamen final.
Medidas Técnicas STIC	- Auditorías de Seguridad TIC. Metodología de Auditorías. Inspecciones ENS. Inspecciones STIC	4,8	2,4	2,4	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.

Modalidad: En línea tutorizada

- Fase asíncrona: 20 horas
- Fase síncrona: 50 horas

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 síncrona 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 síncrona 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 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	- 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 - Sistemas Operativos"** es proporcionar a los asistentes los conocimientos necesarios para que sean capaces de comprobar, con una garantía suficiente, las medidas de seguridad necesarias para proteger sistemas operativos MS Windows y Linux.

En particular la administración e implementación segura, así como las herramientas y configuraciones que permitan reducir la superficie de exposición de los sistemas corporativos, tomando como referencia los aspectos observados en las distintas guías CCN-STIC asociadas a los mencionados sistemas operativos.

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 mencionadas guías.

Créditos / Horas del Plan de estudios

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

- Teoría: 2,3 créditos / 23 horas
- Práctica: 0,2 créditos / 2 horas

La distribución de las 25 horas de la fase síncrona 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 (2) fases (asíncrona y síncrona) será condición imprescindible para participar en la fase síncrona, superar las pruebas correspondientes a los exámenes previstos durante la fase asíncrona en los que se valoran los conocimientos adquiridos en dicha fase.

La fase síncrona se desarrollará en modalidad en línea por lo que los participantes deberán conectarse a la emisión de las clases en directo durante los cinco (5) 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.

La nota final del curso será de "APTO", siendo la nota de la fase asíncrona considerada sólo para el acceso a la fase síncrona 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 y requisitos técnicos

Podrán solicitar el curso los empleados públicos de los subgrupos A1, A2, B 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 relacionadas con la adecuación al Esquema Nacional de Seguridad de su organización.

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:

- Actividad relacionada con la administración de Sistemas de las tecnologías de la información y la comunicación (TIC) bajo entornos Windows y Linux
- 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.

Acceso al curso (fase on-line)

Para poder participar en la fase asíncrona, será necesario que el alumno sea usuario registrado del portal ÁNGELES (https://angeles-privado.ccn-cert.cni.es/), donde está ubicada la plataforma de e-learning. El alumno deberá 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	
Introducción a la acreditación de sistemas (Fase a distancia)	- Introducción a la acreditación de sistemas. Aproximación de mejora continua. Acompañamiento, soporte y mantenimiento de la acreditación.	1,0	0,8	0,2	Introducción a la acreditación de sistemas. Aproximación de mejora continua (objetivos a corto, medio y largo plazo). Análisis de últimos abstracts relacionados. Adaptación al ecosistema de manejo de información sensible. El modelo de seguridad continuo, frente a mecanismos tradicionales más rígidos de evaluación, Riesgos a valorar para que la información sensible se almacena en servicios Cloud. La figura de las empresas de acompañamiento.
Curso Básico STIC Seguridad en Entornos Windows (Fase a distancia)	- 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.
Curso de acreditación STIC - Sistemas Operativos	- Administración Seguridad Sistemas Windows. Seguridad en Active Directory y políticas de grupo. Administración Seguridad Sistemas Linux. Medidas Adicionales de Seguridad. Guías CCN-STIC Asociadas.	2,3	0,5	1,8	Administración de Seguridad en Sistemas Windows: Riesgos de Seguridad en roles y características de Windows Server 2016. Asignación de permisos a recursos. Control de cuentas de usuario (UAC) y elevación de privilegios. Seguridad de la red (protocolos, tipos, seguridad avanzada de Windows Defender). Políticas de seguridad local. Seguridad basada en servicios de dominio de Active Directory y políticas de grupo: Estructura lógica e implementación del Directorio Activo. Controladores de dominio. Administración de Directorio Activo. Gestión de sistemas mediante GPO. Directivas de equipo y usuario: gestión de políticas de seguridad. Filtrado de seguridad y WMI. Filtrado de seguridad y WMI. Guías CCN-STIC asociadas a Sistemas Windows. Estructura y elementos. Administración de Seguridad en sistemas Linux: Sistema de archivos y particiones. Shell y comandos GNU. Inicio, servicios y Kernel. Instalación y configuración segura de servicios y componentes software. Administración de usuarios y grupos. Registro de sistema. Gestión segura con SSH y consola web. Medidas adicionales de seguridad: Conexiones de red y restricciones de Firewall. Control de servicios del sistema y procesos en ejecución. Gestión y protección de archivos y sistema de archivos. Scripts de Shell. Gestión de seguridad y acceso al sistema (SELinux). Guías CCN-STIC asociadas a Sistemas Linux. Estructura y elementos.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC – Seguridad en Infraestructuras de Red"** es proporcionar a los asistentes los conocimientos necesarios sobre las principales amenazas que afectan a las infraestructuras y equipamiento que soportan las redes de comunicaciones, así como conocer y aplicar las medidas adecuadas para garantizar su seguridad. En particular, se pretende:

- Repasar conceptos básicos sobre redes de área local y redes IP, así como sobre la configuración de routers y switches.
- Conocer las principales amenazas que afectan a la seguridad de routers y switches y, por extensión, a las redes y servicios basadas en ellos.
- Conocer y aplicar medidas básicas y buenas prácticas de configuración para mitigar las amenazas, tanto en el acceso a la gestión de los equipos como en el plano de datos y de control.
- Conocer las técnicas de acceso seguro a la gestión remota de equipos mediante redes privadas virtuales.
- Conocer y aplicar herramientas de seguridad para la exploración de redes y sistemas, así como la realización de auditorías de seguridad.

Créditos / Horas del Plan de Estudios

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

- Teoría: 1,5 créditos / 15 horas

La distribución de las 25 horas de la fase síncrona 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 (asíncrona y síncrona) será condición imprescindible para participar en la fase síncrona, superar las pruebas correspondientes a los exámenes previstos durante la fase asíncrona en los que se valoran los conocimientos adquiridos en dicha fase.

La fase síncrona se desarrollará en modalidad en línea por lo que los participantes deberán conectarse a la emisión de las clases en directo durante los cinco (5) días de curso. Durante las sesiones se realizarán una serie de prácticas de laboratorio sobre los contenidos impartidos 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.

La nota final del curso será de "APTO", siendo la nota de la fase asíncrona considerada sólo para el acceso a la fase síncrona 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

Podrán solicitar el curso los empleados públicos de los subgrupos A1, A2, B y C1, y el personal laboral equivalente, que tengan 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.

Acceso al curso (Fase asíncrona)

Para poder participar en la fase asíncrona, será necesario que el alumno sea usuario registrado del portal ÁNGELES (https://angeles-privado.ccn-cert.cni.es/), donde está ubicada la plataforma de e-learning. El alumno deberá 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	
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. VLAN. 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	Conceptos básicos de seguridad. Tipos de amenazas. Políticas de seguridad. Anatomía de un ataque. Seguridad en la configuración y gestión de equipos de red. Concepto de "Hardening". Acceso seguro a la gestión. Recomendaciones básicas: gestión de configuraciones, actualización de software, agregación de logs, etc. Monitorización. Descripción del escenario de prácticas. Configuración segura de equipos de red y uso de herramientas de seguridad (práctica). Amenazas y ataques a switches. Saturación de tablas CAM. Falsificación de direcciones MAC. Falsification de ARP. DHCP starvation/spoofing. Técnicas VLAN hopping: switch spoofing y doble etiquetado. Encaminamiento en LAN: ataques al protocolo Spanning Tree. Medidas de seguridad para mitigar los ataques. Seguridad en redes de área local (práctica). Mecanismos básicos de identificación y autenticación. Control de accesos. Protocolos de autenticación. 802.1x. Autenticación centralizada de usuarios. RADIUS. Sistemas de control de acceso a redes: Network Access Control (NAC). Soluciones Single Sign On (SSO). Redes Privadas Virtuales (VPN). Configuración segura de acceso remoto con VPN y RADIUS como servidor de autenticación (práctica). Amenazas y ataques a routers. Falsificación de direcciones IP (IP spoofing). Ataques de denegación de servicio (DoS). Seguridad en protocolos de encaminamiento: autenticación. Contramedidas: Unicast Reverse Path Forwarding (URPF), listas de acceso (ACL), monitorización de flujos: NetFlow/sflow. Técnicas de encaminamiento para mitigar ataques DoS. Configuración de medidas de seguridad en redes IP (práctica) Herramientas para la realización de auditorías de seguridad de equipos. Herramienta ROCIO. Realización de auditorías de auditorías con ROCIO y otras herramientas (práctica)
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

Modalidad: En línea tutorizada

- Fase asíncrona: 15 horas
- Fase síncrona: 25 horas

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 síncrona 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 síncrona 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 Básico de Auditorías de Seguridad TIC 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 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	- 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 – Detección Temprana"** es 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 los Sistemas de Alerta Temprana y otras soluciones que el CCN-CERT pone a disposición de las Administraciones Públicas.

Créditos / Horas del Plan de Estudios

La distribución de las 20 horas de la fase síncrona del curso (2,0 créditos) es la siguiente:

- Teoría: 1 crédito / 10 horas
- Práctica: 1 crédito / 10 horas

Normas y Certificado de superación

Al desarrollarse el presente Curso en modalidad síncrona será obligatoria la asistencia o conexión a todas las sesiones programadas, así como realizar una serie de prácticas que permitirán valorar si se 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 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	- Introducción a la Gestión de Incidentes - Detección - Casos de uso en la detección temprana de incidentes - Sistemas de Alerta Temprana - Herramienta GLORIA - Casos prácticos	1,9	0,9	1,0	Introducción a la gestión de incidentes: Herramientas CCN-CERT. Fases en la gestión de incidentes. Detección: Tipos de entornos. Tipos de detección. Pyramid of Pain. Riesgos. Casos de uso: Definición de los escenarios. Desarrollo. Validación y despliegue. Sistemas de Alerta Temprana. Herramienta GLORIA: Adquisición – Argos. Correlación – Tritón. Consola de Eventos – EMAS. Estadísticas – Hera. Mapa de activos (ICS). Automatización. Caso práctico completo.
Grupo Varios	- Inauguración y Clausura.	0,1	0,1	0	Inauguración. Juicio Crítico y Clausura.

Finalidad

La finalidad del **"Curso STIC – Gestión de Incidentes de Ciberseguridad"** es 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 síncrona 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 síncrona 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 Básico de Auditorías de Seguridad TIC 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 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	- Sistema de Alerta Temprana - Herramienta LUCIA - Herramienta REYES - Herramienta CARMEN - Casos prácticos	2,3	0,8	1,5	Introducción a la gestión de incidentes. 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. 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.
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 síncrona 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 modalidad síncrona será obligatoria la asistencia o conexión a todas las sesiones programadas, así como realizar una serie de prácticas que permitirán valorar si se 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 Básico de Auditorías de Seguridad TIC 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 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	- Herramienta REYES - Herramienta CLAUDIA - Herramienta CARMEN - Casos prácticos	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 - 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 síncrona 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 síncrona 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 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	- 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.

Finalidad

La finalidad del **"Curso STIC – Ciberinteligencia"** es proporcionar a los asistentes los conocimientos necesarios, mediante un enfoque teórico-práctico, sobre los conceptos relacionados con la ciberinteligencia, cuál es el papel de un analista de inteligencia y qué actividades deben desarrollar a la hora de identificar y analizar la inteligencia asociada a las amenazas a través del estudio del modelo de diamante y poder realizar investigaciones a través de técnicas OSINT.

Una vez finalizado el curso, los participantes deberán conocer los conceptos básicos relacionados con la ciberinteligencia, las distintas tipologías de fuentes de inteligencia existentes, identificar técnicas y tácticas asociadas a grupos de atacantes, la obtención de indicadores de compromiso y su valor, y ser capaces de llevar a cabo investigaciones básicas.

Créditos / Horas del Plan de Estudios

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

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

Normas y Certificado de superación

Al desarrollarse el presente Curso en modalidad síncrona será obligatoria la asistencia o conexión a todas las sesiones programadas, así como realizar una serie de prácticas que permitirán valorar si se 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, B 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 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	
Ciberinteligencia	- Introducción a la ciberinteligencia. - Ciclo de vida de inteligencia. - Conceptos: información, datos e inteligencia. - Fuentes de inteligencia. - Recolección y clasificación de la información. - Indicadores de Compromiso. - Modelo de Diamante y clasificación de actores. - Técnicas de investigación en OSINT.	2,3	0,8	1,5	Conceptos de ciberinteligencia OSINT, IMINT, SOCMINT, HUMINT, GEOMINT, MASINT Bigdata asociado a la recolección de inteligencia. Clasificación de la información y generación de inteligencia. Indicadores de compromiso, tipología, como generarlos y donde aplicarlos. Modelo de diamante asociado a la inteligencia para la identificación de diferentes actores. Investigaciones a través de técnicas OSINT. OSINT en buscadores. Análisis de imágenes. Búsquedas en RRSS.
Grupo Varios	- Inauguración y Clausura.	0,2	0,2	0	Inauguración. Juicio Crítico y Clausura.

3. Formación *online*

La plataforma Ángeles del Centro Criptológico Nacional (www.ccn.cni.es) ofrece varias modalidades de cursos online en función del perfil del usuario. Es posible registrarse a través del sistema CI@ve (con DNI/e, Certificado electrónico, o CI@ve PIN) y permite exportar el expediente relativo a la formación online del alumnado en el que se especifican las horas de formación recibidas, así como los cursos y sesiones de concienciación realizados en la plataforma.

- Básico de Ciberseguridad
- Básico de fundamentos Linux
- INES (Informe Nacional del Estado de la Seguridad)
- Básico STIC - Seguridad en entornos Windows
- Análisis y Gestión de Riesgos de los Sistemas de Información
- Esquema Nacional de Seguridad
- Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC)

ángeles
Formación, capacitación y talento en ciberseguridad

4. Formación a distancia y en *streaming*

La solución VANESA, del CCN-CERT, es una **plataforma de retransmisión de sesiones formativas en directo**, que 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.

</vanesa>

- Soluciones CCN-CERT
- Código Dañino
- Comunicaciones móviles
- Correo electrónico
- Cortafuegos
- Dispositivos móviles
- ENS
- Encuentros ENS
- Forense
- Productos STIC
- Soluciones de terceros
- Web
- Windows

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.

- Exploiting
- Reversing
- Hacking
- Programación

6. ELENA. Simulador de Técnicas de Vigilancia

Es la plataforma del CCN-CERT para practicar técnicas, tácticas y procedimientos en labores de ciberinvestigación. Permite a los usuarios tomar el rol del analista en un entorno simulado de investigación basado en situaciones reales, que posibilita desarrollar y poner en práctica las técnicas, tácticas y procedimientos necesarios para realizar labores de ciberinvestigación.

Sistema

- **Situaciones reales simuladas**
- **Con variados escenarios**
- **Intuitivo y robusto**
- **Testado por expertos**

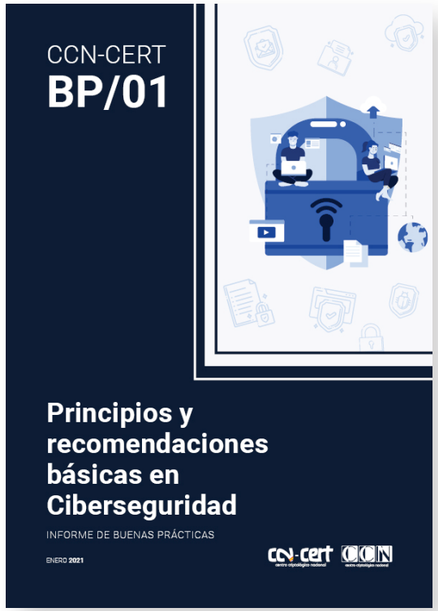
Incluye

- **Todos los recursos necesarios desde el comienzo**
- **Estadísticas detalladas**
- **Ranking de mejores participantes**

7. 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 desde Ángeles, 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
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
19. **BP/19** – Recomendaciones de seguridad en Google Chrome
20. **BP/20** – Buenas Prácticas en la Gestión de Cibercrisis
21. **BP/21** – Gestión de incidentes de ransomware
22. **BP/22** – Recomendaciones de seguridad para Oracle Database 19C
23. **BP/23** – Recomendaciones de seguridad para bases de datos DB2
24. **BP/24** – Recomendaciones de seguridad para bases de datos
25. **BP/25** – Recomendaciones de seguridad para bases de datos DB2 sobre zOS
26. **BP/26** – Recomendaciones de seguridad en Microsoft Edge

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL,
2.5.4.97=VATES-S2800155J, ou=CENTRO
CRIPTOLOGICO NACIONAL, o=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2022.08.25 12:08:22 +02'00'

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

© Centro Criptológico Nacional