

«CURSO BÁSICO TÉCNICO DE CIBERSEGURIDAD» —

Guía didáctica



ÍNDICE

1. OBJETIVOS	4
2. METODOLOGÍA	4
3. DESCRIPCIÓN DEL CURSO	6
3.1. Calendario del curso	12
4. GUÍA DE USO DE LA PLATAFORMA	25
4.1. Registro en la plataforma	25
4.2. Acceso a los contenidos	26
4.3. Participación en los foros	29
4.4. Búsqueda avanzada en los foros	31
4.5. Consultas desde el área personal	31
4.6. Dinámica de gamificación	33
5. EVALUACIÓN Y CERTIFICACIÓN	37
6. TUTORÍAS Y OTROS DATOS DE CONTACTO	38

ÍNDICE DE ILUSTRATIVOS

Ilustración 1. Calendarización orientativa de la ejecución del curso Unidades transversales	12
Ilustración 2. Calendarización orientativa de la ejecución del curso Especialidad 1	13
Ilustración 3. Calendarización orientativa de la ejecución del curso Especialidad 2	13
Ilustración 4. Calendarización orientativa de la ejecución del curso Especialidad 3	14
Ilustración 5. Calendarización orientativa de la ejecución del curso Unidades transversales	14
Ilustración 6. Interfaz de acceso a la plataforma Moodle	25
Ilustración 7. Ventana principal de la plataforma	26
Ilustración 8. Contenido didáctico en formato mosaico	26
Ilustración 9. Lista de recursos en una unidad	27
Ilustración 10. Lista de comprobación finalización de recursos y estado de finalización	28
Ilustración 11. Foro temático en una unidad	29
Ilustración 12. Acceso a los bloques del curso	30

Ilustración 13. Bloque Calendario.....	31
Ilustración 14. Calificaciones y mensajería.....	32
Ilustración 15. Distribución de puntos de experiencia	33
Ilustración 16. Bloque ¡Subes de nivel!	34
Ilustración 17. Ranking bloque «¡Subes de nivel!».....	35
Ilustración 18. Notificación subida de nivel.....	35
Ilustración 19. Insignias del curso.....	36

ÍNDICE DE TABLAS

Tabla 1. Estructura de las unidades didácticas	8
--	---

1 OBJETIVOS

Tras la realización de este curso podrás:

- Transferir conceptos y conocimientos en el ámbito de la ciberseguridad desde la perspectiva de 4 especializaciones diferentes:
 - Administración de sistemas de ciberseguridad.
 - Introducción a la ciberseguridad Industrial.
 - Análisis de incidentes y forense.
 - *Compliance* en ciberseguridad.

- Comprender la importancia de la ciberseguridad y los beneficios de estar protegido en el entorno digital.
- Identificar las principales amenazas y tipos de *hackers* y webs que existen.
- Implementar medidas necesarias para estar ciberprotegido.
- Utilizar diferentes herramientas y técnicas.

METODOLOGÍA

La metodología de este MOOC se basa en el **modelo pedagógico de aprender haciendo**, *Learning by doing*, por eso encontrarás a lo largo del curso gran variedad de ejercicios prácticos, actividades de investigación y cuestionarios de autoevaluación.

El **equipo docente** te apoyará a lo largo del curso, manteniendo una comunicación fluida a través de los medios habilitados para tal fin, como son los **foros** y el sistema de **mensajería interna** de la plataforma.

Además, el curso lleva asociada una **dinámica de gamificación**, mediante la cual podrás obtener puntos a medida que vayas visualizando y realizando cada uno de los recursos de aprendizaje asociados a cada unidad. Estos son **puntos de experiencia, no cuentan para la evaluación**, por lo tanto, no influyen en tu nota del curso. Esta dinámica tiene como único objetivo motivar la participación y mejorar la experiencia de aprendizaje a lo largo de las unidades. De manera opcional, podrás conocer tu posición en un *ranking* grupal.

DESCRIPCIÓN DEL CURSO

La ciberseguridad y la confianza en el ámbito digital son hoy dos de los retos más importantes a los que se enfrentan los ciudadanos y las empresas. Se trata de aspectos de crucial importancia en un contexto global, interconectado y dependiente de la tecnología como es el actual, e imprescindible para alcanzar la necesaria confianza en el ámbito digital. Por ciberseguridad nos referimos a la protección de los sistemas informáticos, las redes y los dispositivos de los ataques cibernéticos y otras formas de violación de la seguridad. La ciberseguridad forma parte de un concepto más amplio que es la seguridad de la información, que consiste en disponer de todos los medios técnicos y operativos para que la información esté protegida.

Se tratará la ciberseguridad y seguridad de la información desde cuatro ámbitos:

- **La administración de sistemas de ciberseguridad.** Aquí se conocerán y analizarán las principales soluciones de apoyo a los responsables de sistemas para proteger el proceso de negocio ante diferentes escenarios de ataque, como los sistemas de detección de *software* malicioso, así como las herramientas de detección y protección contra intrusiones o los cortafuegos, entre otros.

Además, se tratarán los procedimientos correctos y buenas prácticas a la hora de mantener un nivel de madurez de ciberseguridad óptimo, así como los métodos más idóneos en la administración de herramientas y sistemas corporativos.

- **La ciberseguridad industrial,** donde se profundizará en el concepto de

los sistemas de control y automatización industrial para entender su funcionamiento, cuáles son los protocolos de comunicación más utilizados (como TCP o RTU, entre otros); y también se analizará el proceso de reconocimiento de redes OT. Asimismo, se descubrirán las vulnerabilidades más destacadas de estos sistemas.

Además, se hará un recorrido por la ciberseguridad y la convergencia de los entornos IT (tecnologías de la información) y OT (tecnologías de las operaciones), junto con los ataques ciberindustriales más destacados de los últimos años. Se analizará la situación actual de los entornos industriales, las topologías de red seguras de OT, así como las herramientas y procedimientos a seguir para protegerlos.

- **El análisis de incidentes y forense.** Se comenzará presentando los tipos de incidentes más habituales y cómo se originan, estableciendo las pautas para definir cuáles son los procedimientos de reacción ante incidentes, y cómo y a quién reportarlos; y se analizarán las diferentes acciones de detección, contención y respuesta aplicables en cada caso.

También se realizará una introducción al concepto de investigación forense digital, se conocerá cómo establecer un procedimiento estándar a seguir, así como los tipos de evidencia y análisis que se pueden realizar en los distintos escenarios aplicables. Asimismo, se analizarán los conceptos básicos en materia de seguridad en los dispositivos móviles y se describirán las técnicas forenses que más se utilizan en los mismos.

- Por último, conocer el cumplimiento **en ciberseguridad**, también conocido como **compliance**, es importante para garantizar que una organización cumpla con todas las regulaciones y leyes relacionadas con

la seguridad cibernética. Se tratarán las diferentes normativas en materia de ciberseguridad (ENS, ISO 27001, Ley PIC, Directiva NIS, GDPR, etc.) y se analizará su impacto en el ciclo de vida de los servicios.

Asimismo, se conocerá con detalle la RGDP y la LOPDGDD para, posteriormente, descubrir qué medidas de cumplimiento hay que tener en cuenta y a qué ámbitos de aplicación están sujetas.

Y, por último, se reflejará la importancia de tener establecido un Plan de Continuidad de Negocio: se analizará en qué consiste y cuáles son los actores principales, así como el procedimiento de recuperación de servicios y la realización de una labor de lecciones aprendidas.

El material didáctico consta de un total de **17 unidades**, dividiéndose en un primer bloque con **tres unidades transversales** y **cuatro bloques de especialidades** que contienen tres unidades las dos primeras especialidades y cuatro unidades las dos últimas especialidades, distribuidas como se muestran en la siguiente tabla:

Transversales	ESP 1	ESP 2	ESP3	ESP 4
Unidad 1	Unidad 4	Unidad 4	Unidad 4	Unidad 4
Unidad 2	Unidad 5	Unidad 5	Unidad 5	Unidad 5
Unidad 3	Unidad 6	Unidad 6	Unidad 6	Unidad 6
			Unidad 7	Unidad 7

Tabla 1. Estructura de las unidades didácticas

Estas unidades están interrelacionadas y su estudio es secuencial y progresivo.

Cada unidad se compone de contenido teórico y práctico, entre los que se incluyen vídeos dinámicos, *eLearnings* interactivos, pódcast, glosarios interactivos, infografías, cuestionarios tanto de evaluación como de autoevaluación, actividades de investigación y talleres.

Al principio del curso tendrás disponible un vídeo de bienvenida y, cada unidad contará con los siguientes recursos:

- Un **vídeo de presentación**, en el que te mostraremos brevemente el contexto de la unidad, así como los contenidos que se van a desarrollar en ella.
- **Píldoras interactivas** que explican los contenidos teóricos principales de la unidad. Aquí podrás encontrar vídeos explicativos dinámicos, pódcast, infografías y distintas preguntas de autoevaluación. Una vez completadas todas las píldoras de la unidad, se habilitará el acceso al cuestionario de evaluación de dicha unidad.
- Un **manual**, en formato PDF para descargar, donde encontrarás todo el contenido teórico de la unidad. Podrás descargar el manual una vez hayas finalizado y superado el cuestionario de evaluación de dicha unidad.
- Un **vídeo de conclusiones**, en el que se hará un breve repaso por los conceptos y los diferentes conocimientos que se han presentado y desarrollado a lo largo de la unidad.
- **Actividades de laboratorio y talleres**. Estos representan una simulación que puede tener lugar en un contexto profesional de un problema relacionado con diversos conceptos presentados a lo largo de

la unidad, con el fin de que, como alumno, realices un análisis de los entornos y máquinas virtuales, identificando la problemática o situación planteada y resolviéndola de manera óptima. Además, favorecen la capacidad de que el alumno comprenda e integre los conceptos y conocimientos adquiridos a lo largo de la unidad para comprender el funcionamiento de diferentes entornos y herramientas virtuales lo cual implica extraer información específica, saber diferenciar los aspectos relevantes y desarrollar la capacidad de aplicación a una situación profesional. Como consecuencia de ello, como alumno deberás desarrollar, de manera organizada y estructurada, el ejercicio práctico, dando respuesta a las cuestiones planteadas a resolver.

Las actividades de la parte práctica no se evalúan, por lo tanto, no cuentan para nota final del curso. No obstante, **recomendamos la realización de estas actividades para poner en práctica lo que has aprendido en la parte teórica**, además, se habilitarán los solucionarios para que puedas realizar tu propia evaluación de las actividades.

- **Actividades de investigación y análisis de la información.** Estas representan un caso real que te permitirá conocer, observar y evaluar en primera persona lo que sucede en el entorno social. Se tratan, además, de una estrategia pedagógica que desarrolla en el alumno la capacidad de identificación y análisis de los fenómenos y tendencias sociales a través de la observación y la investigación de la problemática planteada con el fin de ser un elemento de motivación que logra la conexión del aprendizaje teórico y práctico. Como consecuencia de ello, el alumno argumentará, de manera organizada y estructurada, su

explicación e interpretación de los diferentes aspectos presentados en el enunciado y dará respuesta a las cuestiones planteadas a resolver.

- Un **cuestionario de evaluación** que te permitirá conocer tu nivel de aprendizaje, verificando si has comprendido adecuadamente los contenidos de la unidad. Cada unidad didáctica incluye un cuestionario de evaluación con 20 preguntas. **Los cuestionarios deberán ser superados con un 75% de respuestas acertadas, tendrás 3 intentos para cada cuestionario y son obligatorios en todas las unidades, incluido el cuestionario final, y la encuesta de satisfacción si deseas obtener el certificado de superación del curso. No podrás acceder al cuestionario de una unidad sin haber finalizado el cuestionario de la unidad previa.**
- Las últimas unidades de cada especialidad son **unidades de conclusión**, en las que se recoge todos aquellos conceptos y términos, así como las ideas más relevantes de cada especialidad.

Al finalizar todas las unidades te propondremos un **examen final** que contiene 25 preguntas y que deberás superar con un 75% de respuestas correctas; al igual que en las unidades, este examen es **obligatorio** y tendrás 3 intentos para resolverlo. Asimismo, a la finalización de la formación deberás rellenar una **encuesta de satisfacción** para obtener el certificado de **superación del curso**.

3.1. Calendario del curso

El curso contempla una duración estimada en **250 horas** distribuidas en **17 semanas**, siendo la **fecha de inicio el 11 de abril** y la **fecha de finalización el 8 de agosto**. Para el curso, se seguirá una planificación orientativa que se indica a continuación [ver *Ilustración 1-5*].

A pesar de la flexibilidad que permite el curso, te sugerimos abordar los distintos elementos ajustándote a la secuencia de estudio recomendada. La estructura del contenido del curso es la siguiente:

Ejecución del curso durante 17 semanas (250 horas de curso)

Semana 1	Semana 2	Semana 3
<p>BLOQUE: UNIDADES TRANSVERSALES</p> <p>Unidad 1. Parte teórica (7h) Ejercicios prácticos – Laboratorios y talleres (1h) Actividades de investigación (3h) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: UNIDADES TRANSVERSALES</p> <p>Unidad 2. Parte teórica (6h) Ejercicios prácticos – Laboratorios y talleres (4h) Actividades de investigación (4h) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: UNIDADES TRANSVERSALES</p> <p>Unidad 3. Parte teórica (5h30min) Ejercicios prácticos – Laboratorios y talleres (2h) Actividades de investigación (4h) Test de evaluación (30 min) Participación en los foros (30min)</p>

Ilustración 1. Calendarización orientativa de la ejecución del curso Unidades transversales

Ejecución del curso durante 17 semanas (250 horas de curso)

Semana 4	Semana 5	Semana 6
<p>BLOQUE: ESPECIALIDAD 1 (ASC)</p> <p>Unidad 4. Parte teórica (8h30min) Ejercicios prácticos – Laboratorios y talleres (6h) Actividades de investigación (9h30min) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: ESPECIALIDAD 1 (ASC)</p> <p>Unidad 5. Parte teórica (8h) Ejercicios prácticos – Laboratorios y talleres (5h30min) Actividades de investigación (9h30min) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: ESPECIALIDAD 1 (ASC)</p> <p>Unidad 6*. CONCLUSIONES Parte teórica (2h) Test de evaluación (30 min)</p> <p><i>*Nota: Durante esta semana se habilita período para finalizar recursos pendientes de unidades anteriores</i></p>

Ilustración 2. Calendarización orientativa de la ejecución del curso Especialidad 1

Ejecución del curso durante 17 semanas (250 horas de curso)

Semana 7	Semana 8	Semana 9
<p>BLOQUE: ESPECIALIDAD 2 (ICI)</p> <p>Unidad 4. Parte teórica (7h30min) Ejercicios prácticos – Laboratorios y talleres (7h) Actividades de investigación (9h30min) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: ESPECIALIDAD 2 (ICI)</p> <p>Unidad 5. Parte teórica (7h30min) Ejercicios prácticos – Laboratorios y talleres (6h) Actividades de investigación (9h30min) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: ESPECIALIDAD 2 (ICI)</p> <p>Unidad 6*. CONCLUSIONES Parte teórica (2h) Test de evaluación (1h)</p> <p><i>*Nota: Durante esta semana se habilita período para finalizar recursos pendientes de unidades anteriores</i></p>

Ilustración 3. Calendarización orientativa de la ejecución del curso Especialidad 2

Ejecución del curso durante 17 semanas (250 horas de curso)

Semana 10	Semana 11	Semana 12	Semana 13
<p>BLOQUE: ESPECIALIDAD 3 (AIF)</p> <p>Unidad 4. Parte teórica (6h) Ejercicios prácticos – Laboratorios y talleres (2h) Actividades de investigación (7h) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: ESPECIALIDAD 3 (AIF)</p> <p>Unidad 5. Parte teórica (7h) Ejercicios prácticos – Laboratorios y talleres (4h) Actividades de investigación (5h) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: ESPECIALIDAD 3 (AIF)</p> <p>Unidad 6. Parte teórica (7h) Ejercicios prácticos – Laboratorios y talleres (2h) Actividades de investigación (7h) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: ESPECIALIDAD 3 (AIF)</p> <p>Unidad 7*. CONCLUSIONES Parte teórica (2h) Test de evaluación (1h)</p> <p><i>*Nota: Durante esta semana se habilita periodo para finalizar recursos pendientes de unidades anteriores</i></p>

Ilustración 4. Calendarización orientativa de la ejecución del curso Especialidad 3

Ejecución del curso durante 17 semanas (250 horas de curso)

Semana 14	Semana 15	Semana 16	Semana 17
<p>BLOQUE: ESPECIALIDAD 4 (CeC)</p> <p>Unidad 4. Parte teórica (7h30min) Ejercicios prácticos – Laboratorios y talleres (2h) Actividades de investigación (6h30min) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: ESPECIALIDAD 4 (CeC)</p> <p>Unidad 5. Parte teórica (7h) Ejercicios prácticos – Laboratorios y talleres (3h) Actividades de investigación (6h) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: ESPECIALIDAD 4 (CeC)</p> <p>Unidad 6. Parte teórica (5h30min) Ejercicios prácticos – Laboratorios y talleres (2h) Actividades de investigación (6h30min) Test de evaluación (30 min) Participación en los foros (30min)</p>	<p>BLOQUE: ESPECIALIDAD 4 (CeC)</p> <p>Unidad 7*. CONCLUSIONES Parte teórica (2h) Test de evaluación (1h) Test final (1h) Encuesta de satisfacción (1h)</p>

Ilustración 5. Calendarización orientativa de la ejecución del curso Especialidad 4

De acuerdo con esta planificación de carácter orientativo, te planteamos abordar una unidad de estudio por semana. En las siguientes tablas puedes consultar el temario del curso y los recursos formativos disponibles en cada unidad:

UNIDADES TRANSVERSALES

Introducción a la tecnología

UNIDAD 1

1. Presentación
 2. Introducción
 3. ¿Qué son las Tecnologías de la Información y la Comunicación (TIC)? ¿cuáles son sus inicios?
 4. Características y componentes de las TIC
 5. Evolución de las tecnologías de la información y la comunicación
 6. Tipos de infraestructuras tecnológicas ↓
 7. Servicios TI y nuevas tendencias
 8. Parte práctica
 9. Conclusiones
 10. Manual ↓
- Cuestionario de evaluación**

Aspectos básicos de ciberseguridad

UNIDAD 2

1. Presentación
 2. Seguridad de la información
 3. Riesgos para los sistemas de información
 4. Tipos de ciberdelincuentes
 5. El ciclo de vida de un ciberataque
 6. Tipos ataques
 7. Ciberseguridad en los entornos OT
 8. Métodos y tipos de protección
 9. Parte práctica
 10. Conclusiones
 11. Manual ↓
- Cuestionario de evaluación**

Aspectos avanzados de ciberseguridad

UNIDAD 3

1. Presentación
 2. *Hacking* ético
 3. Comandos básicos de Linux ↓
 4. Fases del *hacking* ético
 5. *Surface Web*, *Deep Web* y *Dark Web*
 6. Introducción a la informática forense
 7. Fases de la informática forense
 8. Introducción a la ingeniería inversa
 9. Criptografía
 10. Introducción al blockchain
 11. *Blockchain*: diccionario de términos
 12. *Blockchain*
 13. *Big data*
 14. Parte práctica
 15. Conclusiones
 16. Manual ↓
- Cuestionario de evaluación**

ESPECIALIDAD 1 - ASC

Administración de sistemas de ciberseguridad

UNIDAD 4

1. Presentación
 2. Planificación y administración de redes y direcciones IP
 3. Protocolos y herramientas de seguridad en redes
 4. Modelo de seguridad en redes ↓
 5. Principios básicos de la gestión de accesos
 6. Tipos o métodos de identificación ↓
 7. Gestión o control de accesos
 8. Sistemas de detección de *software* malicioso
 9. Cortafuegos
 10. Sistemas de detección y protección contra intrusiones
 11. Sistemas de detección y gestión de eventos de seguridad
 12. Principales ataques a redes
 13. Modelo de seguridad por capas
 14. Buenas prácticas para el bastionado de sistemas ↓
 15. Parte práctica
 16. Conclusiones
 17. Manual ↓
- Cuestionario de evaluación**

Seguridad en la administración de sistemas

UNIDAD 5

1. Presentación
2. Administración de sistemas operativos
3. Administración de procesos del sistema
4. Administración de sistemas gestores de bases de datos
5. Servicios de Red e Internet
6. Aplicaciones de autenticación [↓](#)
7. Seguridad en el correo electrónico
8. Seguridad web
9. Seguridad en *cloud*
10. Seguridad y gestión de dispositivos IoT
11. Seguridad y alta disponibilidad
12. Parte práctica
13. Conclusiones
14. Manual [↓](#)

Questionario de evaluación

Conclusiones

UNIDAD 6

Actividad en plataforma

ESPECIALIDAD 2 - ICI

Sistemas de control y automatización industrial, protocolos más utilizados y sus vulnerabilidades

UNIDAD 4

1. Presentación
2. La evolución de la industria [↓](#)
3. La industria 4.0
4. Seguridad en protocolos industriales
5. Topologías de red
6. Principales protocolos de comunicación industrial
7. Reconocimiento de redes OT
8. Vulnerabilidades OT
9. Vulnerabilidades: Modelos de defensa
10. *Industrial Internet of Things* (IIoT)
11. Infraestructuras críticas
12. Parte práctica
13. Conclusiones
14. Manual [↓](#)

Cuestionario de evaluación

Introducción a la ciberseguridad industrial

UNIDAD 5

1. Presentación
2. Convergencia IT/OT [↓](#)
3. Principales ataques ciberindustriales
4. Situación actual en la ciberseguridad industrial
5. Estándares de ciberseguridad industrial
6. Ciclo PDCA [↓](#)
7. Topologías de red segura de OT
8. Herramientas de protección de un entorno OT [↓](#)
9. Herramientas de protección de un entorno OT: inventario de activos
10. Herramientas de protección de un entorno OT: SIEM
11. Herramientas de protección de un entorno OT: IDS e IPS
12. Herramientas de protección de un entorno OT: *firewall* y antivirus
13. Herramientas de protección de un entorno OT: *honeypot* industrial, sistemas EDR y XDR
14. Herramientas de protección de un entorno OT: SOC y NOC
15. Pronóstico de seguridad industrial
16. Parte práctica
17. Conclusiones
18. Manual [↓](#)

Cuestionario de evaluación

Conclusiones

Actividad en plataforma

UNIDAD 6

ESPECIALIDAD 3 – AIF

Análisis de incidentes

1. Presentación
2. Introducción
3. ¿Cuáles son los equipos de gestión de incidentes?
4. Fases en la respuesta ante incidentes
5. Buenas prácticas en la gestión de incidentes
6. Herramientas en la gestión de incidentes
7. Marco de gestión
9. Plan de Continuidad del Negocio (BCP)
10. Plan de Recuperación ante Desastres (DRP)
11. Tipos de planes en función de su alcance ↓
12. Parte práctica
13. Conclusiones
14. Manual ↓

UNIDAD 4

Cuestionario de evaluación

Análisis forense

UNIDAD 5

1. Presentación
2. Introducción
3. Fases en la investigación forense. Fase 1
4. Fases en la investigación forense. Fase 2
5. Fases en la investigación forense. Fase 3
6. Fases en la investigación forense. Fase continua
7. Análisis de *malware*
8. Análisis especiales
9. Metodología forense
Metodología EC-COUNCIL (CHFI) ↓
10. Parte práctica
11. Conclusiones
12. Manual ↓

Questionario de evaluación

Análisis forense en dispositivos móviles

UNIDAD 6

1. Presentación
2. Introducción
3. Dispositivos Android y iOS
4. Obtención de datos
5. Tipos de vulnerabilidades
6. Aprovechamiento de vulnerabilidades y ataques comunes
7. Artefactos en investigación forense en dispositivos móviles
8. Diferencias entre análisis forense a un ordenador y a dispositivos móviles ↓
9. Proceso de análisis de evidencias
10. Adquisición de evidencias del dispositivo
11. Métodos de obtención de la información
12. Herramientas para la adquisición de evidencias del dispositivo
13. Vulnerabilidades OWASP
14. Métodos de adquisición de evidencias y documentación
15. Informe final
16. Buenas prácticas y normativa
17. Parte práctica
17. Conclusiones
18. Manual ↓

Cuestionario de evaluación

Conclusiones

UNIDAD 7

Actividad en plataforma

ESPECIALIDAD 4 – CeC

**Compliance. Las
normas son
importantes**

UNIDAD 4

1. Presentación
2. Introducción
3. ¿Qué son las normas?
4. ¿Qué es la estandarización?
5. El riesgo en los sistemas de gestión y las normas de estandarización internacionales ↓
6. Principales normativas: introducción
7. Principales normativas: Directiva NIS
8. Principales normativas: RGDP y ENS
9. Principales normativas: Ley PIC
10. Principales normativas: LOPDGDD y LSSI
11. Los estándares ISO ↓
12. Principales normativas: ISO 27001
13. Principales normativas: ISO 22301, ISO 27701, ISO 37301 e ISO 31000
14. Afectación de las principales normativas al ciclo de vida de los servicios
15. ISO 27001: Objetivos de control y controles ↓
16. Parte práctica
17. Conclusiones
18. Manual ↓

Cuestionario de evaluación

Protección de datos y cumplimiento de RGPD

UNIDAD 5

1. Presentación
2. Introducción
3. Ciclo de vida de los datos
4. AEPD, LOPD, RGPD y LOPDGDD
5. Principales diferencias entre LOPD y RGPD ↓
6. Aplicación del RGPD
7. Derechos ARCO-POL
8. Figuras relevantes
9. Medidas de cumplimiento
10. Infracciones y sanciones por incumplimiento
11. Garantías de los derechos digitales
12. Estándar normativo ISO 27701
13. Parte práctica
14. Conclusiones
15. Manual ↓

Cuestionario de evaluación

La importancia de la continuidad de negocio

UNIDAD 6

1. Presentación
2. Introducción
3. Diccionario de términos
4. Beneficios de tener elaborado un Plan de Continuidad de
5. Actores que conforman la continuidad
Niveles de respuesta ante incidentes ↓
6. ¿Qué es la continuidad de negocio?
7. Fases de un Plan de Continuidad de Negocio. Fase 0
8. Fases de un Plan de Continuidad de Negocio. Fase 1
9. Fases de un Plan de Continuidad de Negocio. Fase 2 y 3
10. Fases de un Plan de Continuidad de Negocio. Fase 4 y 5
11. Tipos de contingencia existentes y cómo abordarlas
12. Lecciones aprendidas
13. Parte práctica
14. Conclusiones
15. Manual ↓

Cuestionario de evaluación

Conclusiones

Actividad en plataforma

UNIDAD 7

Examen final

Examen final

Encuesta de satisfacción

Encuesta de satisfacción

4 GUÍA DE USO DE LA PLATAFORMA

4.1. Registro en la plataforma

El acceso al curso se realiza desde la URL del aula virtual:

<https://formacion-incibe.es/login/index.php>

Este enlace te redirigirá directamente a la siguiente pantalla:

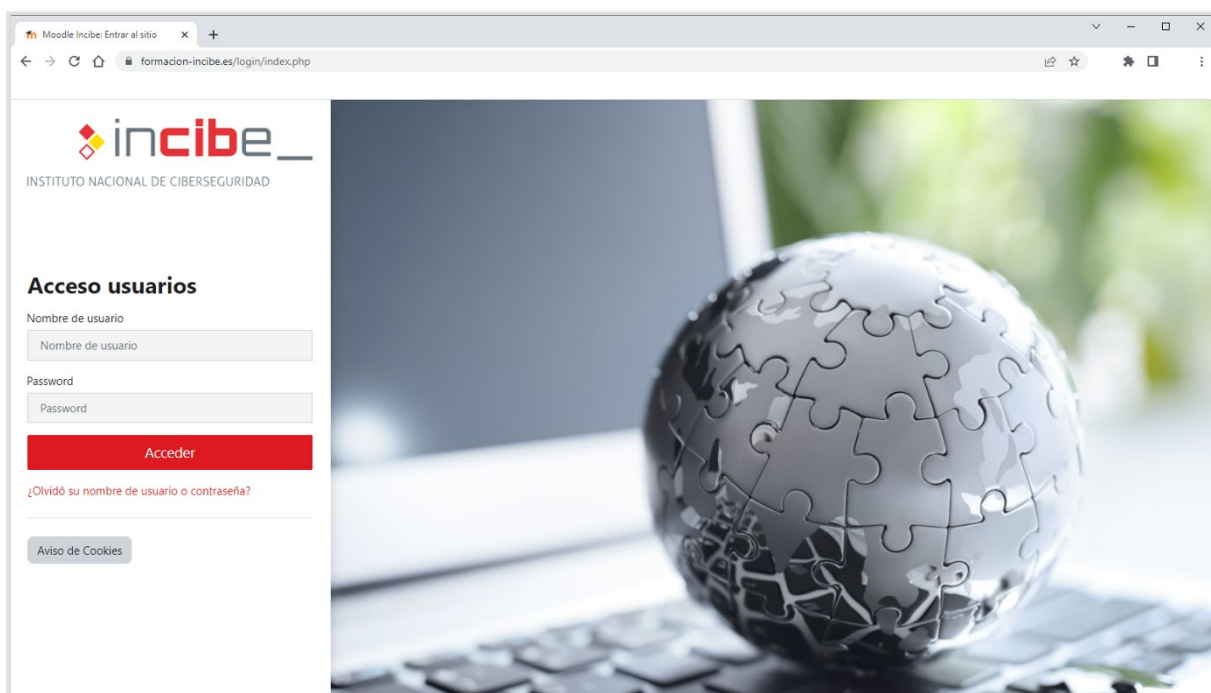


Ilustración 6. Interfaz de acceso a la plataforma Moodle

Para acceder a la plataforma debes utilizar las credenciales que recibirás por correo electrónico al inicio de la formación. El usuario y contraseña provisional sirven para acceder por vez primera a la plataforma Moodle, recomendándote cambiar la contraseña en ese momento.

4.2. Acceso a los contenidos

La primera vez que accedas con tus claves de usuario, aparece la ventana principal de la plataforma, en la que encontrarás el «Curso básico técnico de ciberseguridad», en el que estás matriculado.

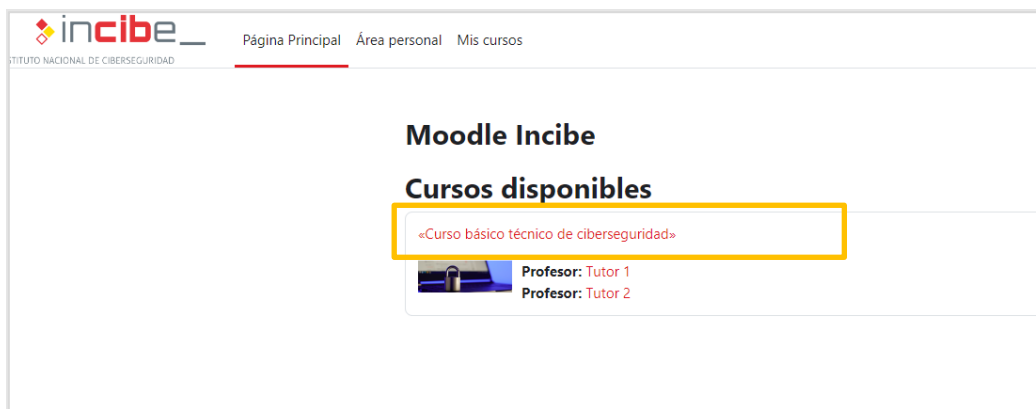


Ilustración 7. Ventana principal de la plataforma

Puedes acceder al curso indicado, seleccionando la propia imagen del curso. Una vez dentro se muestran los contenidos por unidades temáticas en el centro de la interfaz.

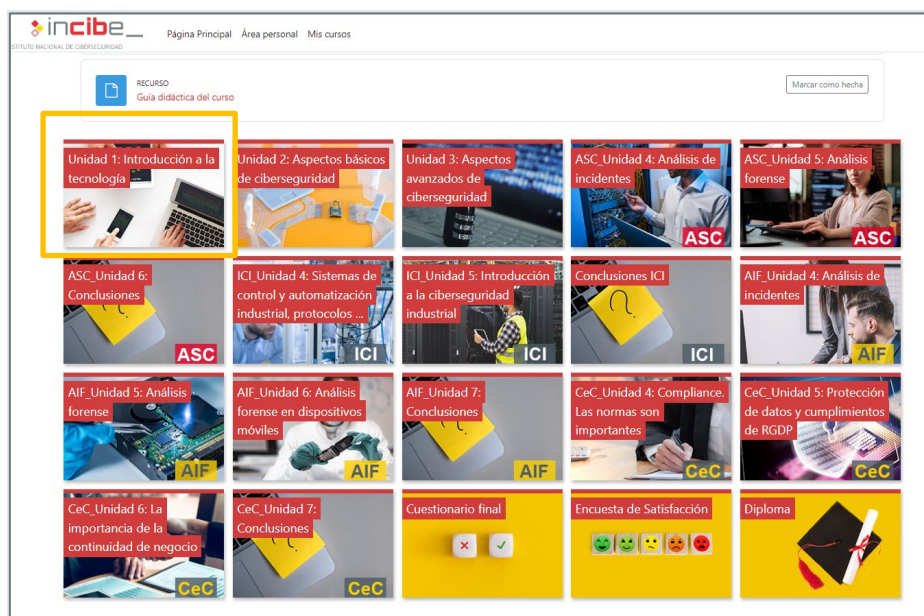


Ilustración 8. Contenido didáctico en formato mosaico

Al seleccionar una unidad, se despliegan los recursos formativos que la integran.

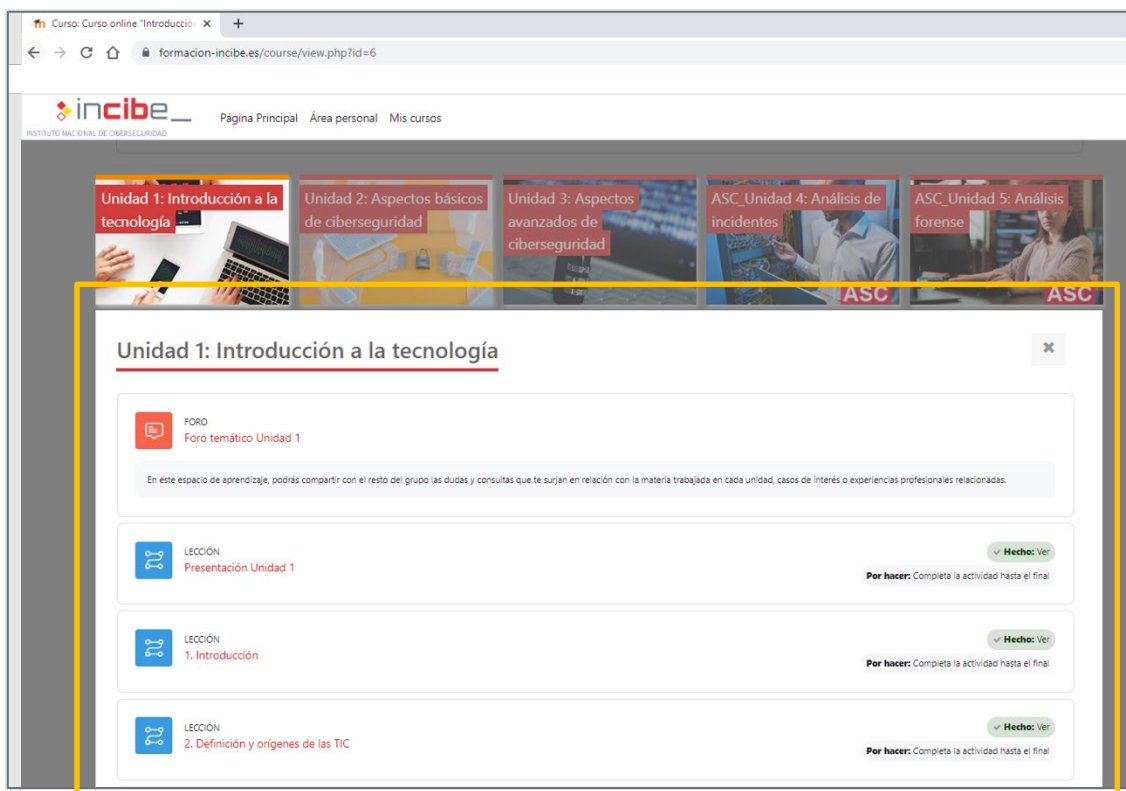


Ilustración 9. Lista de recursos en una unidad

Cada elemento de aprendizaje se asocia con un icono que te permite reconocer qué tipo de recurso didáctico es, a modo de ejemplo:



Al lado de cada recurso aparece un resalte en verde que te indica si has completado el recurso de aprendizaje.

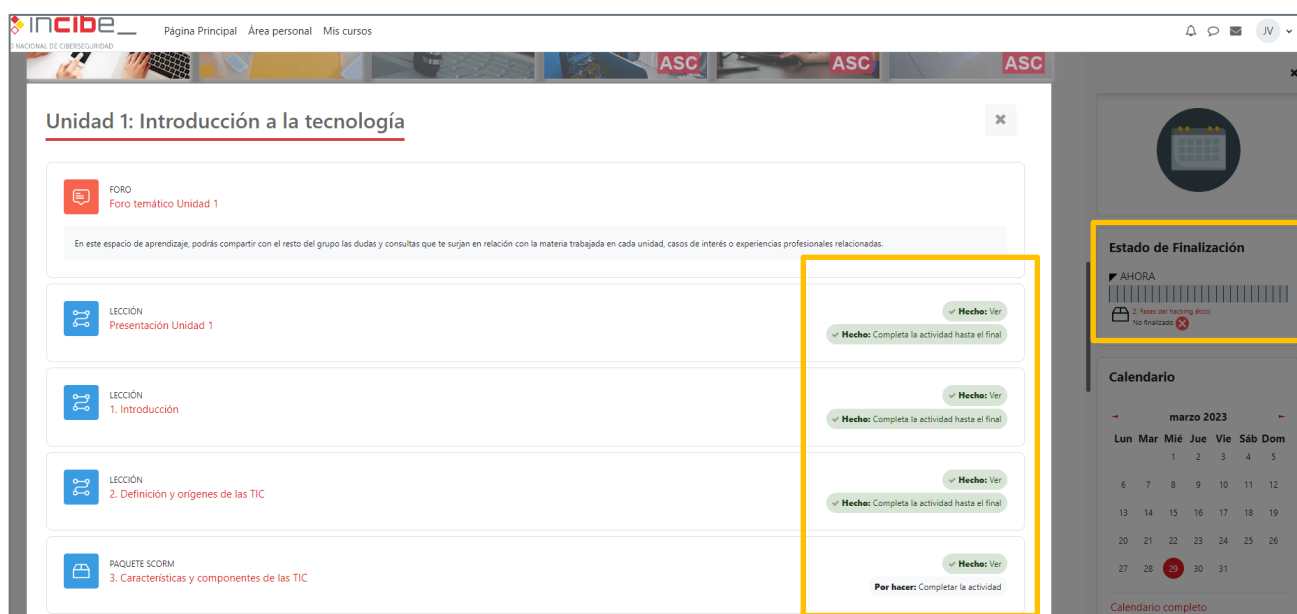


Ilustración 10. Lista de comprobación finalización de recursos y estado de finalización

Recuerda que debes **aprobar el cuestionario** de cada unidad para poder acceder al cuestionario de la siguiente.

4.3. Participación en los foros

Al principio de cada unidad se habilita un foro donde podrás plantear tus dudas acerca de una temática o hacer recomendaciones.

Para cualquier cuestión en relación con el **funcionamiento del curso**, te recomendamos utilizar el foro «**Uso técnico de la plataforma**». Para estar al día de información general del curso, deberás consultar el foro «**Novedades/publicaciones del tutor**», en este foro no podrás generar debates ni comunicaciones, pero sí comentar al hilo de las publicaciones del tutor.

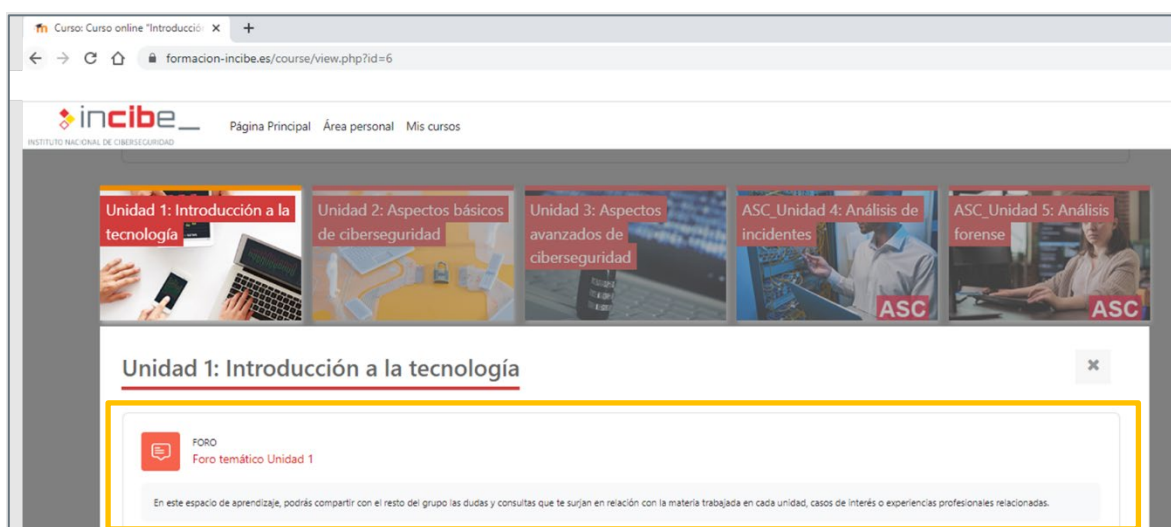


Ilustración 11. Foro temático en una unidad

El **chat «Cafetería»** es un espacio donde podrás compartir con el resto de los compañeros tus puntos de vista, inquietudes, casos reales, experiencias, etc. relacionados con la ciberseguridad. Es un espacio dirigido a generar sinergias y crear compañerismo durante el desarrollo del curso. Se establecerán días de debate que podrás revisar desde el calendario.

¡Importante! La participación en los foros es de carácter obligatorio para conseguir el certificado de aprovechamiento.

4.4. Bloques del curso

Durante el curso tendrás acceso a diferentes bloques, por defecto en la página principal del curso aparecen ocultos, puedes acceder a ellos de la siguiente manera:

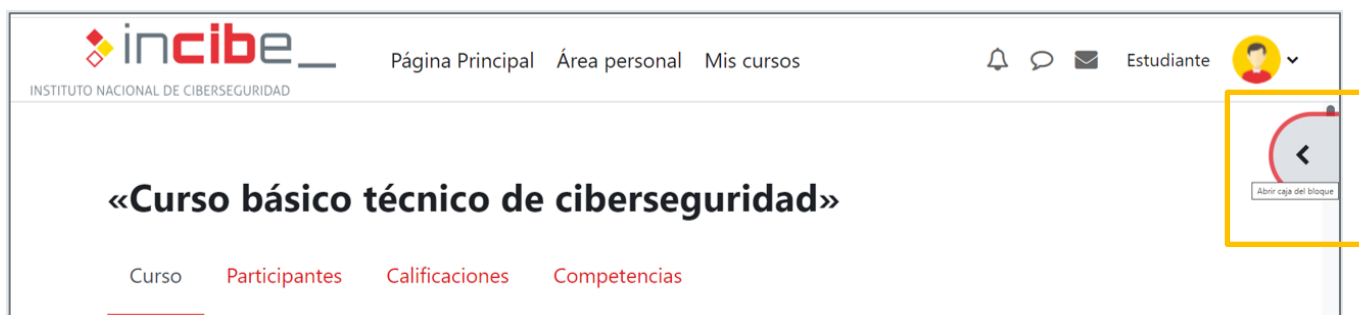


Ilustración 12. Acceso a los bloques del curso

Si haces clic en la pestaña del lateral derecho de la interfaz, se desplegarán todos los bloques disponibles en el curso que, a continuación, explicaremos.

4.5. Calendario

En el bloque de calendario que aparece a la izquierda de la interfaz y podrás consultar fechas y eventos importante durante el desarrollo del curso, esto te permitirá estar al día y seguir el ritmo marcado por la planificación orientativa.



Ilustración 13. Bloque Calendario

4.6. Consultas desde el área personal

Desde el área personal podrás realizar tareas como la consulta de calificaciones o el envío de mensajes mediante el correo interno de la plataforma.

Para consultar las calificaciones de tu expediente virtual, debes seleccionar la opción «Calificaciones» [ver *Ilustración 14*]. Desde este apartado podrás consultar los resultados obtenidos en cada cuestionario de evaluación de las unidades y en la prueba final.

Para enviar un mensaje [ver *Ilustración 14*] deberás seleccionar al destinatario entre la lista de contactos o buscar alguna conversación o notificación más

reciente. Puedes utilizar esta opción para consultar con el personal docente cualquier duda referente al curso.

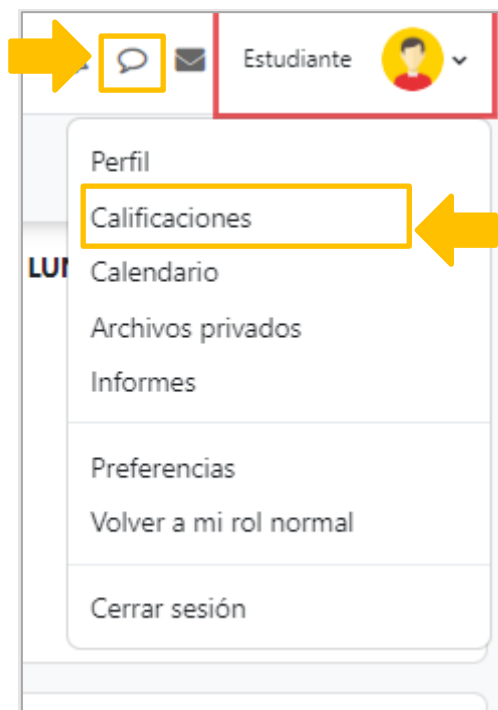


Ilustración 14. Calificaciones y mensajería

4.7. Dinámica de gamificación

4.7.1. ¡Subes de nivel!

A lo largo del curso irás obteniendo puntos por cada recurso de aprendizaje visualizado o realizado (contenido teórico, vídeos, descarga de archivos, cuestionarios de evaluación, actividades de aprendizaje, etc.) y en función de la puntuación acumulada, irás subiendo de nivel. Recuerda que estos puntos de experiencia no afectan a tu nota final del curso.

No todos los recursos tienen la misma puntuación, sino que varían en función de la complejidad de los materiales y del esfuerzo que debes realizar.

Recurso	Puntos
Infografía / Manual / Documento .pdf	5 pts
Vídeos / <i>e-learning</i> interactivo / Actividad H5P	10 pts
Cuestionarios de evaluación de las unidades	15 pts
Recurso Tarea	15 pts
Examen final	40 pts
Encuesta de satisfacción	40 pts

Ilustración 15. Distribución de puntos de experiencia

La información sobre tu progreso, nivel de puntos obtenidos (hay 18 niveles) y posición en el *ranking*, se encuentra en el bloque «¡Subes de nivel!» (situado en el margen derecho de la interfaz).

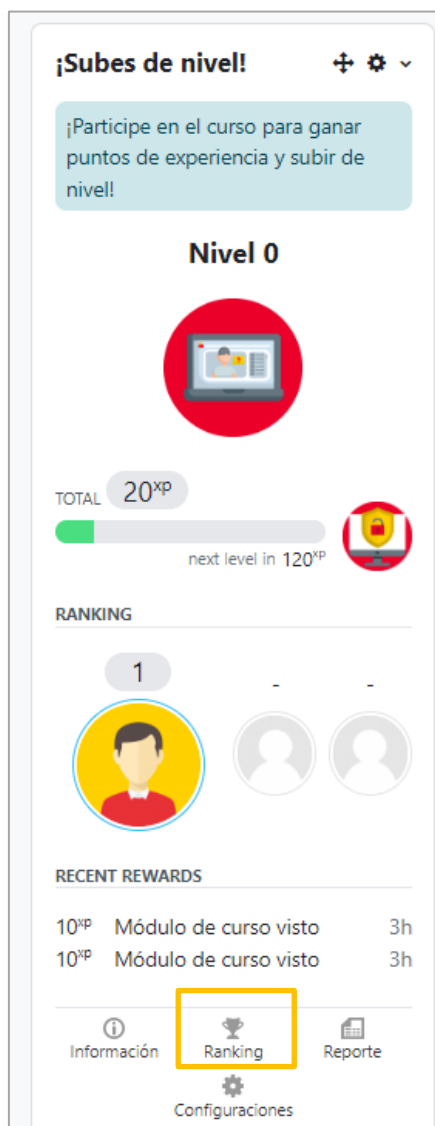


Ilustración 16. Bloque ¡Subes de nivel!

Además, para conocer en qué posición te encuentras con respecto al resto de compañeros, basta con pulsar sobre la pestaña «*Ranking*» dentro del bloque «¡Subes de nivel!».



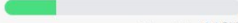
Ranking	Nivel	Participant	Total	Progreso
1		 Usuario	30 ^{xp}	 next level in 110 ^{xp}

Ilustración 17. Ranking bloque «¡Subes de nivel!»

Cada vez que superes el número de puntos otorgados a cada uno de los niveles, aparece una ventana emergente, que te informará del nuevo nivel alcanzado.

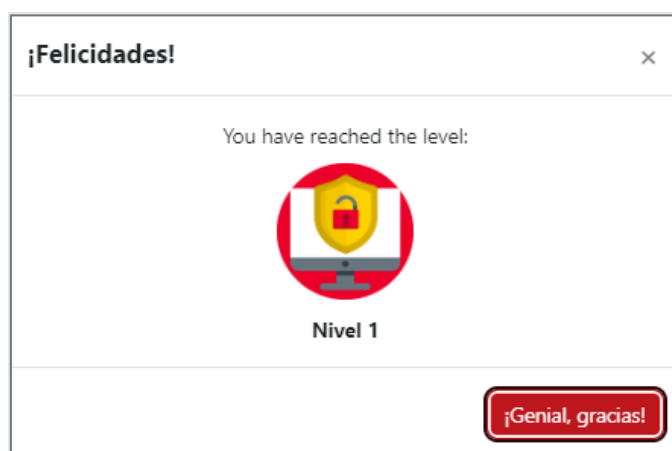


Ilustración 18. Notificación subida de nivel

4.7.2. Recompensa por insignias

Las insignias se utilizarán para celebrar tus logros y progreso en el curso. En total puedes conseguir un total de **6 insignias** que corresponde con la superación de diferentes contenidos:



Unidades transversales	
ASC: administración de sistemas de ciberseguridad	
ICI: introducción a la ciberseguridad industrial	
AIF: análisis de incidentes y forense	
CeC: compliance	
Examen final	

Ilustración 19. Insignias del curso

Como puedes ver en la *Ilustración 19* cada insignia se otorga a la finalización de los diferentes bloques formativos y una extra por la finalización del examen final. **La consecución de estas insignias no se tiene en cuenta para evaluación.**

EVALUACIÓN Y CERTIFICACIÓN

Al final de cada unidad, tendrás disponible un **cuestionario de evaluación** con 10 preguntas. Este cuestionario te permitirá evaluar tu progreso y comprensión de los contenidos, así como poder identificar tus áreas de fortaleza y debilidades en relación con el material del curso.

En cada cuestionario de evaluación tendrás **tres intentos de realización**, manteniéndose la nota más alta de estos tres intentos y en el caso del **cuestionario final** contarás con **dos intentos**. La nota mínima que debes obtener para superar cada unidad y el examen final es de 7,5 puntos.

Para que puedas optar al **certificado** personalizado de aprovechamiento del curso, tendrás que **haber superado todos los cuestionarios de evaluación** con la nota mínima (incluido el examen final), es decir, haber obtenido **al menos un 75% de las respuestas correctas y haber completado la encuesta de satisfacción** del curso.

El certificado estará disponible para su descarga directamente en la plataforma una vez se finalice el curso y se hayan cumplido todos los requisitos de evaluación establecidos.

TUTORÍAS Y OTROS DATOS DE CONTACTO

Tutorías: Las preguntas relacionadas con el manual teórico, actividades prácticas, cuestionarios o cualquier otro contenido del curso, se tratarán en los distintos **foros de participación** y colaboración habilitados en cada unidad, o a través del servicio de mensajería interna, poniéndote directamente en contacto con el tutor para las cuestiones más específicas, podrás hacerlo en el siguiente horario:

- Horario de atención tutorial: **8:30 a 17:30** horas de **lunes a jueves** y de **8:00 a 15:00** los **viernes**.

En caso de **pérdida u olvido de la contraseña**, deberás contactar con formacion-incibe@dicampus.es en horario de lunes a viernes de 8:00h a 19:00h (hora peninsular).

Las incidencias o problemas que pudieran surgir respecto al **funcionamiento general de la plataforma en lo relativo a su rendimiento o disponibilidad**, debes comunicarlás a través del foro «**Uso técnico de la plataforma**» o por mensajería privada directamente al Tutor.