

PROGRAMACIÓN DIDÁCTICA

Departamento: **Informática**

Curso de especialización:

**Ciberseguridad en entornos de las tecnologías
de la información.**

Módulo: ***Bastionado de redes y sistemas***

Profesor/es: **María Felisa Aldea Jiménez**

Año académico: *2024-2025*

Índice

1.- UNIDADES DE COMPETENCIA ASOCIADA/S AL MÓDULO	3
2.- COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES DEL TÍTULO A LAS QUE CONTRIBUYE EL MÓDULO	3
3.- OBJETIVOS.....	4
3.1.-OBJETIVOS GENERALES DEL TÍTULO QUE DESARROLLA EL MÓDULO	4
3.2.-OBJETIVOS EXPRESADOS EN RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN	4
4.- CONTENIDOS DEL MÓDULO Y DISTRIBUCIÓN TEMPORAL.....	8
5.- METODOLOGÍA DIDÁCTICA.....	10
5.1.-ESTRATEGIAS DE ENSEÑANZA-APRENDIZAJE	10
5.2.-ATENCIÓN A LA DIVERSIDAD.....	10
5.3.-MATERIALES Y RECURSOS DIDÁCTICOS	10
5.4.-LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)	11
5.5.-ACTIVIDADES INTERDISCIPLINARES	11
6.- PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN	12
7.- CRITERIOS DE CALIFICACIÓN	12
8.- PÉRDIDA DE EVALUACIÓN CONTINUA	13
9.- PLANIFICACIÓN DE LAS ACTIVIDADES DE RECUPERACIÓN	13
9.1.-SISTEMA DE RECUPERACIÓN DE EVALUACIONES SUSPENSAS	13
10.-CONTRIBUCIÓN DEL MÓDULO A FOMENTAR LA CULTURA Y EL ESPÍRITU EMPRENDEDOR EN EL ALUMNADO.....	14
11.-COMPETENCIAS Y CONTENIDOS DE CARÁCTER TRANSVERSAL ..	14
12.-PROCEDIMIENTO DE RECLAMACIÓN DE LAS CALIFICACIONES	14
13.-ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES RELACIONADAS CON EL MÓDULO	14
14.-MEDIDAS PARA ESTIMULAR EL INTERÉS Y HÁBITO DE LECTURA Y LA CAPACIDAD DE EXPRESARSE CORRECTAMENTE	15

1 UNIDADES DE COMPETENCIA ASOCIADA/S AL MÓDULO

2 COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES DEL TÍTULO A LAS QUE CONTRIBUYE EL MÓDULO

Según el *Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo*, las competencias profesionales, personales y sociales que se desarrollarán en este módulo serán el c, d, e, l, m, n y ñ.

c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.

d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.

e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.

l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.

m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.

n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.

ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

3 OBJETIVOS

3.1 OBJETIVOS GENERALES DEL TÍTULO QUE DESARROLLA EL MÓDULO

Según el *Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo*, los Objetivos generales que se persiguen con este módulo son el e,f,g,h,i,y j

- e) Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.
- f) Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.
- g) Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.
- h) Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.
- i) Configurar dispositivos de red para cumplir con los requisitos de seguridad.
- j) Administrar la seguridad de sistemas informáticos en red aplicando las políticas de seguridad requeridas para garantizar la funcionalidad necesaria con el nivel de riesgo de red controlado.

3.2 OBJETIVOS EXPRESADOS EN RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN

1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.

Criterios de evaluación:

- a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.
- b) Se ha evaluado las medidas de seguridad actuales.
- c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización
- d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.
- e) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.
- f) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización.

2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.

Criterios de evaluación:

- a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.
- b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.
- c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.
- d) Se han definido protocolos y políticas de autenticación basados en *tokens*, *OTPs*, etc., en base a las principales vulnerabilidades y tipos de ataques.
- e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.

3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.

Criterios de evaluación:

- a) Se han identificado los tipos de credenciales más utilizados.
- b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
- c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio *web*.
- d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.
- e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo *RADIUS - Remote Access Dial In User Service*)

4. Diseña redes de computadores contemplando los requisitos de seguridad.

Criterios de evaluación:

- a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.
- b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (*VLANs*).

- c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de *subnetting* para incrementar su segmentación respetando los direccionamientos existentes.
- d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (*routers*, puntos de acceso, etc.).
- e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.

5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.

Criterios de evaluación:

- a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
- b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
- c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (*Logs*), de un cortafuego.
- d) Se han implementado contramedidas frente a comportamientos no deseados en una red.
- e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.

Criterios de evaluación:

- a) Se ha configurado la *BIOS* para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.
- b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.
- c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.
- d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.
- e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.

7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.

Criterios de evaluación:

- a) Se han enumerado y eliminado los programas, servicios y protocolos

- b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.
- c) Se ha incrementado la seguridad del sistema de administración remoto *SSH* y otros.
- d) Se ha instalado y configurado un Sistema de detección de intrusos en un *Host (HIDS)* en el sistema informático.
- e) Se han instalado y configurado sistemas de copias de seguridad.

4 CONTENIDOS DEL MÓDULO Y DISTRIBUCIÓN TEMPORAL

Contenidos del módulo:

Diseño de planes de securización:

- Análisis de riesgos.
- Principios de la Economía Circular en la Industria 4.0.
- Plan de medidas técnicas de seguridad.
- Políticas de securización más habituales.
- Guías de buenas prácticas para la securización de sistemas y redes.
- Estándares de securización de sistemas y redes.
- Caracterización de procedimientos, instrucciones y recomendaciones.
- Niveles, escalados y protocolos de atención a incidencias.

Configuración de sistemas de control de acceso y autenticación de personas:

- Mecanismos de autenticación. Tipos de factores.
- Autenticación basada en distintas técnicas:

Administración de credenciales de acceso a sistemas informáticos:

- Gestión de credenciales.
- Infraestructuras de Clave Pública (*PKI*).
- Acceso por medio de Firma electrónica.
- Gestión de accesos. Sistemas NAC (*Network Access Control*, Sistemas de Gestión de Acceso a la Red).
- Gestión de cuentas privilegiadas.
- Protocolos *RADIUS* y *TACACS*, servicio *KERBEROS*, entre otros.

Diseño de redes de computadores seguras:

- Segmentación de redes.
- *Subnetting*.
- Redes virtuales (*VLANs*).
- Zona desmilitarizada (*DMZ*).
- Seguridad en redes inalámbricas (*WPA2*, *WPA3*, etc.).
- Protocolos de red seguros (*IPSec*, etc.).

Configuración de dispositivos y sistemas informáticos:

- Seguridad perimetral. Firewalls de Próxima Generación.
- Seguridad de portales y aplicativos web. Soluciones *WAF* (*Web Application Firewall*).
- Seguridad del puesto de trabajo y endpoint fijo y móvil. *AntiAPT*, antimalware.
- Seguridad de entornos cloud. Soluciones *CASB*.
- Seguridad del correo electrónico
- Soluciones *DLP* (*Data Loss Prevention*)

-
- Herramientas de almacenamiento de logs.
 - Protección ante ataques de denegación de servicio distribuido (*DDoS*).
 - Configuración segura de cortafuegos, enrutadores y proxies.
 - Redes privadas virtuales (*VPNs*), y túneles (protocolo *IPSec*).
 - Monitorización de sistemas y dispositivos.
 - Herramientas de monitorización (*IDS*, *IPS*).
 - *SIEMs* (Gestores de Eventos e Información de Seguridad).
 - Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: *NOCs* y *SOCs*.

Configuración de dispositivos para la instalación de sistemas informáticos:

- Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la *BIOS*, bloqueo del orden de arranque de los dispositivos, entre otros.
- Seguridad en el arranque del sistema informático, configuración del arranque seguro.
- Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.

Configuración de los sistemas informáticos:

- Reducción del número de servicios, *Telnet*, *RSSH*, *TFTP*, entre otros.
- *Hardening* de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar *exploits*, etc.).
- Eliminación de protocolos de red innecesarios (*ICMP*, entre otros).
- Securitización de los sistemas de administración remota.
- Sistemas de prevención y protección frente a virus e intrusiones (antivirus, *HIDS*, etc.).
- Configuración de actualizaciones y parches automáticos.
- Sistemas de copias de seguridad.
- *Shadow IT* y políticas de seguridad en entornos *SaaS*.

Los contenidos del módulo se distribuirán durante 20 semanas, realizándose una evaluación cada 10 semanas.

5 METODOLOGÍA DIDÁCTICA

5.1 ESTRATEGIAS DE ENSEÑANZA-APRENDIZAJE

En cada unidad de trabajo, el profesor, realizará la exposición verbal con abundante soporte gráfico y demos prácticas de los puntos fundamentales que componen la unidad temática acompañada de numerosos ejemplos prácticos de aplicación. Se utilizará el bloc de notas de aula en la plataforma virtual TEAMS como repositorio de los materiales teóricos y prácticos del módulo.

Durante el trabajo en el aula, que incluirá necesariamente la realización de abundantes prácticas con y sin soporte informático, el profesor actuará como asesor intentando orientar las tareas de autoaprendizaje en lugar de facilitar directamente la solución a los problemas planteados. Se trata de conseguir que el alumno participe en la elaboración de los procesos conducentes a su propia instrucción creando así el marco de referencia adecuado para la generación de situaciones de aprendizaje significativo.

Siempre que el nivel de autonomía y motivación del alumnado lo permita, se tratará de realizar un ABP en coordinación con el resto de las docentes del curso cuyo producto final sea un plan de securización de los sistemas informáticos del centro educativo, así como su implementación total o parcial.

La distribución de los espacios en el aula será flexible, pero dando tratamiento de preferencia a las agrupaciones de trabajo de dos o tres miembros sobre todo para las fases de resolución de tareas propuestas.

Para la realización de prácticas, se utilizará un entorno de máquinas virtuales, mediante la aplicación de software libre VirtualBox así como los materiales de red necesarios como switches configurables, puntos de acceso wifi... etc. Para la gestión de tareas y comunicaciones se utilizarán las herramientas office365 centralizadas en la plataforma virtual TEAMS.

5.2 ATENCIÓN A LA DIVERSIDAD

Tanto los criterios de evaluación como los procedimientos de evaluación descritos en los apartados anteriores se adaptarán al alumnado con necesidades educativas especiales, o con algún tipo de discapacidad, siguiendo las directrices marcadas por los informes de evaluación psicopedagógica proporcionados por el equipo de orientación.

Estas adaptaciones siempre deberán garantizar la accesibilidad a las pruebas de evaluación por parte de los mencionados alumnos, y podrán ser, entre otras, la modificación en el soporte de realización del examen o prueba, ampliación del tiempo disponible para su realización, modificación del formato de alguna prueba, modificación de alguna práctica en concreto, etc.

5.3 MATERIALES Y RECURSOS DIDÁCTICOS

Libro digital creado en el bloc de notas de clase, en el cual se incluirán los contenidos teóricos y prácticos del módulo.

5.4 LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)

Se empleará la plataforma TEAMS como aula virtual (comunicación, tareas, cuaderno de calificaciones...etc), y diferentes herramientas de la suite office365 para la elaboración de materiales y evaluación del alumnado.

5.5 ACTIVIDADES INTERDISCIPLINARES

En función del grado de coordinación con el equipo docente y del grado de implicación y autonomía del alumnado, se analizará la posibilidad de realizar actividades o proyectos interdisciplinarios durante el curso.

6 PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN

La evaluación del alumnado se realizará mediante:

- Evaluación de prácticas individuales o grupales entregadas en la plataforma virtual o guardadas en el cuaderno digital del alumno.
- Evaluación de pruebas teórico y prácticas realizadas en el aula.
- En caso de realizarse un ABP, valoración de su desarrollo y producto final obtenido.
- Observación de la actitud y comportamiento del alumnado.

6.1 CRITERIOS DE CALIFICACIÓN

A.- DE CADA EVALUACIÓN

Cada una de las evaluaciones trimestrales del curso se calificará mediante:

- Realización de los trabajos propuestos en clase y entrega de estos en los plazos previstos. Serán valorados entre 1 y 10 puntos, siendo estos acumulativos para la nota de evaluación, con una ponderación del 50 % de dicha nota. La no realización en el plazo previsto de uno de los trabajos propuestos por el profesor, sin una causa justificada, u obtener una calificación inferior a 5 en un trabajo, supondrá el suspenso en la evaluación y por tanto de la nota final.
- Los exámenes que se realicen en la evaluación trimestral tendrán peso específico del 50% de la nota final de dicha evaluación. La nota final de este apartado se obtendrá como la nota media de los exámenes aprobados, siendo necesario obtener al menos un 5 en cada examen para poder hacer media y superar la evaluación.
- Las faltas ortográficas encontradas en los trabajos entregados, y en los exámenes, serán valoradas negativamente en los mismos hasta un máximo del 10% del total de la calificación, y dicha nota negativa podrá ser recuperada a través de las actividades de lectura y redacción propuestas por el profesor.
- En el caso de trabajar parte de los contenidos mediante ABP, la calificación obtenida en el proyecto será equivalente a la que se obtendría mediante prácticas y exámenes para calificar dichos contenidos.

NOTA:

- Todas las pruebas escritas, orales, individuales o en grupo que hayan sido copiadas bien en parte bien en su totalidad, serán calificadas con cero puntos.

-

B.- DEL CURSO COMPLETO

Para aprobar el módulo se requiere tener una calificación de al menos cinco puntos sobre diez en cada una de las evaluaciones trimestrales. La nota final se obtendrá como la media aritmética de las calificaciones obtenidas en las evaluaciones trimestrales.

Además de los exámenes realizados en cada evaluación, existirá una prueba final en mayo y otra en junio para:

- Alumnos que han perdido el derecho a evaluación continua
- Alumnos que tengan suspensas algunas de las evaluaciones trimestrales. En marzo, recuperaran sólo las evaluaciones trimestrales que tengan pendientes.
- En la segunda convocatoria ordinaria de junio, los alumnos se examinarán de todos los contenidos del módulo, aunque tuvieran alguna evaluación trimestral aprobada.

Es necesario tener entregados todos los trabajos prácticos del curso para poder optar a realizar las pruebas de recuperación de marzo y junio.

6.2 PÉRDIDA DE EVALUACIÓN CONTINUA

Se aplicará la normativa común establecida en el Departamento:

- 10% de faltas injustificadas

La justificación de las faltas se hará de acuerdo a ley, dejando bajo decisión del departamento los casos excepcionales.

Esta pérdida de evaluación se comunicará por escrito al alumno y se informará a jefatura de estudios.

En el caso de que un alumno perdiera el derecho a la evaluación continua y hubiera superado alguna prueba y/o evaluación, deberá volver a superarla en el procedimiento de evaluación alternativo. Es decir, perderá la calificación obtenida anteriormente.

6.3 PLANIFICACIÓN DE LAS ACTIVIDADES DE RECUPERACIÓN

6.4 SISTEMA DE RECUPERACIÓN DE EVALUACIONES SUSPENSAS

La normativa vigente contempla que *“la matrícula de primer curso implica la posibilidad de evaluación de módulos profesionales en dos convocatorias, la primera en junio y la segunda en el momento que determine la Consejería competente en materia de educación.”* Además, indica la realización de evaluaciones trimestrales para asegurar el progreso del alumnado, así como garantizar el proceso de evaluación continua. De este modo, el alumnado con evaluaciones trimestrales suspensas tendrá la posibilidad de recuperar dicha evaluación trimestral en una prueba realizada antes de la primera convocatoria de evaluación. En caso de no superar el módulo en dicha evaluación, podrá

recuperar el módulo en la prueba realizada previa a la segunda convocatoria de evaluación, en cuyo caso los contenidos de la prueba abarcarán los de todo el módulo. En cualquier caso, será necesario entregar y obtener una calificación igual o superior a 5 puntos sobre 10 en todas las prácticas realizadas durante el curso. Para tal fin se abrirá un plazo de entrega en los días anteriores a la realización de las pruebas de evaluación de las dos convocatorias, finalizando el plazo el día de realización de la prueba.

7 CONTRIBUCIÓN DEL MÓDULO A FOMENTAR LA CULTURA Y EL ESPÍRITU EMPRENDEDOR EN EL ALUMNADO

Durante el módulo, se realizarán referencias a la valoración de las competencias y habilidades que van adquiriendo en el sector. En algunas prácticas se hará referencia a antiguos alumnos del centro que han emprendido, explicando para que le sirvieran las competencias adquiridas en la práctica que están realizando en ese momento cuando se enfrentaron a problemas reales.

8 COMPETENCIAS Y CONTENIDOS DE CARÁCTER TRANSVERSAL

Durante el desarrollo del módulo se trabajarán las siguientes competencias transversales:

- Trabajo en equipo.
- Comunicación.
- Curación de contenidos.
- Autonomía de aprendizaje.

9 PROCEDIMIENTO DE RECLAMACIÓN DE LAS CALIFICACIONES

En base a la Orden EDU/2169/2008, de 15 de diciembre de 2008 publicada en el BOCYL con fecha 17-12-2008 que regula la forma de realizar las evaluaciones en Formación Profesional nuestro departamento establece que el alumno dispondrá de dos días lectivos para realizar las posibles reclamaciones después de la evaluación trimestral y una vez expuestas las calificaciones en el tablón de anuncios del departamento.

Las reclamaciones se presentarán por escrito, utilizando el modelo de instancia, que se podrá solicitar en Jefatura de Estudios. Así mismo el departamento establece que resolverá dichas reclamaciones en el plazo de un día lectivo.

10 ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES RELACIONADAS CON EL MÓDULO

Inicialmente no se proponen actividades. No obstante, este apartado queda abierto a la propuesta de actividades que realice el departamento o a actividades que surjan por intereses del propio grupo de alumnos.

11 MEDIDAS PARA ESTIMULAR EL INTERÉS Y HÁBITO DE LECTURA Y LA CAPACIDAD DE EXPRESARSE CORRECTAMENTE

Se empleará en la plataforma un canal dedicado a noticias de tecnológicas relacionadas con el módulo. Estas noticias serán comentadas y debatidas en la propia plataforma, realizando un seguimiento de la participación del alumnado que será tenido en cuenta en el apartado de calificación de actitud y comportamiento.

12 CRITERIOS DE EVALUACIÓN DE LA PROGRAMACIÓN

- Grado de cumplimiento en la impartición de los contenidos.
- Porcentaje (real) de los alumnos que superan el módulo.
- Evaluación subjetiva, por parte del profesor, de los materiales y recursos didácticos.

En Ávila, a día 29 de septiembre de 2024

Fdo. Maria Felisa Aldea Jiménez