De la oficina al hogar inteligente: asegurando el acceso remoto, la domótica y la continuidad del negocio en una PYME

Seguridad y Alta Disponibilidad

Guía didáctica

Arnau Martínez Benavent

Índice

1. Contextualización

Entorno educativo

Este proyecto se desarrolla en el marco de un Ciclo Formativo de Grado Superior en Administración de Sistemas Informáticos en Red (ASIR), en un centro educativo público con orientación tecnológica. El módulo de "Seguridad y alta disponibilidad" se imparte en el segundo curso, tras haber superado los estudiantes asignaturas como fundamentos de hardware, implantación de sistemas operativos y planificación y administración de redes, lo que garantiza una base técnica sólida.

El centro cuenta con un aula equipada con ordenadores de sobremesa modernos, acceso a Internet de banda ancha y dispositivos de red configurables. Además, dispone de recursos para trabajar con Single Board Computers (SBC) como Raspberry Pi u Orange Pi, lo que permite la realización de prácticas reales y simuladas de administración de sistemas, tanto en entornos virtualizados como sobre hardware físico. El alumnado tiene acceso a una plataforma de gestión de aprendizaje (Aules) donde se centralizan materiales, guías y entregas.

Nivel de los estudiantes

El alumnado está compuesto por jóvenes y adultos, habitualmente de entre 19 y 30 años, que han superado el primer curso del ciclo formativo. Presentan un nivel medio-alto en competencias digitales y conocimientos previos sobre sistemas operativos, redes, virtualización y administración básica de servicios. Muchos de ellos ya han realizado prácticas en empresas o tienen experiencia previa en entornos informáticos, aunque su dominio en ciberseguridad y alta disponibilidad suele ser inicial.

Se detectan diferentes ritmos de aprendizaje y perfiles: desde estudiantes muy autónomos y proactivos, hasta otros que requieren mayor acompañamiento y refuerzo en la planificación y documentación técnica. Por ello, se fomenta el trabajo colaborativo, el aprendizaje basado en proyectos y el uso de rúbricas claras para la autoevaluación y coevaluación.

Recursos disponibles

- Aula de informática con 20-25 puestos, cada uno con doble sistema operativo (Windows/Linux).

- Dispositivos SBC (Raspberry Pi o similar) para cada grupo de trabajo.
- Red local dedicada para prácticas de administración y seguridad.
- Acceso a Internet de banda ancha para pruebas de conectividad.
- Material de red: switches, routers, cables y puntos de acceso para simulaciones de topologías empresariales.
- Plataforma LMS (Moodle/Aules) para la gestión de recursos, entregas y foros de dudas.
- Software libre: DietPi, Docker, OpenVPN, WireGuard, Home Assistant, Pi-hole, Nginx Proxy Manager, herramientas de backup y monitorización.
- Documentación oficial y recursos didácticos proporcionados por el profesorado, incluyendo guías paso a paso, plantillas de documentación profesional y ejemplos de informes de auditoría.
- Soporte técnico del centro para incidencias con hardware y red.

2. Justificación pedagógica

Este proyecto se basa en el Aprendizaje Basado en Proyectos (ABP) como metodología principal, respaldado por evidencias científicas que demuestran su eficacia en la formación profesional. La implementación de esta metodología activa responde a las demandas actuales del sistema educativo y del mercado laboral, que requieren profesionales capaces de resolver problemas complejos, trabajar en equipo y adaptarse a entornos tecnológicos cambiantes.

Además, el proyecto responde directamente a las necesidades reales de las pequeñas y medianas empresas (PYME) en materia de ciberseguridad y transformación digital. En un contexto post-pandémico donde el teletrabajo se ha consolidado como modalidad habitual, los futuros administradores de sistemas deben dominar tecnologías de acceso remoto seguro, alta disponibilidad y automatización empresarial.

La propuesta fomenta el desarrollo integral de competencias técnicas y transversales esenciales para el perfil profesional ASIR:

- Pensamiento crítico y resolución de problemas: análisis de vulnerabilidades, toma de decisiones ante incidentes de seguridad.

- Creatividad e innovación: diseño de soluciones personalizadas para cada contexto empresarial.
- Comunicación efectiva: documentación técnica profesional y presentación de resultados.
- Colaboración: trabajo en equipo simulando entornos profesionales reales.
- Competencia digital avanzada: dominio de herramientas actuales de ciberseguridad y automatización.

Cabe destacar que el aprendizaje basado en proyectos presenta una serie de ventajas pedagógicas:

- Mayor motivación y retención: el ABP genera un incremento significativo en la motivación del alumnado al trabajar sobre proyectos y problemas reales. Los estudiantes perciben la utilidad inmediata de sus aprendizajes, conectando directamente con situaciones que encontrarán en su futuro profesional. Esta motivación intrínseca favorece un aprendizaje más profundo y duradero.
- Aprendizaje significativo y contextualizado: frente a metodologías tradicionales basadas en la transmisión unidireccional de contenidos, el proyecto sitúa al estudiante como protagonista activo de su aprendizaje. La contextualización en una PYME real permite que los conocimientos adquiridos sean directamente transferibles al mundo laboral, mejorando la retención y aplicación de conocimientos.
- Desarrollo de la autonomía y responsabilidad: la estructura del proyecto por fases progresivas fomenta la adquisición de autonomía, competencia fundamental para el perfil profesional de administrador de sistemas. Los estudiantes aprenden a gestionar su tiempo, planificar tareas complejas y tomar decisiones técnicas fundamentadas.
- Ritmos de aprendizaje diferenciados: el ABP permite adaptar el proyecto a diferentes ritmos y estilos de aprendizaje. Mientras algunos estudiantes pueden profundizar en aspectos más complejos de ciberseguridad, otros pueden centrarse en la documentación y planificación, garantizando que todos alcancen los resultados de aprendizaje establecidos.

Además, el proyecto ofrece diversas modalidades de evaluación (técnica, documental, oral), permitiendo que cada estudiante pueda demostrar sus competencias según sus

fortalezas individuales, y desarrolla competencias directamente demandadas por el mercado laboral actual:

- Administración segura de sistemas en la nube e híbridos.
- Implementación de políticas de ciberseguridad empresarial.
- Gestión de la continuidad del negocio.
- Cumplimiento normativo (RGPD, LOPDGDD).
- Integración de tecnologías emergentes (IoT, automatización).

Otro de los puntos fuertes reside en que la estructura del proyecto replica los procesos de trabajo de una empresa del sector TIC. Los estudiantes experimentan la presión de plazos reales, la necesidad de documentación técnica rigurosa y la responsabilidad de tomar decisiones que afectan a la seguridad empresarial.

Asimismo, se incorporan tecnologías actuales y emergentes (Docker, contenedores, automatización domótica, DDNS), preparando a los estudiantes para un mercado laboral en constante evolución tecnológica, sin dejar de lado el desarrollo de una mentalidad de "seguridad por diseño", fundamental en el contexto actual de ciberamenazas crecientes, formando profesionales conscientes de los riesgos y capaces de implementar medidas preventivas efectivas.

De igual manera, se ha cuidado la contribución al desarrollo personal y social, ya que la inclusión del módulo de legislación y cumplimiento normativo (RA7) desarrolla la conciencia ética necesaria para el manejo responsable de datos personales y sistemas críticos empresariales. Además, la exigencia de documentación técnica de calidad y presentaciones orales permite desarrollar competencias comunicativas esenciales para el liderazgo técnico y la interacción con diferentes *stakeholders* empresariales.

En último lugar y a modo de conclusión, el proyecto contribuye directamente a alcanzar los objetivos generales del ciclo ASIR establecidos en el Real Decreto 1629/2009, especialmente aquellos relacionados con la seguridad, alta disponibilidad y gestión de sistemas, mientras que las orientaciones metodológicas empleadas promueven el enfoque por competencias en la formación profesional, desarrollando capacidades complejas que integran conocimientos, habilidades y actitudes aplicables en contextos profesionales reales.

3. Tabla de relación entre fases del proyecto y el currículum oficial

Resultado de Aprendizaje	Criterios de Evaluación seleccionados	Objetivo General	Competencia Prof./ Personal/Social	Actividad del Proyecto
RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos e) Se han adoptado políticas de contraseñas h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral	10) Seleccionar sistemas de protección y recuperación 11) Identificar condiciones de equipos e instalaciones	11) Asegurar el sistema y los datos según las necesidades de uso	Fase 1: Instalación segura de DietPi - Configuración SSH sin root - Políticas de contraseñas - Análisis inicial de vulnerabilidades
RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema	c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas i) Se han descrito los tipos y características de los sistemas de detección de intrusiones	12) Aplicar técnicas de protección contra amenazas externas	11) Asegurar el sistema y los datos 13) Diagnosticar disfunciones del sistema	Fase 2: Implementación de fail2ban - Configuración de reglas de detección - Análisis de logs de seguridad - Respuesta ante intentos de intrusión
RA3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad	c) Se han identificado los protocolos seguros de comunicación d) Se han configurado redes privadas virtuales mediante protocolos seguros e) Se ha implantado un servidor como pasarela de acceso f) Se han identificado y configurado métodos de autenticación	12) Aplicar técnicas de protección contra amenazas externas 13) Aplicar técnicas de protección contra pérdidas de información	11) Asegurar el sistema y los datos 10) Supervisar la seguridad física	Fase 4: Configuración de VPN - Instalación OpenVPN/WireGuard - Certificados y autenticación - Túneles seguros para teletrabajo - Pruebas de conectividad
RA4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna	c) Se ha planificado la instalación de cortafuegos para limitar accesos d) Se han configurado filtros en un cortafuegos a partir de reglas de filtrado h) Se ha elaborado documentación relativa a la instalación y configuración	12) Aplicar técnicas de protección contra amenazas externas	11) Asegurar el sistema y los datos	Fase 2: Configuración de cortafuegos - Reglas iptables personalizadas - Pi-hole para filtrado DNS - Documentación de reglas implementadas

Resultado de Aprendizaje	Criterios de Evaluación seleccionados	Objetivo General	Competencia Prof./ Personal/Social	Actividad del Proyecto
RA5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio	h) Se ha configurado un servidor «proxy» en modo inverso i) Se ha elaborado documentación relativa a la instalación y configuración	10) Seleccionar sistemas de protección y recuperación 16) Establecer planificación de tareas	5) Optimizar el rendimiento del sistema 9) Implementar soluciones de alta disponibilidad	Fase 3: Nginx Proxy Manager - Balanceo de carga entre servidores - Certificados SSL automáticos - Protección contra ataques DDoS
RA6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba	c) Se han evaluado las posibilidades de la virtualización g) Se ha evaluado la utilidad de los sistemas de «clusters» i) Se han esquematizado y documentado soluciones para diferentes supuestos	10) Seleccionar sistemas de protección y recuperación 16) Establecer planificación de tareas	6) Evaluar el rendimiento de dispositivos hardware 9) Implementar soluciones de alta disponibilidad	Fase 3: Docker y DDNS - Contenedores para servicios críticos - Cloudflare DDNS para IP dinámica - Estrategias de backup y recuperación
RA7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia	a) Se ha descrito la legislación sobre protección de datos b) Se ha determinado la necesidad de controlar el acceso a información personal c) Se han identificado las figuras legales e) Se ha descrito la legislación sobre servicios de la sociedad de la información f) Se han contrastado las normas sobre gestión de seguridad g) Se ha comprendido la necesidad de respetar la normativa legal	17) Identificar cambios tecnológicos, organizativos y laborales	18) Resolver problemas siguiendo normas y procedimientos	Fase 6: Auditoría legal - Análisis RGPD aplicado al proyecto - Identificación de datos personales tratados - Documentación de cumplimiento normativo - Políticas de privacidad empresariales

4. Referencias normativas

Marco normativo general

Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOMLOE)

Artículo 6. Currículo

Apartado 1: el currículo estará integrado por los objetivos de cada enseñanza y etapa educativa; las competencias, o capacidades para activar y aplicar de forma integrada los contenidos propios de cada enseñanza y etapa educativa, para lograr la realización adecuada de actividades y la resolución eficaz de problemas complejos; los contenidos, o conjuntos de conocimientos, habilidades, destrezas y actitudes que contribuyen al logro de los objetivos de cada enseñanza y etapa educativa y a la adquisición de competencias; los métodos pedagógicos, que comprenden tanto la descripción de las prácticas docentes como la organización del trabajo de los docentes; los estándares y resultados de aprendizaje evaluables; y los criterios de evaluación del grado de adquisición de las competencias y del logro de los objetivos de cada enseñanza y etapa educativa.

Apartado 3: con el fin de asegurar una formación común y garantizar la validez de los títulos correspondientes, el Gobierno fijará, en relación con los objetivos, competencias, contenidos y criterios de evaluación, los aspectos básicos del currículo que constituyen las enseñanzas mínimas. Para la Formación Profesional, el Gobierno fijará así mismo los resultados de aprendizaje correspondientes a las enseñanzas mínimas.

Apartado 5: las Administraciones educativas establecerán el currículo de las distintas enseñanzas reguladas en la presente Ley, del que formarán parte los aspectos básicos señalados en apartados anteriores. Los centros docentes desarrollarán y completarán, en su caso, el currículo de las diferentes etapas y ciclos en uso de su autonomía y tal como se recoge en el capítulo II del título V de la presente Ley.

Normativa específica del título

Real Decreto 1629/2009, de 30 de octubre, por el que se establece el título de Técnico Superior en Administración de Sistemas Informáticos en Red y se fijan sus enseñanzas mínimas

Norma fundamental que:

- Establece el título con carácter oficial y validez en todo el territorio nacional
- Define el perfil profesional, competencias y resultados de aprendizaje
- Fija las enseñanzas mínimas del módulo "Seguridad y alta disponibilidad"
- Determina la duración total del ciclo formativo (2.000 horas)
- Sustituye la regulación anterior del título de Técnico Superior en Administración de Sistemas Informáticos

Orden EDU/392/2010, de 20 de enero, por la que se establece el currículo del ciclo formativo de Grado Superior correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red

Desarrolla el currículo específico a nivel estatal, estableciendo:

- Objetivos generales del ciclo formativo
- Módulos profesionales y sus contenidos específicos
- Orientaciones metodológicas y criterios de evaluación
- Distribución horaria y temporal

Normativa de protección de datos y ciberseguridad

Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD)
Normativa europea de aplicación directa desde el 25 de mayo de 2018 que:

- Regula el tratamiento de datos personales en la Unión Europea
- Establece principios fundamentales de protección de datos
- Define derechos de los interesados y obligaciones de responsables del tratamiento
- Establece sanciones de hasta 20 millones de euros por incumplimiento

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

Complementa y adapta el RGPD al ordenamiento jurídico español:

- Desarrolla los principios de protección de datos en el ámbito nacional
- Establece los derechos digitales de la ciudadanía
- Regula las figuras del responsable y encargado del tratamiento
- Mantiene en 14 años la edad mínima para el consentimiento de menores

Estándares internacionales de seguridad

ISO/IEC 27001:2013 - Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos

Estándar internacional que:

- Establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI)
- Proporciona un enfoque sistemático para gestionar información sensible
- Es especialmente relevante en instituciones educativas para proteger datos académicos y administrativos
- Facilita la certificación en gestión de seguridad de la información

Actualizaciones normativas recientes

Real Decreto 405/2023, de 29 de mayo, por el que se actualizan los títulos de la formación profesional del sistema educativo

Aunque se centra en la actualización de otros títulos de la familia profesional Informática y Comunicaciones (Desarrollo de Aplicaciones Multiplataforma y Web), establece precedentes para la modernización curricular en el ámbito tecnológico.

Real Decreto 207/2025, de 18 de marzo, por el que se regulan aspectos específicos de la formación profesional

Confirma la vigencia del título de Técnico Superior en Administración de Sistemas Informáticos en Red establecido por el Real Decreto 1629/2009, manteniéndolo dentro del catálogo actualizado de títulos de formación profesional.

Esquema Nacional de Seguridad (ENS)

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Marco de referencia para la seguridad de la información en el sector público español que:

- Establece principios básicos y requisitos mínimos de seguridad
- Define medidas de seguridad aplicables según el nivel de riesgo
- Proporciona metodologías para la gestión de riesgos
- Sirve como referencia para buenas prácticas en el sector privado

Justificación de la selección normativa

Esta selección normativa proporciona el marco legal completo que sustenta el proyecto educativo, cubriendo:

1. Fundamento educativo: LOMLOE y normativa de formación profesional
2. Contenido curricular: Real Decreto 1629/2009 y desarrollos autonómicos
3. Marco legal aplicado: RGPD, LOPDGDD
4. Estándares técnicos: ISO 27001 y ENS
5. Actualización normativa: decretos recientes que confirman la vigencia

La integración de estas referencias en el proyecto garantiza que el alumnado desarrolle competencias técnicas actualizadas y conocimientos jurídicos fundamentales para el ejercicio profesional responsable en el ámbito de la administración de sistemas informáticos en red.