

Gestión, Coordinación, Seguridad informática e Ingeniería de las TIC aplicadas a los centros preuniversitarios



Área: Computer-supported
collaborative learning

13/06/2017

Autor: Miguel Bragado Pérez

Consultor: Gregorio Robles Martínez

Máster Universitario en Ingeniería Informática.

Índice

1. INTRODUCCIÓN

- 1.1 ANTECEDENTES
- 1.2 PROPÓSITO Y JUSTIFICACIÓN DEL TFM
- 1.3 OBJETIVO DEL PROYECTO
- 1.4 OBEJTIVOS GENERALES
- 1.6 ENFOQUE Y MÉTODO A SEGUIR
- 1.7 PLANIFICACIÓN CON HITOS Y TEMPORIZACIÓN
 - 1.7.1 TAREAS
 - 1.7.2 CALENDARIO
 - 1.7.3 PRODUCTOS ESPERADOS

2. PLAN DE ACCIÓN DE MEJORA DE LA GESTIÓN TIC DEL CENTRO EDUCATIVO

- 2.1 CADENA DE VALOR
- 2.2 ANÁLISIS DE SITUACIÓN ACTUAL DEL CENTRO EDUCATIVO EN MATERIA SI/TI
- 2.3 INVENTARIO GENERAL DE EQUIPOS Y SISTEMAS
- 2.4 ARQUITECTURA DE LOS SISTEMAS
- 2.5 DETECCIÓN DE NECESIDADES Y APLICACIÓN
- 2.6 GESTIÓN DE INCIDENCIAS
 - 2.6.1 OBJETIVOS DE LA GESTIÓN DE INCIDENCIAS EN EL CENTRO
 - 2.6.2 ALCANCE DE LA GESTIÓN DE INCIDENCIAS EN EL CENTRO
 - 2.6.3 PROCESO DE LA GESTIÓN DE INCIDENCIAS EN EL CENTRO
 - 2.6.4 KPI DE LA GESTIÓN DE INCIDENCIAS EN EL CENTRO
 - 2.6.5 CREACIÓN DE BASE DE DATOS DE ERRORES CONOCIDOS
 - 2.6.6 MEJORA CONTÍNUA DEL SOPORTE INFORMÁTICO EN EL CENTRO EDUCATIVO

3. PLAN DE ACCIÓN: SEGURIDAD INFORMÁTICA EN EL CENTRO DE ENSEÑANZA

- 3.1 ANÁLISIS Y MEJORA DE LA INFRAESTRUCTURA DE LA RED
- 3.2 GESTIÓN DE CONTRASEÑAS
 - 3.2.1 GESTIÓN DE ACCESOS DE INFORMACIÓN A USUARIOS:
PROFESORADO Y ALUMNADO
- 3.3 GESTIÓN DE LOS BACKUPS DEL CENTRO
 - 3.3.1 DEFINICIÓN DEL PLAN DE COPIAS DE SEGURIDAD
- 3.4 GESTIÓN DE CUENTAS DE USUARIOS
- 3.5 APLICACIÓN DE NORMAS DE PROTECCIÓN DE DATOS Y PRIVACIDAD
- 3.6 OTRAS MEDIDAS DE SEGURIDAD A IMPLANTAR DESDE EL DEPARTAMENTO SI/TI DEL CENTRO DE ENSEÑANZA
- 3.7 FICHEROS DEL CENTRO DE ENSEÑANZA Y SU CUMPLIMIENTO EN MATERIA DE LA LOPD
 - 3.7.1 PROCESO DE SEGURIDAD EN FICHEROS AUTOMATIZADOS Y NO AUTOMATIZADOS DEL CENTRO
 - 3.7.2 RESPONSABILIDADES DE LOS FICHEROS
- 3.8 PLAN DE CONVIVENCIA EN EL CENTRO EN EL USO DE LAS NUEVAS TECNOLOGÍAS Y LA RED

4 DESARROLLO DE PRODUCTOS TECNOLÓGICOS DE MAYOR COMPLEJIDAD DESDE EL DEPARTAMENTO DE TECNOLOGÍA PARA SU POSTERIOR REALIZACIÓN EN LAS AULAS

4.1 REALIZACIÓN DE UN PROYECTO COMPLEJO DE ROBÓTICA EN ARDUINO CON SENSORES DE ULTRASONIDOS

4.2.1 ANÁLISIS DEL PROYECTO

4.2.2 REQUERIMIENTOS DE MATERIALES Y TÉCNICOS NECESARIOS

4.2.3 CONSTRUCCIÓN Y FASES DEL PROYECTO: RÓBÓTICA

4.2.4 ENTREGA FINAL DEL PRODUCTO Y DEL CÓDIGO FUENTE

4.2.5 ANÁLISIS DE LA DIFICULTAD PARA SU POSTERIOR DESARROLLO POR EL ALUMNADO

4.3 ANÁLISIS y REFLEXIÓN GLOBAL DE LA REALIZACIÓN DE PRODUCTOS TECNOLÓGICOS COMPLEJOS EN LAS AULAS SEGÚN NIVELES EDUCATIVOS

5. RESUMEN

6. VALORACIÓN DEL TFM

6.1 APRENDIZAJE EN EL PROYECTO

6.2 APLICACIÓN DEL MÁSTER DE INGENIERÍA AL PROYECTO

7. CONCLUSIONES.

8. BIBLIOGRAFÍA

1. INTRODUCCIÓN

1.1 ANTECEDENTES

Las nuevas Tecnologías nos facilitan la gestión y automatización de los diferentes procesos no solamente en un entorno empresarial, también en entornos educativos donde el buen funcionamiento de las TIC son clave para la consecución de los objetivos y buen hacer de dichos centros educativos en materia de gestión de las TIC.

La figura del Ingeniero en informática tiene en la educación una de sus salidas laborales aunque quizá no sea tan conocida debido a que la tendencia del titulado en ingeniería en informática es en disposición de trabajar en un entorno empresarial, en sus diferentes áreas como desarrollo, sistemas, big data, ciberseguridad...

En un centro de enseñanza, el ingeniero en informática tiene el papel de coordinación TIC y el de responsable de seminario o departamento de tecnología y TIC. Mi puesto de trabajo actual es precisamente el de la coordinación TIC y el responsable departamento de tecnología.

El proyecto que será de aplicación real, tiene como una de sus metas ser aplicado para cualquier centro de enseñanza (por lo que será transversal en la medida de lo posible) y ser un TFM de gran utilidad para cualquier ingeniero que trabaje en un puesto de trabajo en el que deba llevar la informática de un centro de enseñanza y la responsabilidad del departamento de tecnología.

La realización de un TFM que aporte un valor añadido a la figura del ingeniero en informática en un centro y que sea de gran utilidad para futuros compañeros que se embarquen en esta área tanto a nivel de gestión TIC como de responsables de un departamento de tecnología en un centro de enseñanza es una de mis grandes motivaciones para la realización de este trabajo.

A su vez poner en práctica siendo mi figura el cargo de Responsable TIC y Responsable del departamento de Tecnología, los conocimientos adquiridos en el máster en pos de mejorar la gestión, coordinación y seguridad en mi trabajo (un centro de enseñanza reglada) ya que hay identificadas carencias a mejorar y desarrollar.

Así como realizar proyectos de ingeniería de alta complejidad en Robótica, que me aporten conocimientos más profundos, y en el que quede plasmado y sirva me sirva tanto para ampliar mis conocimientos como referencia como mencionaba a futuros compañeros de profesión el potencial que podemos desarrollar en un centro de enseñanza con nuestros conocimientos adquiridos tanto en gestión de las TIC como en Ingeniería mediante proyectos tecnológicos complejos y coordinación de las TIC.

El Trabajo final “Gestión, Coordinación, Seguridad e Ingeniería de las TIC aplicadas a los centros preuniversitarios” consta de:

Un primer bloque la realización de un plan de acción con el propósito primero de revisar el estado actual de un centro de enseñanza, identificando la situación idónea y la planificación de los cambios en el centro necesarios para alcanzar dicho estado y determinar acciones futuras en materia de gestión, coordinación y seguridad de las TIC.

Realizando la implantación real de procesos de mejora en gestión, coordinación y seguridad de las TIC en el centro mediante mejores prácticas IT (ITIL), de Seguridad informática (LOPD, privacidad, SGSI..) , y privacidad en la red en el centro.

Un segundo bloque en el que se desarrolla un producto tecnológico de ingeniería complejos como pueden ser proyectos de Robótica con Arduino con la finalidad del aprendizaje e investigación por mi parte para que posteriormente puedan realizarlos los alumnos con mi soporte y conocimientos y puedan servir de línea futuras para desarrollar proyectos tecnológicos de mayor envergadura en este tipo de centros.

Se tendrán en cuenta a su vez diferentes factores como la situación actual del centro, el estudio de necesidades detectadas en el centro de enseñanza y el análisis de la cadena de valor del centro tomando las decisiones siempre justificadas, teniendo en cuenta las posibles limitaciones presupuestarias, técnicas y humanas que puedan tener impacto en el trabajo.

1.2 PROPÓSITO Y JUSTIFICACIÓN DEL TFM

El objetivo del trabajo final de máster “Gestión, Coordinación, Seguridad e Ingeniería de las TIC aplicadas a los centros preuniversitarios” tiene como principales objetivos diferenciados dos áreas: Plan de acción de mejora de Gestión y Seguridad de las TIC en un centro educativo, y Desarrollo de complejos productos tecnológicos reales de mayor dificultad que aumenten mi capacitación y la de este tipo de proyectos de mayor complejidad en un centro educativo.

La necesidad de un plan de mejora o en su caso de implantación en un centro de enseñanza mediante acciones a desarrollar en el ámbito de la gestión, coordinación y seguridad de las TIC; y la creación de proyectos de mayor envergadura en el ámbito de la ingeniería desde el departamento de tecnología, justifican la puesta en marcha de las motivaciones o diferentes argumentos que son necesarios en un centro de enseñanza desde la figura del ingeniero en informática analizando referente al centro de enseñanza la cadena de valor y el valor añadido a otorgar en este tipo de centros educativos.

1.3 OBJETIVO DEL PROYECTO

Al final del proyecto, se debe haber logrado:

1. La realización del plan de acción con implantación real de procesos de mejora en gestión, coordinación y seguridad de las TIC en un centro de enseñanza (de aplicación real en el TFM en un centro docente y a su vez aplicable a cualquier tipo de centro educativo) mediante mejores prácticas IT (ITIL), y de Seguridad informática, y privacidad en la red previa identificación de la situación idónea y la planificación de los cambios en el centro necesarios para alcanzar dicho estado y determinar acciones futuras en materia de gestión, coordinación y seguridad de las TIC.
2. Haber llevado a cabo el desarrollo de productos tecnológicos reales y tangibles que aumenten mi capacitación y sirvan de líneas futuras para la realización de proyectos de mayor complejidad en Robótica (Arduino).

El centro educativo obtendrá el beneficio de una excelente gestión de servicio de SI/TI, coordinación y Seguridad de la información capaz de dar soporte a las necesidades en materia de servicios de sistemas de información que el centro pueda requerir. Y a su vez alcanzar un mayor nivel de exigencia en la creación por parte de los alumnos de proyectos de ingeniería en tecnología en los ámbitos más actuales como la Robótica

Se creará en este segundo bloque el desarrollo de un producto tecnológico que posteriormente puedan ser llevado a cabo por alumnos de dicho en centro en las etapas preuniversitarias:

- Desarrollo de un producto complejo tecnológico de Robótica, Ultrasonidos con Arduino UNO, con creación de código en el lenguaje C++.

1.4 OBEJTIVOS GENERALES

El Trabajo final de Máster “*Gestión, Coordinación, Seguridad e Ingeniería de las TIC aplicadas a los centros preuniversitarios*” consta de:

Un primer bloque la realización de un plan de acción con el propósito primero de revisar el estado actual de un centro de enseñanza, identificando la situación idónea y la planificación de los cambios en el centro necesarios para alcanzar dicho estado y determinar acciones futuras en materia de gestión, coordinación y seguridad de las TIC.

Realizando la implantación real de procesos de mejora en gestión, coordinación y seguridad de las TIC en el centro mediante mejores prácticas IT (ITIL), de Seguridad informática (LOPD, privacidad, SGSI..) , y privacidad en la red en el centro.

Un segundo bloque en el que se desarrollen diferentes productos tecnológicos de ingeniería complejos como pueden ser proyectos de Robótica con Arduino o Impresión 3D con la finalidad del aprendizaje e investigación por mi parte para que posteriormente puedan realizarlos los alumnos con mi soporte y conocimientos y puedan servir de línea futuras para desarrollar proyectos tecnológicos de mayor envergadura en este tipo de centros.

Se tendrán en cuenta a su vez diferentes factores como la situación actual del centro, el estudio de necesidades detectadas en el centro de enseñanza y el análisis de la cadena de valor del centro tomando las decisiones siempre justificadas, teniendo en cuenta las posibles limitaciones presupuestarias, técnicas y humanas que puedan tener impacto en el trabajo.

1.5 OBJETIVOS ESPECÍFICOS

Los 4 objetivos específicos del trabajo son los siguientes una vez se analiza la situación actual del centro educativo:

Uno de los objetivos del proyecto, es en materia lograr la excelencia en la gestión y coordinación de servicios de SI/TI del centro de educación, en el que el mismo se beneficiará de mediante las mejores prácticas de servicio de gobierno IT basadas en el modelo ITIL mejorando la gestión de incidencias y peticiones.

Al final del proyecto, se debe haber logrado la perfecta implementación del soporte TIC para excelente gestión y coordinación del equipo humano que forman parte del centro educativo mediante las mejores prácticas de servicio de SI/TI por medio de medidas de Gobierno TI.

La institución deberá beneficiarse de una excelente gestión de servicio de SI/TI, capaz de dar soporte a las necesidades en materia de servicios de sistemas de información que pueda requerir.

Un segundo apartado en materia de seguridad en el que para alcanzar dicho objetivo, se deben conocer nuestras obligaciones técnicas, y trazar un plan definiendo como se va a lograr, donde se deberán obtener procedimientos que permitan garantizar la confidencialidad de los datos del centro educativo, teniendo definidos planes de seguridad de la información, obteniendo en todo momento la excelencia en cuanto a confidencialidad de los datos respetando la LOPD.

Un tercer y cuarto objetivo con el fin de lograr realizar proyectos de ingeniería de alta complejidad en Robótica que aumenten el prestigio del centro en beneficio del mismo y de los alumnos y en el que a su vez mediante su investigación, me aporten conocimientos más profundos, y sirvan referencia como referencia a futuros compañeros de profesión del potencial que podemos desarrollar en un centro de enseñanza.

1.6 ENFOQUE Y MÉTODO A SEGUIR

La estructura del trabajo será llevar a cabo mediante la planificación mostrada en el Diagrama de Gantt los 4 grandes apartados que se enumeran a continuación:

- PLAN DE ACCIÓN DE MEJORA DE LA GESTIÓN TIC DEL CENTRO EDUCATIVO
- PLAN DE ACCIÓN: SEGURIDAD INFORMÁTICA EN EL CENTRO DE ENSEÑANZA
- DESARROLLO DE PRODUCTOS TECNOLÓGICOS DE MAYOR COMPLEJIDAD DESDE EL DEPARTAMENTO DE TECNOLOGÍA PARA SU POSTERIOR REALIZACIÓN EN LAS AULAS COMPUESTO DE:
 - REALIZACIÓN DE UN PROYECTO COMPLEJO DE ROBÓTICA EN ARDUINO CON SENSORES DE ULTRASONIDOS

1.7 PLANIFICACIÓN CON HITOS Y TEMPORIZACIÓN

1.7.1 TAREAS

Desglose de tareas del trabajo:

Tarea 1: Análisis de la situación general del centro en materia de Gestión de las TIC y seguridad informática

Descripción de la tarea:

Realizar un análisis general en el centro en materia de gestión de las TIC y seguridad

Objetivos de la tarea:

Obtener estado de la situación actual en general del centro de enseñanza.

Tarea 2: Estudio de Alcance, Objetivos y Escenario actual.

Descripción de la tarea:

Realización de los puntos 1 al 2.4 de la memoria y sus correspondientes apartados previo estudio de la necesidad y problemática que plantea el proyecto.

Objetivos de la tarea:

Definir en la memoria el alcance del proyecto, así como sus objetivos y escenario de la problemática a la que el proyecto dará solución en materia de gestión de las TIC del centro así como su seguridad. Realización de los puntos 1 al 2.4 de la memoria y sus correspondientes apartados.

Tarea 3: Plan de acción de mejora de la gestión y coordinación TIC del Centro Educativo:

Descripción de la tarea:

Estudio y realización del Plan de acción de mejora de la gestión y coordinación TIC del Centro Educativo propuesto en el índice.

Objetivos de la tarea:

Lograr llevar a cabo todos los puntos del Plan de acción de mejora propuesto en materia de mejora de la gestión y coordinación TIC del Centro Educativo.

Tarea 4: Análisis de la necesidad y ejecución de un plan de mejora en seguridad informática en el centro de enseñanza

Descripción de la tarea:

Realizar un estudio detallado sobre la seguridad informática del centro de enseñanza tomando las medidas necesarias reflejadas en la memoria y realizar del punto 3 de la memoria hasta el punto 3.5

Objetivos de la tarea:

Realizar las acciones necesarias para dar respuesta a las necesidades en materia de seguridad informática que aparecen en la memoria desde el punto 3 a punto 3.5,

Tarea 5: Análisis de la necesidad y ejecución de un plan de mejora en seguridad informática en el centro de enseñanza (II)

Descripción de la tarea:

Previo repaso a la LOPD, realizar las acciones necesarias para tal efecto en el centro de enseñanza, y la realización de un breve plan de convivencia del centro en el uso de las nuevas tecnologías.

Objetivos de la tarea:

Realizar las acciones necesarias para dar respuesta a las necesidades en materia de seguridad informática que aparecen en la memoria desde el punto 3.6 a punto 3.7

Tarea 6: Desarrollo del Proyecto de Robótica con Arduino

Descripción de la tarea:

Estudio, desarrollo y ejecución del producto tecnológico de Robótica con Arduino

Objetivos de la tarea:

Realizar el proyecto propuesto en Robótica con Arduino. Puntos 4 al 4.3.6 de la memoria.

Tarea 7: Valoración TFM

Descripción y objetivos de la tarea:

Estudio de la valoración final del TFM

Tarea 8: Preparación de la entrega final

Descripción y Objetivos de la tarea:

Asegurar que todo está perfecto para la realización de la entrega final, revisar la documentación a entregar y posibles erratas así como preparar la presentación final que será incluida junto con el trabajo final de máster.

1.7.2 CALENDARIO

Se muestra el Diagrama de Gantt para la realización de las diferentes etapas del TFM:

Nombre de la tarea:	Duración	Inicio	Finalizar
Definición del TFM, aprobación y estudio con el consutor	11d	21/02/18	07/03/18
Preparación de la planificación del TFM	11d	21/02/18	07/03/18
ENTREGA DE LA PAC1	11d	21/02/18	07/03/18
Realización de las tareas 1 y 2:Análisis de la situación general Gestión de las TIC y seguridad informática. Alcance y Objetivos	10d	05/03/18	16/03/18
Realización de la tarea 3: Análisis de la herramienta de gestión de incidencias y peticiones para su posible mejora o implantación	17d	10/03/18	02/04/18
Realización de la tarea 4:PARTE 1 Análisis de la necesidad y ejecución de un plan de mejora en seguridad informática en el centro c	20d	15/03/18	11/04/18
ENTREGA DE LA PAC2	25d	08/03/18	11/04/18
Realización de la tarea 5: PARTE 2 Análisis de la necesidad y ejecución de un plan de mejora en seguridad informática en el centro	23d	11/04/18	11/05/18
Tarea 6: Desarrollo del Proyecto de Robótica con Arduino	23d	11/04/18	11/05/18
ENTREGA DE LA PAC3	22d	12/04/18	11/05/18
Tarea 7: Desarrollo del Proyecto de Robótica con Arduino	24d	11/05/18	13/06/18
Realización de la Tarea 8 : Valoración TFM	4d	08/06/18	13/06/18
Realización de la Tarea 9: Preparación de la entrega final del TFM	4d	08/06/18	13/06/18
ENTREGA FINAL (PAC4)	10d	31/05/18	13/06/18

1.7.3 PRODUCTOS ESPERADOS

- MEJORA EN GESTIÓN DE LAS TIC DEL CENTRO DE ENSEÑANZA (MEDIDAS ADPOTADAS POR MEDIO DE ITIL)
- MEJORA EN LA COORDINACIÓN DE LAS TIC.
- MEJORA EN LA INFRAESTRUCTURA DE RED
- MEJORA EN LA SEGURIDAD DEL CENTRO
- MEJORA EN EL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS (LOPD)
- DESARROLLO DE LOS PRODUCTOS COMPLEJOS TECNOLÓGICOS EN ROBÓTICA

2. PLAN DE ACCIÓN DE MEJORA DE LA GESTIÓN TIC DEL CENTRO EDUCATIVO

2.1 CADENA DE VALOR

El llamado concepto de cadena nace por Michael Porter en 1985 con la publicación del libro *The Competitive Advantage: Creating and Sustaining Superior Performance*.

Permite describir las actividades de una organización para generar valor al cliente final y a la misma empresa.

En un centro docente, consiste en lograr alcanzar los objetivos planteados en las distintas etapas educativas de los alumnos. El valor del producto por tanto en este caso, se mide en el grado de cumplimiento de los objetivos y en parámetros de enseñanza.

El margen del centro de enseñanza es la diferencia entre el valor obtenido y los costes necesarios para llevarlos a buen término.

La cadena de valor, en el trabajo a desarrollar es estratégica ya que se van a lograr mediante dicho trabajo en tecnologías de la información y comunicación mejoras en todas las tareas/actividades del centro,

Gracias a los procesos tecnológicos que se adopten aumentará la ventaja competitiva ya que se lograrán ahorrar costes y tiempo en la realización de las tareas.

En el punto actual no hay satisfacción por parte del equipo directivo y de los trabajadores tanto a nivel de infraestructura del centro como de los recursos informáticos por lo que se debe trazar un plan de mejora en el centro que logre una diferenciación para un mayor beneficio que se debe reflejar en la cadena de valor.

2.2 ANÁLISIS DE SITUACIÓN ACTUAL DEL CENTRO EDUCATIVO EN MATERIA SI/TI

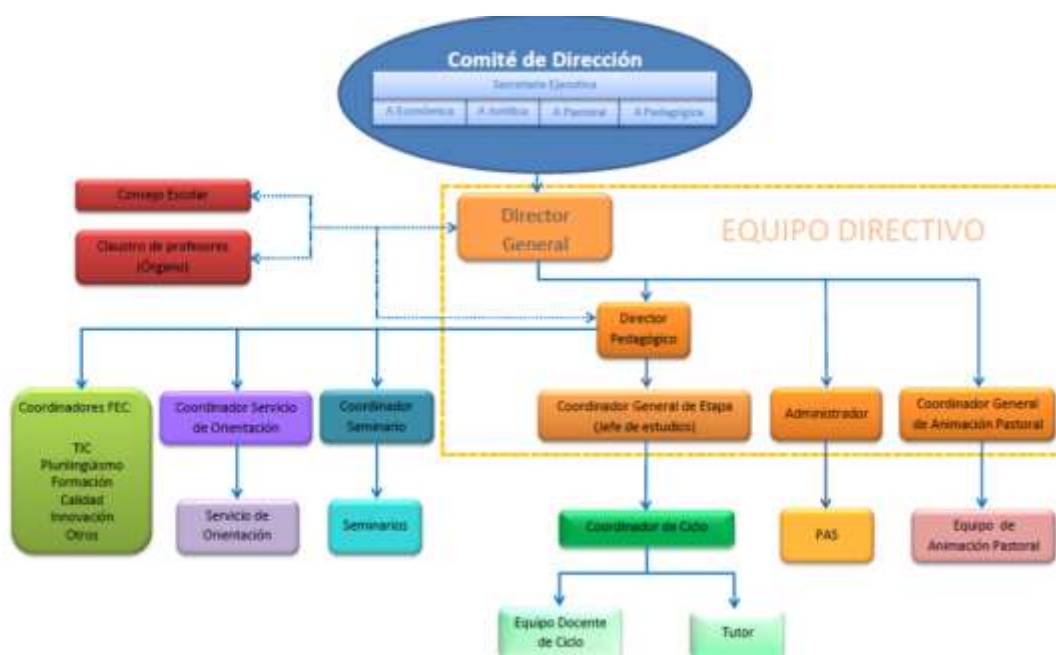
Los antecedentes en los que nos situamos en el centro docente en el que se realiza el Trabajo, es una institución que consta de clases equipadas con ordenadores, proyectores, pizarras digitales en cada aula. En este caso el centro dispone de las etapas de Infantil, Primaria y dos líneas en Secundaria. A su vez hay 6 despachos de los diferentes componentes del equipo directivo (Director General, Jefe de Estudios, Orientador...) cada uno con su correspondiente equipo informático.

El centro docente dispone también en materia en la que se encuentran componentes informáticos de una recepción equipada con impresora multifunción de oficina en red, de una sala de informática con 30 ordenadores, laboratorio, biblioteca con 12 ordenadores, salón de actos con equipo multimedia para las diferentes presentaciones y un taller de tecnología en la que se encuentra ubicada una impresora 3D.

Dispone de 4 carros para el almacenamiento y carga de ordenadores portátiles que utilizan los alumnos, con un total de 32 ordenadores por carro (total de 128 ordenadores portátiles).

En la situación actual se ha detectado entre otros, la necesidad de mejora la infraestructura de la red, ya que será necesario crear diferentes redes y subredes que se detallarán en el apartado correspondiente de la memoria. Así como una mejora en la Gestión, Coordinación y Seguridad de las TIC que es uno de los objetivos enmarcados en el trabajo.

El organigrama del centro es el siguiente:



2.3 INVENTARIO GENERAL DE EQUIPOS Y SISTEMAS

Se realiza un inventario general del parque informático del centro docente:

Ubicación	Tipo Ordenador	Cantidad	NOTAS
Sala Profesores	pc sobremesa	5	
Biblioteca	pc sobremesa	4	Uno central para el programa de gestión de libros y 3 de consulta para los alumnos
Aula Informática	portátil	32	
Secretaría	pc sobremesa	1	
Administración	todo en uno	1	
Despacho Equipo Directivo	todo en uno	4	Solo Jefe de Estudios se encuentra en otra ubicación, pero el modelo de ordenador es el mismo. B de la Directora General (provisional)
Aula	portátil	1	En E. Infantil 5 años
Aula	pc sobremesa	28	Se incluyen optativas.
Aula	todo en uno	1	En E. Primaria 3º A
Aula	Netbook	4	En una clase de apoyo en E. Primaria
Sin ubicación (dispositivo móvil)	portátil	4	2 en Armario de la sala de profesores, 1 en Dep. Patrol y 1 en Administración (antiguo ordenador de Administración)
Sin ubicación (dispositivo móvil)	Netbook	2	En Armario de Material de Informática
Departamento de Pastoral	portátil	1	Conectado fijo al cañón y pizarra digital (se utiliza también como clase de desdoble o apoyo)
Sala Profesores	pc sobremesa	2	
Secretaría/Administración	portátil	2	1 está conectado al Plotter
Secretaría/Administración	MAC	1	(Directora General)
Sala Profesores	ipad	1	(Directora General)
Aula Informática	Sobremesa	2	
Aula Informática	Sobremesa	2	
Aula Informática	Sobremesa	2	
Aula Informática	Sobremesa	2	
Aula Informática	Sobremesa	2	
Aula Informática	Sobremesa	2	
Aula Informática	Sobremesa	2	
Aula Informática	Sobremesa	2	
Aula Informática	Sobremesa	2	

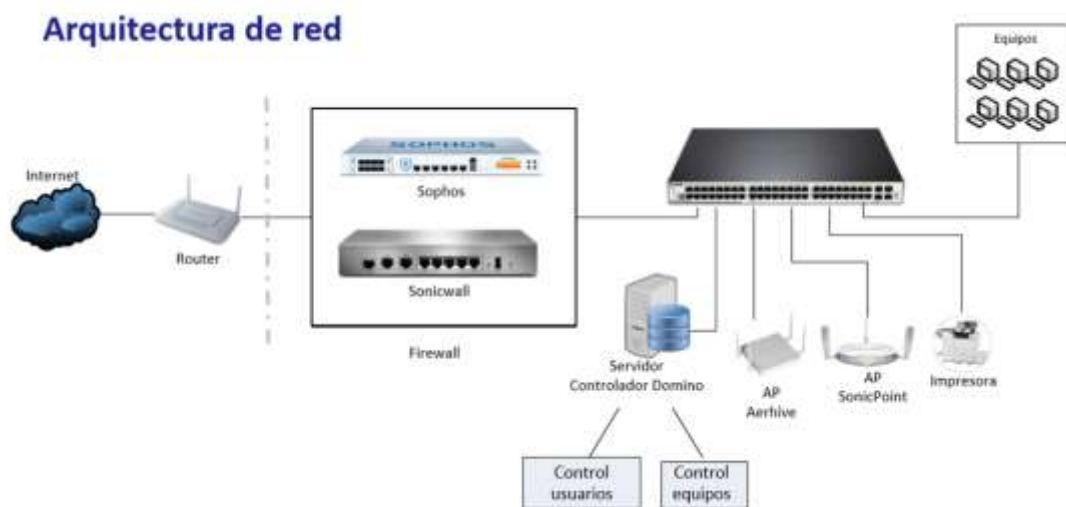
HP ProOne400	5 Primaria A	Windows	40-AB-FO-A5	i4-4150T	4	CZC4423FW	3
HP ProOne400	5 Primaria B	Windows	00-25-AB-A5	i3-6100T	4	CZC7119C2	3,2
HP	6 Primaria A	Windows	00-25-AB-A5	i3-6100T	4	NO	3,20
HP	6 Primaria B	Windows	00-25-AB-A5	i3-6100T	4	CZC77119C	3,20
LENOVO	1 ESO A	Windows	54-AB-3A-E4	i5-7200T	4	NO	2,70
LENOVO	1 ESO B	Windows		i5-7200T	4	no	2,70
LENOVO	2 ESO A	Windows	54-AB-3A-E4	i5-7200T	4	NO	2,70
LENOVO	2 ESO B	Windows	54-AB-3A-E4	i5-7200T	4	NO	2,70
LENOVO	3 ESO A	Windows	24-AB-3A-E4	i5-7200T	4	NO	2,70
LENOVO	3 ESO B	Windows	54-AB-3A-E4	i5-7200T	4	NO	2,70
LENOVO	4 ESO A	Windows	24-AB-3A-E4	i5-7200T	4	NO	2,70
LENOVO	4 ESO B	Windows		i5-7200T	4	NO	2,70

Cantidad	Ubicación	Tipo Ordenador	Nombre	S.O.	Window	Licencia Office	Licencia
	Aula de Informática móvil Info	portátil	Infantil 1				
1		portátil	Infantil 2				
1		portátil	Infantil 3				
1		portátil	Infantil 4				
1		portátil	Infantil 5				
1		portátil	Infantil 6				
1		portátil	Infantil 7				
1		portátil	Infantil 8				
1		portátil	Infantil 9				
1		portátil	Infantil 10				
1		portátil	Infantil 11				
1		portátil	Infantil 12				
1		portátil	Infantil 13				
1		portátil	Infantil 14				
64		portátil	Secundaria				
64		portátil	Primaria				
		portátil					

En total tenemos en el parque informático con cerca de 210 ordenadores, entre ordenadores de sobremesa y portátiles.

2.4 ARQUITECTURA DE LOS SISTEMAS

Esquema de la arquitectura de red del centro educativo:



Se crean diferentes redes según la necesidad para garantizar el acceso seguro a la red corporativa:

Equipo directivo → Red DirecciónN

Profesores → Red ProfesoradoN

Alumnos → Red AlumnadoN

Red para realizar diferentes pruebas de Seguridad →SSCC

A su vez se crean otras redes externas para aquellos usuarios que visiten el centro y necesiten conectarse a la red (Red Pública).

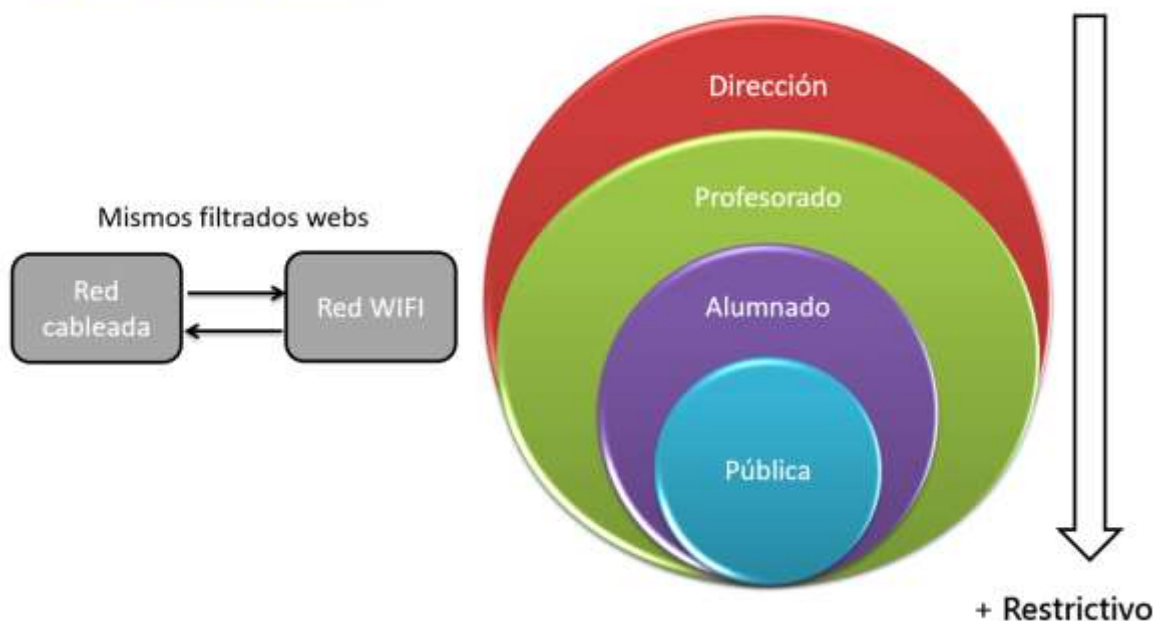
Esquema Infraestructura de red y algunos ejemplos de puntos de acceso utilizados para lograr llevar a cabo la señal WIFI a todo el centro educativo:

WIFI



De este modo, por medio de las diferentes redes creadas se logra un mayor filtrado de contenido, como muestra el siguiente esquema realizado:

Filtrado de contenido

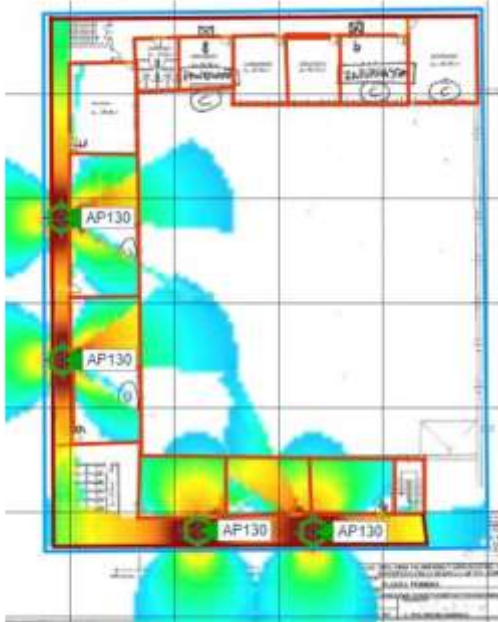


Para lograr llevar a cabo la correcta señal WIFI a todo el centro, se llevan a cabo las siguientes acciones:

Se tiene en cuenta los materiales del edificio para la simulación: paredes de cemento/madera, ventanas, baños, aulas cristal, etc.

- Se tiene en cuenta el uso y concurrencia necesaria
- Monitorización completa de qué usuarios hay conectados, dónde navegan y calidad de la señal
- Reinicio, actualizaciones de SO
- Se consigue una estimación de qué cobertura global tendrá el centro.
- Casos excepcionales: “punto móvil”

Simulación WIFI en el centro educativo:



En el apartado de la memoria del TFM relativo a la Seguridad, se detallarán las medidas tomadas a este respecto. Se muestran en el siguiente no obstante las directivas que se deben tener en cuenta en función de las necesidades detectadas en el centro educativo:

- Contraseñas: caducidad de las contraseñas para cumplir LOPD
- Instalación de Software: VNC, Paquete Office
- Control de Actualizaciones
- Imagen Corporativa
- Creación de usuarios administrador
- Configuraciones específicas para equipos y usuarios:
- Tiempo de bloqueo de equipos • Restricciones de acceso a los alumnos.

2.5 DETECCIÓN DE NECESIDADES Y APLICACIÓN

Se detectan las siguientes necesidades para la Organización educativa:



A su vez se muestran las necesidades para el Coordinador TIC del centro educativo:



Se muestran la necesidades detectadas para los profesores del centro educativo:



2.6 GESTIÓN DE INCIDENCIAS

2.6.1 OBJETIVOS DE LA GESTIÓN DE INCIDENCIAS EN EL CENTRO EDUCATIVO

Se implantan los siguientes objetivos diseñados, los cuales deben seguirse siempre por Coordinador TIC del centro docente:

- Registro de incidencias de empleados (profesores, dirección, secretarías...) con todo detalle así como peticiones de servicio, que deben incluir: apertura de la incidencia, la fecha de apertura del caso y el estado actual en que se encuentra el caso.
- Asignación de códigos de prioridad y categorías según el nivel de la incidencia.
- Informar a los usuarios (profesores y equipo directivo del centro) en todo momento del estado de la incidencia que se está tratando.
- Contacto con el “usuario” informado referente a un posible cambio a realizar.

- Cierre de todas las incidencias y peticiones de servicio que hayan sido resueltas.
- Actualizar la base de datos de conocimiento y base de datos de errores conocidos en función de las incidencias resueltas, de modo que se pueda encontrar solución a incidencias ya resueltas.
- Cerrar el ticket de la incidencia o petición de servicio en el momento en que se finalice ya que el cómputo del tiempo de la apertura y cierre formará parte de la estadística en el número y tiempo de resolución de incidencias.
- Seguimiento de procesos en creación de equipos nuevos, instalaciones... por medio de los mapas de procesos creados para el correcto seguimiento de los procesos.
- Seguimiento con el proveedor de reparaciones de hardware en ordenadores e impresoras según SLA firmado con proveedores (si lo hubiese)
- Control del stock informático del centro educativo.
- Informar sobre posibles mejoras, que pueda ser relevante para la gestión de los servicios, transmitiendo la información que proviene de los usuarios que no es una incidencia pero puede ser importante para la mejora de los servicios.
- Envío y realización de encuestas a los profesores y equipo directivo del centro educativo.
- Envío proactivo de informes solicitando la necesidad de algún tipo de soporte informático.
- Las Peticiones de Servicio serán responsabilidad del Coordinador del centro educativo, las cuales no incluyen las incidencias (tratadas en la gestión de incidencias) ni los cambios (tratados en la gestión de cambios), siendo recibidas y gestionadas dichas solicitudes o peticiones de los usuarios por el centro de atención al usuario.

2.6.2 ALCANCE DE LA GESTIÓN DE INCIDENCIAS EN EL CENTRO

- ✓ Las funciones definidas que se ha decidido que soporte el servicio SI son:
- ✓ Herramienta de Soporte al usuario (Profesorado, equipo directivo)
- ✓ Gestión de aplicaciones de Software
- ✓ Gestión de Hardware

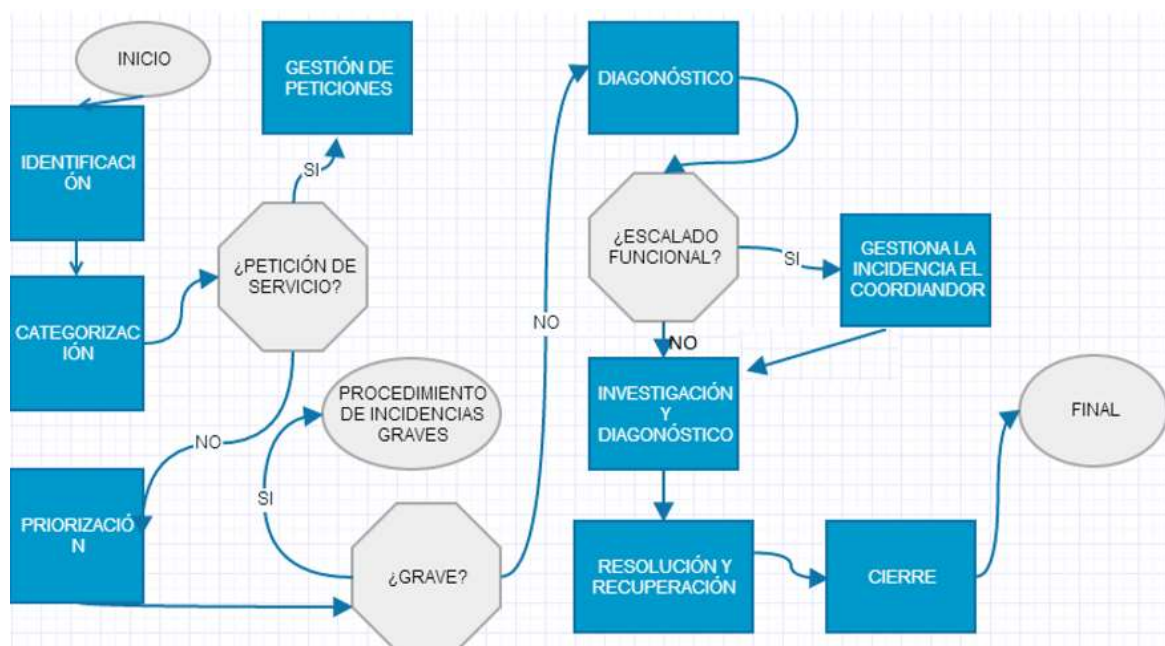
- ✓ Gestión de Sistemas
- ✓ Gestión Técnica
- ✓ Gestión de operaciones TI
- ✓ Gestión de Seguridad
- ✓ Gestión de Bases de Datos

2.6.3 PROCESO DE LA GESTIÓN DE INCIDENCIAS EN EL CENTRO

Referente a los procesos se decide lleva a cabo la siguiente gestión:

- Gestión de Peticiones de Servicio
- Gestión de Incidencias
- Gestión de Problemas
- Gestión de Accesos
- Gestión de eventos

Se muestra el diagrama que se ha creado con la herramienta gratuita Gliffy para la gestión de incidencias:



Como objetivo de la gestión principal de la gestión de incidencias se define restaurar la operación del servicio con la mayor brevedad posible minimizando el impacto negativo sobre las operaciones de negocio, de modo que se aseguren los mejores niveles de calidad y disponibilidad del servicio.

En referencia a las incidencias graves como se ha decidido y reflejado en el diagrama, requieren de un tiempo más corto y una mayor urgencia. Por lo que se redacta un procedimiento a seguir para este tipo de incidencias el cual puede requerir personal dedicado a una tecnología concreta.

2.6.4 KPI DE LA GESTIÓN DE INCIDENCIAS EN EL CENTRO EDUCATIVO

Se ha decidido utilizar los siguientes indicadores y métricas (KPI de la gestión de incidencias):

- Tiempo medio para resolver cada incidencia y cerrarla.
- Número de tickets total.
- Porcentaje de incidencias resueltas al momento.
- Porcentaje de incidencias no resueltas en el acto.
- Porcentaje de incidencias escaladas resueltas
- Satisfacción del usuario.
- Porcentaje de peticiones de los usuarios que se derivan al proveedor de reparaciones de hardware de ordenadores e impresoras.
- Porcentaje de cumplimiento de los SLA (proveedor).
- Cantidad de incidencias no resueltas.
- Número y porcentaje de incidencias graves.
- Número y porcentaje de incidencias categorizadas de modo incorrecto
- Porcentaje total de incidencias cerradas.
- Especificación de las incidencias según franja horaria.

2.6.5 CREACIÓN DE BASE DE DATOS DE ERRORES CONOCIDOS PARA EL CENTRO DOCENTE

Se ha decidido la creación y mantenimiento de una base de datos de errores conocidos, de modo que las incidencias solucionadas pasen a formar parte de dicha base de datos, lo que logra el consiguiente beneficio en posteriores resoluciones de problemas que ya han sido tratados. La base de datos de errores conocidos (KEDB), nos permite el almacenamiento centralizado de errores ya tratados, así como las incidencias y resoluciones de los casos.

Se dictamina que por tanto que aparezcan detallados los fallos y el número de incidencias clasificadas por tipología (dirección, referente a los alumnos, profesorado...) de modo que ayuden a la priorización de problemas futuros.

Antes de introducir un contenido, el KEDB buscará que el contenido que se pretende añadir ya no exista, analizando la entrada para evitar duplicidad de casos iguales.

Tenemos el objetivo de indicar que se logra realizar con mayor rapidez la resolución de incidencias ya tratadas debido a que ya conoceremos gracias a KEDB, como ofrecer solución a las incidencias ya resueltas de nuestro centro que tengan tendencia a la repetición. De este modo se logra por tanto evitar pérdidas de tiempo innecesarias en la búsqueda de soluciones a incidencias que ya hemos solucionado.

2.6.6 MEJORA CONTÍNUA DEL SOPORTE INFORMÁTICO EN EL CENTRO EDUCATIVO

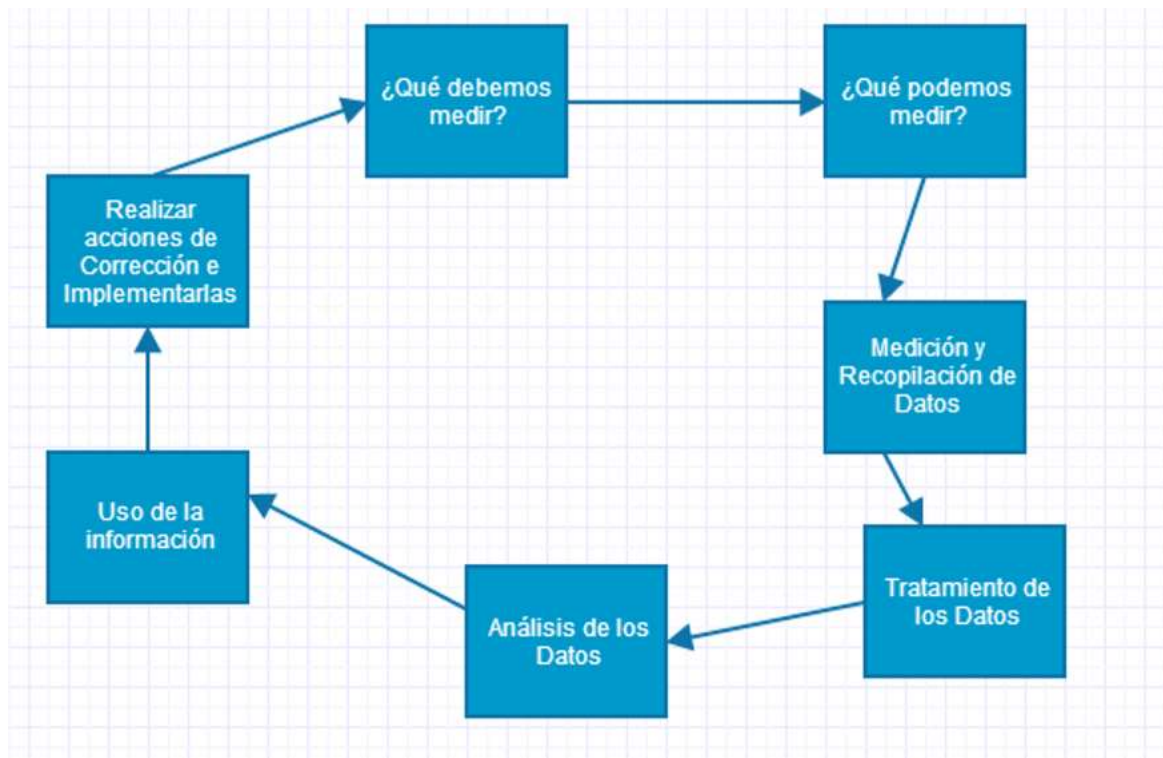
La mejora continua en este caso, define analizar, revisar, y hacer recomendaciones ante las posibles oportunidades de mejora detectadas en el centro.

Deberemos realizar, propuestas de mejora mediante la identificación de actividades que mejoren la calidad del servicio en el centro educativo, mejorando la eficiencia y efectividad de los procesos de la organización.

Se seguirá el estándar del Ciclo de Deming para la mejora de los procesos. Lo que incluye la planificación de la definición de los objetivos, realizar las implementaciones oportunas (hacer), verificar que se logra el objetivo propuesto (analizar), actuar mediante la ejecución de las propuestas detectadas y realizando nuevas propuestas de mejora continua.

Las métricas definidas, permitirán lograr medir la calidad (así como cantidad) del servicio propuesto, lo que nos ofrece la posterior evaluación de los objetivos cumplidos. Y a su vez nos va a permitir un mejor análisis de la mejora continua a implementar durante el ciclo continuo del soporte en el centro docente.

Se muestra el diagrama con los pasos adoptados en la mejora continua, propuestos a seguir por el Coordinador TIC (realizado por medio de la herramienta Gliffy):



3. PLAN DE ACCIÓN: SEGURIDAD INFORMÁTICA EN EL CENTRO DE ENSEÑANZA

De mi experiencia de profesor y Coordinador TIC ,he apreciado en reiteradas ocasiones, el desconocimiento por parte de alumnos y docentes en el área de seguridad y protección de datos.

Al no haber un plan de convivencia del centro adaptado al uso de las Nuevas tecnologías, en el cual se debería dejar constancia de la aplicación de privacidad y normas de protección de datos en el centro considero una parte importante de trabajo profundizar en este aspecto.

La constitución española de 1978 garantiza “el derecho al honor, a la intimidad personal y familiar y a la propia imagen” (art. 18.1 CE). A su vez, cita que “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos” (art. 18.4 CE).

Los centros de enseñanza por consiguiente, deben ser conscientes de que sus alumnos son titulares de los derechos fundamentales que se deben respetar:

- El derecho a su intimidad, recogido en el art. 18 de la Constitución Española (8).
- El derecho a la protección de sus datos de carácter personal, consagrado en la Sentencia del Tribunal Constitucional 292/2000.(9)

La Ley Orgánica de Protección de Datos (10), nace con el objetivo de “garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar” (art. 1 LOPD), siendo aplicable “a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado” (art. 2 LOPD).

Con la entrada en vigor de la Ley Orgánica 15/1999(8) de Protección de datos de carácter personal se establece la obligación de tener que notificar a la Agencia de Protección de Datos los ficheros con datos de carácter personal registrados en soporte físico, así como inscribirlos en el Registro General de Protección de Datos. Y el deber de crear una documentación de seguridad en la que aparezcan los artículos del Reglamento de Medidas de Seguridad de los ficheros automatizados que tengan incluidos datos de carácter personal como se aprobó en el Real Decreto 994/1999 del 11 de Junio.

La Disposición adicional vigesimotercera de la LOE (11) establece que “la incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad”. Por lo cual, el hecho de la incorporación del alumno o la alumna al centro de enseñanza implica el consentimiento para el tratamiento de sus datos.

En los centros de enseñanza pública es necesario notificar los ficheros en el Registro General de Protección de Datos por medio de un responsable del fichero “la obligación de notificación corresponderá al responsable del fichero, definido por el artículo 3 d) de la Ley Orgánica 15/1999 como “Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”.

Los ficheros tratados de un centro docente concertado deberán acogerse al régimen establecido para los ficheros de titularidad privada tal y como se establece en el artículo 5.1.1 del Real Decreto 1720/2007, por el cual se aprueba del Reglamento de desarrollo de la LOPD. Entendiendo como centro concertado tales los centros privados acogidos al régimen de conciertos legalmente establecido. En cuanto a los centros privados concertados el fichero tendrá el mismo tratamiento que el régimen establecido para los ficheros de titularidad privada.

El centro de enseñanza necesita según el reglamento de la Protección de datos (1720/2007), analizar en referencia a los ficheros registrados un documento de seguridad, donde designaremos a los responsables de los ficheros y de seguridad, de los administradores y usuarios de seguridad.

3.1 ANÁLISIS Y MEJORA DE LA INFRAESTRUCTURA DE LA RED

3.2 GESTIÓN DE CONTRASEÑAS

En este punto, la gestión correcta de contraseñas será de vital importancia para evitar accesos no deseados ya sea los servidores o los ordenadores personales de los usuarios.

El usuario, ya sea profesor, alumno, personal administrativo, directivo... debe ser responsable de la confidencialidad de su contraseña, y en caso de que detecte que le ha sido robada, deberá comunicarlo al administrador de sistemas con la mayor brevedad posible.

Se crea en el servidor, por medio del Active Directory una contraseña a cada persona trabajadora del centro, donde obligaremos a su cambio cada 3 meses para una mayor seguridad.

Se controla el acceso al sistema donde pueda intentar acceder un máximo de 5 veces, y en caso de bloqueo el usuario le comunicará al Coordinador TIC del centro docente el bloqueo para que vuelva a poder tener el acceso correspondiente.

Con tal de mejorar la seguridad, el usuario deberá introducir una contraseña y tener en cuenta unas determinadas reglas:

- Contraseña con más de 8 caracteres y deberá tener mayúsculas, minúsculas y caracteres.
- No se podrá repetir contraseña en la futura petición para que sea diferente.
- Prohibición de usar contraseñas sencillas como puede ser el nombre, fecha de nacimiento...
- No decir la contraseña a otros empleados
- No escribir la contraseña ya sea en papel o digitalmente.

3.2.1 GESTIÓN DE ACCESOS DE INFORMACIÓN A USUARIOS: PROFESORADO Y ALUMNADO

Para el acceso a la información para profesores y alumnos, se crearán diferentes grupos de acceso en el servidor otorgando a cada usuario que accede al sistema la conexión a las unidades mapeadas del servidor que necesita para su trabajo diario en la empresa tal y como se ha comentado en el punto del trabajo relacionado con este aspecto

Por lo que se garantizará una relación de este modo eficaz definiendo las personas y grupos que son partícipes del centro donde se podrá asegurar la seguridad de los datos gracias a la concesión de permisos controlando que accesos deben tener los diferentes usuarios.

Se darán permisos sólo para acceder a la información que necesite cada miembro de la comunidad docente o también permisos para acceder a la información y permitir cambios.

Ya que LOPD nos dice que debe haber una relación siempre actualizada de los perfiles o usuarios y los accesos que tienen autorizados, documentando el mecanismo que eviten el acceso a zonas no autorizadas, en este caso, cada usuario tendrá una conexión por medio de un login individual donde directamente al entrar al sistema acceda a sus unidades del servidor en función del perfil del usuario, si es un componente del equipo directivo, un profesor, un alumno...

Para el control de acceso elaboraremos con listas de control de acceso donde se establecerán los diferentes permisos.

3.3 GESTIÓN DE LOS BACKUPS DEL CENTRO

Se decide la medida de realizar copias de seguridad cada día debido a la importancia de la actividad del centro docente y la importancia de los datos.

Estamos hablando de datos como la introducción de notas diarias por parte de los profesores, informes de tutorías, incidencias con alumnos que pueden verse reflejadas en el expediente, por lo que es de vital importancia el backup diario.

Se cuenta con procedimientos que nos garanticen la recuperación total de fichero, especificando la ubicación física de los ficheros.

Se asegura en caso de necesidad de restauración, mediante un procedimiento, como puede ser reconstruir el sistema operativo o la recuperación de las bases de datos, archivos o documentos.

Se decide a su vez contar con imágenes de los portátiles para su restauración en cuanto sea necesaria de modo que tengamos siempre preparadas imágenes para los portátiles según el perfil. Por ejemplo, si es de un alumno una imagen con aquel software que usa en el aula (Arduino, Scratch, Software de Impresión 3D...). En caso de que sea el portátil del aula de un profesor, disponer de una imagen para restaurar el perfil básico del profesor (el software que utiliza como el Office, accesos directos a la plataforma de los profesores, al correo...)

3.3.1 DEFINICIÓN DEL PLAN DE COPIAS DE SEGURIDAD

Se adopta por tanto la medida de realizar copias de seguridad diarias debido a la importancia de los datos del centro docente.

Se especifica la ubicación física de los ficheros donde contaremos con procedimientos que nos garanticen la recuperación total de fichero.

Los procedimientos han de garantizar la correcta reconstrucción del fichero.

Se muestra la medida tomada referente a uno de los ficheros declarados, en este caso el fichero PROFESORES-CONTRATADOS, el proceso será similar para el resto de ficheros declarados o que se declaren en un futuro:

Archivos de logging y procedimientos de recuperación propios del sistema:
Existe un log de acceso al fichero gestionado por la aplicación que lo mantiene. Sí se realizan copias de seguridad del fichero. Las copias de seguridad están programadas

Procedimiento de respaldo y recuperación del fichero de PROFESORES-CONTRATADOS:

- ✓ Respaldo: Se realizan copias de seguridad diariamente del servidor de ficheros a una cinta de resguardo. Las copias se realizan de la unidad de datos del servidor.

Recuperación: El procedimiento de recuperación es el siguiente:

1. En caso que se estropeará alguno de los discos del servidor es el siguiente:

Ponerse en contacto con el fabricante. En el transcurso de 4 horas un técnico se persona en las instalaciones y en caliente (sin parar el servidor) procede a intercambiar en el servidor el disco estropeado por el disco en mirroring. El disco estropeado se sustituye por uno nuevo.

2. En caso que se estropearan todos los discos de una misma unidad (C o D).

Problemas con la unidad C:

- Reinstalar el servidor con los programas de base necesarios para su funcionamiento en la unidad C. (Sistema Operativo, red, Antivirus, configuración centralita de teléfonos y herramientas de administración)
- Establecer una contraseña para el usuario administrador e informar a los administradores del servidor.

Problemas con la unidad D:

- Volcar de la copia en cinta más reciente en la unidad D todos los datos de los directorios del servidor.
- Restablecer las contraseñas en los directorios.
- Restablecer las listas de acceso a los directorios.
- Restablecer la impresora como recurso compartido.
- Activar las copias de seguridad.

3. En caso de que se estropeará el ordenador que da acceso a la carpeta del servidor:

1. Recuperar del servidor o cinta según sea el caso, la última copia del programa.
2. Reinstalar el ordenador con los programas de base necesarios para su funcionamiento. (Sistema Operativo, red, etc)
3. Crear la carpeta “control” en la unidad c:\
4. Copiar el directorio con los ficheros recuperados del servidor de copia de seguridad a esta carpeta.
5. Habilitar la compartición del directorio de acceso total con contraseña.
6. Crear la unidad E:\ que apunta a la carpeta “tempo”.
7. Revisar los ordenadores que se conectan a este directorio para aplicar la nueva contraseña.

8. Informar a los usuarios que tienen acceso al fichero de la nueva contraseña del directorio.

9. Activar las copias de seguridad.

3.4 GESTIÓN DE CUENTAS DE USUARIOS

La gestión de cuentas de usuarios y permisos se va a llevar desde el Active Directory, con las normas previamente descritas y otorgando los niveles de seguridad que se han mencionado durante el trabajo según el perfil que estemos tratando.

Los miembros de mismos equipos, como el equipo directivo, el claustro de la ESO, de Primaria, Infantil, Equipo de Pastoral, Secretaria... tendrán acceso a sus recursos compartidos de modo que se logre un mejor nivel de seguridad y un mejor acceso al poder compartir recursos entre mismos “departamentos”

3.5 APLICACIÓN DE NORMAS DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Medidas obtenidas siguiendo las recomendaciones y normativa de la LOPD:

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS DE NIVEL BÁSICO

- 1. Elaborar un documento de seguridad que recoja medidas técnicas y organizativas referentes a la normativa vigente de seguridad.*
- 2. Registrar las incidencias: Tener a disposición un procedimiento para notificar y registrar las incidencias.*
- 3. Funciones y obligaciones del personal: Definir y documentar las personas con acceso a los datos de carácter personal.*
- 4. Usuarios: Crear relación de los usuarios con acceso autorizado a los ficheros con datos de carácter personal, de los responsables de Seguridad y otras figuras que estipula la ley.*
- 5. Gestionar los usuarios y contraseñas en la red. Cada empleado debe disponer de un usuario personal y contraseña para el acceso al sistema operativo de su equipo y a los servicios por lo que se elaborará un procedimiento definido y documentado de asignación, distribución y renovación de códigos de acceso, no será superior a un año.*
- 6. Creación de un sistema que permita añadir perfiles de acceso para asegurar que los usuarios únicamente tienen acceso a los datos y recursos necesarios para el desarrollo de sus funciones.*

7. *Realización de Backups diarios.*

8. *Dispositivos de almacenamiento: Se diseñarán mecanismos que hagan difícil su visualización/apertura.*

9. *Dispositivos portátiles: Tomar medidas de seguridad necesarias para este tipo de dispositivos.*

10. *Vigilancia de soportes: Impedir que a la documentación pueda acceder personal no autorizada.*

Medidas obtenidas siguiendo las recomendaciones y normativa de la LOPD:

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS DE NIVEL MEDIO

1. *Identificación y autenticación de acceso: Crear un mecanismo que limite la posibilidad de intentar varias veces el acceso no autorizado al sistema de información por ejemplo mediante la creación de políticas del sistema operativo limitando el número de intentos desde una misma IP.*

2. *Gestión de soportes y de documentación: Creación de un registro de entrada de soportes que facilite conocer el tipo de documento, la fecha y hora, el emisor, el número de documentos, el tipo de información que contenga, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.*

3. *Control de accesos físico: Sólo el personal autorizado tendrá acceso a las ubicaciones donde se encuentren los equipos físicos de los sistemas de información.*

4. *Registro de incidencias: Deberán documentarse los procedimientos de recuperación de datos, indicando la persona que va ejecutar el proceso y los datos restaurados.*

El centro de enseñanza tiene que tener presente que existen ficheros especialmente protegidos con una protección más fuerte y que debe garantizar mayor seguridad, (art. 7 de la Ley Orgánica 15/1999). En este contexto encontramos los siguientes ejemplos para el centro:

- *Datos de origen racial de determinados estudiantes del centro de enseñanza*
- *Datos referentes al grado de minusvalía de algunos estudiantes del centro de enseñanza que requieren necesidades educativas especiales.*
- *Datos de determinados estudiantes del centro de enseñanza que tienen problemas de salud y les imposibilita hacer ejercicio físico.*
- *Datos referentes a la salud de los estudiantes del centro de enseñanza obtenidos en diferentes test realizados por los orientadores del centro.*

3.6 OTRAS MEDIDAS DE SEGURIDAD IMPLANTAR DESDE EL DEPARTAMENTO SI/TI DEL CENTRO DE ENSEÑANZA

Otras medidas necesarias que se decide implantar en fruto a la experiencia de trabajar en este tipo de centros es la siguiente:

Los Sistemas operativos en los portátiles de los alumnos deberán estar preinstalados para que los alumnos del centro no puedan ejecutar comandos como root, impidiendo que instalen nuevo software lo que incluyen videojuegos.

Se decide restringir el acceso en el centro de enseñanza a páginas de internet no destinadas a fines educativos.

Se otorgará acceso libre a la web a los docentes del centro de enseñanza sin restricción a la vez que se realiza la restricción de páginas web a los portátiles de los alumnos.

Se adoptan las siguientes medidas que siempre me han dado buen resultado:

- Se limita el acceso del usuario, solo a las carpetas del servidor que sean necesarias para desempeñar su trabajo, para que no pueda acceder a documentación que no le atañe.
- Se prohíbe el uso de herramientas de conexión remota a los ordenadores del centro de enseñanza. Se realizará por medio de políticas en el servidor, permitiendo solo que usuarios autorizados previamente puedan hacer uso de conexiones remotas.
- Se obliga a la activación de un salvapantallas de modo que se active al cabo de unos minutos cuando el usuario no haga uso de su equipo, y así le tendrá que solicitar la contraseña y se evita que otro usuario pueda acceder a su ordenador.
- En caso de que un empleado del centro de enseñanza necesita copiar archivos de carácter personal a un dispositivo móvil o un ordenador portátil, deberá solicitarlo previamente Coordinador TIC del propio centro de enseñanza, en este caso a mi persona.
- Si se crea un fichero propio de datos de carácter personal se deberá solicitar la autorización correspondiente
- Se limitan las propiedades avanzadas del sistema operativo, de modo que el usuario no pueda cambiar la configuración, solo bajo autorización del Coordinador TIC.
- Se Prohíbe acceder a redes externas que no sean las que maneja el centro docente debido a su peligrosidad ya que hay multitud de redes libres que podrían ser un riesgo su conexión.

3.7 FICHEROS DEL CENTRO DE ENSEÑANZA Y SU CUMPLIMIENTO EN MATERIA DE LA LOPD

3.7.1 PROCESO DE SEGURIDAD EN FICHEROS AUTOMATIZADOS Y NO AUTOMATIZADOS DEL CENTRO

Para los ficheros del centro docente, se definirá el escenario de obligaciones mediante la siguiente tabla, en la que se crean las diferentes medidas de seguridad y procedimientos de los ficheros automatizados donde se dan los diferentes niveles de seguridad, las obligaciones a tener en consideración, la documentación de seguridad y el control y revisión en función de nuestras necesidades:

Medida de Seguridad Procedimiento FICHEROS	NIVEL DE SEGURIDAD	DOCUMENTO DE SEGURIDAD	CONTROL Y REVISIÓN	OBLIGACIONES
Responsable de Seguridad	Alto	Documentado	OK	Obligaciones propias de los responsables definidas
Identificación y autenticación	Alto	Documentado	OK	Limitar intentar varias veces el acceso no autorizado al sistema de información
Control de Acceso	Alto	Documentado	OK	Adoptar políticas de control desde el servidor de acceso a los recursos de la red de cada usuario
Control de Acceso físico	Alto	Documentado	OK	Solo el personal autorizado tendrá acceso a las ubicaciones donde se encuentren los equipos físicos
Gestión de soportes y documentos	Medio	Documentado	OK	Se debe inventariar los soportes y

				documentos que contengan datos de carácter personal
Ficheros temporales	Básico	Documentado	OK	Una vez que el fichero temporal o copia de trabajo ha dejado de ser necesario para los fines de su creación deberá ser eliminado del sistema
Registro de incidencias	Medio	Documentado	OK	Siempre el Coordinador TIC del Centro a petición de usuarios.
Backups	Alto	Documentado	OK	Copias de Seguridad semanales
Pruebas reales con datos	Medio	Documentado	OK	Coordinador TIC
Funciones y obligaciones del personal	Medio	Documentado	OK	Documento redactado
Teletrabajo	Medio	Documentado	OK	Gestión de acceso externo

3.7.2 RESPONSABILIDADES DE LOS FICHEROS

El Coordinador TIC del centro docente tendrá la función de controlar, supervisar y coordinar las medidas de seguridad.

En función de cada departamento (equipo directivo, tecnología, seminario de matemáticas...), se designarán a los diferentes responsables de seguridad que se encargarán de controlar las medidas de seguridad, se debe realizar un fichero con la relación de los componentes que se han nombrado como responsables de seguridad, de modo que se tenga documentada esta información.

Las personas que se asignen, deberán hacerse responsables del fichero asignado, controlando y coordinando las medidas de seguridad aplicadas.

Será necesario entonces que el responsable del fichero adopte las medidas necesarias para llevar a cabo la tarea encomendada y tenga la capacidad de conocer y saber adoptar tales medidas..

3.8 PLAN DE CONVIVENCIA EN EL CENTRO EN EL USO DE LAS NUEVAS TECNOLOGÍAS Y LA RED

Se decide proponer al centro docente, dentro del plan que se está realizando, unas indicaciones en materia de nuevas tecnologías para lograr que se reflejen el plan de convivencia del centro de enseñanza, por medio de las normas de comportamiento y reglamentos oportunos en la materia.

Son una serie de indicaciones que en unas prácticas que había realizado en otro colegio, tuvieron un gran éxito para que formaran parte del plan de convivencia del centro:

Información y colaboración con las familias: El centro educativo debe informar a las familias en referencia al correcto uso de las TIC. De modo que colaboren con el centro de enseñanza en seguir las directrices marcadas por el propio centro para lograr el correcto proceso educativo en formación en la seguridad de los alumnos en la materia.

Respeto a los alumnos y personal del centro de enseñanza: No se permite difundir en las redes sociales y por ende internet, ningún tipo de imagen, foto o video de cualquier miembro de la comunidad educativa del centro.

Protección de la imagen del alumno: Los alumnos y alumnas del centro de enseñanza, deberán evitar subir imágenes propias e información que los pueda identificar a las redes sociales sin el permiso de la familia.

Uso responsable y seguro de las TIC: El centro debe promover el uso responsable y seguro de las TIC en los alumnos del centro de enseñanza.

Restricción del uso de los móviles: No se permite el uso de dispositivos móviles en horario escolar, a excepción de autorización específica de un profesor por una causa o motivo completamente justificado.

Inculcar al alumno comportamientos adecuados en el uso de las redes sociales: El centro debe fomentar valores a sus alumnos en el correcto uso de las redes sociales, de modo que se eviten riesgos y todas aquellas actividades que ponen en riesgo al alumno como la suplantación de identidad, acoso, robo de datos, o la adicción.

Asesoramiento y apoyo del centro de enseñanza al alumno en conflictos derivados de las TIC: El centro de enseñanza, ante cualquier conflicto, falta de respeto o acoso en materia de las tecnologías de la información y comunicación, apoyará y asesorará al alumno tomando las medidas oportunas para la resolución del conflicto.

4 DESARROLLO DE PRODUCTOS TECNOLÓGICOS DE MAYOR COMPLEJIDAD DESDE EL DEPARTAMENTO DE TECNOLOGÍA PARA SU POSTERIOR REALIZACIÓN EN LAS AULAS

4.1 REALIZACIÓN DE UN PROYECTO COMPLEJO DE ROBÓTICA EN ARDUINO CON SENSORES DE ULTRASONIDOS

Un complemento imprescindible para muchos de robots o vehículos controlados a distancia es por medio de un sensor que nos haga saber la distancia libre de obstáculos para movernos. En caso de que las distancias van a ser pequeñas podemos emplear sensores de infrarrojos, pero si en caso de querer movernos en áreas grandes y poder medir distancias en un rango de varios metros el complemento perfecto es un sensor de ultrasonidos.

Su funcionamiento es igual que el de un radar. Emitirá un pulso de sonido a una frecuencia tan alta que es imperceptible para el oído humano y a su vez cronometra el tiempo que el sonido tarda en llegar a un obstáculo, rebotar y volver al sensor. Como la velocidad de propagación del sonido en el aire es un dato conocido (343.2 m/s) por medio de mano la conocida fórmula ($e = v * t$) calculamos la distancia recorrida por el sonido.

Se decide realizar un complejo proyecto en Arduino de Ultrasonidos mediante el que se pretende recrear el sistema de aparcamiento en un coche, el cual realizará las siguientes funciones:

- Sistema de detección de distancia por el que el robot nos marcará por medio de unos leds de colores la distancia a la que nos acercamos del siguiente modo: Se encenderán dos leds azules en una primera aproximación al sensor de ultrasonidos, a continuación, se encenderán dos leds de color verde si se está más próximo aún del sensor de ultrasonidos, dos leds amarillos más cerca aún y cuando se está prácticamente tocando el objeto se encenderán dos leds rojos de alerta. Estos leds realizarán el proceso inverso cuando el objeto se aleje del sensor de ultrasonidos, realizando el proceso inverso.

- A su vez, constará de un zumbador igual que en el sistema de un coche, que irá aumentando la vibración del pitido cuanto más cerca estemos del objeto.

- Por medio de una pantalla programable LCD 1602 mostraremos igual que en sistema de un coche por medio de pantalla la distancia a la que está el sensor de ultrasonidos del objeto.

- Se utilizará un Relé para Arduino de modo para conmutar grandes picos de tensión o intensidad y el que en este caso se activará del mismo modo que los leds para marcar la situación como corresponde a una señal de alarma.

4.2.1 ANÁLISIS DEL PROYECTO

4.2.2 REQUERIMIENTOS DE MATERIALES Y TÉCNICOS NECESARIOS

Para llevar a cabo el trabajo de la recreación del Sistema de Aparcamiento de un coche, se han utilizado los siguientes materiales de Robótica:

- ✓ Placa con Microcontrolador Arduino Uno con 14 entradas/salidas digitales y 6 de estas pueden utilizarse para salidas PWM
- ✓ Placa Board 830 Puntos
- ✓ 10 Resistencias de 220h
- ✓ Potenciómetro 10 K
- ✓ Shield Relé
- ✓ 2 Leds Diodos color Verde 5mm
- ✓ 2 Leds Diodos color Ámbar 5mm
- ✓ 2 Leds Diodos color Rojo 5mm
- ✓ 2 Leds Diodos color Azul 5mm
- ✓ 10 Latiguillos Board Macho-Macho

- ✓ 10 Latiguillos Board Macho-Hembra
- ✓ Zumbador Eléctrico activo para C.I
- ✓ Display LCD 1602 II

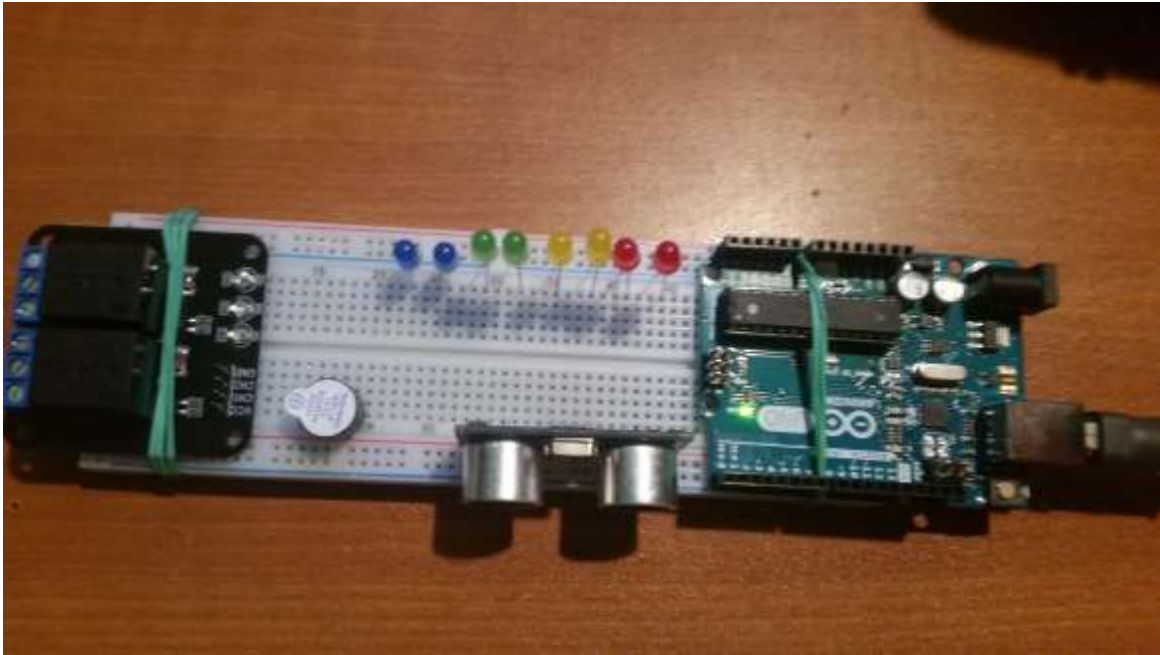
Se ha necesitado descargar el IDE de Arduino disponible en su página web

4.2.3 CONSTRUCCIÓN Y FASES DEL PROYECTO: RÓBÓTICA

Debemos de tener presente que un pulso ultrasónico se transmite y se refleja en un objeto, el sensor recibe el pulso y lo convierte en una señal eléctrica. El siguiente pulso podrá ser transmitido cuando el eco desaparezca. Si un pulso de anchura $10\ \mu\text{s}$ es mandado al pin de trigger (en nuestro caso el pin digital número 8), el ultrasonido enviará ocho señales y detectará el eco desde el pin de ECHO (en nuestro caso será el pin digital 7). La medida de la distancia es proporcional al ancho de pulso del eco, el cual puede ser calculado por fórmula.

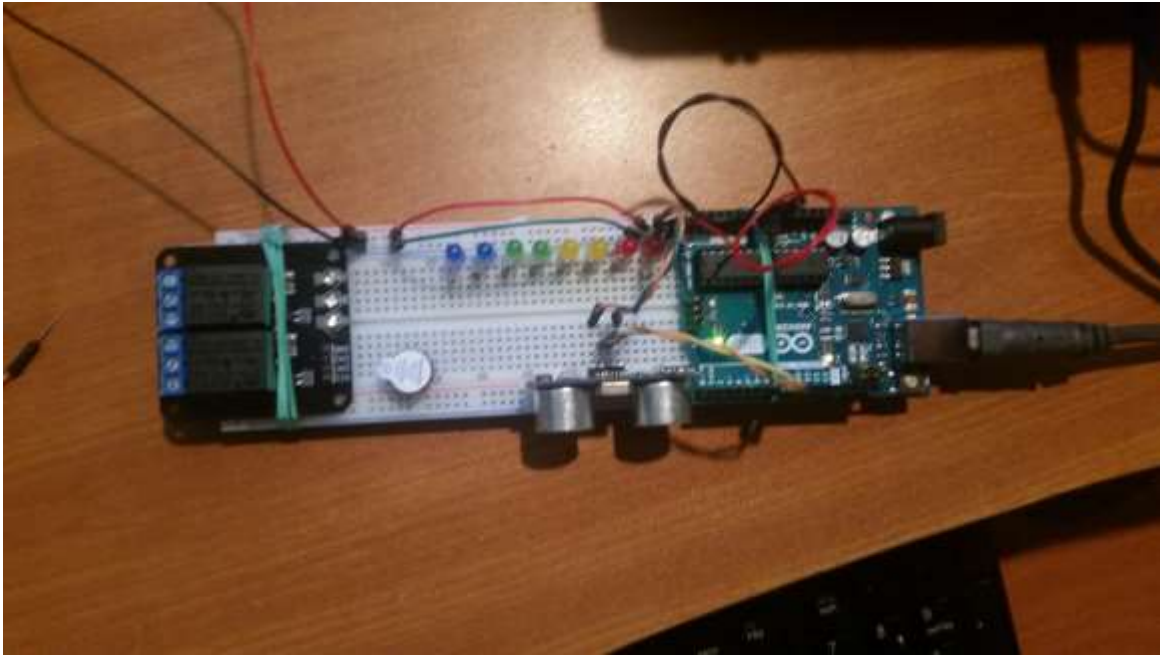
Se muestra la foto del proyecto en el que se pretende recrear el sistema de aparcamiento en un coche en su primera fase que recordemos era la siguiente:

Sistema de detección de distancia por el que el robot nos marcará por medio de unos leds de colores la distancia a la que nos acercamos del siguiente modo: Se encenderán dos leds azules en una primera aproximación al sensor de ultrasonidos, a continuación, se encenderán dos leds de color verde si se está más próximo aún del sensor de ultrasonidos, dos leds amarillos más cerca aún y cuando se está prácticamente tocando el objeto se encenderán dos leds rojos de alerta. Estos leds realizarán el proceso inverso cuando el objeto se aleje del sensor de ultrasonidos, realizando el proceso inverso.

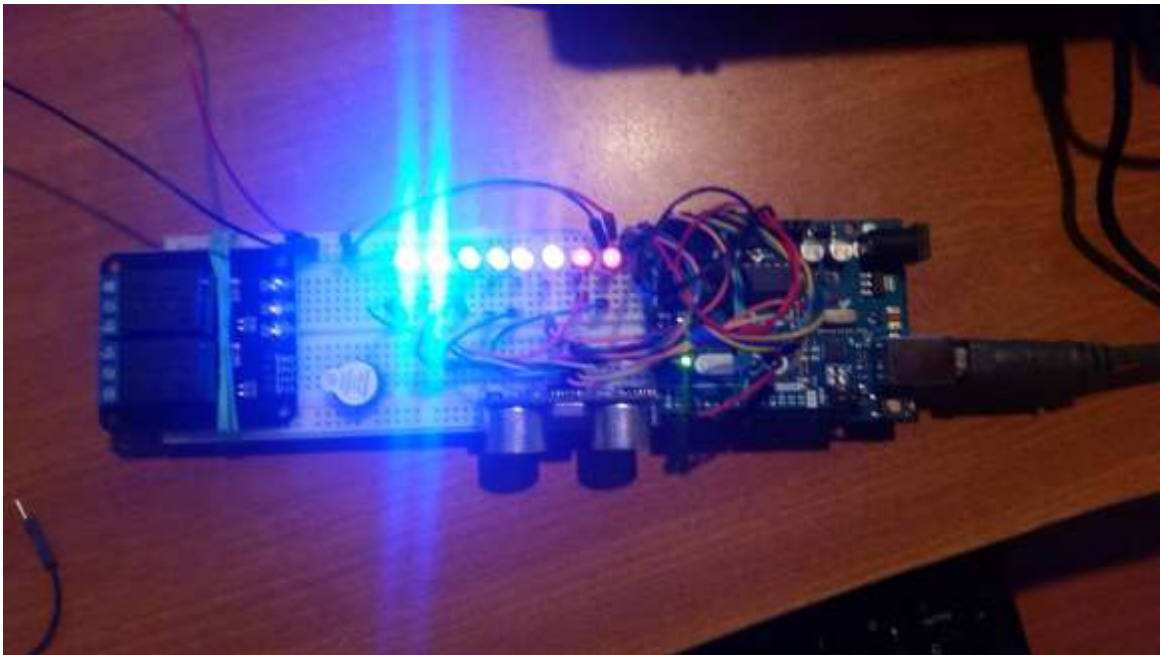


A su vez, constará de un zumbador igual que en el sistema de un coche, que irá aumentando la vibración del pitido cuanto más cerca estemos del objeto.

Se añaden unas resistencias para controlar el flujo de la corriente y el Zumbador que deberá ser programado de modo que cuando más cerca esté del objeto el robot mayor sea la vibración del sonido que emite igual que en el sistema de un vehículo y añadimos también el Relé.



Se realizan las conexiones del circuito:



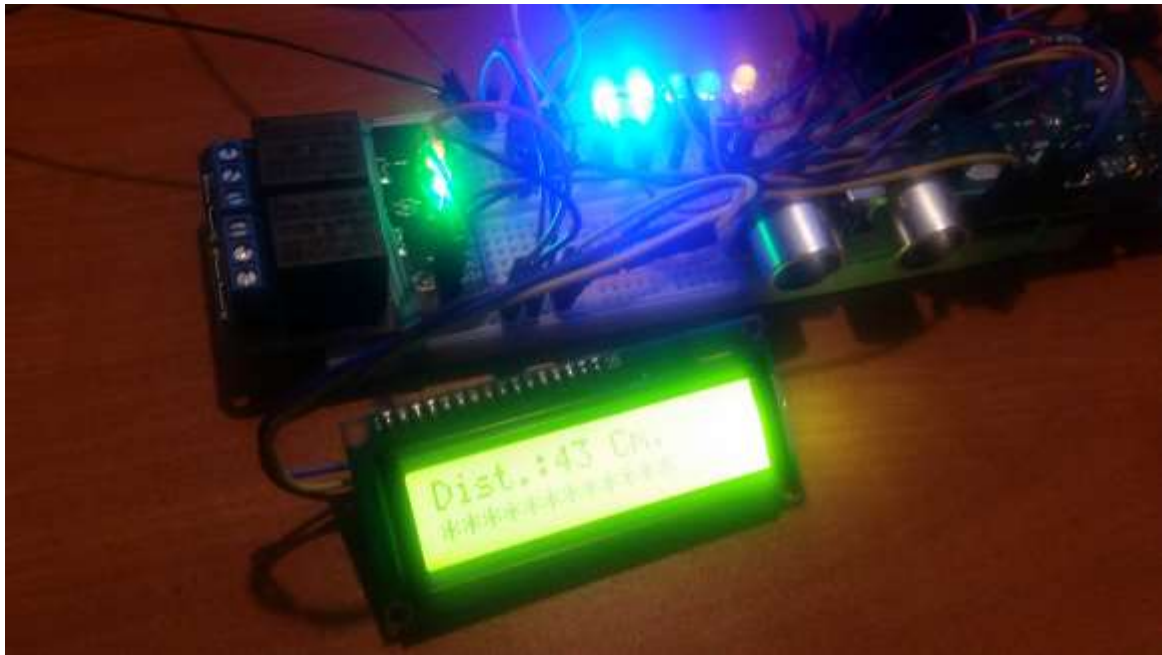
Por medio de una pantalla programable LCD 1602 mostraremos igual que en sistema de un coche por medio de pantalla la distancia a la que está el sensor de ultrasonidos del objeto.



4.2.4 ENTREGA FINAL DEL PRODUCTO Y CÓDIGO FUENTE

Se muestra el desarrollo final del producto tecnológico que imita al Sistema de un aparcamiento en un Vehículo (a su vez se incluye un vídeo adjunto fuera de la memoria) que muestra el mismo en el que se aprecia el modo en el que al acercarse al sensor de ultrasonidos, las luces comienzan a cambiar de color en función de la cercanía, recordemos Azul muy lejos → Verde lejos → Amarillo cerca → Rojo casi tocando (al alejarse del sensor de ultrasonidos, he programado el paso inverso de luces pasando de Rojo → Amarillo → Verde → Azul).

El Relé igualmente comienza a encender leds en función de la cercanía, el zumbador comienza a pitar elevando el tono cuando más cerca estamos del objeto y el Display programado nos muestra la información por pantalla de los cm a los que estamos aproximados al objeto.



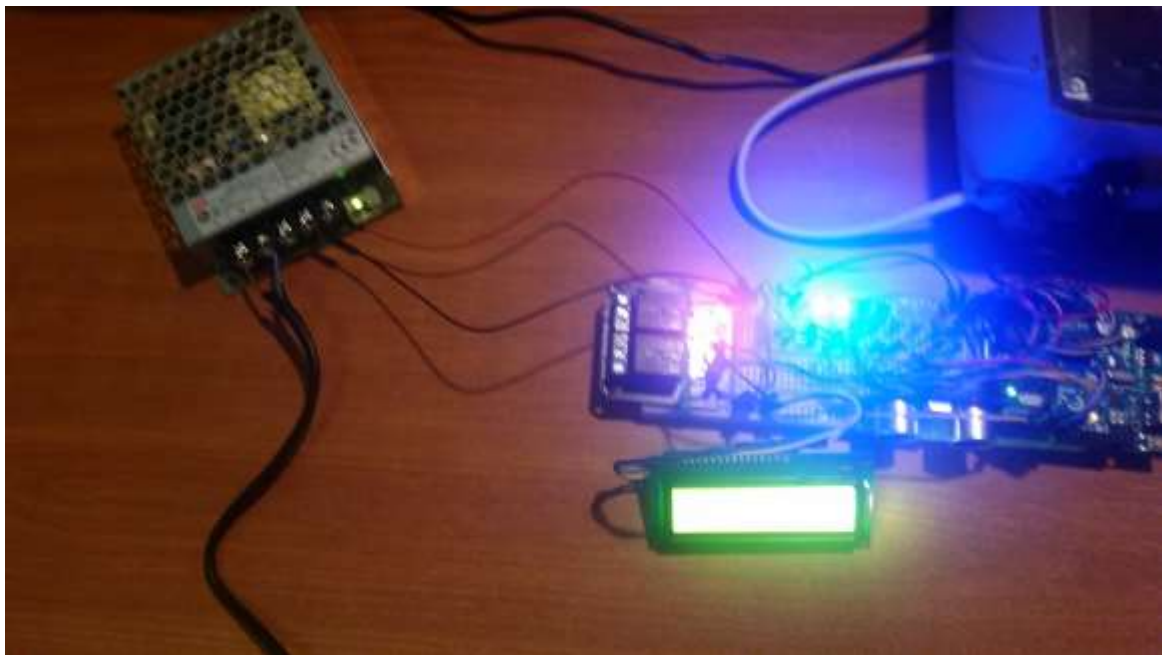
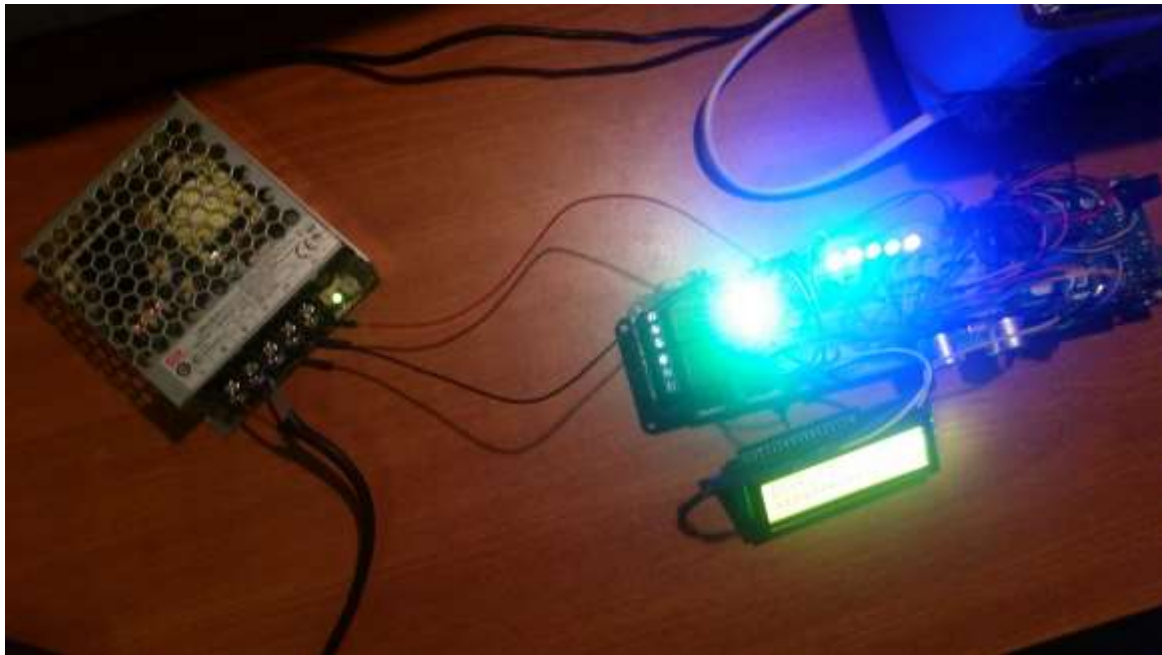
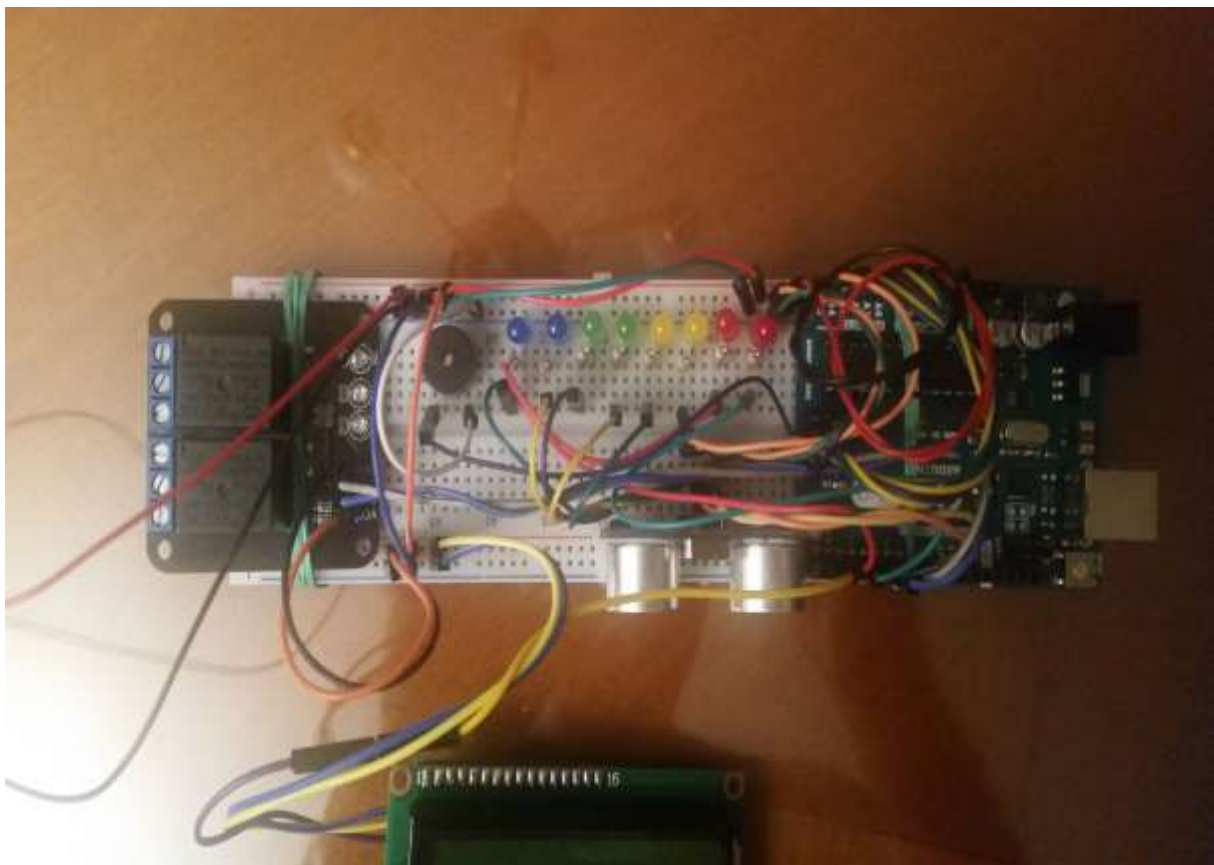
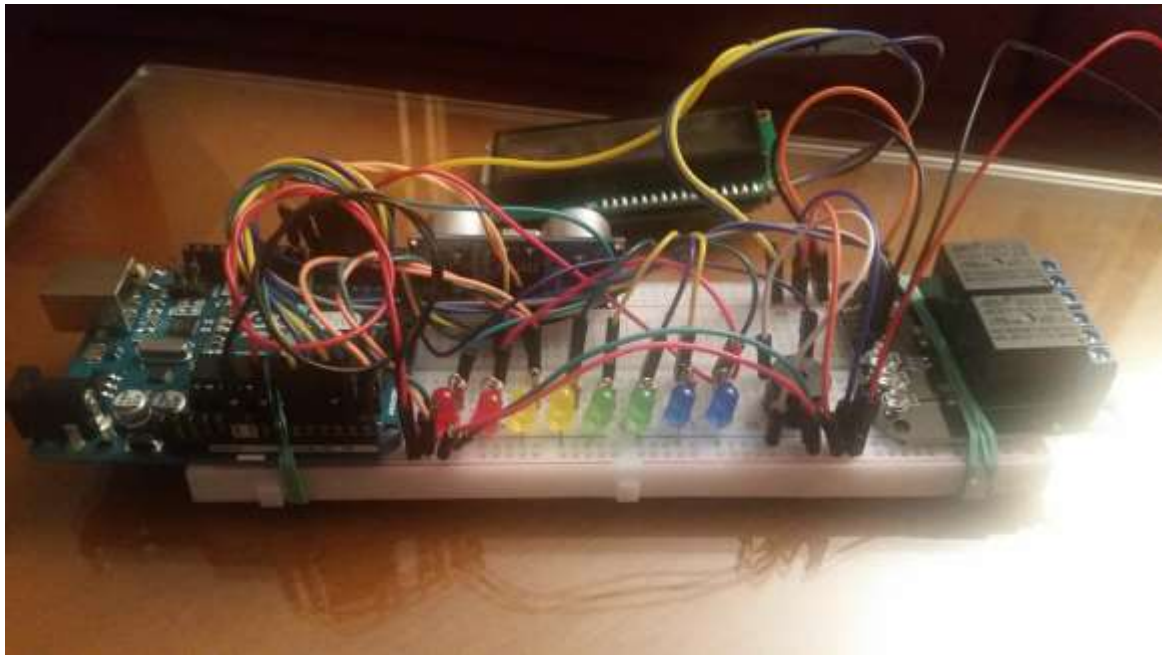


Imagen del producto tecnológico en estático:



Código fuente del desarrollo del producto tecnológico del sistema de Aparcamiento en Arduino, código de creación propia del autor del trabajo.

```
//DECLARAMOS LOS PINES DE LOS LEDS
int LED_1=A0;
int LED_2=A1;
int LED_3=A2;
int LED_4=A3;
int LED_5=A4;
int LED_6=A5;
int LED_7=2;
int LED_8=3;

int pinZumbador=4;

int pinRele_1=5;
int pinRele_2=6;

//VARIABLE GLOBALES
int maximo_rango = 400; //cm
int minimo_rango = 5; // cm
long duracion, distancia;
int valoresReferencia[]={150, 125, 100, 75, 50, 30, 20, 10};
int valoresReferenciaRele[]={100, 50};

void encenderLeds(int valor){
  if(valor<=valoresReferencia[0])
    digitalWrite(LED_1, HIGH);
  else
    digitalWrite(LED_1, LOW);

  if(valor<=valoresReferencia[1])
    digitalWrite(LED_2, HIGH);
  else
    digitalWrite(LED_2, LOW);
```

```
if(valor<=valoresReferencia[2])
    digitalWrite(LED_3, HIGH);
else
    digitalWrite(LED_3, LOW);

if(valor<=valoresReferencia[3])
    digitalWrite(LED_4, HIGH);
else
    digitalWrite(LED_4, LOW);

if(valor<=valoresReferencia[4])
    digitalWrite(LED_5, HIGH);
else
    digitalWrite(LED_5, LOW);

if(valor<=valoresReferencia[5])
    digitalWrite(LED_6, HIGH);
else
    digitalWrite(LED_6, LOW);

if(valor<=valoresReferencia[6])
    digitalWrite(LED_7, HIGH);
else
    digitalWrite(LED_7, LOW);

if(valor<=valoresReferencia[7])
    digitalWrite(LED_8, HIGH);
else
    digitalWrite(LED_8, LOW);
}
```



```
}  
void encenderReles(int valor){  
    if(valor<=valoresReferenciaRele[0])  
        digitalWrite(pinRele_1, HIGH);  
    else  
        digitalWrite(pinRele_1, LOW);  
  
    if(valor<=valoresReferenciaRele[1])  
        digitalWrite(pinRele_2, HIGH);  
    else  
        digitalWrite(pinRele_2, LOW);  
}  
  
void zumbador(int valor){  
    bool activarZumbador=false;  
    byte numRepeticiones=0;  
  
    for(int cont=7; cont>3; cont--){  
        if(valor<=valoresReferencia[cont]){  
            activarZumbador=true;  
            numRepeticiones=cont-3;  
            break;  
        }  
    }  
  
    if(activarZumbador){  
        for(int cont=0; cont<numRepeticiones; cont++){  
            digitalWrite(pinZumbador, HIGH);  
            delay(50);  
            digitalWrite(pinZumbador, LOW);  
            delay(50);  
        }  
    }  
}
```

```
long obtener_distancia(void) {
    digitalWrite(trigPin, LOW);
    delayMicroseconds(2);

    digitalWrite(trigPin, HIGH);
    delayMicroseconds(10);

    digitalWrite(trigPin, LOW);
    duracion = pulseIn(echoPin, HIGH);

    distancia = duracion/58.2;
    return(distancia);
}

void imprimirLcd(int valor) {
    delay(100);
    Serial.print("sd0,0;");
    delay(100);
    Serial.print("ssDist.:"+String(valor)+" Cm.   ;");

    delay(100);
    Serial.print("sd1,0;");
    delay(100);
    Serial.print("ss           ;");

    int aux=16-(valor/10);
    String medida="";

    Serial.println("---->"+String(aux));

    for(int cont=0; cont<aux; cont++){
        medida+="*";
    }
}
```

```
    delay(100);
    Serial.print("sd1,0;");
    delay(100);
    Serial.print("ss"+medida+");");

}

void setup() {
    Serial.begin (9600);

    Serial.print("sc;");
    delay(100);
    Serial.print("sd0,0;");
    delay(100);
    Serial.print("ssInicializando;");
    delay(100);
    Serial.print("sd1,0;");
    delay(100);
    Serial.print("ssEl Sistema;");

    pinMode(trigPin, OUTPUT);
    pinMode(echoPin, INPUT);

    //DEFINIMOS LOS PINES DE LOS LEDS, ZUMBADOR Y RELES COMO OUTPUT
    pinMode(LED_1, OUTPUT);
    pinMode(LED_2, OUTPUT);
    pinMode(LED_3, OUTPUT);
    pinMode(LED_4, OUTPUT);
    pinMode(LED_5, OUTPUT);
    pinMode(LED_6, OUTPUT);
    pinMode(LED_7, OUTPUT);
    pinMode(LED_8, OUTPUT);
```

```
pinMode (pinZumbador, OUTPUT);

pinMode (pinRele_1, OUTPUT);
pinMode (pinRele_2, OUTPUT);

digitalWrite (LED_1, HIGH);
digitalWrite (LED_2, HIGH);
digitalWrite (LED_3, HIGH);
digitalWrite (LED_4, HIGH);
digitalWrite (LED_5, HIGH);
digitalWrite (LED_6, HIGH);
digitalWrite (LED_7, HIGH);
digitalWrite (LED_8, HIGH);

digitalWrite (pinZumbador, HIGH);

digitalWrite (pinRele_1, HIGH);
digitalWrite (pinRele_2, HIGH);

delay (1000);

digitalWrite (LED_1, LOW);
digitalWrite (LED_2, LOW);
digitalWrite (LED_3, LOW);
digitalWrite (LED_4, LOW);
digitalWrite (LED_5, LOW);
digitalWrite (LED_6, LOW);
digitalWrite (LED_7, LOW);
digitalWrite (LED_8, LOW);

digitalWrite (pinZumbador, LOW);
```

```
digitalWrite(pinRele_1, LOW);  
digitalWrite(pinRele_2, LOW);  
  
delay(3000);  
}  
  
void loop() {  
  distancia=obtener_distancia();  
  
  Serial.println(distancia);  
  encenderLeds(distancia);  
  encenderReles(distancia);  
  imprimirLcd(distancia);  
  zumbador(distancia);  
  
  delay(1000);  
}
```

4.2.5 ANÁLISIS DE LA DIFICULTAD PARA SU POSTERIOR DESARROLLO POR EL ALUMNADO

El desarrollo del producto tecnológico construido, recreando el Sistema de Aparcamiento de un coche, es claramente de un nivel de dificultad elevado para alumnos de la etapa de secundaria. La idea era precisamente crear un producto tecnológico de mayor dificultad que me otorgue nuevas competencias y que sea extrapolable al aula en pequeñas partes por lo que se podrían hacer de este desarrollo pequeños proyectos para los alumnos con tal de adaptar su dificultad.

- Un proyecto del uso de los Leds codificado en C++ para aprender a su vez las primeras nociones del lenguaje de programación.
- Un proyecto de un sencillo sensor de ultrasonidos codificado en C++
- Un proyecto de funcionamiento de un zumbador codificado en C++
- Un proyecto del funcionamiento de un Display codificado en C++
- Un proyecto del funcionamiento de un relé codificado en C++

Lo idóneo del aprendizaje del producto realizado es la capacidad que ofrece dentro de su sistema de poder crear nuevos proyectos a partir de los conocimientos adquiridos.

A nivel de codificación parece complicado para los alumnos pero creo que es un buen comienzo poder hacer pequeños proyectos de robótica a partir de este proyecto para aprender tanto a crear desarrollo de productos complejos como aprender a codificar en lenguajes de programación.

4.3 ANÁLISIS Y REFLEXIÓN GLOBAL DE LA REALIZACIÓN DE PRODUCTOS TECNOLÓGICOS COMPLEJOS EN LAS AULAS SEGÚN NIVELES EDUCATIVOS

Las tecnologías de la información, la robótica, la informática en general cada vez están tomando un papel más relevante en la sociedad, indispensable me atrevería a decir.

Desde los centros preuniversitarios cada vez se está dando más importancia a la tecnología y a las TIC ya que es el presente y futuro de nuestra sociedad y estamos formando a nuevas generaciones que se van a enfrentar a trabajos que a día de hoy son desconocidos.

Hace años conceptos como Big Data, Cloud, Ciberseguridad... eran grandes desconocidos y hoy se están convirtiendo en trabajos con altísimas cotas de empleabilidad. Por tanto desde las aulas se deben formar en las nuevas tecnologías a los alumnos, debiendo desde mi perspectiva salir con conocimientos de Programación, robótica, impresión 3D, desarrollo Web...ya que es posible según el avance de la era de informática que programar se convierta en algo importante como pueden ser las matemáticas en cuanto a ser una asignatura troncal.

Considero que con la parte de mi trabajo referente a la creación del sistema de aparcamiento de un coche, me ha aportado valor para aplicar nuevos conocimientos avanzados que no tenía en Arduino y que al poder realiza proyectos complejos en el aula, el centro docente se beneficiará de una mejor formación en robótica y programación por parte del alumnado.

No me cabe duda de que la figura de un Ingeniero en Informática en un centro preuniversitario da un valor añadido ya que es una figura capaz no solamente de copar todas las materias relacionadas con las matemáticas, también de dar valor al centro con proyectos complejos de ingeniería, programación, impresión 3D, y de llevar la Coordinación TIC del centro al que pertenezca.

5. RESUMEN

Se ha realizado un trabajo real de aplicación directa en un centro docente que ha consistido en mejorar la gestión y coordinación del mismo así como la realización del desarrollo de un producto tecnológico que me aporta valor y nuevos conocimientos de aplicación directa (desglosado en pequeños proyectos) en aulas preuniversitarias.

El trabajo ha tenido la dificultad añadida de que no ha sido realizado en un marco teórico, sino que ha sido de aplicación en el centro docente por lo que he podido apreciar el valor que se le ha otorgado al centro con su puesta en marcha.

Es el primer año que trabajaba en el puesto de Responsable de Tecnologías de la Comunicación e Información del centro y ha sido una gran motivación poder haber llevado a cabo este trabajo de aplicación real en el centro observando las mejoras tanto en materia de gestión, como de coordinación y seguridad así como la adquisición de poder llevar a cabo el desarrollo de productos más complejos en el aula.

6. VALORACIÓN DEL TFM

Valoro el TFM en una oportunidad excepcional de haber podido mejorar un centro docente en el puesto de máximo responsable de tecnologías de la información y la comunicación, puesto que entraba a cargo este año siendo Ingeniero y ha sido un reto el poder tomar un centro necesitado de todas las mejoras aquí creadas y ver la evolución desde el primer día de la puesta en marcha del TFM.

He podido desarrollar dos de las áreas que más me apasionan que son la gestión/coordinación y la seguridad informática junto con el aprendizaje intenso de Robótica con Arduino por medio del desarrollo de un producto tecnológico.

Ha sido una experiencia inmejorable observar que ha habido en el centro un antes y un después de este trabajo avalado por el equipo directivo del centro docente en el que he realizado el trabajo.

La valoración por tanto es muy positiva ya que ha dado nuevas competencias en materias de gestión informática, seguridad informática y robótica y la satisfacción de apreciar en el día a día la transformación del centro docente mediante la aplicabilidad real de este trabajo.

6.1 APRENDIZAJE EN EL PROYECTO

Debido a la total libertad y confianza depositada en mí del centro docente, en la figura no solamente de profesor de ciencias, informática, TIC, tecnología, programación y robótica también como máximo responsable del departamento de tecnología y responsable de informática del centro coordinado las TIC he podido llevar a cabo este trabajo.

Y se ha podido llevar a cabo con implantación real de cada apartado desarrollado en la memoria, como citaba en el apartado anterior en mi primer año en este cargo de máximo responsable. Por tanto he podido desarrollarme en materias de gestión, coordinación seguridad e ingeniería por medio de robótica aprendiendo nuevos campos en los que no había tenido la oportunidad de desarrollarme previamente.

Uno de los aprendizajes a destacar es la toma de decisiones al aplicar cada medida observando la responsabilidad que ello implica con cada decisión tomada ya que tiene repercusión directa en el trabajo de los compañeros.

Destacar también haber puesto en marcha conceptos que si bien para mí eran conocidos como puede ser ITIL (al estar yo certificado) o seguridad informática eran un reto ponerlos en marcha en un centro docente en el que hasta ahora no se había hecho absolutamente nada en esta materia, por lo que el impacto creado ha sido elevado tanto para mí como para los compañeros del centro docente.

Mediante la creación del desarrollo del producto tecnológico de un Sistema de Aparcamiento, he podido profundizar más en robótica con Arduino y en su codificación/programación de código en la que a la vez al utilizar diferentes componentes de Arduino he aprendido como utilizarlos y programarlos de modo que a partir de este desarrollo sea capaz de generar nuevos modelos de robótica.

6.2 APLICACIÓN DEL MÁSTER DE INGENIERÍA AL PROYECTO

Siendo un trabajo final de máster ad hoc, se han podido aplicar varias de las materias aprendidas a lo largo del máster. Para mí lo más importante es que una de las muchas finalidades del máster universitario en ingeniería informática es la de trabajar tanto en ámbitos de dirección TIC como de la Ingeniería Informática, y con este trabajo se ha logrado copar ambas competencias.

Por una parte se han realizado tareas en el trabajo de gestión (con implicación directa en el trabajo) que se pueden estudiar en materias como dirección estratégica de sistemas y tecnologías de la información, gestión avanzada de proyectos. Asignaturas que me han otorgado una mayor competencia reflejada en este trabajo en la adquisición y capacidad para dirigir, planificar y supervisar equipos y proyectos en el ámbito de la informática y las TIC.

Se han realizado tareas referentes a la seguridad informática que se pueden estudiar en la materia sistemas de gestión de seguridad de la información.

Y finalmente el desarrollo de un producto tecnológico con la creación de código propio en el que todas las materias del máster relacionadas con el desarrollo del software, han sido de gran aportación.

Una de las apreciaciones que quiero hacer al máster es que me ha ayudado a abrir aún más la mente si cabe en cuanto a ingeniería, ya que asignaturas como inteligencia artificial avanzada, simulación, computación de altas prestaciones, o técnicas avanzadas de ingeniería del software me han hecho desarrollar la capacidad de analizar problemas complejos en entornos nuevos o poco conocidos como era este, así como evaluar las posibles alternativas y, posteriormente, desarrollar e implantar la solución más adecuada igual que en el caso que aquí se presenta.

7. CONCLUSIONES.

Se ha realizado un trabajo de Gestión, Coordinación, Seguridad informática e Ingeniería de las TIC aplicadas a los centros preuniversitarios mediante el cual, a nivel profesional he adquirido unos altos conocimientos referentes gestión, coordinación de las TIC y en robótica, fruto de la labor de investigación realizada para llevar a buen término el Proyecto.

El máster me ha otorgado habilidades, a las anteriormente mencionadas, de aprendizaje que permiten continuar cualquier tipo de reto o formación de manera autónoma. Adaptándome a nuevas situaciones como la realizada con éxito en este trabajo final, gracias a haber entre otros desarrollado una capacidad innovadora y creativa que se ha visto reflejada en el buen hacer del trabajo.

Destacar que ha sido realmente estimulante ver como cada medida adoptada, toma de decisiones tenía una repercusión directa para el buen y mejor funcionamiento del centro.

Estoy satisfecho tanto con el trabajo realizado que ha tenido impacto en el centro docente que se ha podido beneficiar de los resultados, objetivo clave del trabajo, como por el aprendizaje obtenido y la gran experiencia que me ha dado realizar un trabajo final de este tipo.

8. BIBLIOGRAFÍA

La Bibliografía consultada para la realización del proyecto es la detallada a continuación:

- Materiales UOC asignaturas: dirección estratégica de sistemas y tecnologías de la información, gestión avanzada de proyectos, gestión de seguridad de la información.
- Recursos de Robótica:
 - <https://www.arduino.cc>
 - http://forefront.io/a/beginners-guide-to-arduino/#what_is_arduino
 - <https://programmingelectronics.com/arduino-crash-course/>
 - <http://www.ardumania.es>
- Recursos de Seguridad de la información:
 - <http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>
 - <https://ayudaleyprotecciondatos.es/2016/08/25/proteccion-de-datos-para-centros-educativos/>
 - <https://ayudaleyprotecciondatos.es/ciudadanos/>
 - <https://delitosinformaticos.com/protecciondatos/legislacion.shtml>
 - <http://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/preguntasFrecuentes.jsf>
 - http://www.gesdatos.com/descargas/Compendio_LOPD_para_Centros_Educativos.pdf
- Recursos Gestión, Coordinación:
 - <http://www.itilv3.es/>
 - <https://www.axelos.com/best-practice-solutions/itil>
 - <http://www.itinfo.am/eng/information-technology-infrastructure-library-guide/>
 - <https://searchcio.techtarget.com/definition/ITIL-v3>
 - http://www.bmcsoftware.es/forms/ESM_TL_ITIL_ReferenceBooks_BMCcom_EN_Apr2012_V2.html?intcmp=inpage