**Práctica 2: Auditoría**

**AUTORES:**

**Daniel Bastarrica**

**Javier Cortés**

**Paloma Gutierrez**

**Adrián Martínez**

**Rocío Santos**

**Gabriel Sellés**

**ACFI UCM 2018**

Informe de auditoría de la aplicación Carnicería

**DESTINATARIO**

El destinatario de este informe es Adrián Riesco.

**ENTIDAD AUDITADA**

La entidad auditada es Rerfler. Esta empresa de desarrollo de software está especializada en aplicaciones web. En particular, se audita el proyecto “Página web carnicería Riesco” desarrollado para el cliente Adrián Riesco.

**ALCANCE**

Como veremos en la sección de objetivos, en esta auditoría vamos a analizar los siguientes puntos:

* Contrato, estudiando cómo se gestionaron los requisitos y cómo se tuvieron en cuenta los riesgos.
* Plan de desarrollo, estudiando si el desarrollo está correctamente documentado y si se han establecido hitos y tareas críticas.
* Requisitos, analizando si existen requisitos bien definidos y documentados.
* Diseño, estudiando si existen revisiones por pares y el diseño está claramente documentado y con revisiones formales.
* Implementación, analizando si existen pruebas de unidad, documentación de dichas pruebas y revisiones por pares.
* Seguimiento, comprobaremos el cumplimiento de los hitos y el seguimiento de los riesgos.
* Documentación, analizando que existan documentación para instalación y uso, testing y que se encuentran controlados los documentos y tienen un responsable.

**COMPARABILIDAD**

No se dispone de información sobre informes de auditoría anteriores.

**SALVEDADES**

Se han detectado las siguientes salvedades:

* No se pudo contactar con los desarrolladores para tratar ciertos aspectos del proyecto que no estaban claros.
* La mayoría de la documentación del software desarrollado estaba incompleta e incluso presentaba incongruencias.

**INCUMPLIMIENTOS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ITEM | OBJETIVO | SÍ | NO | PARCIAL | N.A. |
| **1.** | **Contrato** |  |  |  |  |
| 1.1 | Se reflejan los requisitos |  |  | X |  |
| 1.2 | Se justifican los requisitos rechazados |  | X |  |  |
| 1.3 | Se tienen en cuenta los riesgos |  |  | X |  |
| **2.** | **Plan de desarrollo** |  |  |  |  |
| 2.1 | Plan de desarrollo definido |  |  | X |  |
| 2.2 | Plan de desarrollo documentado |  | X |  |  |
| 2.3 | Tareas críticas establecidas |  | X |  |  |
| 2.4 | Hitos establecidos |  |  | X |  |
| **3.** | **Requisitos** |  |  |  |  |
| 3.1 | Requisitos claramente definidos |  |  | X |  |
| 3.2 | Requisitos claramente documentados |  |  | X |  |
| 3.3 | Existen requisitos de mantenibilidad |  | X |  |  |
| **4.** | **Diseño** |  |  |  |  |
| 4.1 | Diseño claramente documentado |  |  | X |  |
| 4.2 | Revisiones formales de diseño |  |  | X |  |
| 4.3 | Revisiones por pares |  | X |  |  |
| **5.** | **Implementación** |  |  |  |  |
| 5.1 | Pruebas de unidad |  |  | X |  |
| 5.2 | Testing documentado |  | X |  |  |
| 5.3 | Revisiones por pares |  | X |  |  |
| 6. | **Seguimiento** |  |  |  |  |
| 6.1 | Hitos seguidos |  |  | X |  |
| 6.2 | Riesgos seguidos |  |  | X |  |
| 6.3 | Riesgos solucionados |  |  | X |  |
| **7.** | **Documentación** |  |  |  |  |
| 7.1 | Documentos controlados |  |  | X |  |
| 7.2 | Responsable de documentos controlados |  |  |  | X |
| 7.3 | Documentación para testing |  |  |  | X |
| 7.4 | Documentación de instalación y uso |  |  | X |  |

**1 - CONTRATO**

**1.1. Se reflejan los requisitos**

Los requisitos vienen reflejados en las páginas de la 1-11 del documento *Anexo.pdf* ; así como en el documento llamado *Documentación Carnicería.pdf* en las páginas 7-17. Pero en ningún momento aparecen indicados en el contrato.

**Recomendación:** Se recomienda tener una cláusula en el contrato con los requisitos explicados para que el cliente sea capaz de identificar sus peticiones en estos y asegurarse de que el cliente está totalmente de acuerdo con ellos.

**1.2. Se justifican los requisitos rechazados**

No se tiene constancia alguna de requisitos rechazados o de su justificación.

**Recomendación:** En caso de existir requisitos rechazados, deben indicarse en el contrato junto con su justificación. Para ello es de gran ayuda tener un responsable para el seguimiento de documentos en el que se incluye el contrato, para llevar un control absoluto de los cambios.

**1.3. Se tienen en cuenta los riesgos**

Aunque los riesgos se mencionan en la página 2 del documento *Documentación Carnicería.pdf*, no hay ninguna otra medición en el resto de la documentación, por lo que se considera que en este aspecto, el proyecto es más pobre. Teniendo en cuenta que a medida que evaluamos el proyecto en mayor profundidad los riesgos aumentan.

**Recomendación**: Al igual que en el punto anterior se recomienda tener un control exhaustivo de la documentación junto con un responsable que controle los cambios en los documentos.

**2 - PLAN DE DESARROLLO**

**2.1. Plan de desarrollo definido**

El plan de desarrollo está definido de forma parcial. Algunos aspectos, como la especificación de requisitos o la definición de hitos se aparecen de forma correcta. Otros, como la planificación temporal o la gestión de riesgos, aparecen de forma muy simplificada e incompleta. Se pueden destacar más aspectos de la totalidad del plan de desarrollo pero como se mencionan en otros puntos de este informe de auditoría, no los mencionaremos aquí.

**Recomendación:** Se recomienda rehacer la planificación temporal. La nueva planificación temporal debería hacer referencia a las actividades/tareas/subobjetivos necesarios para el desarrollo del sistema en lugar de a fases vagamente definidas que no aportan la concreción que la planificación temporal suele ofrecer. Esto, junto a modificar el orden de los artefactos (poner la especificación de requisitos antes que la planificación, entre otras cosas) le daría un mayor sentido y coherencia a este documento. Las recomendaciones de los demás aspectos del plan de desarrollo se encuentran en otros puntos del informe de auditoría.

**2.2. Plan de desarrollo documentado**

El plan de desarrollo está documentado de forma sencilla y demasiado simplificada. En artefactos como la gestión de los riesgos se limita a nombrar los propios riesgos sin detallar su criticidad, su causa,etc. En la planificación temporal se utilizan fases de referencia distintas a las descritas anteriormente (páginas 3 y 4) e ignora información de especial interés como con qué recursos de trabajo realizará la actividad y cómo los distribuirá. Los artefactos que componen el documento carecen de formalidades en la documentación que completan y concretan muchos aspectos del desarrollo.

**Recomendación:** Uso de plantillas o modelos de documentos que incluyan los artefactos de la entrega (planificación temporal, especificación de requisitos, gestión de riesgos, etc) para cubrir todos los aspectos necesarios y que la documentación sea completa. También dotar de un orden más lógico a todos estos artefactos. No tiene sentido hacer la planificación temporal, el cual debería utilizar los requisitos para extraer las actividades a realizar, antes de la especificación de requisitos, por ejemplo. Existen más recomendaciones pero, como se mencionan en los demás puntos del documento, no las describiremos aquí.

**2.3. Tareas críticas establecidas**

No existe una mención explícita o un listado de cuáles son las tareas críticas en el proceso de desarrollo del producto descrito en el documento proporcionado.

**Recomendación:** Inserción en el plan de desarrollo de un listado de tareas críticas al que poder hacer referencia desde los demás apartados o añadir en la especificación de requisitos una mención de si cada requisito es crítico o no.

**2.4. Hitos establecidos**

Se establecen una serie de hitos en base a unas fases y luego se obvian para utilizar otras fases, de modo que estos hitos no tienen cabida ni sentido el resto del documento proporcionado. En las páginas 3 y 4 se describen unas fases con una serie de hitos en cada una de ellas y en la planificación (página 6) se empiezan a utilizar otras fases.

**Recomendación:** Unificar esas fases, que sean las mismas en la totalidad del documento, y luego describir una serie de hitos, ligados directamente a estas fases o no. También es recomendable hacer mención o marcar estos hitos en la planificación temporal para mostrar qué estará hecho en cada entrega/hito.

**3 - REQUISITOS**

Todas las evidencias descritas a continuación provienen del documento “Documentación Carniceria.pdf”.

**3.1. Requisitos claramente definidos**

Aunque a grandes rasgos se entiende el alcance y funcionalidades básicas de la aplicación, en cuanto se intenta entrar en detalles casi no hay información específica.

**Recomendación**: ser más específicos y entrar en detalles más concretos en todos los aspectos.

**3.2. Requisitos claramente documentados**

* **Página 8:** “los listados con muchos productos serán paginados”.
* **Recomendación**: definir qué cantidad de productos se considerarán “muchos”.
* **Página 9:** “se enviará un correo en copia oculta”.
* **Recomendación**: comprobar la legalidad de este proceso respecto a la protección de datos.
* **Página 10:** “navegación intuitiva y amigable” y “web atractiva y agradable visualmente” (no hay documentación de las indicaciones).
* **Recomendación**: se debe explicar en qué consistirán estas especificaciones.
* **Página 10**: “la interacción no refrescará completamente en cada cambio”. **Recomendación**: especificar qué cambios refrescarán la página y cuáles no.
* **Página 10**: “páginas ágiles”.
* **Recomendación**: definir un tiempo máximo.
* **Página 10**: “datos de tarjetas viajarán de forma segura”.
* **Recomendación**: definir quién tratará los datos de las tarjetas y qué se hará con ellas.
* **Páginas 11-12**: se habla de que ciertos elementos se sincronizarán desde la BBDD y otros no.
* **Recomendación**: especificar qué significa que se “sincronicen”.
* **Página 12**: “los productos ‘No Web’ no se sincronizarán”.
* **Recomendación**: especificar de dónde saldrá la información.
* **Página 12**: “definir ficha propia con información detallada”.
* **Recomendación**: definir qué información podrá tener asociada y cómo se almacenará en la BBDD.
* **Página 13**: “productos nuevos”.
* **Recomendación**: definir cuánto tiempo se considerará que un producto es novedad.
* **Página 14**: “visualizar y editar contenido de secciones a través de interfaz gráfica potente y fácil de usar”.
* **Recomendación**: definir mejor qué significarán ambos conceptos.
* **Página 16**: “gestionar los valores de parámetros del sistema”.
* **Recomendación**: definir qué valores serán los que se podrán configurar.
* **Página 16**: “almacenar información para control de cambios”.
* **Recomendación**: definir qué información se almacenará y cómo será accesible.
* **Página 17**: “navegación ágil e intuitiva” y “rendimiento aceptable”.
* **Recomendación**: definir todos estos parámetros.
* **Página 17**: “no se guardarán contraseñas sino su Hash”.
* **Recomendación**: ante la vulnerabilidad de ciertos algoritmos de Hash, definir uno que todavía se considere seguro, así como métodos de seguridad de tipo “sal y pimienta”.
* **Página 17**: “se realizarán frecuentemente copias de seguridad”.
* **Recomendación**: definir frecuencia de las copias y qué información guardará.

**3.3. Existen requisitos de mantenibilidad**

Los únicos requisitos encontrados son en la página 10 del documento, donde se habla al respecto de esto en el apartado de “modularidad”; y en la página 21, donde se habla de “una estructura común entre las páginas”. Sin embargo, sólo se hace mención a la escalabilidad y a la reusabilidad.

**Recomendación**: definir unos requisitos claros de mantenibilidad. Esto ayudará en un futuro a poder seguir utilizando la aplicación, arreglar posibles problemas encontrados en la misma y a poder ser modificada por un equipo ajeno al de desarrollo de una manera rápida y sencilla.

**4 - DISEÑO**

**4.1. Diseño claramente documentado**

En el documento “DocumentacionCarniceria.pdf”, pág.19, existe un apartado dedicado al diseño. También, en el “manualDeUsuario.pdf”, se puede observar cómo se resolvieron los aspectos visuales del cliente.

**Recomendación:** A pesar de dedicar un apartado al diseño, se podrían especificar más detalles. Lo importante es tratar todos los aspectos, cumplir y ajustarse a los requisitos del cliente, y garantizar en un futuro su funcionamiento.

**4.2. Revisiones formales**

En el documento “DocumentacionCarniceria.pdf”, pág.24, trata las revisiones técnicas formales. Aunque mencionan, que por falta de tiempo, se hicieron vía Skype en lugar de presenciales.

**Recomendación:** Es muy aconsejable mantener estas reuniones con el cliente en persona para así poder aclarar sin malentendidos cualquier problema que surja.

**4.3. Revisiones por pares**

No se incluyen este tipo de revisiones para evaluar la calidad del trabajo construido. Generalmente, aporta sus opiniones de mejoras a tener en cuenta en el sistema.

**Recomendación:** Es una buena práctica de revisión si se dispone del personal suficiente. Aporta distintas visiones y ayuda a mejorar la calidad del proceso.

**5 - IMPLEMENTACIÓN**

**5.1. Pruebas de unidad**

No están claramente documentadas las pruebas de unidad llevadas a cabo a lo largo del proceso de desarrollo.

**Recomendación:** Es una buena práctica realizar pruebas de unidad a todas y cada una de las partes, haciendo un resumen acerca de cómo se han hecho y los resultados obtenidos.

**5.2. Testing documentado**

No se incluyen documentos concretos sobre cómo se han realizado las pruebas.

**Recomendación:** Es una buena práctica de revisión si se dispone del personal suficiente. Aporta distintas visiones y ayuda a mejorar la calidad del proceso.

**5.3. Revisiones por pares**

No se mencionan las revisiones por pares en la fase de test.

**Recomendación:** Es una buena práctica de revisión si se dispone del personal suficiente. Aporta distintas visiones y ayuda a mejorar la calidad del producto.

**6 - SEGUIMIENTO**

**6.1. Hitos seguidos**

Los hitos se encuentran definidos, pero en ninguno de los documentos que se incluyen aparece un seguimiento de ellos o un documento que acredite que estos hitos se han cumplido.

**Recomendación:** Para poder justificar cada hito, la entrega o presentación de cualquier parte del software (documentación, código o el propio programa) se podría realizar un documento que se apruebe por ambas partes. Estos documentos serán otros que se incluirán a las recomendaciones anteriores del control de la documentación.

**6.2. Riesgos seguidos**

En el documento llamado *Documentación Carnicería.pdf* donde están contemplados los riesgos, se puede encontrar también que al tomar ciertas decisiones en el proyecto se han tenido en cuenta los riesgos. Solo se han tenido en cuenta algunos riesgos y no todos.

**Recomendación:** Para tener en cuenta todos los riesgos y poder minimizarlos es útil contar con un plan de gestión de riesgos, en el que se indiquen los posibles riesgos junto con su criticidad y un plan de acción en caso de que estos sucedan.

**6.3. Riesgos solucionados**

Al igual que en el punto anterior, se puede destacar que algunas tomas de decisión se han solucionado algunos de los riesgos contemplados, pero no se encuentra documentado en ningún documento concreto, solo es mencionado en el documento llamado *Documentación Carnicería.pdf*.

**Recomendación:** Al igual que en el apartado anterior, se propone emplear un plan de gestión de riesgos donde se indique todo lo anterior y pudiendo añadir, en el caso pertinente, que se ha hecho para solucionar el riesgo llevado con un control de versiones.

**7 - DOCUMENTACIÓN**

**7.1. Documentos controlados**

En el apartado de diseño se expone el esquema de la aplicación, se habla de patrones de diseño y se concreta que no se entrará en profundidad en las tecnologías aplicadas. En esta documentación no se hace referencia en ningún momento a los patrones de diseño ya mencionados, solo se da una idea de las capas del sistema:

**Recomendación**: sería conveniente mover toda la documentación sobre el diseño a un archivo aparte y añadirlo como anexo al contrato. También convendría explicar los patrones de diseño si se han mencionado previamente en la documentación.

En la documentación solo aparece un párrafo sobre la descripción de la base de datos en que se describe cómo se documentará dicho apartado y que se usará para ello (UML), sin embargo no hay ningún diagrama que lo desarrolle. Además hay más información sobre este apartado en otro punto del documento.

**Recomendación**: se debería describir las bases de datos en un fichero aparte al igual que en el caso anterior. También convendría añadir los diagramas si se dice que los hay y centralizar la información en al menos un apartado del documento ùes sería muy útil para manejar la documentación en sí al estar todo ordenado.

No se menciona nada sobre los planes de instalación.

**Recomendación**: describir en un documento el despliegue de la plataforma web así como el resto de servicios que use.

No se menciona nada sobre el mantenimiento de la aplicación. De hecho en los requisitos aparece que se llevarán a cabo copias de seguridad periódicas de la DB pero no se habla nada más en todo el documento.

**Recomendación**: se debería explicar en un documento el tipo de mantenimiento a llevar a cabo así como el tiempo durante el cual se va a realizar.

Dentro del fichero “documentacion.pdf” nos encontramos con un apartados donde se exponen los casos de uso con diagramas, luego hay otro fichero con más diagramas y otro más pero con una descripción exhaustiva de los requisitos, lo cual es bastante confuso en ambos casos.

**Recomendación**: sería una buena idea relegar toda esta documentación a un fichero sin necesidad de disponer de fragmentos de información de un mismo tipo repartidos por la documentación.

**7.2. Responsable de documentos controlados**

No se especifica en ningún momento a lo largo del documento quienes son los encargados de guardar los documentos controlados ni el nivel de acceso de cada integrante los mismos. Tampoco se han determinado el número de copias ni el modo de almacenamiento ni si serán en físico o digital.

**Recomendación**: convendría describir este procedimiento en un anexo al contrato.

**7.3. Documentación para testing**

En el apartado “7.Pruebas” se describe el proceso de testing, pero de forma muy vaga. No se define qué pruebas en concreto se hacen ni tasas de errores descubiertos, solamente se afirma que se han hecho “muchas pruebas, y muy duras”

**Recomendación**: describir la estructura de las pruebas realizadas y los resultados obtenidos de las mismas.

**7.4. Documentación de instalación y uso**

Hay un manual de usuario pero solo son capturas de pantalla y alguna frase suelta.

**Recomendación**: sería recomendable redactar un guión de uso y hacer uso de imágenes de mejor calidad, este documento debe explicar de pasada como se usa la aplicación.

**ÉNFASIS**

Podemos decir que los tres problemas más destacables son los siguientes:

1. En primer lugar, la falta de documentación. El desarrollo está documentado de forma incompleta y sin seguir plantillas o estándares formales que doten a dicha documentación de sentido. Es por ello que se recomienda seguir un estilo común de documentación para cada artefacto de la misma con el fin de evitar información innecesaria y completar todos los aspectos mínimos requeridos.
2. En segundo lugar, la falta de consistencia entre los distintos apartados que forman el plan de desarrollo. Por un lado, el documento se contradice en distintos puntos. Por ejemplo, inicialmente se utilizan unas fases que luego se desechan para utilizar otras. Por otro lado, se especifica la planificación temporal y después los requisitos del sistema, práctica no recomendable ya que utilizar los requisitos como guía para la planificación dota a la misma de mayor concreción a la hora de desarrollar el producto.
3. Por último, la mala gestión del contrato, error puede suponer problemas a lo largo de todo el proyecto. Debido a la importancia de dicho documento, gran parte del éxito del proyecto dependerá del mismo. Entonces, incluir correctamente en él los riesgos, los requisitos y demás aspectos como costes y fechas es más imprescindible.

**INFORME DE GESTIÓN**

En esta auditoría no hemos tenido acceso a documentación sobre la gestión.

**RESUMEN**

Hemos encontrado incumplimientos en el contrato y una documentación incompleta e incoherente. Tal y como se puede ver en la tabla anterior, ninguno de los requisitos para considerar éste como un buen desarrollo se han cumplico de forma total, y gran parte de ellos ni siquiera se han cumplido de forma parcial. Es por ello que estos inclumplimientos parecen haber tenido gran impacto durante la fase de desarrollo pues hay carencias en muchos aspectos del mismo.

En consecuencia, recomendamos reformular el contrato para que incluya aspectos que no están presentes (riesgos, requisitos, costes, etc..) para que el problema quede completamente especificado desde un primer momento. También creemos necesario el uso de estándares de documentación para dotar a cada artefacto del documento de sentido como un todo y para evitar la falta de contenido necesario. Por último recomendamos revisar el documento en su totalidad para evitar que haya incoherencias entre las partes que lo forman.

**RESULTADO: NO APTO**.

**FECHA Y FIRMA**

Gabriel Sellés Salvà en representación de iTec S.L.