Universitat Oberta de Catalunya uoc.edu

Análisis de una plataforma de captura de evidencias electrónicas online

Nombre estudiante

Eduardo Hervás Rosa

Programa

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Telecomunicaciones.

Aplicación profesional.

Consultor

Pau del Canto Rodrigo

Responsable de la asignatura

Víctor García Font

Fecha de entrega

4 de junio de 2018

© Eduardo Hervás Rosa

Reservados todos los derechos. Está prohibido la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Análisis de una plataforma de captura de evidencias electrónicas online*
Nombre del autor:	*Eduardo Hervás Rosa*
Nombre del consultor/a:	*Pau del Canto Rodrigo*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2018
Titulación::	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Telecomunicaciones*
Área del Trabajo Final:	*M1.730 - TFM-Ad hoc*
Idioma del trabajo:	*Castellano*
Palabras clave	*evidencias digitales* *captura de evidencias* *pruebas electrónicas*

Resumen del Trabajo*:*

El objetivo de este TFM es realizar un análisis técnico y jurídico de una plataforma de captura de evidencias digitales.

Diariamente se presentan en los juzgados de todo el mundo pruebas en formato digital, muchas de las cuales acaban siendo impugnadas al no poder garantizarse su autenticidad e integridad. De ahí la importancia de capturar estas evidencias digitales utilizando servicios de terceros como la plataforma objeto de estudio.

Esta plataforma tiene como objetivo certificar el contenido de una página web, una sesión de navegación web o un fichero en el instante de tiempo en el cual el usuario solicita el servicio. Entendemos como certificar el generar un informe que contenga las evidencias que prueban la existencia y el contenido objeto de la certificación.

Hay dos pilares fundamentales que sustentan este TFM: por un lado el legal y por otro el técnico. Ambos sumados tienen como objetivo que los informes (comercialmente certificados) generados por esta plataforma sean admitidos

como prueba en un proceso judicial con un alto valor probatorio evitando así su impugnación.

Esta plataforma nace con un objetivo claro: facilitar una herramienta con la que probar casos de ciberacoso en Internet y acabar así con la impunidad con la que actúan los agresores, muchas veces envalentonados por el aparente anonimato que les facilita la red. No obstante, son casi infinitos los motivos que pueden llevar a un usuario a querer certificar contenido en formato digital.

Abstract:

The objective of this TFM is to carry out a technical and legal analysis of a platform for the capture of digital evidence.

On a daily basis, proof in digital format is presented to judges around the world, many of which end up being challenged, since they cannot guarantee their authenticity and integrity. Hence comes the importance of capturing digital evidence, using third-party tools, such as the platform presented in this study.

This platform has as its objective to certify the content of a web page, a web-browsing session or a file at the certain instant that the user makes use of this certification service. We understand as a certification the generation of a report that contains the evidence that prove the existence and the content of the object to be certified.

There are two fundamental pillars that support this TFM: on the one hand, the legal and on the other hand the technical. Both pillars combined aim to the objective that the reports (commercially certificates) generated by this platform are admitted as proof in a judicial process with a high evidential value, thus avoiding their dismissal.

This platform is born with a clear objective: to facilitate a tool with which to test cases of cyber-bullying on the Internet and thus give an end to the impunity that the aggressors act with, often emboldened by the apparent anonymity that the network is giving to them. Nevertheless, there are almost infinite reasons that can make a user want to certify any content in digital format.

Índice

1. Introducción 2
   1.1. Contexto y justificación del Trabajo 2
   1.2. Objetivos del Trabajo 3
   1.3. Enfoque y método seguido 4
   1.4. Planificación del Trabajo 5
   1.5. Breve sumario de productos obtenidos 5
   1.6. Breve descripción de los otros capítulos de la memoria 6
2. Validez jurídica de los servicios de certificación 7
   2.1. Análisis de la legislación vigente 7
      2.1.1. Legislación vigente, eIDAS. 7
   2.2. Regulación sobre la presentación de pruebas a un juicio. 11
3. Captura de evidencias digitales 13
   3.1. Introducción 13
   3.2. Docu-Certificado 14
   3.3. Certificado Directo 16
   3.4. Vídeo-Certificado 18
4. Módulo de sellado electrónico y sello de tiempo 22
   4.1. Introducción 22
   4.2. La firma electrónica avanzada en un documento PDF 22
      4.2.1. Validación del estado de revocación del certificado en el momento de la firma 24
      4.2.2. El sello de tiempo (timestamp) 25
   4.3. El módulo de sellado electrónico y tiempo 26
5. Log de auditoría 28
   5.1. Introducción 28
   5.2. El log de auditoría 28
      5.2.1. ¿Qué loguear? 28
      5.2.2. Formato del log en la Plataforma 31
      5.2.3. ¿Cómo loguear? 32
      5.2.4. Retención de los logs 34
      5.2.5. Visualización de los logs 35
6. Ciclo de vida del desarrollo de software 38
   6.1. Introducción 38

6.2. El repositorio de código fuente 38
6.3. El ciclo de vida del software (SDLC) 39
7. Redacción de textos legales 46
7.1. Introducción 46
7.2. Aviso legal y condiciones de uso 47
7.3. Política de privacidad 47
7.4. Política de cookies 50
7.5. Condiciones generales de contratación 51
8. Conclusiones 53
9. Glosario 56
10. Bibliografía 58

Lista de ilustraciones

Ilustración 1: Estadística evolución cibercriminalidad 2
Ilustración 2: Procedimiento DOCU-CERTIFICADO 14
Ilustración 3: Procedimiento CERTIFICADO DIRECTO 16
Ilustración 4: Procedimiento VIDEO-CERTIFICADO 20
Ilustración 5: Proceso de firma 27
Ilustración 6: Consola AWS CloudWatch 33
Ilustración 7: Arquitectura CloudWatch y ELK 35
Ilustración 8: Consola Kibana 36
Ilustración 9: Dashboard Kibana 37
Ilustración 10: Ciclo de vida del software (SDLC) 39
Ilustración 11: Metodología TDD 40
Ilustración 12: Entornos preproductivos y productivo 41
Ilustración 13: Esquema ejemplo de Gitflow 42
Ilustración 14: Informe scan Qualys 45

1. Introducción

1.1. Contexto y justificación del Trabajo

Términos como delito informático, ciberbullying, fraude en la red,... son términos que desafortunadamente empiezan a ser habituales en nuestra sociedad y que propician que la cibercriminalidad sea uno de los ámbitos delictivos que crece a más velocidad.

El anonimato, la inmediatez y la amplitud del alcance que facilitan las nuevas tecnologías hacen que muchos se atrevan a delinquir en la red.

En el caso de España el Ministerio del Interior en su portal estadístico de criminalidad [1] ha incluido un apartado dedicado a las infracciones penales relacionadas con la cibercriminalidad. Podemos ver en la Figura 1 la imparable evolución de delitos como el fraude informático, amenazas y coacciones o contra el honor entre otros.

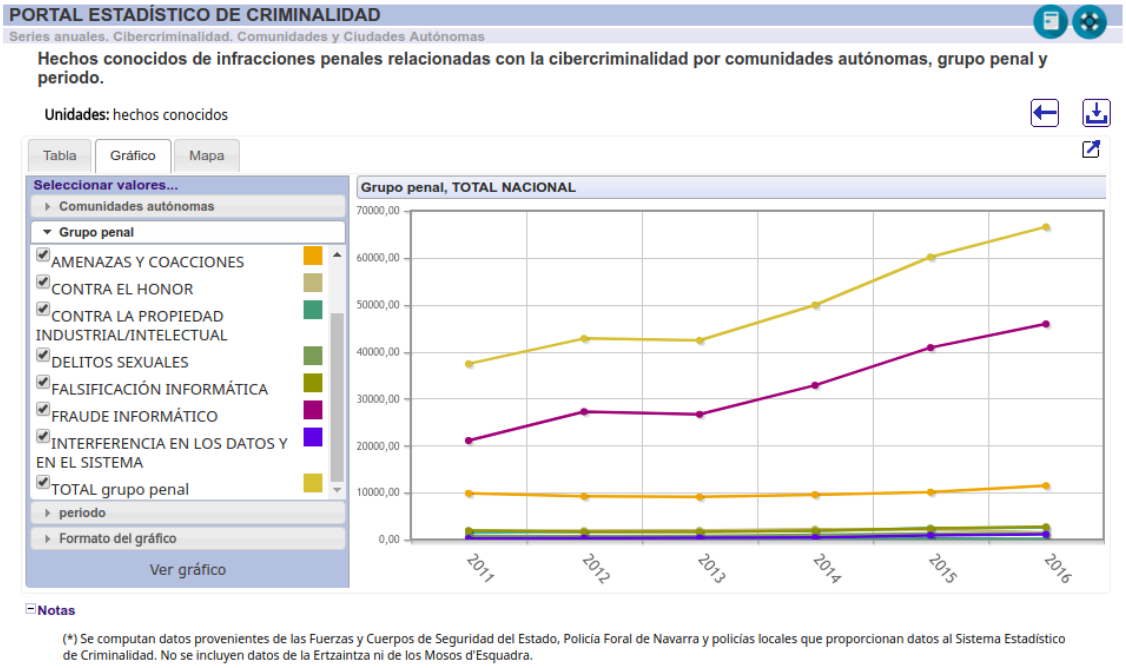


Ilustración 1: *Estadística evolución cibercriminalidad*

Esto se traduce en que cada día es más habitual ver en los juzgados como se aportan pruebas en formato digital (mensajes de WhatsApp, Facebook, Twitter, capturas de pantalla, ficheros de imágenes, audios, documentos,...).

En el ámbito judicial las pruebas, evidencias, se clasifican en documentos privados y públicos.

Los documentos públicos son aquellos expedidos o autorizados por un funcionario público o fedatario público competente y que da fe de su contenido por sí mismo.

Una captura de pantalla tomada por un usuario para demostrar la existencia de una prueba (un mensaje en una red social, una página web,...) es en consecuencia un documento privado.

Aunque los documentos privados tienen carácter probatorio en un juicio si el juzgado los admite a trámite, son más fáciles de impugnar por la parte demandada que los documentos públicos.

Pongamos un caso práctico:

María acusa y denuncia a Juan de un delito de injurias, derivado de la publicación de un mensaje por parte de este en la red social Facebook:

"@María es una **j* d* p**a que utiliza Internet para intercambiar pornografía infantil"

Juan está haciendo una acusación extremadamente grave. De ser verdad, María se enfrentaría a muchos años de prisión.

Pero, ¿qué ocurre si Juan miente? Desprestigiar a alguien por Internet es gratis, y puede ser fruto de un acto de rebeldía incontrolado amparado por una mal supuesta impunidad en la red.

Imaginemos que Juan ha mentido y minutos después se arrepiente de la publicación y decide eliminar el mensaje. No obstante, María lo ha leído y ha hecho una captura de pantalla desde su teléfono móvil.

María rápidamente contacta con su abogado y proceden a querellarse contra Juan por un delito de calumnias en injurias aportando como única prueba la fotografía de su móvil (recordemos que el mensaje se eliminó de la red social).

Ante el juez, la parte demandada (el abogado de Juan) solicita al juez la impugnación de la prueba presentada por el abogado de María alegando que la fotografía está manipulada y que jamás se publicó dicho mensaje.

María tiene un problema: no va a tener modo de acreditar la autenticidad de la prueba.

Este ejemplo no es un caso real, pero esto se produce cada día en los juzgados de todo el mundo.

El problema está claro: Las evidencias digitales adquiridas por medios clásicos son fácilmente impugnables en un procedimiento judicial. Es necesario trasladar a una tercera parte independiente la responsabilidad de capturar y certificar evidencias digitales con seguridad jurídica.

1.2. Objetivos del Trabajo

El objetivo de este TFM es realizar un análisis técnico y jurídico de una plataforma (en adelante Plataforma) de captura de evidencias digitales.

Esta Plataforma tiene como objetivo certificar el contenido de una página web, una sesión de navegación web o un fichero en el instante de tiempo en el cual el usuario solicita el servicio. Entendemos como certificar el generar un informe que contenga las evidencias que justifican la existencia y el contenido objeto de la certificación.

Este TFM se centra en tres áreas:

- Estudio de la legislación actual entorno a la presentación de pruebas digitales en sede judicial.
- Análisis técnico y documentación de una Plataforma que captura evidencias digitales poniendo especial énfasis en el proceso de firma electrónica.
- Análisis de medidas adicionales tanto de carácter técnico como legal, para ofrecer al mercado los servicios de la Plataforma objeto de estudio con garantías legales: redacción de textos legales en la web y log de auditoría en la Plataforma.

1.3. Enfoque y método seguido

Este TFM surge de la pregunta: ¿Qué características debería tener una Plataforma de captura de evidencias digitales para generar pruebas con un alto valor probatorio en sede judicial?

Para esto reprodujimos sobre el papel un caso basado en la realidad y fuimos viendo las necesidades a cubrir:

- ¿Cómo se presentan pruebas digitales en un proceso judicial? ¿Qué formato deben tener? ¿Qué validez tiene su contenido?
- ¿Cómo se pueden capturar a nivel técnico las evidencias para los casos contemplados (una página web, una sesión de navegación o un fichero)?
- ¿Cómo se puede securizar el proceso de firma para evitar problemas de seguridad?
- Además de los informes (comercialmente conocidos como certificados) generados con las evidencias (mensajes de una red social, una página web, un fichero,...), ¿qué otra información podría ser requerida de la Plataforma para reforzar la validez legal de estos?
- El servicio se ofrece a través de una Plataforma web. ¿Qué obliga la ley a que cumplan los proveedores de servicios de la información, como nuestra Plataforma web, teniendo en cuenta además que va a ser un servicio de pago?

Y de estas preguntas nacieron los capítulos del TFM para darles respuesta:

Capítulo 1: Validez jurídica de los servicios de certificación ofrecidos por la Plataforma.

Capítulo 2: Captura de evidencias digitales.

Capítulo 3: Módulo de sellado electrónico y sello de tiempo.

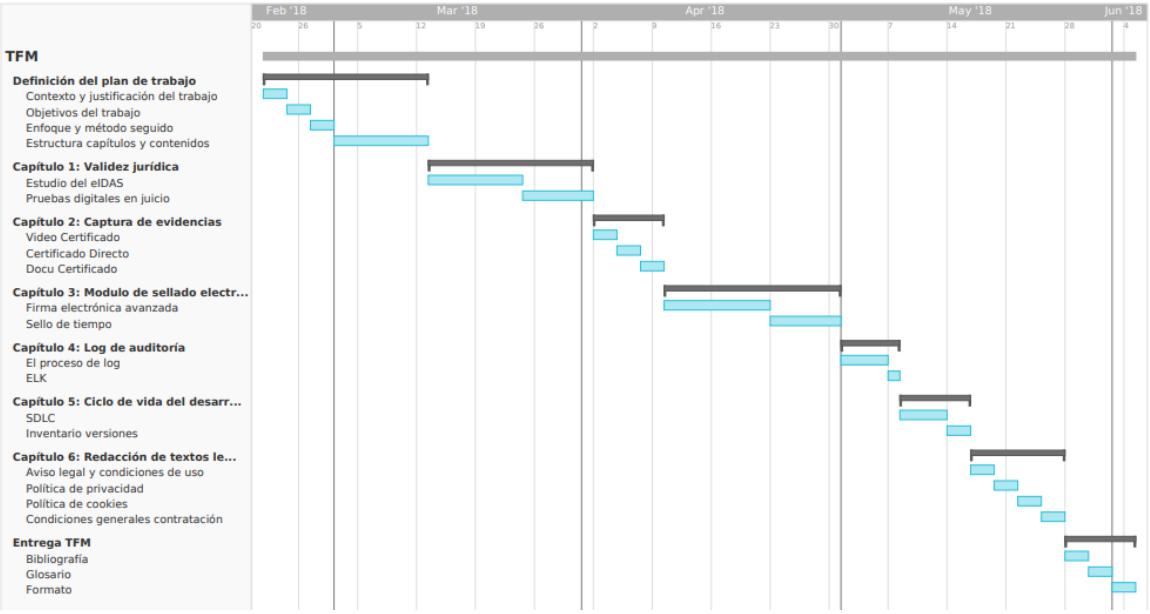
Capítulo 4: Log de auditoría.

Capítulo 5: *Ciclo de vida del desarrollo de software.*

Capítulo 6: Redacción de textos legales.

1.4. Planificación del Trabajo

A continuación se incluye el diagrama de Gantt con la planificación de las tareas necesarias para la elaboración de este TFM.



1.5. Breve sumario de productos obtenidos

El producto final obtenido ha sido por una parte este documento, el TFM en sí, y por la otra el desarrollo de la propia Plataforma.

Los dos se han ido ampliando en paralelo y de la mano. Este TFM además de su carácter analítico, ha servido para corregir errores que se habían cometido, por desconocimiento, en la Plataforma web, y también para implementar otros aspectos que han surgido tras el estudio de las diferentes materias comprendidas en este trabajo.

Por lo tanto, este trabajo no se limita a este documento, sino que está también el traslado de esta teoría a un producto real, y que por lo tanto es la conjunción TFM + Plataforma web lo que realmente tiene valor.

1.6. Breve descripción de los otros capítulos de la memoria

Capítulo 1: Validez jurídica de los servicios de certificación ofrecidos por la Plataforma.

En este capítulo se ha hecho un estudio del elDAS, el reglamento europeo que da un marco legal a la firma electrónica y al sello de tiempo, entrando en detalle en aquellos artículos que son de aplicación para los informes generados por la Plataforma.

También se ha estudiado la presentación de pruebas digitales en sede judicial y la validez y robustez de estas.

Capítulo 2: Captura de evidencias digitales.

Se ha detallado el proceso de captura de evidencias digitales y la generación de los informes (certificados) para los tres servicios que ofrece nuestra Plataforma:

- Certificación de un fichero.
- Captura y certificación del contenido de una URL.
- Captura y certificación de una sesión de navegación web.

Capítulo 3: Módulo de sellado electrónico y sello de tiempo.

Se ha especificado la implementación técnica de la firma electrónica avanzada (sello para el caso de entidades jurídicas) y sello de tiempo en los informes generados por la Plataforma.

Capítulo 4: Log de auditoría

Se ha explicado la importancia de tener un log de auditoría y un sistema para poder acceder a este de forma ágil. Esto ayudará a avalar la validez del sistema de certificación de la Plataforma en caso de incidentes.

Capítulo 5: Ciclo de vida del desarrollo de software.

Se ha demostrado la importancia de seguir un procedimiento durante el desarrollo de software para obtener un producto competente y rentable. También se ha destacado la importancia de tener implementados controles para adelantarse a incidencias de seguridad.

Capítulo 6: Redacción de textos legales.

Se han estudiado los requisitos legales que tiene que cumplir la empresa titular de la Plataforma para cumplir con los requisitos legales vigentes en la Unión Europea.

2. Validez jurídica de los servicios de certificación ofrecidos por la Plataforma

2.1. Análisis de la legislación vigente

Es de vital importancia que los documentos generados por la Plataforma tengan un respaldo jurídico robusto. En consecuencia se va a realizar un análisis de la normativa, legislación y buenas prácticas que directa o indirectamente aplican a los servicios ofrecidos por dicha Plataforma.

2.1.1. Legislación vigente, eIDAS.

El 23 de julio de 2014 el Parlamento Europeo y el Consejo de la Unión Europea presentaban el reglamento 910/2014 (eIDAS) [2] relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (por lo tanto de aplicación en los Estados miembros y prestadores de servicios de confianza establecidos en la Unión Europea).

Este reglamento a su vez derogaba la Directiva 1999/93/CE que venía aplicando a estos servicios con efectos a partir del 1 de julio de 2016.

Podemos resumir los objetivos del reglamento eIDAS en tres:

- Reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas e incrementando la eficacia de los servicios, negocios electrónicos y comercio electrónico de la Unión.
- Establecer las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro. (Art. 1.1 eIDAS)
- Establecer normas para los **servicios de confianza**, en particular para las transacciones electrónicas, estableciendo un marco jurídico para las **firmas electrónicas**, los **sellos electrónicos**, los **sellos de tiempo electrónicos**, los **documentos electrónicos**, los servicios de entrega electrónica certificada y los servicios certificados para la autenticación de sitios web. (Art. 1.2 y 1.3 eIDAS)

Hemos remarcado en negrita algunos términos a los que hace referencia el eIDAS y que desarrollamos a continuación:

<u>Documento electrónico</u>

Un **documento eléctrico** (Art. 3.35 eIDAS) es por definición cualquier contenido almacenado en formato electrónico, texto, audio o vídeo. En nuestro caso el documento que vamos a firmar y sellar en el tiempo va a ser lo que

comercialmente llamamos en la Plataforma "certificado" y que no deja de ser un informe en formato PDF con texto e imágenes (las evidencias).

Servicio de confianza

Un **servicio de confianza** (Art. 3.16 eIDAS) es el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en al menos uno de los siguientes puntos:

- La creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios.
- La creación, verificación y validación de certificados para la autenticación de sitios web.
- La preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

Sello electrónico

El eIDAS introduce el concepto de **sello electrónico** (Art. 3.25 eIDAS), con las mismas características y variaciones (avanzada y cualificada) que la firma electrónica, pero para personas jurídicas.

Puesto que la Plataforma está respaldada por una persona jurídica: Full digital S.L., y no una física, hablaremos de sello electrónico en lugar de firma electrónica.

Un **sello electrónico** son los datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

Dispone de dos variaciones:

- **Sello electrónico avanzado** (Art. 3.26 eIDAS), un sello electrónico que cumple los requisitos contemplados en el artículo 36 del eIDAS;
- **Sello electrónico cualificado** (Art. 3.27 eIDAS), un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico;

Veamos qué requisitos debe cumplir un sello electrónico avanzado según el artículo 36 del eIDAS:

> *a) estar vinculado al creador del sello de manera única;*
>
> *b) permitir la identificación del creador del sello;*

c) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo, y

d) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Sello de tiempo

Un **sello de tiempo** (Art. 3.33 eIDAS) se define como los datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.

El sello de tiempo también dispone de su variación cualificada y el artículo 42 del eIDAS indica los requisitos que debe tener:

a) vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte;

b) basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado, y

c) haber sido firmada mediante el uso de una firma electrónica avanzada o sellada con un sello electrónico avanzado del prestador cualificado de servicios de confianza o por cualquier método equivalente.

Ya tenemos definidos todos los conceptos que vamos a necesitar para emitir con validez legal dentro de la UE los informes generados por la Plataforma.

El objetivo principal es firmar digitalmente los documentos generados con un sello electrónico y sellarlos en el tiempo para garantizar la autenticidad, integridad y fecha de creación.

Respecto al sello electrónico, el proyecto está respaldado por una persona jurídica: Full Digital S.L.. Por esto, para sellar utilizaremos un sello electrónico que vincularemos a dicha sociedad. De esta manera los documentos emitidos por la Plataforma estarán inequívocamente vinculados a Full Digital S.L. con plenas garantías legales.

Dicho sello, será un sello electrónico avanzado (equivalente en personas físicas a la firma electrónica avanzada) generado con un certificado cualificado de sello electrónico, es decir, un certificado expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III del eIDAS.

Es importante destacar que nuestros documentos no tendrán un sello electrónico cualificado ya que el proceso de sellado debería realizarse utilizando un

dispositivo cualificado de creación de sello electrónico (tarjeta inteligente o token conforme el artículo 39 del eIDAS) lo cual es inviable en un proceso automatizado de generación de documentos y sellado como el utilizado por nuestra Plataforma.

En resumen necesitamos un certificado de sello electrónico y un servicio de sellado de tiempo.

Aunque el sello de tiempo que se acabe añadiendo a nuestros documentos será avanzado y no cualificado, buscaremos que el certificado con el que se genere sí sea cualificado. En el caso del sello de tiempo sí que será cualificado. Estos dos serán los **servicios de confianza** que necesitamos que nos ofrezca un **prestador cualificado de servicios electrónicos**.

El eIDAS, en el artículo 22, obliga a cada país miembro de la UE a que publique y mantenga un listado (**lista de confianza**) con los prestadores de servicios electrónicos de confianza cualificados y sus servicios, que dependan de dicho país.

En el caso de España el Ministerio de Energía, Turismo y Agenda Digital publica este listado en la URL: https://sedeaplicaciones.minetur.gob.es/Prestadores/

En este momento existen en España 22 prestadores de servicios de confianza, algunos públicos como el Ministerio de Empleo y Seguridad Social, la Dirección General de Policía,... y otros privados como ANCERT (Agencia Notarial de Certificación) o Firmaprofesional S.A. entre otros.

Es importante escoger bien a nuestro prestador de servicios por dos motivos: por una parte que ofrezca los servicios que necesitamos y en segundo lugar, que podamos identificarnos ante él evitando desplazamientos y costes.

Los servicios que vamos a necesitar del prestador son:

- Certificado corporativo de Sello Empresarial, para generar el sello electrónico avanzado.
- Servicio de Sello cualificado de Tiempo Electrónico.

Respecto a la identificación ante el prestador el artículo 24 del eIDAS especifica los requisitos para los prestadores cualificados de servicios de confianza:

1. Al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios de confianza verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado.

La información a que se refiere el párrafo primero será verificada por el prestador de servicios de confianza bien directamente o bien por medio de un tercero de conformidad con el Derecho nacional:

a) ***en presencia*** *de la persona física o* ***de un representante autorizado de la persona jurídica****, o*

b) ***a distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia*** *de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad «sustancial» o «alto», o*

c) ***por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado*** *expedido de conformidad con la letra a) o b), o d) utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física. La seguridad equivalente será confirmada por un organismo de evaluación de la conformidad.*

Finalmente por ofrecer los servicios que necesitamos y por estar situados en Barcelona, donde tiene su domicilio social Full Digital, S.L. hemos optado por Firmaprofesional S.A.

Profundizaremos más sobre el proceso de sellado electrónico y de tiempo en el capítulo 3.

2.2. Regulación sobre la presentación de pruebas a un juicio.

Hemos visto en el apartado anterior que uno de los objetivos del eIDAS es establecer un marco jurídico para los documentos electrónicos firmados digitalmente.

En el ámbito judicial podemos diferenciar dos tipos de documentos: los públicos y los privados.

Serán documentos públicos aquellos que estén firmados por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

El resto de documentos serán considerados privados.

En ambos casos, tanto los documentos públicos como los privados, se podrán aportar a juicio como prueba en formato electrónico. Aun así no es de extrañar que los documentos privados son los que más controversia generan y los que requieren de una mayor garantía y confianza a efectos de poder suponer prueba plena en un procedimiento judicial.

Si nos centramos en la ley española, en el artículo 326 de la Ley de Enjuiciamiento civil [3] se establece que los documentos privados serán prueba plena en el proceso judicial.

Artículo 326 Fuerza probatoria de los documentos privados

1. Los documentos privados harán prueba plena en el proceso, en los términos del artículo 319, cuando su autenticidad no sea impugnada por la parte a quien perjudiquen."

Ningún documento, sea cual sea su naturaleza, está exento de ser impugnado por la parte contraria en un procedimiento judicial. En el artículo 427.1 de la Ley de Enjuiciamiento Civil se establece tal posibilidad:

"En la audiencia, cada parte se pronunciará sobre los documentos aportados de contrario hasta ese momento, manifestando si los admite o impugna o reconoce o si, en su caso, propone prueba acerca de su autenticidad."

El artículo 35 del eIDAS indica en su punto primero que no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos del sello electrónico cualificado.

Los tres tipos de sello electrónico (simple, avanzado y cualificado) tienen valor legal y son por tanto admisibles a juicio como pruebas legalmente válidas. Sin embargo, una de las principales diferencias entre ellos, si se produjera la impugnación del documento, radica en a quién corresponde la carga de la prueba: El sello electrónico cualificado tiene a su favor la presunción *iuris tantum*, lo que significa que la autoría del sello se presume como demostrada salvo que se aporten pruebas en contra por parte de quien sostenga lo contrario.

En cambio, en el caso del sello electrónico simple o avanzado (este último nuestro caso) se invierte la carga de la prueba: si se cuestiona la autoría de un sello corresponde demostrar la validez del mismo a quien sostenga que es auténtico.

Hemos de tener en cuenta que la impugnación va dirigida a cuestionar la autenticidad del documento y no el valor que pueda tener el mismo a efectos de la resolución del procedimiento, valoración que realizará el juez en función de las reglas de la sana crítica.

4. Módulo de sellado electrónico y sello de tiempo

4.1. Introducción

En los capítulos anteriores hemos explicado que los documentos generados por la Plataforma están en formato PDF e incorporan un sello electrónico (análogo a la firma electrónica en personas físicas) y un sello de tiempo. En este capítulo vamos a entrar en el detalle de este proceso. Lo dividiremos en dos bloques, en primer lugar veremos el proceso de firma en un documento PDF y su implementación en JAVA y en un segundo bloque estudiaremos cómo hemos aislado este proceso a nivel de infraestructura para hacerlo más seguro.

En el capítulo 1 veíamos que el eIDAS introducía el concepto de sello electrónico, equivalente a la firma electrónica para entidades jurídicas. Aunque en nuestro caso los documentos PDFs están **sellados** al ser generados por una persona jurídica, utilizaremos el concepto de **firma** en lugar de sello como especifica el eIDAS. A efectos prácticos es el mismo procedimiento y el concepto firmar está más "arraigado" que no el de sellar.

A modo resumen, tal y como se explicó en el capítulo 1, son tres los objetivos básicos que persigue la firma electrónica de documentos:

- Asegurar que el documento no ha sido alterado desde su generación (integridad).
- Asegurar que el autor del documento es quien dice ser (autenticidad).
- Asegurar que el autor no puede denegar la autoría (no repudio).

4.2. La firma electrónica avanzada en un documento PDF

El formato de firma es la forma como se genera el documento de firma y como se guarda o estructura la información de firma en el documento generado.

Existen diferentes formatos de firma y elegir uno u otro dependerá del formato del documento en sí a firmar y las necesidades que se requieran satisfacer con dicha firma.

Algunos de estos formatos son CAdES, XAdES, PAdES, OOXML o ODF.

Además del formato del documento a firmar, nos ayudará a seleccionar el formato de firma el hecho de que el documento original se incluya o no en el documento de firma. La ventaja de que sea incluido es que no hay que almacenar por separado el documento original y el de firma, ya que el de firma incluye el original.

En nuestro caso, para los documentos generados por nuestra Plataforma, nos hemos decantado por el estándar PAdES porque:

- El documento a firmar tiene formato PDF.
- La firma se incorporará al mismo fichero PDF.
- La firma puede ser validada fácilmente desde el lector de PDFs.
- Cumple con el formato de firma electrónica avanzada.
- La firma puede validarse muchos años después de su generación.

PAdES (PDF Advanced Electronic Signatures - ETSI TS 102 778) [5] es un conjunto de restricciones y extensiones al formato PDF y a la ISO-32000-1 [6] que hace posible implementar firmas electrónicas avanzadas en los documentos PDFs, concretamente así lo especifica la parte 3 de las 5 que lo conforman. Esta parte 3, titulada "PAdES Enhanced - PAdES-BES and PADES-EPES Profiles" define el perfil en el que nos centraremos: PAdES-BES.

Este perfil está basado en CAdES-BES especificado en ETSI TS 101 733 – 2 [7] e incorpora la posibilidad de incluir en la firma un sello de tiempo (CAdES-T).

A su vez el formato CAdES es un conjunto de extensiones de CMS (Cryptographic Message Syntax) que cumple con los requisitos de firma electrónica avanzada, o en nuestro caso sello electrónico avanzado, que especifica el eIDAS y que ya veíamos en el capítulo 1:

> *a) estar vinculado al creador del sello de manera única;*
>
> *b) permitir la identificación del creador del sello;*
>
> *c) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo, y*
>
> *d) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.*

Como información adicional decir que PAdES-BES ha sido incorporado en la ISO-32000-2 [8] publicada en Julio del 2017 y que define el PDF 2.0.

También destacar que aunque el último estándar definiendo perfiles PAdES es ETSI EN 319 142-1&2 [9], el eIDAS todavía hace referencia a ETSI TS 102 778. Esto se debe a que los perfiles definidos en el último estándar proveen requisitos equivalentes a los establecidos en el anterior y por lo tanto igualmente válidos. Así se hace constar en la sección "1-Scope" de ETSI EN 319 142-1&2:

> *The profiles defined in the present document provide equivalent requirements to profiles found in ETSI TS 102 778 [i.10].*

Además de permitirnos generar una firma electrónica avanzada, el perfil PAdES-BES puede utilizarse junto al perfil PAdES-LTV, el formato de firma longeva (parte 4 del PAdES titulada PAdES Long Term—PAdES-LTV Profile). Este perfil permite

prorrogar por tiempo indefinido la validez de las firmas en formato PDF aunque los algoritmos criptográficos subyacentes estén rotos. Técnicamente esto se consigue al incrustar en el cálculo del algoritmo de la firma electrónica dos informaciones fundamentales:

- **La validación del estado de revocación del certificado en el momento de la firma**: se puede conseguir mediante dos sistemas, que pueden utilizarse conjuntamente: realizando una consulta mediante el protocolo OCSP y/o a través de listas de revocación de certificados (CRL). Entraremos en más detalle en la sección 3.2.1.
- **El sello de tiempo (timestamp)** mediante el que un tercero de confianza indicará la hora exacta del momento de la firma. Más detalle en la sección 3.2.2.

Es importante destacar la importancia de este perfil LTV en nuestro caso. Los documentos generados por nuestra Plataforma están directamente vinculados a un instante en el tiempo. Al fin y al cabo estamos creando una instantánea del contenido de una URL, una sesión de navegación web o un fichero en un momento de tiempo concreto. No obstante, no podemos asegurar en qué momento se utilizará por parte del usuario el documento generado. En la mayoría de los casos seguramente el intervalo de tiempo entre la generación de la prueba, su firma, y utilización y verificación será corto, pero en otros quizás puedan pasar años. Por eso, no podemos conformarnos sólo con mantener válida la prueba generada (el PDF, comercialmente 'certificado') durante el tiempo de vida útil del certificado utilizado para su firma, sino que hay garantizar que su autenticidad e integridad se puedan validar más allá de este tiempo.

Una duda que nos surgió fue la necesidad o no de "resellar" los PDFs generados. Entendemos resellar al hecho de volver a firmar o sellar un documento con un certificado vigente. En nuestro caso llegamos a la conclusión de que no necesitamos resellar los documentos porque estos no tienen como objetivo ir "reafirmando" su validez periódicamente. Diferente sería si estuviéramos por ejemplo trabajando con pólizas de seguros o contratos bancarios. Estos sí necesitan ir renovando su validez cada X tiempo, utilizando para ello el "resellado" del documento con un certificado válido en cada instante.

4.2.1. Validación del estado de revocación del certificado en el momento de la firma

Existen dos métodos para verificar en el momento de la firma el estado de revocación del certificado utilizado para generar ésta: lista de revocación de certificados (CRL) y consulta mediante el protocolo OCSP.

Escoger un sistema u otro, o incluso ambos conjuntamente, dependerá de las necesidades de cada caso.

Las CRLs son listas que incluyen los números de serie de todos los certificados revocados que publican las CA (Certification Authority) periódicamente

(habitualmente semanalmente) y que se actualizan cada vez que se revoca algún certificado.

Cada certificado de la cadena de certificados que interviene en la firma puede tener asociado una CRL. Dependiendo de la CA, la CRL puede tener un tamaño considerable, lo cual habrá que tener en cuenta por dos motivos:

- Idealmente habría que solicitar la CRL (descargar el fichero) de la CA en cada petición de firma para asegurarnos que es la última versión disponible. Esto puede provocar un importante tráfico de red dependiendo del número de firmas y del tamaño de la CRL. Es cierto que se podría descargar de manera periódica y utilizar una versión "cacheada" en el servidor de firma, pero cabe la posibilidad de que no se tenga la última versión.
- El tiempo que el servidor de firma tarde en la descarga y procesado de la CRL es tiempo que se añade al proceso de firmado en sí.

Por otro lado está el protocolo OCSP para validar el estado de revocación de un certificado. Es una consulta http que se hace al servidor OCSP de la CA que responderá con el estado del certificado. La respuesta tiene un tamaño pequeño y constante.

En ambos casos, la CRL y/o la respuesta al OCSP son incrustadas en la firma. Idealmente se utilizarían ambos sistemas, pero en la práctica OCSP se impone a la inclusión de CRLs. Tal y como hemos comentado, el tamaño resultante de un PDF que incluye CRLs puede ser sustancialmente mayor al que utiliza sólo OCSP.

4.2.2. El sello de tiempo (timestamp)

Otro de los aspectos importantes es tener la garantía del momento exacto en el que el documento fue firmado. No sólo es importante por el hecho de que los documentos que genera la Plataforma tienen como objetivo probar el contenido de una URL, sesión de navegación o fichero en un momento determinado, sino también garantizar las fechas de expiración y revocación del certificado de firma. Si estas fechas están vinculadas al reloj del servidor que realiza la firma podría darse el caso de que esta no fuera la real. Por este motivo, para tener certeza de la fecha, interviene una tercera parte, una TSA (Time Stamping Authority). Esta TSA concatenará y firmará la fecha real del momento de firma añadiéndose así esta información a la firma del documento.

En el caso de nuestra Plataforma el proceso de firma está pensado para tener un grado de protección alto contra ataques (en el siguiente bloque veremos en detalle cómo hemos aislado este proceso). No obstante, y puesto que ningún sistema es invulnerable, en caso de que nuestro certificado y su clave privada se vieran comprometidos, podríamos pedirle a la CA su revocación y hacer uso del valor que conlleva la incrustación de la CRL y/o respuesta del OCSP y del timestamp. De esta manera podríamos repudiar documentos generados fraudulentamente en nuestro nombre.

4.3. El módulo de sellado electrónico y tiempo

Una vez queda claro el formato de firma a utilizar (PAdES-LTV junto PAdES-BES) es momento de buscar una implementación en JAVA.

Para la Plataforma utilizaremos iText, una librería JAVA ampliamente utilizada y reconocida que facilita la generación y manipulación de PDFs. Concretamente utilizaremos la versión 5.5 (PAdES-LTV y PAdES-BES están disponibles desde la versión 5.3).

La librería iText permite en pocas líneas de código firmar documentos PDFs compatibles con la especificación PAdES.

Básicamente necesita:

- Fichero PDF a firmar.
- Un "security provider" (La librería BouncyCastle para JAVA en nuestro caso).
- La cadena de certificados de firma.
- Un cliente para recuperar las CRL de los certificados.
- Un cliente para la consulta OCSP.
- Un cliente para la petición a la TSA.
- El estándar criptográfico a utilizar (CADES en nuestro caso).

Los tres clientes (CRL, OCSP y TSA) ya están implementados en la librería iText por lo que utilizaremos estos.

En el capítulo 2 ya veíamos que en nuestra arquitectura el proceso de firma está aislado en una función Lambda de AWS.

Como ya explicábamos Lambda es un servicio ofrecido por AWS que permite la ejecución de una función (un programa JAVA en nuestro caso).

Utilizar Lambda de AWS para la firma tiene dos grandes ventajas:

- El código se ejecuta en un entorno virtual que se crea y destruye automáticamente para cada firma. Por lo tanto es un sistema auto escalable de por sí.
- Ni el servidor de aplicaciones donde corre la Plataforma ni el usuario tienen posibilidad de acceder a este entorno. Esto es importante porque en caso de que el servidor de aplicaciones se viera comprometido y un usuario malintencionado consiguiera acceder al sistema de ficheros, no encontrará ahí ni el certificado de firma ni su clave privada. El servidor de aplicaciones únicamente puede solicitar mediante eventos al módulo de firma la firma de documentos PDFs. Somos conscientes de que existen soluciones más seguras para almacenar la clave privada, un HSM

(Hardware Security Module) idealmente, pero su coste lo hace inviable en este momento.

A continuación vamos a ver el proceso de firma:

Ilustración 5: *Proceso de firma*

1. El servidor de aplicaciones hace llegar al módulo de firma un evento indicándole la ubicación donde está el PDF generado por la Plataforma con el contenido del certificado (información técnica, capturas de pantalla,...).
2. Lambda ejecuta la función JAVA que realiza el proceso de firma. Sólo la función tiene acceso a la clave privada.
3. Se almacena el documento PDF firmado y se comunica al servidor de aplicaciones de la finalización del proceso.

5. Log de auditoría

5.1. Introducción

En este capítulo explicaremos qué es un log de auditoría y por qué es importante que nuestra Plataforma disponga de uno.

El término "log" se refiere a la grabación secuencial en un archivo (o en una base de datos) de todos los acontecimientos que suceden en un proceso, en nuestro caso en una aplicación web y sus dependencias. De esta manera se constituye una evidencia del comportamiento del sistema.

Durante el capítulo utilizaremos el anglicismo "loguear" para referirnos a la acción de insertar información en el fichero de registro o "log".

5.2. El log de auditoría

Loguear y monitorizar los eventos que ocurren en una aplicación web son componentes clave si queremos cumplir con unas buenas prácticas en el campo de la seguridad y de la operatividad. Además, dependiendo del sector, dejar registro de cierta información puede llegar a ser un requisito legal.

Tener un buen log de auditoría nos puede ayudar a depurar errores, monitorizar componentes críticos del sistema, detectar intrusos, adelantarnos a futuros problemas, tareas de análisis forense, cumplir con la ley, estudiar patrones de comportamientos de usuarios, tomar decisiones respecto a la infraestructura, y un largo etcétera de aplicaciones.

Decidir qué se loguea, cómo y cuánto tiempo retener los logs, no es una tarea fácil, y la mayoría de ocasiones no suele tenerse en cuenta durante la etapa de diseño. No obstante, en nuestra Plataforma pensamos que es un componente indispensable. Los certificados emitidos serán cuestionados por terceros desde el minuto cero. Nacen con esa condición. Por eso es importante que el sistema esté fuertemente auditado para resolver dudas en caso de conflicto.

5.2.1. ¿Qué loguear?

Vamos a definir tres planos en los que será necesario tener un registro:

- Acciones del usuario.
- Eventos de la aplicación web y sus dependencias.
- Eventos de la infraestructura.

<u>Acciones del usuario</u>

Incluye cualquier interacción que tenga directamente el usuario con la Plataforma. Esto supone entre otros:

- Login / logout.
- Listar certificados.
- Solicitar un certificado.
- Recargar de saldo la cuenta.
- Cambio de contraseña.
- ...

Eventos de la aplicación web y sus dependencias

Incluye cualquier evento que se produzca en la aplicación web u otros módulos relacionados y que puedan tener interés para los objetivos del log de auditoría. Esto supone:

- Actualización de datos en BBDD.
- Peticiones al módulo de firma.
- Errores controlados y no controlados durante la ejecución.
- Acciones para escalar servicios (por ejemplo aumentar el número de instancias EC2 atendiendo peticiones durante un pico).
- ...

Eventos de la infraestructura

Aunque hemos hablado en muchas ocasiones de Amazon, cabe recordar que toda la infraestructura está en el cloud, concretamente en AWS de Amazon. Además de las ventajas que hemos ido viendo en capítulos anteriores, la gestión de logs de auditoría en los servicios proporcionados por Amazon también es ventajosa. Amazon ha desarrollado AWS CloudTrail, un servicio web que almacena todos los eventos que se producen en su infraestructura. Esto supone:

- Todas las operaciones realizadas por la aplicación web hacia cualquier servicio de AWS a través de la API.
- Accesos a la consola de administración vía web.
- Accesos mediante CLI.
- Creación de nuevas instancias.
- Accesos a Amazon S3.
- Cambios en la configuración de los servicios.
- ...

Amazon basándose en estándares como ISO 27001, PCI DSS v2.0, FedRAMP, etc. [10] registra eventos con un alto nivel de detalle. Podemos ver un ejemplo:


```
{
  "eventVersion":"1.04",
  "userIdentity":{
    "type":"AssumedRole",
    "principalId":"AROAJNHL6R6MXKVPB5MQA:LogsToElasticsearch_xxxxxx",
    "arn":"arn:aws:sts::392443884275:assumed-
role/lambda_elasticsearch_execution/LogsToElasticsearch_xxxxx",
    "accountId":"392443884275",
    "accessKeyId":"ASIAJH7O4S6GBNW5V5UA",
    "sessionContext":{
      "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2018-05-13T12:05:55Z"
      },
      "sessionIssuer":{
        "type":"Role",
        "principalId":"AROAJNHL6R6MXKVPB5MQA",
        "arn":"arn:aws:iam::392443884275:role/lambda_elasticsearch_execution",
        "accountId":"392443884275",
        "userName":"lambda_elasticsearch_execution"
      }
    }
  },
  "eventTime":"2018-05-13T14:00:38Z",
  "eventSource":"logs.amazonaws.com",
  "eventName":"CreateLogStream",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"18.206.125.131",
  "userAgent":"awslambda-worker",
```

```
  "requestParameters":{

"logStreamName":"2018/05/13/[$LATEST]b7fb8a13469a4bed8130eb4d46e315ad",
    "logGroupName":"/aws/lambda/LogsToElasticsearch_xxxxx"
  },
  "responseElements":null,
  "requestID":"03e759de-56b6-11e8-80ed-49fe406728fc",
  "eventID":"f283ab5b-52cd-4f17-8940-466eb5c97ee0",
  "eventType":"AwsApiCall",
  "apiVersion":"20140328",
  "recipientAccountId":"392443884275"
}
```


5.2.2. Formato del log en la Plataforma

En el apartado anterior veíamos los diferentes eventos que puede registrar la Plataforma y algunos ejemplos. Para nuestra Plataforma nos hemos basado en la implementación que ha hecho AWS Trail y el PCI DSS [11] (el estándar de seguridad para la industria del pago mediante tarjeta). Nos hemos fijado en ambas implementaciones al ser referentes fuertes en sus respectivos ámbitos. Este es el formato que utilizará nuestra Plataforma:

```
{
  "eventTime": "2018-06-25T02:13:20.500Z",
  "userId": "user@test.com",
  "sourceIP": "1.2.3.4",
  "origin": "web",
  "event": {
    "id": "12345678",
    "type": "login",
    "result": "KO"
  }
}
```

Dependiendo del tipo de evento el objeto JSON con key “event” será diferente. En el ejemplo hemos registrado un intento fallido de login desde la web para el usuario user@test.com desde la IP 1.2.3.4 a la hora indicada en el eventTime.

Lo que en cualquier caso debe registrarse siempre es:

- La fecha exacta del evento (en formato GMT para evitar conflictos con zonas horarias).
- El usuario vinculado al evento.
- El origen del evento (puede ser el cliente o un componente de software interno).
- El contenido del evento

5.2.3. ¿Cómo loguear?

Ahora que ya sabemos qué loguear, hay que decidir la manera en la que lo hacemos.

Esto es importante por varios motivos:

- El sistema de log no tiene que interferir en el funcionamiento del sistema.
- El sistema de log debe estar siempre disponible.
- Los logs deben estar centralizados para que su consulta y gestión sea práctica.
- Los registros del log no deben poderse alterar una vez generados. Ni modificar ni eliminar.
- No se debe poder insertar logs anteriores a la fecha actual.
- El acceso a los logs debe poderse realizar únicamente por un usuario autorizado y el proceso debe estar auditado.
- Cada fichero de log debe tener su política de retención.

Para cumplir con todos estos requisitos nos hemos decantado por utilizar el servicio CloudWatch de AWS junto Amazon Elasticsearch Service.

Amazon CloudWatch es un servicio de monitorización y almacenamiento de logs en la nube capaz de recibir logs mediante el uso de una API o un agente que puede instalarse en cualquier instancia EC2.

Toda nuestra computación está alojada en servidores EC2 de Amazon. Esto hace que el agente de CloudWatch sea la mejor solución para nuestro caso. Las aplicaciones y procesos loguearán localmente en la máquina en la que se ejecuten. En tiempo real el agente CloudWatch monitorizará estos ficheros de logs y automáticamente irá enviando los nuevos registros al servicio de CloudWatch.

El agente se configura localmente y se especificará en su fichero de configuración el "log group" (ubicación virtual de almacenamiento) al que se quieren enviar los datos. Cada "log group" tiene diferentes "log streams".

Normalmente un "log stream" es una instancia EC2. Pongamos un ejemplo:

Una aplicación web ha configurado el agente CloudWatch para enviar logs al log group "AppWeb". Esta aplicación web está configurada para auto escalar y puede haber entre 1 y n instancias ejecutando la aplicación. Si todos los agentes escribieran en el mismo lugar (log group) sería difícil poder diferenciar a qué instancia pertenece cada registro, a excepción de que el contenido del log incluya esa información.

CloudWatch soluciona esto generado un "log stream" por cada instancia. De esta manera aunque los tres servidores escribirán en el mismo grupo, cada uno escribe en un stream diferente.

Así se verían los logs en la consola de AWS CloudWatch:

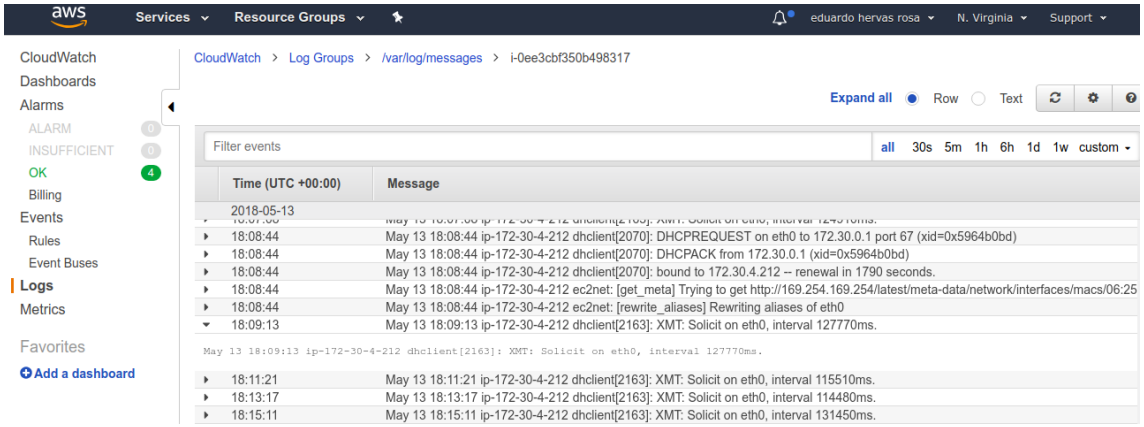


Ilustración 6: *Consola AWS CloudWatch*

Cada entrada va identificada con su fecha en formato GMT. Esta fecha es en la que el agente ha leído del fichero de log original la entrada. La fecha registrada no es cuestionable puesto que no es la del sistema donde se generó el log, sino que es la gestionada por el agente conectado a AWS. En la figura vemos que el mensaje de log también contiene una fecha aparte de la generada por CloudWatch. Como hemos indicado anteriormente, los logs contienen en cada registro la fecha del evento. Se puede ver en la imagen que la fecha de CloudWatch y la del propio log coinciden. Habitualmente será así. Los servidores mantienen sincronizado su reloj con servicios externos. Pero si por cualquier motivo la fecha local del sistema se modificara, la fecha de referencia pasará a ser la de CloudWatch.

¿Por qué esto es tan importante? Porque si un usuario malintencionado consiguiera acceso al fichero de log en la instancia EC2 e intentara alterar logs pasados, el agente CloudWatch ignorará todas las líneas del fichero anteriores a la última enviada al sistema.

También hay que destacar que si por algún motivo CloudWatch se cayera temporalmente y no pudiera procesar logs del agente, o el agente no pudiera por cualquier motivo enviar durante un tiempo logs a CloudWatch, tan pronto como el servicio quedara restaurado se enviarían automáticamente los logs correspondientes a ese intervalo de tiempo.

Otro aspecto positivo de CloudWatch es que una vez los logs son entregados por el agente estos no se pueden modificar. Son de solo lectura, y su lectura sólo puede realizarse por un usuario autorizado con acceso al servicio.

5.2.4. Retención de los logs

En el apartado anterior veíamos que los logs se almacenan localmente en los servidores que los generan y son subidos a la nube mediante el agente de AWS CloudWatch. Dependiendo de las operaciones que se realicen el volumen de logs tanto en local como en AWS puede ser importante. En el primer caso tenemos una limitación de tamaño de disco y en el segundo caso AWS facturará por espacio ocupado. Tanto por un motivo como por el otro se hace necesario establecer una política de retención de logs.

Dependiendo del contenido de cada log se establecen las siguientes retenciones:

Log de operaciones	1 año
Otros logs (Servidor de aplicaciones, Módulo de firma,…)	30 días

En el caso de la retención, igual que con el contenido de los eventos como hemos indicado anteriormente, nos hemos basado en el estándar de seguridad PCI DSS, al estar destinado a nuestro entender a un sector donde la seguridad es un requerimiento estricto. Por eso, al igual que en el estándar, los logs que contengan operaciones se mantendrán por un mínimo de 1 año.

Otros logs que genere el servidor de aplicaciones u otros componentes se mantendrán sin embargo 30 días, tiempo suficiente para su revisión en caso necesario.

Localmente, en los servidores, la rotación y la retención viene gestionada por la librería JAVA log4j. Se configura esta para que automáticamente elimine los ficheros de log anteriores a n días. Además puede configurarse para que comprima logs anteriores a los del día actual para ahorrar espacio en disco.

En AWS CloudWatch la configuración de retención es mucho más sencilla ya que simplemente hay que indicar en la consola de administración el número de días que se mantendrá cada grupo. Pasada esa fecha los logs son automáticamente eliminados sin necesidad de acción por parte del usuario.

5.2.5. Visualización de los logs

CloudWatch ofrece una consola para visualizar logs con algunas opciones de filtrado de contenido y tiempo, pero no es demasiado flexible. Cuando el número de eventos es muy alto, intentar localizar datos, y ya no digamos correlacionar, se hace muy complicado.

Si hay una solución opensource excelente para la visualización de logs esa es ELK (Elastic Stack).

Elasticsearch es el motor de ELK basado en Apache Lucene. Se encarga de indexar contenido, logs en nuestro caso, para que sea fácil y sobre todo rápido poder hacer consultas sobre esos logs.

Por otro lado tenemos Kibana, la consola web de visualización y búsqueda de logs.

AWS también dispone del stack ELK que instala un Elasticsearch y un Kibana. Elasticsearch normalmente consume datos directamente de un agente instalado en la máquina donde se encuentran los logs, pero en nuestro caso, los logs se encuentran en CloudWatch (recordemos que ya han sido subidos mediante el agente de CloudWatch a AWS).

De una manera muy sencilla podemos ver los logs que antes teníamos en la consola de CloudWatch, y que eran difíciles de gestionar, en un entorno mucho más amigable lleno de posibilidades.

A continuación un esquema de cómo se gestionan logs en AWS mediante CloudWatch y ElasticSearch:

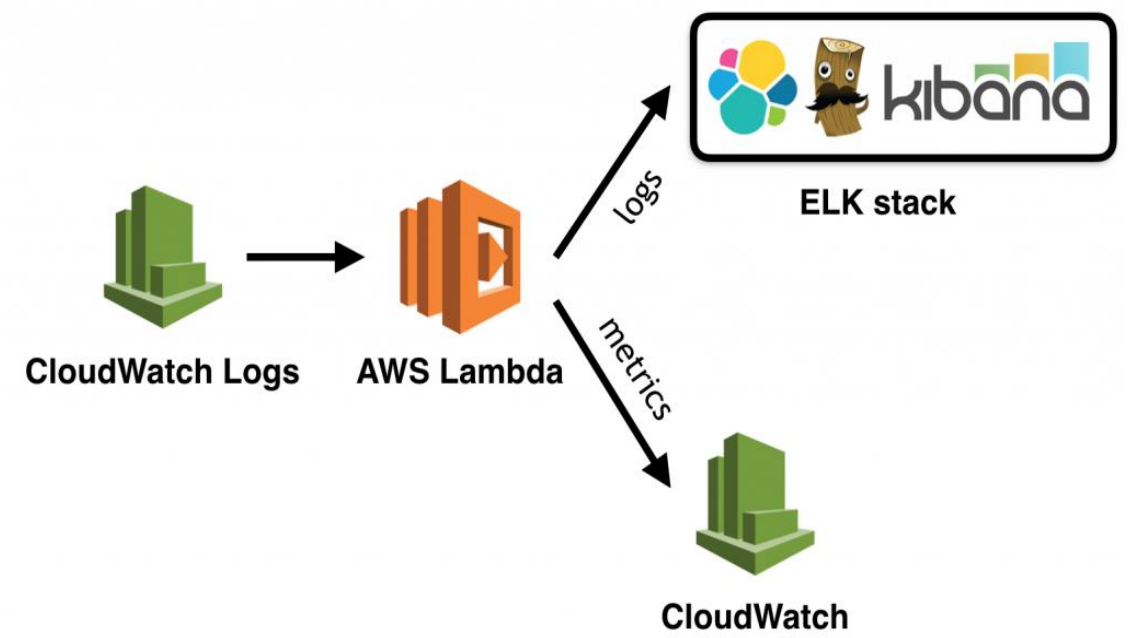


Ilustración 7: *Arquitectura CloudWatch y ELK*

Aunque el objetivo de este TFM no es explicar cómo funciona ElasticSearch y Kibana sí podemos ver un ejemplo de cómo se visualizaría una entrada del log en la siguiente figura:

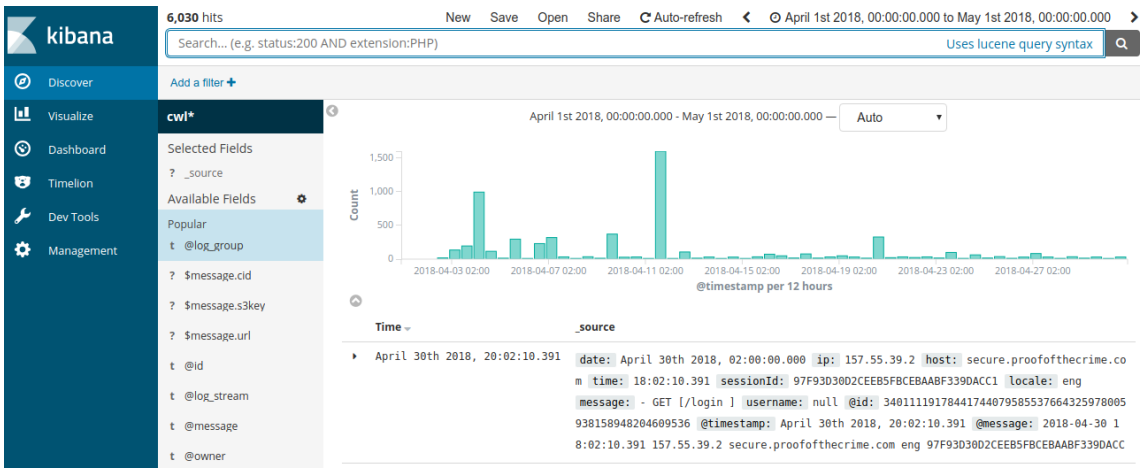


Ilustración 8: *Consola Kibana*

En la parte superior de la pantalla podemos ver una caja de texto para poder realizar búsquedas utilizando la sintaxis de búsquedas de Lucene [12]. Esto permite buscar logs filtrando por cualquier campo. También en la parte superior se puede ver un selector de tiempo en el que limitar los resultados o un selector para "auto-refrescar" los datos.

En la parte izquierda vemos los campos más populares y sus valores si clicamos en ellos. En la parte central vemos fácilmente los eventos resultantes en ese periodo de tiempo, y después, el detalle de cada entrada con su fecha.

Esta forma de visualizar de manera ágil los logs es muy útil a lo hora de tener una visión global del sistema, pero también para reproducir las acciones que ha llevado a cabo un usuario, detectar errores, intentos de acceso, volumen de llamadas para ayudarnos a escalar el sistema,…

Además de la visualización de logs, ELK dispone de la extensión (de pago) X-Pack. Este componente permite la generación de alertas mediante el servicio Watcher. Utilizando la misma sintaxis que en la búsqueda se puede programar para alertar mediante por ejemplo el envío de un correo electrónico, que cierto evento ha ocurrido en el periodo de tiempo definido. Esto puede ser muy útil para adelantarse a posibles ataques, degradación del sistema,…

Si la extensión X-Pack no es viable siempre queda la opción de tener dashboards con gráficos y búsquedas que ayuden de manera rápida y visual a detectar anomalías en el sistema.

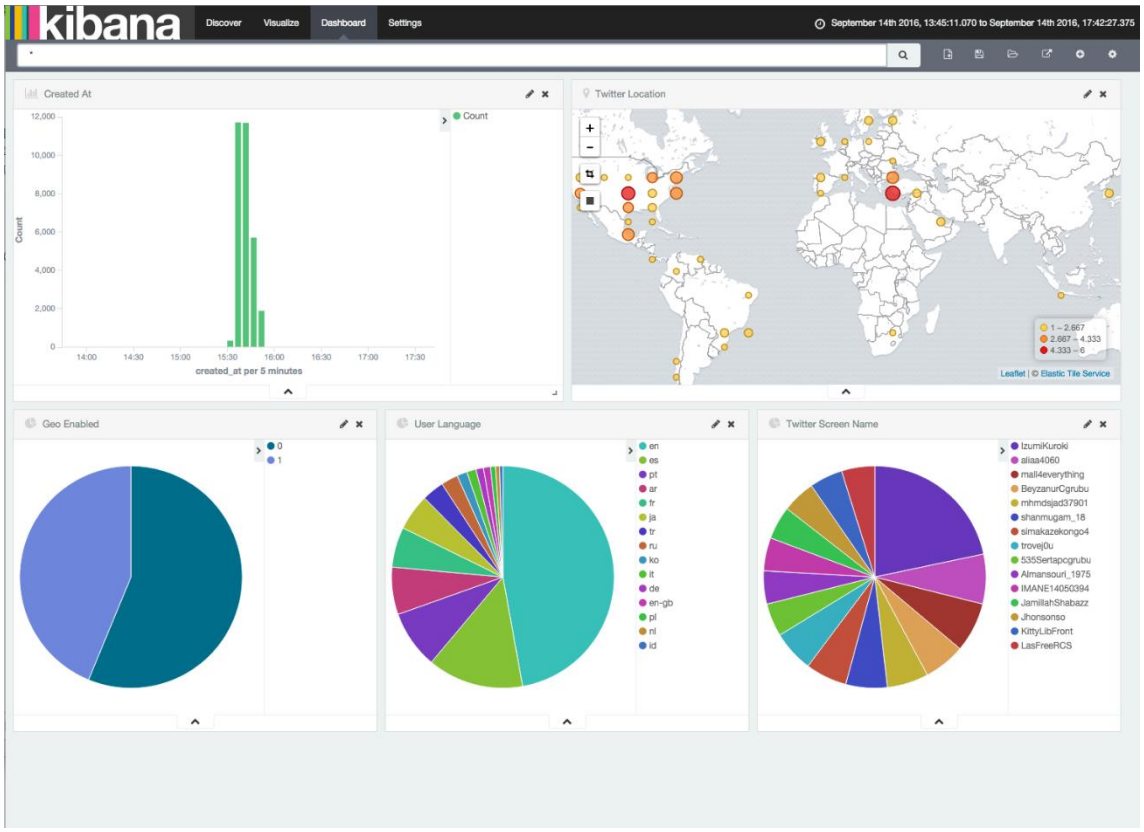


Ilustración 9: *Dashboard Kibana*

6. Ciclo de vida del desarrollo de software

6.1. Introducción

A medida que el número de líneas de código aumenta y se van añadiendo progresivamente nuevas librerías de terceros a nuestros programas se hace necesario definir qué fases seguirá el software incorporado.

No disponer de un repositorio de código fuente o de un entorno de pruebas (entre otros) acabará suponiendo un coste en tiempo y dinero mayor del que supone implementar esto desde un principio.

Para el desarrollo de nuestra Plataforma hemos ido adaptando soluciones y procedimientos con el fin de hacer un producto fácil de mantener y lo más robusto y seguro posible. Lo iremos viendo en los próximos apartados.

6.2. El repositorio de código fuente

Aunque en un principio tener un repositorio de código fuente puede parecer innecesario, a medida que el código empieza a tener cierto volumen se hace necesario disponer de un repositorio donde almacenar código.

Principalmente tener un repositorio de código fuente soluciona:

- **Concurrencia:** Varias personas pueden aportar al proyecto al mismo tiempo, facilitando la integración de código proveniente de diferentes programadores.
- **Trazabilidad:** Se pueden controlar todas las versiones que se han ido generando en el tiempo de cualquier componente. Útil para compararlas entre ellas e identificar errores.
- **Retornar a una versión anterior:** En caso de incidencia puede volverse fácilmente a una versión anterior que no contenga el error.
- **Seguridad:** Solamente los usuarios con acceso al repositorio pueden ver y modificar el código fuente, dejando en todo momento traza de los cambios.
- **Facilidad para incorporar nuevos desarrollos y desarrolladores:** Se facilita poder compartir código con nuevos desarrolladores que vayan a colaborar en el proyecto ni que sea puntualmente.
- **Inventario:** Se hará más fácil poder inventariar los diferentes componentes de software, sus versiones, las fecha en la que se introdujeron,...
- **Análisis estático de código fuente:** Utilizando un repositorio será más fácil realizar análisis de código utilizando por ejemplo herramientas de terceros como las que veremos más adelante.

- **Integración continua:** Para incorporar una solución de integración continua y mejorar así el proceso de deployment agilizando la publicación de nuevas versiones, se hace necesario tener un repositorio de código fuente.

Son estas entre otras las ventajas que ofrece disponer de un repositorio de código fuente. Por eso en nuestra Plataforma esta opción se contempló desde el primer momento.

En nuestro caso escogimos BitBucket (https:// bitbucket.org), un repositorio en la nube gratuito y escalable que permite utilizar el protocolo GIT o SVN.

6.3. El ciclo de vida del software (SDLC)

Es interesante definir desde un principio el ciclo de vida que seguirá el software. Esto supone el seguimiento de una serie de fases:

1. Análisis y requisitos
2. Desarrollo y tests
3. Deployment y tests de QA & Seguridad
4. Mantenimiento

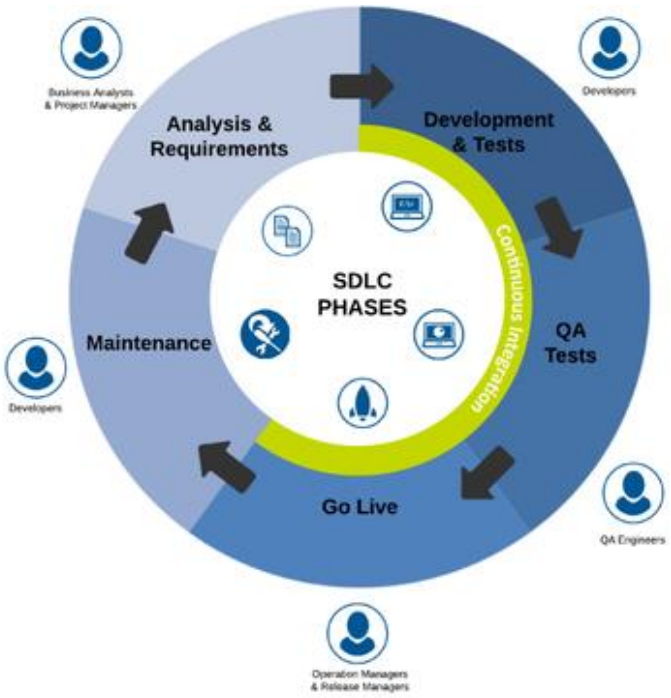


Ilustración 10: *Ciclo de vida del software (SDLC)*

<u>Análisis y requisitos</u>

Aunque pueda no haber equipo y todo el proceso recaiga sobre la misma persona es interesante ser disciplinado y seguir un procedimiento en el desarrollo. Todo empieza con el análisis y la toma de requisitos.

Esta primera fase, no siempre todo lo específica que se quisiera, es clave para el éxito del proyecto. A veces los desarrolladores caen en la tentación de comenzar a programar sin tener las especificaciones claras y esto acaba provocando la detección de errores en el desarrollo en una fase avanzada con la consecuente pérdida de tiempo y dinero.

Cuanto más desarrollado esté el análisis y menos margen se dé a la improvisación más probabilidades de éxito.

Desarrollo y tests

En nuestro caso hemos escogido la metodología TDD (test-driven development). El TDD es una práctica de programación que consiste en escribir primero las pruebas (generalmente unitarias), después escribir el código fuente para que pase la prueba satisfactoriamente y finalmente, refactorizar el código. Con esta práctica se garantiza un código más robusto, más seguro, más mantenible y una mayor rapidez en el desarrollo.

En la siguiente figura se puede ver un esquema del funcionamiento básico de TDD:

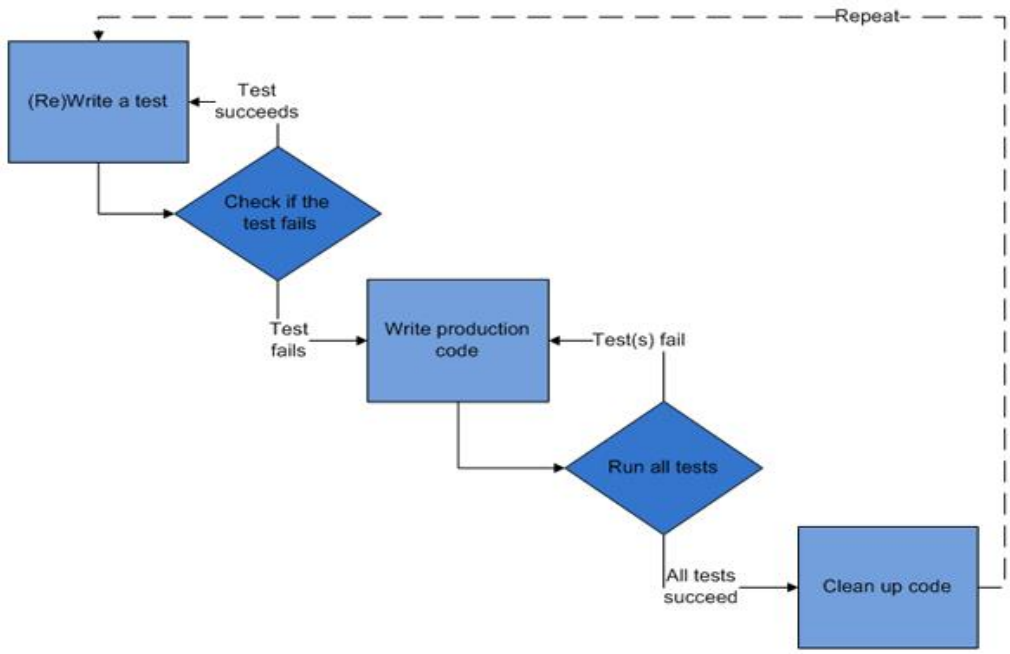


Ilustración 11: *Metodología TDD*

Tal y como se desprende de la figura, se comienza escribiendo el test conforme a las especificaciones y criterios de aceptación definidos. A partir del test, se va codificando hasta conseguir que éste pase. En consecuencia, si el test pasa es porque se ha cumplido con los requisitos de diseño y el código queda por tanto validado. Esta prueba se sumará al resto de pruebas unitarias formando progresivamente una "suite" (conjunto) de tests cada vez mayor, consiguiendo también que todo el código generado se vaya validando a medida que se codifica.

Todo nuestro código es Java y nuestro entorno de desarrollo Eclipse. Es recomendable apoyarse en *plugins* que ayuden al programador durante su codificación para evitar generar errores.

Deployment y tests de QA & Seguridad

El proceso de *deploy* es la fase por la cual se implanta en producción la solución desarrollada. No existe una única forma de implementar este proceso pero lo más común es seguir este camino:

Ilustración 12: *Entornos preproductivos y productivo*

La solución se desarrolla localmente por uno o varios programadores para posteriormente implementarla en un entorno de pruebas (QA) y finalmente en producción. Trabajar con un entorno local facilita al desarrollador su trabajo al poder hacer sus pruebas sin afectar al entorno real. Cuando el servicio que se ofrece en producción requiere de una estabilidad y su no disponibilidad es un problema, o hay varios desarrolladores programando simultaneamente, se hace necesario un entorno de QA. Este entorno tiene como objetivo ser en origen un clon del de producción al que se van añadiendo los cambios que se incorporarán en la próxima versión –release- y donde programadores y otros roles pueden probar la plataforma antes de publicarla en producción.

Este proceso es recomendable que esté automatizado. Es lo que se conoce como integración continua y permite al usuario ir incorporando sus modificaciones de manera progresiva mediante el uso de "*commits*" al repositorio. Un "*commit*" es un conjunto de cambios en el código que sube al repositorio de código fuente.

Vamos a explicar a continuación como se ha implementado todo el proceso de deployment en nuestra Plataforma, pero antes tenemos que conocer en qué consiste la metodología "*Gitflow*".

Gitflow es una metodología, exactamente un flujo de trabajo, ampliamente utilizado cuando se trabaja con repositorios Git. La idea es definir una serie de ramas de trabajo que ayuden al proceso de publicación de una nueva versión.

Veamos un esquema de ejemplo:

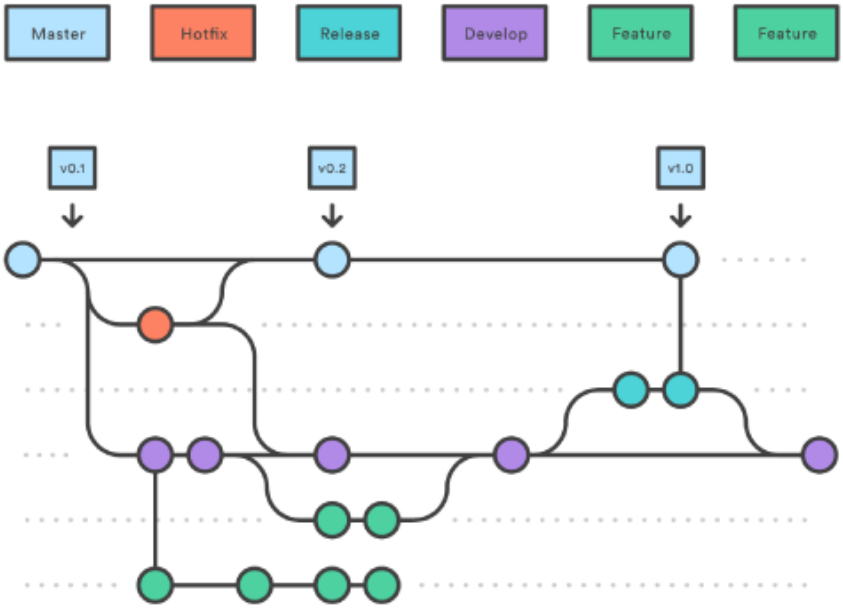


Ilustración 13: *Esquema ejemplo de Gitflow*

Analizaremos el ejemplo de arriba abajo y de izquierda a derecha:

- La primera línea horizontal con puntos azules corresponde a la rama de producción. Esta rama en git contendrá las versiones que hay en producción. Podemos ver cómo la primera versión es la v0.1 y va aumentando a medida que nos desplazamos a la derecha (en el tiempo).
- La segunda línea, con puntos naranja, es la rama de hotfix, donde residen los cambios de código necesarios para corregir un error –bug- crítico en producción.
- La siguiente línea, puntos turquesa, es la rama de *releases*. Esta rama es importante ya que contiene los cambios "*commits*" que serán utilizados para la futura versión en producción.
- La siguiente, con puntos violeta, es la rama de desarrollo. En esta rama se irán integrando los cambios que generen los programadores para la futura *release*.

- La última, con puntos verdes, corresponde a desarrollos específicos, tareas que han hecho los programadores (corrección de errores, nuevas funcionalidades,…) para próximas versiones.

Como se desprende de la imagen, las ramas de más arriba se alimentan de las inferiores.

Este sistema que a simple vista puede parecer abstracto, se corresponde con la realidad de la siguiente manera:

- El código de la rama de producción es el que hay en los servidores de producción.
- El código de la rama de desarrollo es el que habrá desplegado en los servidores de QA.
- El código de las ramas inferiores estará desplegado en el servidor local del desarrollador.

Esta relación entre ramas del repositorio y código desplegado en el servidor suele estar automatizado. En nuestro caso utilizamos Jenkins, que es el software encargado de lanzar los procesos necesarios para ejecutar los traspasos (la copia del código de una rama al servidor).

A continuación vamos a ver los pasos que seguiría la integración de un supuesto cambio desde que se detecta la necesidad hasta que está disponible en producción:

- **Paso 1:** Se detecta una necesidad que es trasladada al equipo de desarrollo que codifica la solución. Los programadores crean una nueva rama en el repositorio partiendo de la rama de desarrollo, que de no haber cambios en curso será idéntica a la de producción. Descargan el código en su máquina local y trabajan sobre esta nueva rama.
- **Paso 2:** El equipo de desarrollo da por finalizada la programación de la tarea. Ha lanzado los tests en local y estos han sido superados. Los cambios locales se sincronizan con el repositorio.
- **Paso 3:** El equipo de desarrollo integra los cambios de esta rama local en la rama de desarrollo.
- **Paso 4:** Se lanza la tarea Jenkins que básicamente copia el código de la rama de desarrollo (incorpora la nueva funcionalidad) al servidor de desarrollo.
- **Paso 5:** Se hacen las pruebas en el entorno de desarrollo para validar la solución.

- **Paso 6:** Se genera una nueva rama, correspondiente a la nueva *release*, partiendo de la de producción y se integra la nueva funcionalidad.
- **Paso 7:** Se integran los cambios de la *release* en la rama de producción.
- **Paso 8:** Se lanza la tarea en Jenkins que copia en los servidores de producción el código de la rama de producción.

Vamos a detenernos en el paso 4. Hemos visto que la principal función de Jenkins en este paso es copiar el código al servidor de desarrollo, pero vamos a incluir algunas funciones de seguridad. Independientemente de que a nivel local se hayan implementado *tests* unitarios y el programador pueda ayudarse de extensiones al entorno de desarrollo, el mejor momento para ejecutar *tests* es en el momento de traspaso al entorno de QA y producción.

Durante el proceso de traspaso hemos implementado las siguientes herramientas de análisis en nuestra Plataforma:

- **PMD:** Un analizador de código estático disponible para Java entre otros lenguajes. Buscará errores de programación como variables no utilizadas, excepciones no controladas,... El "exit status" del analizador, el código que devuelve tras la ejecución del análisis para nuestro código fuente, indicará si el código ha pasado los controles o no. (La herramienta está disponible en https://pmd.github.io/)
- **OWASP dependency-check:** Una utilidad que busca vulnerabilidades conocidas en las dependencias del proyecto. Está mantenido por OWASP y el objetivo es que el programador pueda ver fácilmente un árbol de dependencias afectadas por alguna vulnerabilidad. De esta manera se podrá actuar rápidamente y proceder a su actualización lo antes posible. (La herramienta está disponible en https://www.owasp.org/index.php/OWASP_Dependency_Check).

Ambas herramientas disponen de plugins en Jenkins por lo que son fácilmente integrables en el proceso de integración continua.

Controles de seguridad

Vamos a diferenciar entre dos tipos de controles de seguridad: los de aplicación y los de infraestructura.

Respecto a los de aplicación hemos visto que tenemos controles de seguridad durante el desarrollo y en el momento de traspaso, tanto a QA como a producción.

No obstante puede que nuestro código, y sobre todo nuestras dependencias, se vean afectados por vulnerabilidades una vez pasadas las fases de desarrollo y

traspaso. Por eso es importante tener una planificación de revisiones periódicas para mitigar riesgos.

En nuestra Plataforma hemos decidido que mensualmente se ejecutará para todos los proyectos la utilidad de OWASP dependency-check. Es una manera eficaz de evitar tener código vulnerable en producción durante demasiado tiempo y que este pueda ser explotado.

Respecto a los controles de infraestructura se ejecutará también con carácter mensual, el escáner de vulnerabilidades Qualys en su versión free (https://qualys.com). Qualys es un analizador de servidores, redes y aplicaciones que ayuda a detectar vulnerabilidades conocidas en este tipo de activos.

En nuestra Plataforma haremos un *scan* de todas las IPs que conforman nuestra infraestructura en busca de cualquier vulnerabilidad conocida.

Un ejemplo de informe que muestra esta herramienta para el *scan* de una de nuestras IPs:

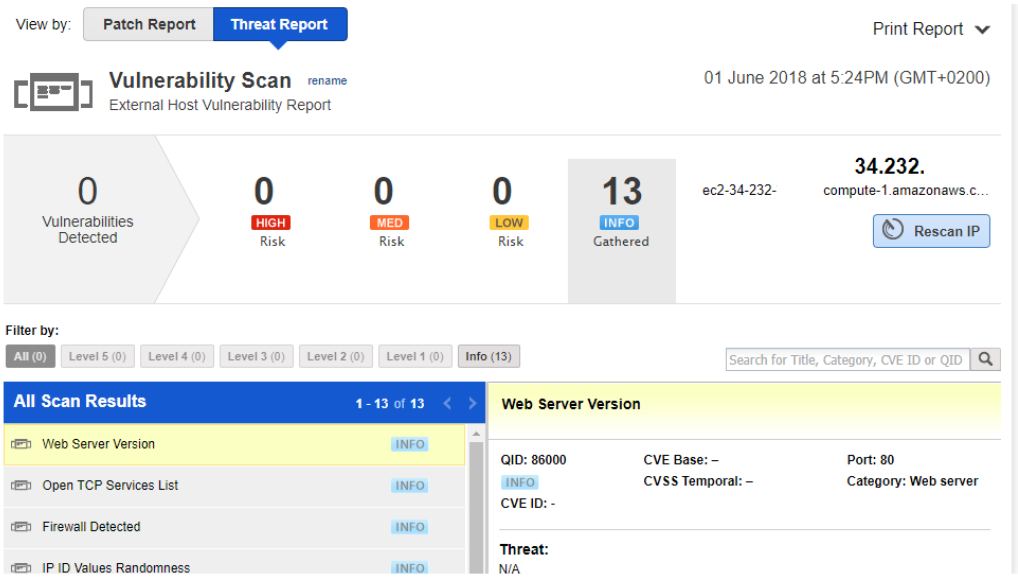


Ilustración 14: *Informe scan Qualys*

Tal y como se puede ver en la imagen, Qualys no ha detectado para este servidor ninguna vulnerabilidad importante, únicamente algunas consideraciones de carácter informativo a tener en cuenta.

Aparte del *scan* mensual con Qualys estamos suscritos a diferentes *feeds* con noticias sobre seguridad relacionadas con servidores de aplicaciones, sistema operativo, aplicaciones,... Lo importante es poder aplicar los parches de seguridad tan pronto como sea posible evitando así que otros desde fuera puedan aprovechar las vulnerabilidades.

7. Redacción de textos legales

7.1. Introducción

Cualquier empresa que publique un sitio web que represente una actividad económica en Internet está obligada legalmente según la Ley de servicios de la sociedad de la información y de comercio electrónico –LSSI– [13] y el Reglamento Europeo de Protección de Datos –GDPR– [14] a poner a disposición de los usuarios, de forma clara y visible, una serie de textos legales adaptados a la actividad que desarrolla su titular a través de la web, sus características y funcionalidades específicas.

Los textos legales requeridos y que en consecuencia contendrá nuestra Plataforma son:

- Aviso legal y condiciones de uso.
- Política de privacidad.
- Política de cookies.
- Condiciones generales de contratación.

En los próximos apartados desarrollaremos cada uno de estos textos.

Todos los textos legales deben poder encontrarse fácilmente en la web. En nuestro caso éstos estarán indicados y enlazados en el *footer* de la página principal. Además, y ya que determinados textos legales deben ser leídos y aceptados por los usuarios antes de prestar su consentimiento, éstos también aparecerán en aquellas partes de la web en las que sea requerido. Por ejemplo, citaremos y enlazaremos la política de privacidad antes del registro de un usuario en la Plataforma. De esta manera nos aseguramos que cualquier usuario registrado ha aceptado las condiciones del servicio.

Como veremos más adelante, incumplir las obligaciones legales puede acarrear al titular de la web importantes sanciones por los organismos reguladores, además de las posibles reclamaciones de los usuarios por incumplimiento y daños y perjuicios.

Especialmente altas son las sanciones en las que se puede incurrir por una vulneración de las previsiones en materia de protección de datos, las cuales, con la entrada en vigor del GDPR, pueden llegar a ser de hasta 20 millones de euros o de hasta un 4% del volumen global de facturación de la empresa. La mejor forma de evitarlas es cumplir con la normativa que básicamente supone:

- Tener identificadas las operaciones de tratamiento.
- Prever los riesgos.
- Tener una política de privacidad correcta.
- Aplicar las medidas de seguridad necesarias.

7.2. Aviso legal y condiciones de uso

Tanto el aviso legal como las condiciones de uso son obligatorios para cualquier página web cuyo titular se beneficie económicamente directa o indirectamente de ésta. Su regulación está prevista en el Artículo 10 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante LSSI) [13] . Citando la ley se obliga a los prestadores de servicios de la sociedad de la información (titulares de una web) a "*disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita.*"

El aviso legal contendrá los datos de identificación del titular responsable de la web y/o titular del dominio:

- Nombre o denominación social.
- Domicilio o razón social.
- Número de identificación fiscal.
- Datos de inscripción en el Registro Mercantil u otro registro público en el que por razón de la actividad se encuentre inscrito el titular de la web para la adquisición de personalidad jurídica.
- Dirección de correo electrónico u otro modo de contacto directo y efectivo.

Las condiciones de uso en cambio se podrían llegar a entender como un acuerdo entre partes, es decir entre usuario y titular de la web, advirtiendo al primero de los usos permitidos respecto de la información, contenidos y servicios disponibles en la web.

7.3. Política de privacidad

Cualquier web que contenga un formulario de registro para acceder a un área de clientes o para realizar transacciones electrónicas como ocurre en nuestra Plataforma, debe tener a disposición de los usuarios, de forma clara, visible y permanente, su política de privacidad para cumplir con lo dispuesto en el Reglamento Europeo de Protección de Datos (GDPR).

La política de privacidad debe ser aceptada de manera expresa por el usuario antes de cumplimentar cualquier formulario donde se recojan datos personales.

De acuerdo al artículo 4 GDPR se entiende como dato de carácter personal: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

El artículo 12 GDPR establece la obligación de informar de los derechos del interesado, debiendo realizarse dicha información de forma transparente, sencilla, inteligible, gratuita y que permita tener una visión de conjunto del tratamiento previsto.

Por lo que respecta al contenido de la política de privacidad, y que detallamos a continuación, se regula en los artículos 13 y 14 GDPR, así como el relativo a las actuaciones a las que tendrá derecho el interesado en los artículos 15 a 22 GDPR.

Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

- La identidad y los datos de contacto del responsable y, en su caso, de su representante.
- Los datos de contacto del delegado de protección de datos.
- Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
- Los intereses legítimos del responsable o de un tercero.
- Los destinatarios o las categorías de destinatarios de los datos personales.
- En su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional.

Además de la información mencionada anteriormente, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

- El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
- La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.
- La existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.
- El derecho a presentar una reclamación ante una autoridad de control.
- Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos.

- La existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22 GDPR, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Además de tener publicada la política de privacidad en los términos que hemos visto anteriormente, hay algunos artículos en la GDPR que obligan a los titulares a mantener un rol activo respecto a la protección de datos. Citamos dos que son muy significativos para entender este cambio de cultura:

24. Responsabilidad del responsable del tratamiento

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

25. Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Tal y como se desprende de estos artículos la seguridad en torno a los datos pasa a ser crítica. En el caso de nuestra Plataforma todo el servicio se encuentra alojado en la nube a través de AWS Amazon y utilizamos diferentes servicios que nos ofrece (EC2, S3, Lambda,...). Lo positivo de tener la infraestructura en Amazon es que todos sus servicios ya cumplen con los requisitos de la GPRD (https://aws.amazon.com/es/blogs/security/all-aws-services-gdpr-ready/). Esto no supone que se pueda delegar la gestión de la seguridad de los datos en Amazon, pero sí nos ayuda en su gestión.

7.4. Política de cookies

Una cookie es cualquier tipo de archivo o dispositivo que se descarga en el equipo terminal de un usuario (ordenador, smartphone o tablet) al acceder a una web, con la finalidad de almacenar datos que podrán ser actualizados y recuperados por el responsable de su instalación.

Nuestra Plataforma utiliza cookies para por ejemplo almacenar el idioma en el que el usuario visualizará la web o para mantener activa la sesión una vez ha hecho login.

La política de cookies se venía regulando en el artículo 22.2 de la LSSI:

> *"Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos…".*

No obstante, la recién llegada GDPR ha hecho en su artículo 30 una mención, que aun pequeña, ha provocado a muchos tener que actualizar la política de cookies:

> *"Las personas naturales pueden estar relacionadas con identificadores en línea […] como una dirección de protocolo de internet, identificadores de cookies y otros identificadores […]. Esto podría dejar rastros que, especialmente en combinación con identificadores únicos y otros datos recibidos por los servidores, pudiera servir para crear perfiles de las personas naturales e identificarlas."*

Ahora los cookies ya están dentro del ámbito de la GPDR y su tratamiento se complica al tener el usuario que dar su consentimiento explícito. Ya no sirve informar al usuario de estas y darlas por aceptadas por defecto, el usuario debe escoger entre si las acepta o no antes de que se haga cualquier tipo de tratamiento. Además, aunque el usuario las haya aceptado en el pasado, tendrá que existir la opción de poder retirar esta aceptación en cualquier momento.

En la política de cookies se informa detalladamente a los usuarios de la definición y función de las cookies, de las cookies utilizadas en la Plataforma, su duración y finalidad, el uso de los datos que las mismas recogen por terceros y las

instrucciones al usuario para configurar su instalación o deshabilitarlas a través de los diversos navegadores existentes.

El principal problema con la política de cookies es que siempre que haya un cambio en alguna de las cookies habrá que modificarla. Seguramente las utilizadas por la propia Plataforma no tengan que variar frecuentemente, o si lo hacen seremos conscientes. En cambio las cookies que son de terceros (por ejemplo Google Analytics, Facebook,…) va a ser más complicado de gestionar. Habrá que estar atentos a los cambios para introducirlos tan pronto se produzcan.

En nuestra plataforma, lo primero que ve el usuario al entrar a la web es un banner que enlaza con la política de cookies y privacidad obligándolo a escoger entre si acepta esta o no. Para nuestra Intranet el uso de cookies es necesario por lo que un usuario que decida no aceptar la política de cookies no podrá hacer uso de la Plataforma.

7.5. Condiciones generales de contratación

Todo negocio en Internet sustentado en una web que realice venta de productos o prestación de servicios online (como ocurre en nuestra Plataforma) deberá incluir entre sus textos legales las Condiciones Generales de Contratación.

Estas condiciones van a suponer el contrato entre el prestador y el consumidor, por lo que deben cumplir los requisitos establecidos para los contratos en el Código Civil, Código de Comercio, Ley de Consumidores y Usuarios, Ley de servicios de la sociedad de la información y del comercio electrónico y la regulación concreta del bien o servicio ofertado.

La Ley de Servicios de la sociedad de la información –LSSI-, en concreto en su artículo 27 y la Ley para la Defensa de Consumidores y Usuarios (Art. 8 y siguientes) obligan a facilitar, antes de la contratación, determinada información mínima sobre el proceso de contratación online:

1. Información clara y detallada de los precios, incluido los impuestos y los gastos de envío.
    1.1. Cualquier pago adicional al precio acordado debe ser informado de forma clara y comprensible, debiendo obtenerse además el consentimiento expreso del consumidor mediante la opción de inclusión. Se prevé que si la empresa dispone de dicha opción por defecto (es decir, que deba buscarse y rechazarse en lugar de verse con claridad y aceptarse expresamente), el consumidor tendrá derecho al reembolso de dicho pago.
    1.2. No podrán cobrarse cargos adicionales por el uso de medios de pago, si estos superan el coste soportado por el empresario por el uso de tales medios.
2. Descripción del proceso de compra.
3. Obligaciones del comprador y del vendedor.

4. Condiciones de compra: plazos, forma de entrega, pago.
5. Soluciones e información relativa al derecho de desistimiento en caso de que el producto o servicio resulte defectuoso.
6. Determinación contractual del plazo legal de garantía y condiciones del servicio post-venta.
7. Idioma o idiomas en los que puede celebrarse el contrato.

Posterior a la compra online el prestador tiene obligación de confirmar la efectividad de la compra mediante:

1. Correo electrónico confirmatorio en un plazo de 24 horas desde la compra.
2. Pantalla de confirmación de compra una vez que esta se haya hecho efectiva.

El eje fundamental sobre el que gira toda la regulación existente es la transparencia, claridad, sencillez… de toda la información prestada, siendo responsable el prestador de servicios del incumplimiento de todo lo expuesto, estableciéndose sanciones e infracciones a fin de proteger a los usuarios de los servicios prestados. El Código Civil, establece, a modo genérico, esa responsabilidad del Prestador de servicios en su artículo 1.288, relativo a la interpretación de los contratos: "*La interpretación de las cláusulas oscuras de un contrato no deberá favorecer a la parte que hubiere ocasionado la oscuridad.*"

Por todo esto es necesario tener redactadas unas condiciones de contratación específicas para la Plataforma y no utilizar plantillas o textos genéricos descargados de Internet. De esta manera evitaremos conflictos y reclamaciones por parte de los usuarios que pueden a llegar a sanciones económicas y peor aún, acabar con la reputación de la marca.

8. Conclusiones

Con este TFM se ha visto la dimensión real de toda la complejidad legal y técnica que supone crear una plataforma de captura de evidencias digitales.

Han sido dos los pilares sobre los que se sustenta el proyecto: el legal y el técnico.

Hemos visto aspectos legales en los capítulos 2 -Validez jurídica de los servicios de certificación ofrecidos por la Plataforma- y 7 –Redacción de textos legales-.

En el capítulo 2 hemos estudiado el reglamento eIDAS y la presentación de pruebas digitales en sede judicial. Es para nuestra Plataforma imprescindible que los informes que ésta genera tengan un alto valor probatorio. Hemos visto que nuestros certificados se considerarán documentos privados en sede judicial. Los certificados se emiten en formato PDF y están firmados digitalmente conforme las especificaciones del reglamento eIDAS, el cual establece un marco común en la Unión Europea para la identificación electrónica y los servicios de confianza para las transacciones digitales. El que nuestros certificados estén firmados digitalmente aporta grandes ventajas: se garantiza la autenticidad del documento, su integridad y el no repudio. Además, todos los certificados incorporan un sello de tiempo generado por un servidor de tiempo cualificado garantizando el momento exacto de captura de la evidencia.

Todo esto hace que sea difícil en sede judicial la impugnación de nuestros certificados, aportando tranquilidad y seguridad a quien se ayuda en nuestros servicios para capturar evidencias digitales.

En el capítulo 7 hemos visto los textos legales que obligatoriamente nuestra web debe facilitar a los usuarios. Especificar las condiciones de uso, de privacidad o la política de cookies dan al usuario un fuerte nivel de control sobre sus datos además de clarificar qué recibirá cada una de las dos partes, cliente y proveedor, en el uso de la Plataforma.

El capítulo 3 –Captura de evidencias digitales- y el 4 –Módulo de sellado electrónico y sello de tiempo- han sido los capítulos más técnicos.

En el capítulo 3 hemos explicado cómo se generan las evidencias para cada uno de los servicios (captura de sesión de navegación web, URL y fichero). Hemos diseñado la plataforma para que sea robusta y escalable. El objetivo es que el servicio tenga una alta disponibilidad y la Plataforma sea capaz de recuperarse automáticamente en caso de fallo. Además, para evitar tener que gestionar la infraestructura hemos optado por los servicios en la nube de AWS Amazon, los cuales facilitan enormemente su administración a la vez que cumplen con la normativa más estricta a lo que seguridad se refiere.

El capítulo 4 ha servido para explicar cómo la Plataforma realiza la firma de los documentos. Este proceso es crítico y por eso le hemos dedicado todo un capítulo. La firma en los certificados garantiza la autoría de los mismos lo cual ofrece seguridad jurídica. En este capítulo hemos tratado dos aspectos: las características técnicas que cumplen nuestras firmas y por otro lado cómo lo

hemos aislado del resto de la Plataforma. Aunque hemos visto que en caso de que el certificado utilizado para la firma digital se viera comprometido tenemos la opción de revocarlo, es mejor adelantarse e intentar blindar no solo el certificado sino todo el proceso.

Este capítulo fue uno de los más complejos. Existen diferentes tipos de firma, especificaciones, versiones,… y había que conseguir que la solución Java escogida pudiera implementar el tipo de firma que nuestra Plataforma necesita. Costó mucho tiempo el conseguir que un PDF generado por la Plataforma se viera en Acrobat Reader con el "check" verde en el panel de firma y con la característica LTV activa.

El capítulo 5 –Log de auditoría- nos muestra la importancia de registrar todos los eventos tanto a nivel de aplicación como de infraestructura para poder demostrar el buen funcionamiento de la Plataforma y el uso que hacen los usuarios de ésta.

Aquí de nuevo AWS de Amazon facilita esta tarea y a día de hoy todos los servicios de la Plataforma envían automáticamente sus logs al cloud. Destacar también que aunque el sistema de subida de logs a AWS estuviera caído temporalmente (algo que todavía no hemos vivido) en ningún caso se perderían, ya que tan pronto como el servicio se recuperara se enviarían todos los logs pendientes.

También en el capítulo 5 hemos visto el potencial del stack ELK y sobre todo de Kibana donde se pueden ver con facilidad todos los logs generados, hacer seguimientos, poner alertas,…

Finalmente el capítulo 6 –Ciclo de vida del desarrollo del software (SDLC)- ha servido para explicar el procedimiento de desarrollo y deploy de la Plataforma. También hemos visto la importancia de poner controles de seguridad para evitar tener vulnerabilidades tanto en la aplicación como en la infraestructura.

Queda mucho por hacer pero también hay mucho hecho. La idea inicial era sencilla: crear una Plataforma web que certifique el contenido de una página web, una sesión de navegación o un fichero.

La realidad es que son muchos los aspectos que se derivan de su implementación. Seguramente los técnicos se podían llegar a prever en parte, pero los jurídicos no por desconocimiento absoluto en la materia.

Lo importante es que en este momento del proyecto ya se puede decir que nuestra Plataforma cumple con los aspectos legales y técnicos y que el proyecto ha pasado a ser comercializable.

Ha supuesto mucho tiempo de desarrollo y mucho tiempo de lectura e investigación, pero ha valido la pena.

La planificación de tareas del TFM se ha visto alterada en más de una ocasión y es que los objetivos de este trabajo eran demasiado abiertos. He pasado en algún momento del convencimiento de avanzar en una línea a tener que descartarla por completo. Esto ha llevado tiempo y a tener que empezar de cero en más de una ocasión. La falta de experiencia en algunos temas ha supuesto

que se haya tenido que dedicar más tiempo del esperado a párrafos que en principio parecían carecer de dificultad.

Aunque son muchos otros, fuera del mundo de la seguridad, los aspectos que tendré que afrontar en el futuro para darle vida a la Plataforma, este TFM ha sido clave y necesario. Las aportaciones del tutor, Pau del Canto, han sido también muy concretas y acertadas, lo que me ha ayudado a retomar el camino correcto en más de una ocasión.

En el futuro próximo habrá que afrontar temas tan importantes como:

- Configuración de cloudflare para protección DDOS.
- Migrar la librería de generación y firma de PDFs de Itext a una solución totalmente opensource como PDFBox.
- Tener una solución para gestionar el ciclo de vida de los certificados.
- Ampliar la información que se registra en los logs y añadir nuevos.
- Generar alertas en Kibana para detectar lo antes posible errores.
- Herramienta tipo Nagios para la monitorización de los servidores.

Y un largo etcétera de tareas que vamos registrando a medida que surge la idea o la necesidad.

9. Glosario

eIDAS

Reglamento 910/2014 (eIDAS) relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (por lo tanto de aplicación en los Estados miembros y prestadores de servicios de confianza establecidos en la Unión Europea).

AWS

Amazon Web Services es un conjunto de servicios ofrecidos por Amazon.com que provee computación en la nube para usuarios particulares y empresas.

https://aws.amazon.com/

Docker

Software que realiza virtualización a nivel de sistema operativo, también conocido como *contenerización*.

https://www.docker.com/

VNC

Software libre basado en una estructura cliente-servidor que permite observar las acciones del ordenador servidor remotamente a través de un ordenador cliente.

OCSP

Protocolo utilizado en Internet para la obtención del estado de revocación de un certificado digital.

CRL (Certificate Revocation List)

Lista de certificados revocados por la autoridad certificadora (CA) que no deben ser en consecuencia utilizados.

CA (Certification Authority)

Entidad que emite certificados digitales.

TSA (Time Stampting Authority)

Entidad de confianza que emite sellos de tiempo

API (Application Programming Interface)

Especificación formal sobre como un módulo de software se comunica o interactúa con otro.

GIT & SVN

Sistemas de control de versiones opensource para el versionado de software.

Bug

Error o fallo en el software que desencadena un resultado no esperado.

OWASP

Proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

10. Bibliografía

[1] Ministerio del Interior del Gobierno de España, «Portal estadístico de criminalidad,» 2018. [En línea]. Available: https://estadisticasdecriminalidad.ses.mir.es.

[2] Parlamento Europeo y Consejo de la Unión Europea, «REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,» 2014. [En línea]. Available: https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf.

[3] Boletín Oficial del Estado, «Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil,» [En línea]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-2000-323.

[4] Departamento de informática de la Universidad de Salerno, «Forensically-Sound Methods to Collect Live Network Evidence,» 2013. [En línea]. Available: https://ieeexplore.ieee.org/document/6531784/.

[5] ETSI, «PDF Advanced Electronic Signature Profiles,» 2009. [En línea]. Available: http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf.

[6] International Organization for Standardization, «ISO 32000-1:2008,» 2008. [En línea]. Available: https://www.iso.org/standard/63534.html.

[7] ETSI, «ETSI TS 101 73,» 2013. [En línea]. Available: http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf.

[8] International Organization for Standardization, «ISO 32000-2:2017,» 2017. [En línea]. Available: https://www.iso.org/standard/63534.html.

[9] ETSI, «ETSI EN 319 142-1,» 2016. [En línea]. Available: http://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/en_31914202v010101p.pdf.

[10] AWS Amazon, «Conformidad de AWS,» [En línea]. Available: https://aws.amazon.com/es/compliance/. [Último acceso: 29 05 2018].

[11] PCI Security Standard Council, «PCI DSS Quick Reference Guide,» 2016. [En línea]. Available: https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf. [Último acceso: 29 5 2018].

[12] Apache, «Apache Lucene - Query Parser Syntax,» [En línea]. Available: https://lucene.apache.org/core/2_9_4/queryparsersyntax.html. [Último

acceso: 06 2018].

[13] Jefatura del Estado, «Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.,» [En línea]. Available: https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf.

[14] PARLAMENTO EUROPEO Y DEL CONSEJO, «REGLAMENTO (UE) 2016/679 GPRD,» 5 2016. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN.