UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

Autenticación segura con Mobile Connect en el sector no lucrativo

Trabajo Fin de Máster

presentado por: Torres Rodríguez, Matías

Director/a: Paniagua Díez, Fidel

Ciudad: Madrid
Fecha: 18/09/2018

Resumen

El objetivo del trabajo es desarrollar un portal de clientes con acceso más ágil y seguro usando la tecnología Mobile Connect para el sector no lucrativo donde los colaboradores necesitan intercambiar datos y documentos sensibles con frecuencia. A mayor dificultad en el proceso mayor es el número de colaboradores que dejan de ayudar a la organización.

La gran mayoría de las organizaciones usan la herramienta *Open Source SuiteCRM* para manejar su relación con los clientes. *SuiteCRM* usa autenticación mediante usuario y contraseña, donde accederán los empleados y desempeñarán tareas en base a sus privilegios.

La página web de la organización ficticia creada, contiene un área privada para clientes que es de desarrollo propio, donde los colaboradores pueden acceder, rectificar, cancelar y oponerse a facilitar sus datos personales como establece el nuevo Reglamento General de Protección de datos. Los colaboradores también podrán descargar sus certificados de donación correspondientes a las donaciones realizadas a la organización. Toda esta información se almacena en *SuiteCRM*. Ambas partes están integradas mediante una *API Rest* propia de *SuiteCRM*.

Partiendo de que nuestros objetivos serán desarrollar un proceso de autenticación fácil y seguro, que la solución cumpla con lo que dice el RGPD en cuanto a los datos personales, y que se puedan descargar los justificantes de donación de forma ágil y rápida, los resultados concuerdan con los objetivos previstos. Se ha obtenido un área privada con autenticación *Mobile Connect* de acceso más ágil y seguro y que cumple con el RGPD. Ahora tanto el acceso como el intercambio de información entre la organización y sus colaboradores se realiza de forma rápida y segura.

La conclusión es que se securiza y facilita el intercambio de datos personales en un sector vulnerable con recursos tecnológicos limitados. Esta tecnología ayudará a fidelizar los colaboradores.

Palabras Clave: autenticación, Mobile Connect, SuiteCRM, portal web, sector no lucrativo.

Abstract

The main target of the dissertation is to get a secure and agile customers area using authentication *Mobile Connect* technology for a non-profit sector. As more difficult is the process more customers will abort their contribution.

On the one hand, the foundation uses open source *SuiteCRM* authenticating with ID and password. Employees work on it in base of their roles.

On the other hand, foundation's website includes a self-developed customers area where they can access, modify, cancel or deny to enter new personal information. This personal information is kept in *SuiteCRM*. As well, customers can download certificates of donation of their payments done to the foundation. Both parts are integrated using an *API Rest* of *SuiteCRM*.

Our targets were an agile and secure authentication process paying attention to RGPD. Results are as expected obtaining a private area using *Mobile Connect* authentication. From now, personal information exchange between foundations and donors will be more secure and quick that it was.

As a conclusion, non-profit sector is now more secure counting that it is a technological poor sector. This technology will help to loyalty donors.

Keywords: authentication, Mobile Connect, SuiteCRM, Customers area, non-profit sector.

Índice

Índice de ilustraciones

Índice de tablas

1 Introducción

1.1 Motivación

La principal motivación que me lleva a desarrollar este trabajo es aplicar mayor seguridad y agilidad en el intercambio de información personal, aumentar la confianza dando cumplimiento al nuevo Reglamento General de Protección de Datos y, ayudar a que los colaboradores (clientes) mantengan su compromiso de colaboración durante un largo periodo de tiempo, todo esto aplicado al tercer sector o sector no lucrativo.

El sector no lucrativo es un sector situado entre el sector privado y el sector público, el cual incluye empresas de trabajo asociado, organizaciones no lucrativas o caritativas, fundaciones, mutualidades, cooperativas y sindicatos, donde la ayuda económica llega por parte del sector privado bien sean personas físicas o entidades jurídicas. Este tipo de organizaciones como cualquier otro tipo de organización de otro sector, cuenta con una estructura, una misión, unos objetivos y un presupuesto que le ayude a conseguirlos.

Debido a los numerosos casos de corrupción y desvío de fondos de entidades sin ánimo de lucro conocidos, pone en alerta a los colaboradores que necesitan saber que sus aportaciones llegan y se destinan a la causa que les conmueve. Este trabajo fin de máster les daría confianza ya que en todo momento los colaboradores podrán ver sus aportaciones online.

El hecho de mostrar agilidad en el acceso a información privada, transparencia y seguridad a los colaboradores de este tipo de entidades, ayuda a que estos sigan colaborando durante más tiempo, cosa que no ocurre cuando el acceso a información de la organización no es claro o el proceso de acceder a su información personal y obtener su justificante de donaciones es difícil.

1.2 Planteamiento del trabajo

Como solución a este problema de intercambio de datos personales y dando cumplimiento al Reglamento General de Protección de Datos, se ha desarrollado un portal web privado para los clientes de cualquier organización, dentro de una página web corporativa ficticia bajo un dominio protegido con un certificado de seguridad SSL[1]. Se puede entrar al portal

[1] **Certificado de seguridad SSL** (Secure Socket Layer): añade procesos criptográficos al intercambio de información entre equipos.

web usando un método de autenticación seguro como es *Mobile Connect* [2] donde podrán acceder, rectificar, cancelar y oponerse además de ejercer su derecho a limitar el tratamiento, derecho al olvido y a la portabilidad de sus datos personales como puede ser su NIF/CIF o números de cuenta bancaria, teléfono móvil y dirección postal, y donde tendrán disponibles los justificantes de sus donaciones que le certifican su colaboración de cara a la declaración de la renta de la agencia tributaria.

Toda la información del colaborador se almacena en la base de datos de la organización usando herramientas CRM[3] de software libre para reducir costes. Un porcentaje elevado de las organizaciones utilizan tanto *SugarCRM* como *SuiteCRM.*

1.3 Estructura del trabajo

El trabajo se ha estructurado desarrollando los siguientes capítulos:

Estado del arte: en este capítulo se describen la Ley de Protección de datos y nuevos conceptos introducidos en el nuevo Reglamento General de Protección de Datos, qué es la autenticación y qué métodos se conocen actualmente, los tipos de ataques que pueden afectar a estos métodos de autenticación y como la tecnología *Mobile Connect* desarrollada mitigaría estos ataques. También se describe qué es y en qué consiste la tecnología *Mobile Conn*ect y se habla de los sistemas CRM *Open Source*[4] que están actualmente disponibles y soluciones que aportan al sector no lucrativo.

Hipótesis de trabajo y objetivos concretos del desarrollo: este capítulo está dedicado a exponer cuál es el *objetivo general del trabajo desarrollado, un portal web con autenticación segura Mobile* Connect, y qué es lo que se pretende mejorar, demostrando que anteriormente no se trabajaba de forma segura y ágil, y como usando este nuevo desarrollo mejora la fluidez de comunicación con los colaboradores de las organizaciones, su confianza en cuanto a la protección de su información y aumenta su compromiso de colaboración.

Desarrollo de la arquitectura: aquí se divide el capítulo en tres partes, la primera donde se explica la configuración de *SuiteCRM Open Source* usada por casi el 80% de las organizaciones no lucrativas, la segunda parte donde se describe todo el desarrollo propio del portal web seguro con *Mobile Connect*, y por último la integración de ambas partes con

[2] Mobile Connect: tecnología de autenticación sin contraseña usando el número de móvil.
[3] CRM: Customer Relationship Management. Herramienta de gestión de clientes.
[4] Open Source: Software con licencia gratuita GLP

la *API Rest* que usan la mayoría de los sistemas CRM para comunicarse con otras aplicaciones.

Evaluación de la herramienta: en este capítulo se hace una evaluación de la herramienta entrevistando a diferentes tipos de usuarios según su perfil. Estos son un colaborador real de una organización, otro genérico que no colabora con entidades no lucrativas, un informático y un último perfil que no está en contacto diario con las tecnologías. Finalmente se obtiene toda esta información y se confirma como el nuevo desarrollo resuelve el problema inicial.

Conclusiones y trabajo futuro: aquí se describe cuales son las conclusiones obtenidas, cuál ha sido el alcance y como el portal web con *Mobile Connect* resulta relevante para mejorar la situación anterior de agilidad y confianza a la hora de tratar datos y certificados de donación personales. Se expone como trabajo de futuro añadir la biometría como un nuevo factor de autenticación junto a *Mobile Connect*.

2 Estado del arte.

2.1 Ley Orgánica de Protección de datos (LOPD) y Reglamento General de Protección de datos (RGPD)

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [LOPD] entra en vigor en el año 1999 y aprobada en el Real Decreto 1720/2007, de 21 de diciembre cuya entrada en vigor fue el 19 de abril de 2008.

La LOPD tiene como objetivo garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar en cuanto al tratamiento de datos personales.

La LOPD será de aplicación para la información de carácter personal almacenada en un soporte físico, susceptible de tratamiento.

Los siguientes principios de la protección de datos presentes en el Título II de la LOPD tienen que estar presentes en las fases de recogida, tratamiento y utilización o cesión de los datos de carácter personal:

- El consentimiento del titular de los datos (art. 6 de la LOPD): el titular de los datos decide cómo, cuándo y dónde se tratan sus datos o se ceden a terceros.
- La calidad de los datos (art. 4 de la LOPD): estos deberán ser adecuados y no excesivos según la finalidad para la que han sido recabados.
- La información al recabar los datos (art. 5 de la LOPD): el interesado deberá ser informado de modo expreso, preciso e inequívoco en la recogida de los datos.
- Los datos especialmente protegidos (art. 7 de la LOPD): datos referentes a religión, saludo, vida sexual, ideología será necesario prestar especial protección. Será necesario el consentimiento expreso y por escrito.
- Datos relativos a la salud (art. 8 de la LOPD): datos que hacen referencia a la salud del interesado.
- La seguridad de los datos (art. 9 de la LOPD): obliga al responsable y encargado del tratamiento a medidas tanto técnicas como organizativas con el fin de garantizar la seguridad de los datos personales.
- El deber de secreto (art. 10 de la LOPD): el responsable y encargado del tratamiento deberán mantener estos datos personales en secreto y bien guardados.
- La cesión o comunicación de datos (art. 11 de la LOPD): deberá ser consentida por el interesado y la cesión solo podrá hacerse para llevar a cabo los fines para los que han sido obtenidos.

- El acceso a los datos por terceros (art. 12 de la LOPD): dicho acceso deberá estar regulado en un contrato que cumpla con los requisitos establecidos en el artículo 12 de la LOPD.

La LOPD hace referencia a los derechos ARCO[5] que afectan a los interesados, estos son, Acceso, Rectificación, Cancelación y Oposición.

Con la entrada en vigor del nuevo reglamento general de protección de datos con el objetivo de homogeneizar la normativa europea sobre protección de datos. El RGPD entra en vigor el 24 de mayo de 2016 pero que sería aplicable a partir del 25 de mayo de 2018, dejando ese periodo de dos años para realizar una adaptación progresiva.

El RGPD, además de los derechos ARCO que menciona la LOPD, añade los siguientes derechos:

- Derecho a la portabilidad de los datos: se trataría de facilitar los datos a otro responsable del tratamiento y bajo petición del interesado en un formato claro y estructurado.
- Derecho al olvido: se trataría de la eliminación de los datos personales del interesado si éste lo solicita.

[5] ARCO: Acceso, Rectificar, Cancelar, Oponerse.

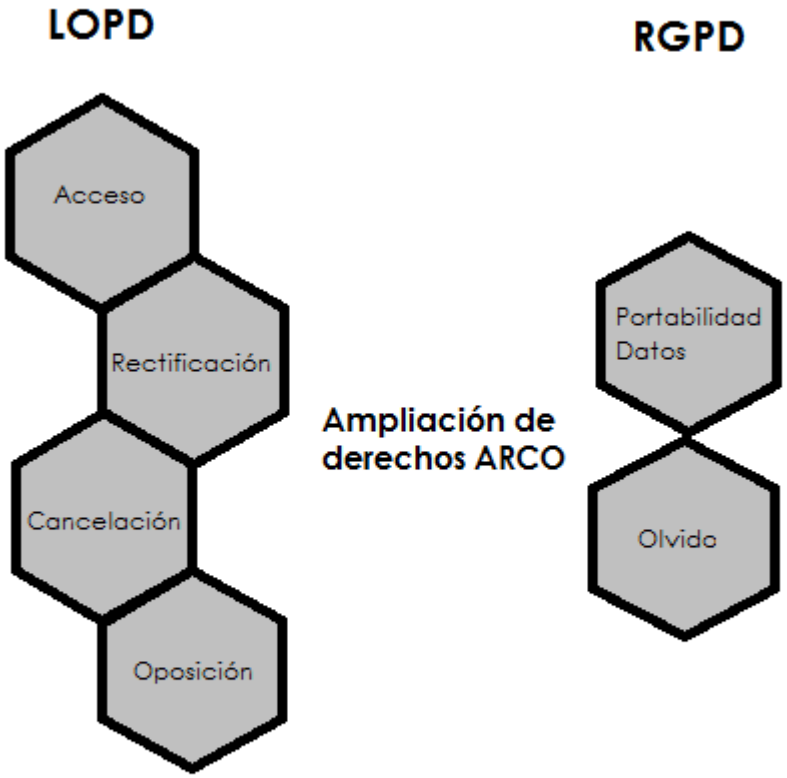

Ilustración 2.1 Derechos ARCO
Fuente. Elaboración propia.

En la siguiente tabla se hace una comparación de las obligaciones que imponen la LOPD y el RGPD:

LOPD	RGPD
Consentimiento tácito	Consentimiento inequívoco y explícito
Consentimiento del Padre/Madre/Tutor para el tratamiento de datos de menores de 14 años	Consentimiento del Padre/Madre/Tutor para el tratamiento de datos de menores de 13 años pero 16 años en los servicios ofrecidos en internet
Derechos ARCO	Derechos ARCO contemplando además el derecho al olvido o derecho de supresión y

	derecho a la portabilidad.
Necesario inscribir ficheros ante la Agencia Española de Protección de datos.	No es necesario inscribir ficheros.
No es necesario realizar evaluaciones de impacto cuando se tratan datos altamente sensibles	Será necesario realizar evaluaciones de impacto PIA para la gestión de riesgos para identificar y mitigar problemas de seguridad en la privacidad
Privacidad básica	Privacidad por diseño y por defecto desde la recogida hasta la cancelación
Multas hasta 600.000€	Aumentan las multas hasta los 100.000.000€
-	*Accountability*[6]: se deberán rendir cuentas ante las autoridades de control cuando se requiera
No existe la figura DPO	Se exige la existencia de la figura DPO responsable de los datos.

Tabla 2.1 RGPD frente a LOPD
Fuente. Elaboración propia

2.2 Simplicidad de los procesos digitales.

Después de estudios estadísticos realizados por agencias y organizaciones relacionadas con el comercio electrónico se ha llegado al resultado de que, solo el 3.3% de los colaboradores o usuarios que acceden a un proceso de compra o colaboración con una organización, finalizan de forma exitosa como se muestra en la **Ilustración 2.2 Porcentaje de conversión en un proceso de comercio electrónico.** "Chaffey, D. (2018, agosto). Smart insights: Ecommerce conversion rates - how do yours compare?. UK: Smart Insights. Recuperado de https://www.smartinsights.com/ecommerce/ecommerce-analytics/ecommerce-conversion-rates/."

El comercio electrónico es el canal más usado y rentable en términos de usuarios y operaciones que se realizan diariamente. Es de vital importancia que el primer acceso de un usuario a una plataforma sea sencillo y ágil, para evitar que la mayoría de los clientes finalicen el proceso con éxito. Será importante simplificar tanto la forma de recolectar los datos (primer acceso), como minimizar el número de pasos hasta llegar al objetivo de

[6] Accountability: rendición de cuentas a las autoridades.

terminar una compra, realizar una donación o para que el interesado acceda a sus datos personales para ejercer alguno de los derechos ARCO.

En este trabajo, lo que se intenta mejorar es que un colaborador que quiera modificar sus datos personales pueda hacerlos de la forma más sencilla y ágil posible para evitar que deje de colaborar, lo que supondría una pérdida importante para la organización que se sustenta nada más que de sus colaboradores.

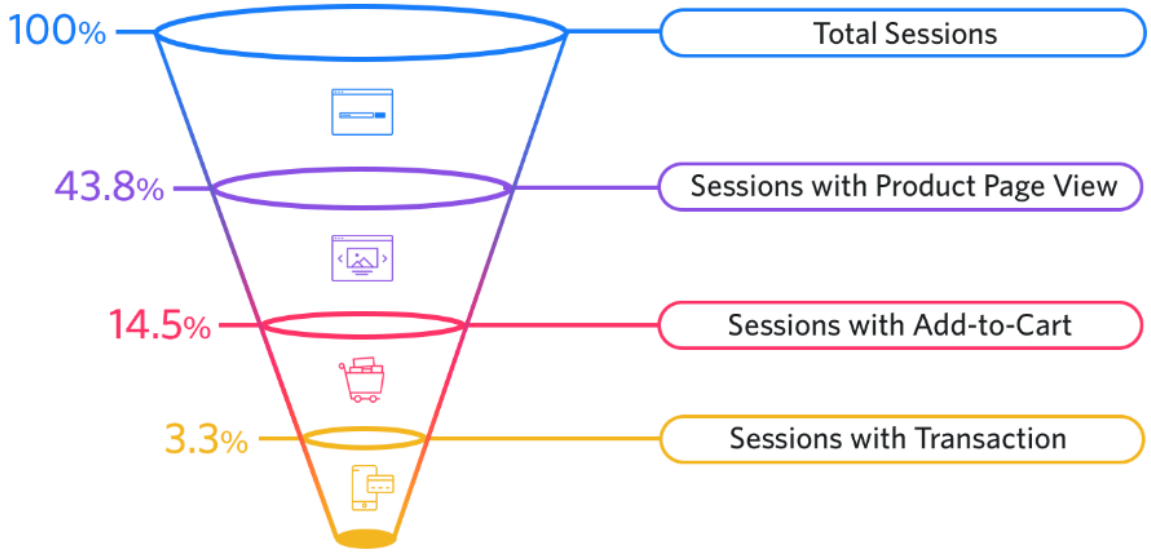

Ilustración 2.2 Porcentaje de conversión en un proceso de comercio electrónico
Fuente. https://www.smartinsights.com (2018)

2.3 ¿Qué es la autenticación?

*"La **autenticación** es el acto o proceso de confirmar que algo (o alguien) es quién dice ser.(Wikipedia, 2018)"*

Para llevar a cabo la autenticación se diferencian dos partes, la parte que va a identificarse (probador) cuya finalidad es acceder a ciertos recursos y la parte que se encarga de corroborar que el probador es quién dice ser (verificador/autenticador) y que tiene los permisos necesarios para obtener los recursos que desea obtener.

2.4 Tipos de autenticación

Hace un tiempo ya que se utilizan tres métodos diferentes de autenticación:

1. Sistemas basados en algo conocido; como puede ser una contraseña.

2. Sistemas basados en algo que poseemos; una tarjeta de coordenadas.
3. Sistemas basados en una características física; huella, reconocimiento de iris.

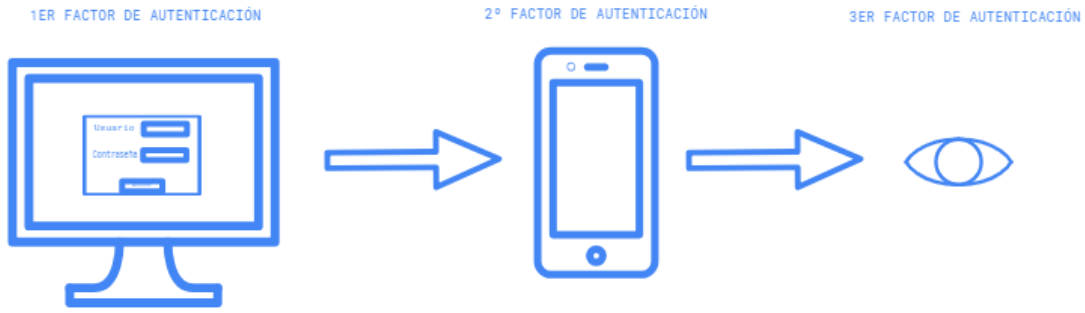

Ilustración 2.3 Factores de autenticación
Fuente. Elaboración propia

Actualmente, se utiliza la autenticación en dos pasos que engloba dos de los métodos anteriormente citados de forma conjunta, normalmente basados en algo que conocemos y algo que poseemos.

El primer factor, algo que conocemos, será un nombre de usuario, y el segundo algo que poseemos, como puede ser nuestro terminal móvil.

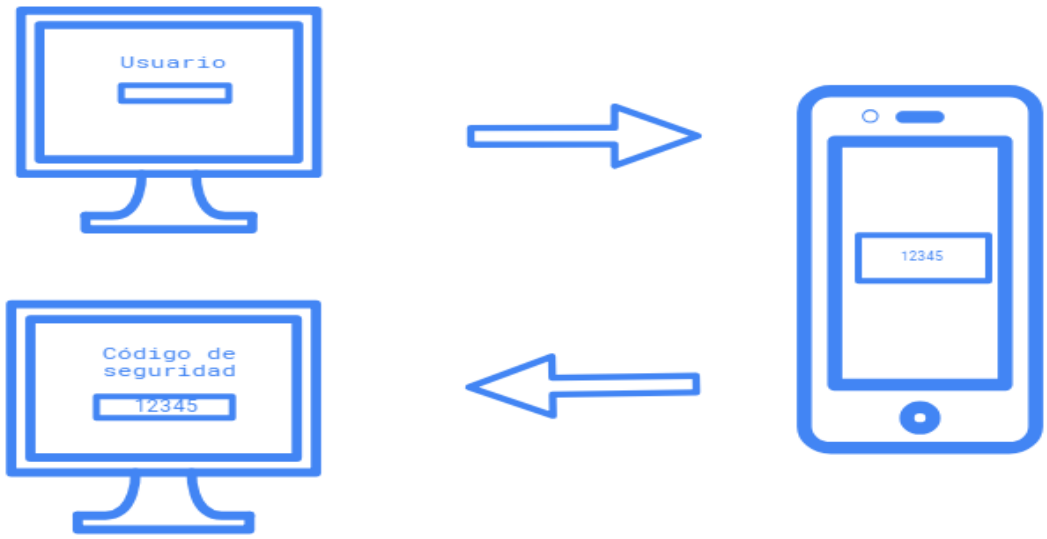

Ilustración 2.4 Autenticación en dos pasos
Fuente. Elaboración propia

La autenticación en dos pasos proporciona un extra de seguridad cuando se quiere acceder a una cuenta personal, ya que si alguien consiguiera capturar nuestro nombre de usuario

mediante un ataque de **phishing**[7] o **ingeniería social**[8], aún necesitaría poseer nuestro teléfono móvil para completar el acceso a nuestra cuenta de forma exitosa.

Existe un inconveniente en la autenticación en dos pasos usando nuestro terminal móvil, y es que si lo perdemos no podríamos acceder a nuestra cuenta. Para remediar esta situación, algunos servicios como Google ofrecen la posibilidad de vincular un dispositivo extra donde recibir el código que permite completar la autenticación de doble factor.

Por ejemplo, las administraciones públicas utilizan como método de autenticación los certificados digitales emitidos por la *Fábrica Nacional de Moneda y Timbre* (FNMT) que son únicos para cada ciudadano y que se obtienen de forma presencial en alguna de sus sedes. El certificado digital solo se debe instalar en un ordenador de uso personal. La forma de autenticación sería accediendo al sitio web de alguna de las administraciones públicas y posteriormente entrando en alguno de los servicios de carácter personal. Una vez aquí, el navegador realiza la petición del certificado digital instalado en el equipo completando así la autenticación.

El inconveniente de este método es que si alguien consigue acceder a nuestro ordenador, podría acceder a todos los servicios de las administraciones públicas en nuestro nombre.

2.5 Ataques conocidos contra la autenticación

Los fallos de autenticación que hasta hoy se conocen, son fallos cuyo riesgo es de nivel medio y cuya forma de mitigarlos normalmente no tiene un alto grado de dificultad. A continuación nombraré los tipos de ataque más relevantes.

2.5.1 Ingeniería social

Gran parte de los ataques se realizan utilizando este método. Consiste en obtener información de particulares o empleados de empresas que consciente o inconscientemente facilitan información para que terceros accedan al sistema de manera ilegítima.

[7] Phishing: técnica para conseguir información personal por medio del correo electrónico.
[8] Ingeniería social: técnica para conseguir información personal mediante conversación.

La mejor forma de mitigarlo es concienciar a las personas de que no deben facilitar información personal a otras personas que bien intentan obtenerla mediante encuestas telefónicas o porque existe una relación personal con el afectado.

Este tipo de ataque es uno de los que atentará contra nuestro sistema y uno de los cuales se quieren evitar desarrollando el portal web para colaboradores con acceso *Mobile Connect* donde no sea necesario usar una contraseña y se aplique un factor de autencación en dos pasos.

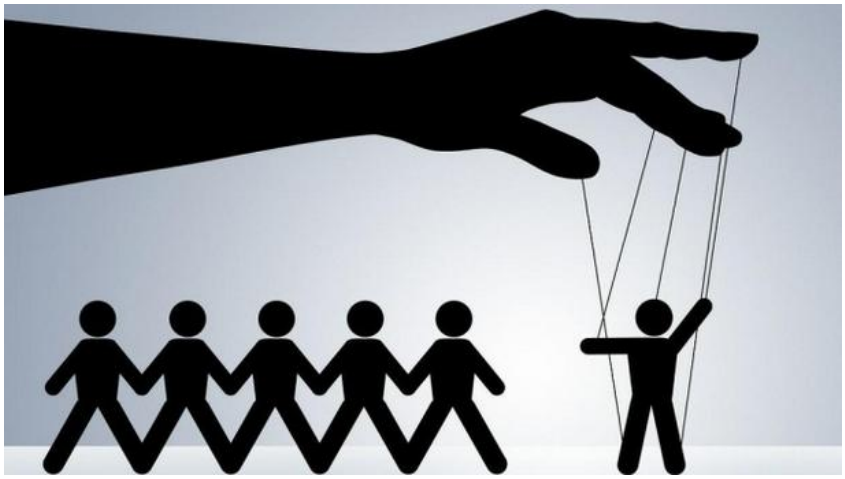

Ilustración 2.5 Representación de Ingeniería Social
Fuente. https://www.babel.es (2016)

2.5.2 La autenticación frente a la fuerza bruta

El ataque por fuerza bruta es uno de los ataques más usados a la hora de intentar obtener contraseñas o nombres de usuario de acceso a un servicio.
El problema ocurre cuando la aplicación a través de la cual se quiere acceder al servicio no es capaz de detectar estos ataques y aún menos aplicar alguna acción de seguridad para evitarlos.

Los ataques por fuerza bruta consisten en, mediante el uso de herramientas como *Hydra* y *Buspsuite* en *Kali Linux* junto con la herramienta *Metasploit* probar con las diferentes posibilidades que nos otorgue un diccionario para intentar adivinar independientemente el nombre de usuario o una contraseña válida para ese usuario, como se puede ver en el siguiente video. "Hernández, P. [El TubePaco]. (2017, julio 22). Fuerza bruta con Hydra desde Kali linux 2017 [Un informático bajo linux].[Archivo de video]. Recuperado de https://www.youtube.com/watch?v=lazHaBkAzZY"

Para mitigarlo se tiene que usar una contraseña con una longitud adecuada que haga que el tiempo para adivinarla mediante este método puede ser elevado, pero si no se aplica ninguna acción de seguridad como la introducción de retardos por cada intento fallido de por ejemplo un periodo de 15 segundos para volver a intentarlo. Otra medida es que tras el tercer intento se envíe al usuario/administrador un mensaje de advertencia.

En este trabajo, aunque se ofrece la posibilidad de acceder mediante usuario y contraseña, lo que se pretende es usar simplemente el método *Mobile Connect* cuando todos los operadores lo permitan y evite así la posibilidad de intentar este tipo de ataque.

2.5.3 Autenticación poco robusta

Uno de los problemas dentro de las empresas, aunque también a nivel particular, es la elección de una contraseña lo suficientemente larga y segura para que al ser atacada sea necesario emplear un largo periodo de tiempo para conseguir adivinarla. Actualmente se recomienda usar contraseñas que incorporen caracteres en mayúscula y minúscula, números y símbolos y de una longitud mínima de 10 caracteres.

A la hora de preparar un ataque contra un usuario, se suele recabar información personal y laborar (ingeniería social) con la intención de conseguir pistas que nos lleven a adivinar la contraseña o crear diccionarios pensados para la víctima.

Para mitigar este tipo de ataques es recomendable restablecer la contraseña cada cierto periodo de tiempo y a ser posible utilizar generadores de claves que nos faciliten contraseñas robustas y aleatorias en el caso de no acceder al portal web mediante *Mobile Connect* porque el proveedor de telefonía móvil no lo permita.

2.5.4 Utilización de métodos POST

Al contrario que los métodos GET, los métodos POST ocultan y cifran las variables que se envían al rellenar un formulario para que no se puedan ver en la dirección URL.

El método GET consiste en obtener información que está almacenada en un servidor (*request*) para ser entregada al cliente con un identificador (*response*). Este método es inseguro ya que los buscadores pueden indexarlos lo que permitiría a otros usuarios ingresar en esa URL y visualizar un servicio.

El método POST consiste en enviar información al servidor para que éste la almacene o actualice en la base de datos (*request*) y devuelva al cliente una redirección a por ejemplo un servicio (*response*).

Este trabajo tiene en cuenta este método POST para obtener los datos almacenados en la base de datos de *SuiteCRM* haciendo de la comunicación entre ambas partes, portal web y *SuiteCRM* más segura.

2.5.5 Intentar reducir los ataques de repetición

Un ataque de repetición consiste en reenviar al servidor las credenciales de autenticación que se habían enviado previamente con éxito.

Cuando se trata de una sesión persistente, el riesgo de que un atacante haga un reenvío de credenciales y obtenga una sesión exitosa es muy alto en comparación con el tipo de sesiones temporal. El acceso tanto temporal como persistente debe ser a un recurso protegido.

Como protección a este problema, sería conveniente proteger el envío de la contraseña en vez de en texto plano enviar su función *hash*[9].

Por otro lado y como decía anteriormente, evitar las sesiones persistentes con la protección de sus *login* persistentes es clave debido a que si la cookie de autenticación (almacena las credenciales permitiendo una autenticación ágil de una sesión a otra sin tener que volver a introducir los datos) es robada, el atacante tendría acceso ilegítimo a todos los recursos.

Mobile Connect usa una cadena de valores del tipo *65asda-5df5-9sd8-355d-a3d5dfs2d2* para asociar una sesión de cliente con el *ID Token*. Este valor no se modifica y se pasa desde la *Authorisation Request* hasta el *ID Token*, para evitar los ataque por repetición este valor será único cada sesión.

[9] Hash: función criptográfica usado para cifrar información privada.

2.5.6 Utilización de puertas traseras (Backdoors)

En muchas ocasiones los desarrolladores escriben trozos de código que permiten saltarse los métodos de autenticación y acceder al programa con el fin de realizar diferentes tareas que sean necesarias en fase de desarrollo. En ocasiones, estos trozos de código son olvidados o no de forma intencionada y esto deja la opción de acceder al programa a aquellos quienes lo conocen o a quienes lo descubran. Idealmente, una vez terminado el desarrollo del programa, estos trozos de código deberían ser eliminados.

Una vez un atacante se ha hecho con la máquina de la víctima, éste puede usarla para atacar a otras personas o empresas ocultando su identidad en máquinas ajenas y que parezca que son estas las que realizan el ataque. Está técnica se conoce como *Looping*.

Para realizar este ataque se hace uso de troyanos, programas desarrollados para saltarse la autenticación y la lógica de programa.

Se puede evitar usando antivirus con base de datos actualizada para una mayor seguridad.

Este ataque no afecta directamente a mi desarrollo pero lo he querido incluir para tener un abanico más amplio de conocimiento sobre ataques a la autenticación.

2.5.7 Ataques Man In The Middle (MitM) o de hombre en el medio

Este es un tipo de ataque por un individuo malintencionado que se realiza desviando o capturando los mensajes que se envían entre las partes implicadas en una comunicación.

Una posibilidad de ataque es que, en un intercambio de mensajes entre ambas partes de una comunicación con el fin de establecer la comunicación, se pregunta por la clave pública a una de las partes y esta es interceptada por el atacante. Son potencialmente peligrosas las redes públicas Wifi donde no existe una clave de acceso robusta.

Las técnicas que se pueden usar para prevenir estos ataques son:

- Usar el protocolo seguro HTTPS
- Hacer uso de la verificación en dos pasos
- Usar un canal seguro VPN

2.6 Los sistemas de autenticación actuales

Los sistemas de autenticación son cada día más sofisticados debido a que las técnicas empleadas para atacarlos han avanzado mucho en los últimos años.

La mayoría de las empresas ya están utilizando la autenticación en dos pasos como explicaba en el **apartado 2.4 Tipos de autenticación** , pero como no puede ser de otro forma habría que preguntarse, ¿es este método totalmente seguro?. No, no lo es.

Se han publicado casos como el de Telegram[10] en los que este sistema en dos pasos ha sido hackeado por un intruso en el que mediante la técnica de ingeniería social se hizo pasar por el propietario de la tarjeta SIM telefónica. Los atacantes consiguieron obtener un duplicado de la tarjeta donde recibirían la clave que les permitiría completar el segundo paso del método de autenticación de doble factor.

Aquí la tecnología *Mobile Connect* aporta un punto extra de seguridad porque, aunque depende de una tarjeta SIM que igualmente podría conseguirse un duplicado, dependiendo del nivel de seguridad (LoA) que se configure (1-4), el atacante aún necesitaría conocer el código de seguridad que se solicita como segundo paso.

Aún siguen quedando empresas y universidades entre otros que no utilizan acceso seguro a sus plataformas y que sus sistemas de autenticación simples se ven comprometidos por ataques de fuerza bruta.

Últimamente se han desarrollado métodos de autenticación más seguros como es el desarrollo del presente trabajo, *Mobile Connect*, donde el acceso se produce de forma muy ágil y segura.

Los métodos de autenticación en dos pasos necesitan:

1. Usuario:
    a. Debe ser recordado por nosotros: recordar un usuario es sencillo pero si tenemos un número de cuentas elevado hay dos opciones,
        i. Utilizar siempre el mismo nombre de usuario: el problema es que si nos averiguan este nombre de usuario podrían intentar acceder a todas las cuentas más fácilmente.
        ii. Cambiar de usuario para cada cuenta: esto favorece la seguridad, pero es difícil recordar los diferentes nombres de usuario que

[10] Ver: https://sbarrera.es/el-ataque-a-telegram

poseemos, aunque existen programas como *keepass*[11] que se usan cada vez más.

b. O bien que el propio dispositivo o navegador nos lo recuerde, lo cual lo hace más vulnerable ante la pérdida del dispositivo o si este es hackeado podrán obtener el fichero donde se almacenan los usuarios y contraseñas y hacerse con toda nuestra información de acceso.

2. Dispositivo: normalmente un teléfono móvil que,

a. Vulnerable a ser sustraído o extraviado.

b. O puede hackearse mediante duplicado de tarjeta SIM.

En tecnologías como las utilizadas en métodos de pago con teléfono móvil, se empiezan a usar además del primer y segundo factor de autenticación otro que se conoce como el tercer factor, la biometría.

Con la combinación de estos tres factores, aunque nuestro terminal sea robado no es posible realizar la autenticación satisfactoriamente al no poseer los datos biométricos del propietario.

Hay que hacer hincapié en que el eslabón más débil de la cadena es el factor humano y que la concienciación en aspectos de seguridad es uno de los puntos más importantes dentro de las organizaciones para paliar cualquier intento de ataque.

2.7 GSMA y la tecnología Mobile Connect

2.7.1 ¿Qué es la GSMA? ¿Quiénes la forman?

La propia página web de GSMA la define como:

"The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors.(GSMA, 2018)"

GSMA lleva más de 20 años ofreciendo servicios móviles alrededor de todo el mundo desde que comenzó ofreciendo simples llamadas móviles hasta hoy en día ofreciendo servicios de autenticación segura y ágil y servicios multimedia.

[11] Keepass: software utilizado para guardar credenciales de acceso a los sistemas

Algunos de los servicios móviles que se han usado y siguen haciéndolo en muchos países son:

- GSM (Global System for Mobile communications): es la tecnología usada para la transmisión tanto de voz como de datos móviles.
- GPRS (General Packet Radio Service): se trata de un amplio servicio de datos Wifi usado incluso por muchas redes GSM.
- EDGE (Enhanced Data rate for GSM Evolution): esta tecnología permite ofrecer hasta tres veces más demanda de servicios móviles que GPRS.
- WCDMA (Wideband Code Division Multiple Access): abarca un mayor ancho de banda espectral permitiendo así multiples accesos a la red. Está basada en estándares de tercera generación (3G) como son UMTS y TDMA o FDMA.
- HSPA (High Speed Packet Access): se trata de un conjunto de tecnologías que permiten a las operadoras de 3G aumentar la velocidad de sus redes para servicios de descarga o subida de datos en internet.
- LTE (Long Term Evolution): esta tecnología de red móvil proporciona velocidades en los servicios de hasta 100Mbps de descarga y 50Mbps de subida. Es compatible con las tecnologías GSM y HSPA y además incorpora tecnología MIMO (Multiple In Multiple Out). LTE soporta un espectro de ancho de banda de canal desde 1.4 MHz hasta 20MHz.

Las compañías telefónicas tienen un rol muy importante en el uso de *Mobile Connect*, y es que desde hace décadas las operadoras llevan ofreciendo servicios de telefonía móvil de forma segura como son las llamadas de voz, mensajes de texto, acceso a internet y todo esto permitiendo a los usuarios autenticarse para acceder a sus datos personales con una alta seguridad.

2.7.2 ¿Qué es la tecnología *Mobile Connect*?

La gran mayoría de la población actualmente trabaja o pasa gran parte del tiempo usando su teléfono móvil. *Mobile Connect* se trata de un novedoso método de autenticación segura mediante el teléfono móvil en el que no es necesario usar ni usuario ni contraseña para logarse ya sea en una página web como en una aplicación.

Mobile Connect está basado en *OpenID Connect/estándares OAuth2*.

OpenID Connect es una capa de identidad simple construida en la parte superior del estándar *OAuth2* y cuya función es proporcionar información al cliente sobre la identidad del usuario y verificarla mediante un servidor de autenticación. También es capaz de obtener información básica del perfil de usuario.

OAuth2 tiene la función de definir cómo se van a obtener y cómo se van a usar los tokens de acceso a recursos protegidos.

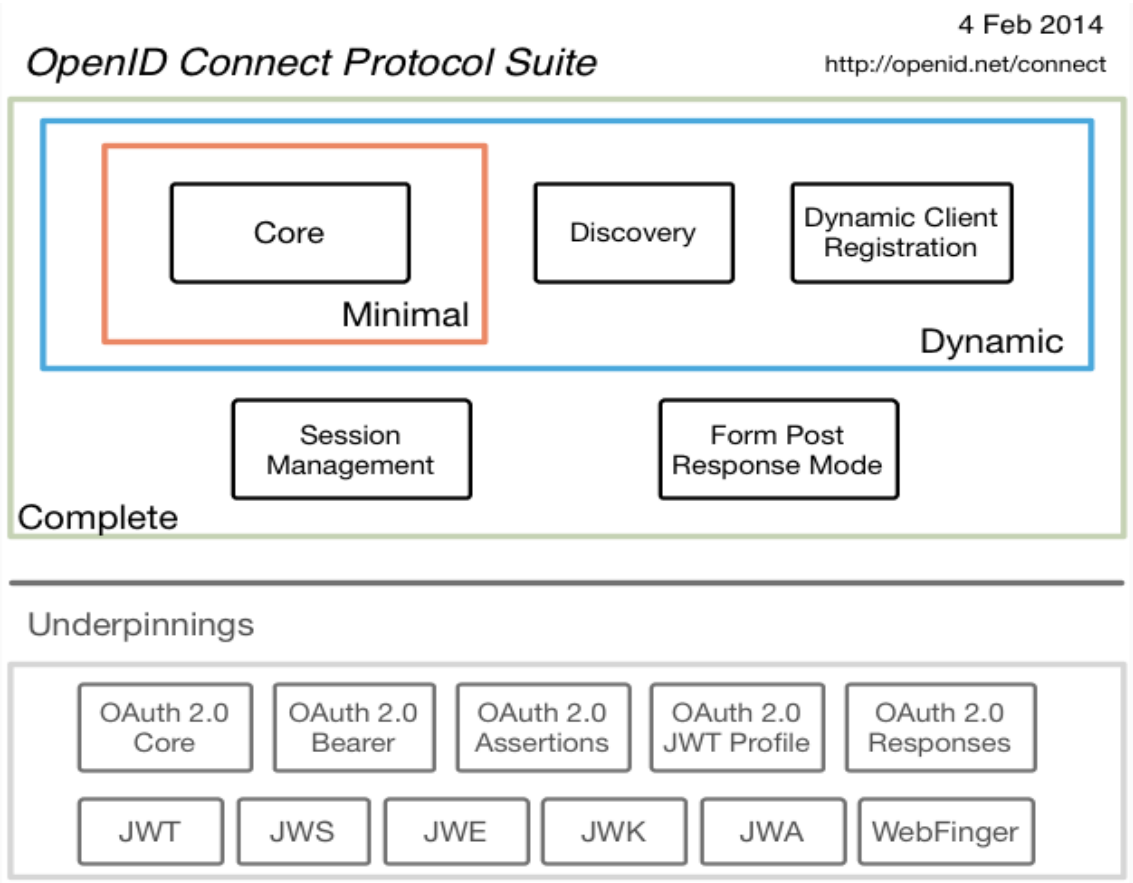

Ilustración 2.6 Suite de protocolos Openid Connect
Fuente. openid.net (2014)

Este servicio lo proporcionan los operadores de redes móviles de forma independiente, es por esto que a día de hoy existen pocos operadores en el sector que ofrezcan logarse con este método.

Uno de los problemas es que debido a la gran cantidad de sitios web donde estamos registrados y en los que se necesita introducir un usuario y contraseña, se hace cada vez más tedioso tener que recordar toda esa cantidad de información y si, por el contrario, utilizamos siempre la misma corremos el riesgo de que sea descubierta y un atacante pueda tener acceso a todos nuestros servicios.

Con esta novedosa tecnología se podría decir adiós a la opción de recuperación de contraseña por olvido que abría otra posibilidad de ataque para un usuario malintencionado.

2.7.3 ¿Quién y dónde se puede utilizar *Mobile Connect*?

Esta solución está pensada para aplicarse en todo tipo de servicios web a diferentes niveles ya sea accediendo a una simple página web en la que no sería necesaria una seguridad de alto nivel y se haría log-in con un simple clic, o bien accediendo a lo que se considerarían sitios de alto nivel como por ejemplo a servicios bancarios, sistemas empresariales o entidades públicas.

Su objetivo es llegar a todos los ámbitos donde se necesite acceder a un servicio mediante autenticación y que sea accesible para todos los públicos y usuarios. Además, a día de hoy no es posible utilizar esta tecnología con todos los operadores de telefonía ya que solo algunos la tienen implementada, estando disponible para Orange y Vodafone entre otras pocas.

2.7.4 ¿En qué consiste *Mobile Connect*?

Dependiendo del nivel de seguridad que se necesite se utilizarán unas medidas de seguridad u otras.

Mobile Connect utiliza dos APIs principalmente:

- *API de descubrimiento*: esta API ha sido desarrollada por la plataforma GSMA API Exchange. Su función es como su propio nombre indica descubrir por parte de la plataforma cuál es la red móvil que se usa para la petición de conexión y si la tecnología Mobile Connect estaría disponible para usarse para esa red.

- *API Mobile Connect*: en mi caso lo voy a implementar para el operador de redes móviles Orange. Orange desarrolló su propia API *aka Authentication API* lo que permite a los usuarios autenticarse usando su propia cuenta de usuario Mobile Connect.

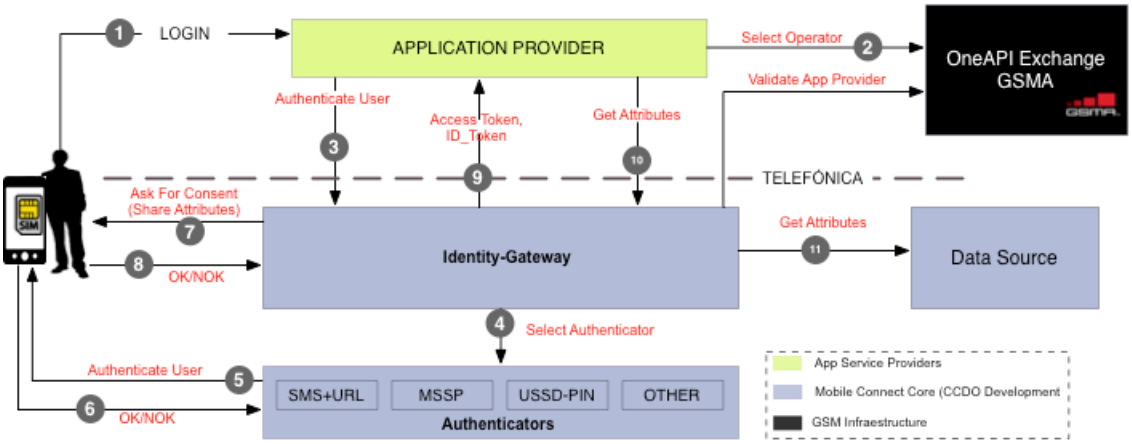

Ilustración 2.7 Conexión Mobile Connect
Fuente. https://blog.elevenpaths.com (2015)

2.7.5 Ataques contra la autenticación y como mitigarlos con Mobile Connect

En el apartado **2.5 Ataques conocidos contra la autenticación**nombraba los diferentes tipos de ataques a la autenticación. En este apartado vamos a describir en una tabla resumen cómo mitigar esos ataques usando la tecnología *Mobile Connect* o en su defecto, cómo minimizar los daños que se puedan ocasionar.

ATAQUES	MITIGACIÓN CON MOBILE CONNECT
Ingeniería social	Si un atacante intenta acceder a un servicio usando nuestro número de teléfono móvil, necesitaría nuestro terminal para confirmar el segundo factor de autenticación, sin éste no podrá acceder.
Suplantación de identidad	Usando doble factor de autenticación, desde pulsando un botón de aceptación hasta introducir un código secreto, cuando un atacante trata de acceder con nuestro número de móvil, no lo puede conseguir ya que necesita disponer de nuestro terminal móvil.
Fuerza bruta	La contraseña es el propio número de teléfono móvil, no será efectivo cualquier intento de ataque por fuerza bruta o diccionario.

Ataque de repetición	*Mobile Connect* evita este tipo de ataque ya que usa un código único de autorización en la petición de la conexión vinculado al ID token [12]de cliente.

Tabla 2.2 Ataques y mitigación con Mobile Connect
Fuente. Elaboración propia

2.7.6 ¿Qué es Level of Assurance (LoA)?

Level of Assurance (LoA), es el nivel de seguridad proporcionado durante el proceso de autenticación. Este nivel de seguridad está definido en el estándar ISO/IEC 29115.

Existen cuatro niveles de confidencialidad que van desde LoA1 hasta LoA4. El más sencillo se empleará en situaciones en las que la seguridad necesaria en el proceso de autenticación no sea alta porque los datos que se van a tratar no sean muy sensibles. En el caso del nivel 4, se utilizará para acceder a aplicaciones bancarias o portales en los que los datos sean muy sensibles, en cuyo caso se requerirá además del número de teléfono un número PIN de 4 dígitos.

El grado de confidencialidad se define cuando se realiza la petición de autenticación con la *API Mobile Connect* y esta devuelve la identidad. El parámetro encargado de asignar el grado de confidencialidad es ***acr_values***.

A continuación se indican los métodos de autenticación soportados por *API Mobile Connect*:

- SMS OTP: se realiza una autenticación mediante un código que se envía desde el terminal móvil desde donde se realiza la consulta el cuál será validado por el equipo de autenticación. El nivel de seguridad es LoA2.

- OK: se realiza una autenticación mediante un desafío que se envía al terminal móvil y que este se valida haciendo click en OK. El nivel de seguridad es LoA2.

- SIM_PIN: se realiza una autenticación mediante un desafío que se envía al terminal móvil que se valida proporcionando un PIN de 4 dígitos. El nivel de seguridad es LoA3.

[12] ID Token: número único aleatorio que identifica a un usuario.

2.7.7 ¿Qué son los autenticadores?

Los autenticadores son los encargados de permitir el uso de la infraestructura de red móvil para autenticar un usuario. El operador de telefonía móvil deberá implementar al menos un tipo de autenticador por cada nivel de seguridad (LoA) lo que le permitirá confirmar que el usuario que está haciendo la petición es quién dice ser.

2.7.7.1 Ventajas y desventajas de códigos basados en SMS

- Ventajas:
  - Los códigos basados en SMS son un método fácil y cómodo de usar.
  - La autenticación SMS en los sistemas de autenticación en dos pasos 2FA[13] pueden avisarnos si nosotros no lo estamos haciendo de que alguien está intentando acceder en nuestro nombre.
- Desventajas:
  - Un atacante puede obtener una copia de nuestra tarjeta SIM de nuestra operadora mediante ingeniería social, quedando bloqueado nuestro teléfono y activado el suyo.

2.7.7.2 Ventajas y desventajas de códigos basados de aplicaciones autenticador

- Ventajas:
  - Los códigos dependen estrictamente de la aplicación y no de la tarjeta SIM por lo que si un atacante consiguiera una SIM en nuestro nombre no podría conseguir autenticarse.
  - Estas aplicaciones pueden trabajar incluso en zonas sin cobertura de red móvil.

- Desventajas:
  - El código 2FA se genera mediante la combinación de una semilla y un secreto compartido entre la aplicación y el servidor que ambos necesitan almacenar. Si un atacante es capaz de romper tanto la aplicación como el

[13] 2FA: Two Factor Authentication

servidor, estos se verán comprometidos y el atacante obtendrá el secreto que le permitirá obtener códigos indefinidamente.

- Si alguien se hace con nuestro terminal podría acceder ya que ambos factores de autenticación se llevan a cabo en el mismo.

2.8 ¿Qué son las herramientas CRM Open Source?

Las herramientas CRM tienen como principal funcionalidad atender a los clientes de una empresa, tratar con ellos de una forma cercana para que se establezca una relación de confianza mutua y de esta forma confíe en la empresa, o dicho con otras palabras, **fidelizar al cliente**.

En el caso del tercer sector, lo que cualquier organización intenta conseguir es que sus colaboradores, bien sean puntuales o recurrentes, sientan que se conoce todo sobre ellos, lo que les gusta y lo que no para así poder ofrecer la mejor atención y permanezcan durante mucho tiempo colaborando.

En las herramientas CRM se pueden registrar datos de cómo los usuarios navegan por la página *web de la organización* para conocer sus preferencias, hábitos, su ámbito laboral, etc.

En definitiva, es posible, aún teniendo cientos de miles de clientes, gracias a las *TICs*[14], acumular gran cantidad de datos de los clientes y construir bases de datos con información sobre los mismos, que permitan tratar a los clientes de forma personalizada y establecer una relación con él, de forma similar a como lo hace un tendero de barrio, básicamente, consiste en una orientación de la organización hacia propiciar relaciones estables con el colaborador, cuestión que se puede conseguir analizando toda la información disponible sobre los colaboradores que llegan a la organización por diferentes canales de relación con éstos para, mediante dicho análisis, poder extraer conclusiones que permitan servirlos mejor.

2.9 Ventajas e inconvenientes de los sistemas CRM Open Source

Los sistemas CRM pueden proporcionar múltiples ventajas a las organizaciones que los utilizan. Entre las ventajas que nos ofrece un sistema CRM, es posible destacar las que se mencionan a continuación:

[14] TICs: Tecnologías de la información y la comunicación

- **Reducción del ciclo de gestión**: Los sistemas CRM permiten disminuir de forma considerable el tiempo utilizado en la atención a los colaboradores debido a que contamos con toda la información al instante sobre las donaciones realizadas y los eventos en los que ha participado o donde nos ha conocido.
- **Aumento de la información sobre los colaboradores**. Los sistemas CRM permiten disponer al instante de toda la información de los colaboradores y esta información puede ser utilizada para tomar decisiones respecto a las relaciones que se establecen con él (ofertas de productos personalizados de la organización, aumentos de cuota de colaboración, *mailing*, regalos directos por fidelidad, etc.).
- **Aumento de la coordinación en la organización (trabajar como un único equipo)**. Utilizar una filosofía CRM, conduce a un aumento del grado de coordinación de la organización. Esto permite que los cargos directivos de la organización puedan ver como se llevan a cabo las actividades de sus áreas de responsabilidad pudiendo visualizar éstas de forma individual o en grupo en general. También sería posible que cada trabajador tenga la posibilidad de ver los resultados de sus compañeros en cuanto a distintas métricas establecidas, como, por ejemplo, el trato a los clientes, las quejas o peticiones atendidas, etc. De este modo, se conocen de forma inmediata el desempeño de cada miembro del equipo, con el objeto de proporcionar un mejor servicio para obtener una mayor satisfacción de los colaboradores.
- **Enfoque en segmentos determinados de colaboradores**. Haciendo uso de los datos recogidos por la organización, se pueden dividir éstos según diferentes criterios, estableciendo segmentos diferenciados de colaboradores sobre los que será posible llevar a cabo campañas específicas diseñadas para cada uno de los segmentos, aumentando así la probabilidad de éxito de estas campañas.
- **Mayor seguimiento de los objetivos de negocio.** En ausencia de una herramienta de información como los sistemas CRM, se hace complicado controlar los procesos que la organización lleva a cabo sobre los colaboradores y, aún más, saber si se están cumpliendo los objetivos inicialmente previstos. Si disponemos de un sistema CRM, podremos saber en cada momento si vamos cumpliendo los objetivos ya que dispondremos de información totalmente actualizada.
- **Coste del sistema CRM**. Quizás la principal ventaja de estos sistemas CRM es que no llevan asociado un coste que, de no ser *Open Source* puede ser elevado para una pequeña o mediana empresa.

En cuanto a las desventajas, realmente éstas son escasas y a continuación se describen algunas de ellas:

- **La tecnología, por sí sola no es efectiva.** En este sentido hay que resaltar que no sólo la tecnología puede proporcionar el éxito de la orientación hacia el colaborador, sino que, además de la tecnología, es necesario utilizar otros activos tangibles e intangibles de la organización, como contar con los recursos humanos necesarios.
- **Personal especializado.** La puesta en operación de un sistema CRM necesita de personal especializado que desarrolle, implante y ponga en operación el sistema, alineándolo con las necesidades reales de la organización.

2.10 Productos Open Source

La idea básica de *Open Source* es la de facilitar el acceso al código de la aplicación para que los desarrolladores puedan leer, redistribuir y modificar el código fuente, ayudando así al desarrollo y evolución de las aplicaciones que se acogen a este sistema. Entre los CRMs alojados en servidores corporativos que se acogen al sistema *Open Source*, destacamos los siguientes.

2.10.1 Vtiger

Vtiger es una empresa que fue fundada en el año 2004 y que dispone de sedes en Sunnyvale, California (EE.UU.), y Bangalore en India. Se trata de una empresa que desarrolla, distribuye y ofrece consultoría sobre su popular *software* de CRM que es utilizado por cientos de miles de organizaciones en todo el mundo, y que cuenta, por ejemplo, con clientes como Nokia.

Su producto, *Vtiger CRM* se trata de una solución personalizable y muy accesible para las pequeñas y medianas empresas, además de ser muy fácil de usar. Dispone de una comunidad activa de usuarios y desarrolladores que hacen posible que éste *software* esté disponible en numerosos idiomas.

La instalación del *software Vtiger CRM* es muy sencilla ya que todo el *software* necesario, como Apache, MySQL y PHP está integrado y son ejecutables, y están disponibles tanto para *Windows*, como para distintas versiones de Linux (*RedHat, Debian, Suse, Fedora, Mandrake*). Para su implantación y uso no se necesita conocimientos avanzados acerca de la configuración de base de datos, servidor *web* y otro *software*.

Nombre de la eGmpresa	•Vtiger •www.vtiger.com
Nombre del producto	• Vtiger CRM
Módulos	• **Gestión de Ventas** • Gestión de cuentas y contactos •**Gestión de Marketing** • Gestión de campañas y envio de correo electrónico •**Gestión de la comunicación** • Gestión del conocimiento •**Gestión del trabajo en grupo** • Calendario
Puntos en los que destaca	•Comunidad de usuarios muy activa

Tabla 2.3 Característica de Vtiger CRM
Fuente. Elaboración propia

2.10.2 SugarCRM

SugarCRM Inc. fue fundada en 2004. Tiene su sede central en Cupertino, California (EE. UU.), con sede central europea en Munich (Alemania) y sede para Asia-Pacífico en Sydney (Australia). SugarCRM Inc., está formada por más de 250 trabajadores.

Al tratarse de un producto *Open Source*, es fácil de personalizar para satisfacer las necesidades que pueden surgir en una organización. También es asequible y fácil de usar y ofrece a las organizaciones una visión muy amplia sobre sus clientes.

Nombre de la empresa	•SugarCRM Inc. •www.sugarcrm.com
Nombre del producto	•SugarCRM
Módulos	• **Gestión de Ventas** • Gestión de cuentas y cuadro de mando •**Gestión de Marketing** • Gestión de campañas •**Gestión de la comunicación** • Gestión de soluciones, bug tracker •**Gestión del trabajo en grupo** • Documentos compartidos y chat
Puntos en los que destaca	•Integración con Facebook •Producto muy flexible

Tabla 2.4 Características de SugarCRM
Fuente. Elaboración propia

2.10.3 SuiteCRM

SalesAgility Ltd. se fundó en el año octubre de 2013. Tiene su sede central en Stirling (Escocia). SalesAgility está formada por una comunidad de 103.911 miembros.

SuiteCRM surge como paso evolutivo de *SugarCRM*. *SuiteCRM* comenzó cuando el equipo de desarrolladores de Sugar decidió dejar de desarrollar en su versión gratuita.

Ahora, la nueva versión incorpora nuevas funcionalidades como *Google Maps*, un *plugin*[15] de Outlook y una de las más importantes, el *Workflow* que permite la interacción entre los distintos módulos que lo convierte en una metodología mucho más ágil.

También en el aspecto de la seguridad incluye mejoras ya que permite asignar privilegios a los empleados en función del rol que tenga dentro de la organización o el grupo al que pertenezca.

[15] Plugin: software para visualizar contenido en Internet.

Nombre de la empresa	•SalesAgility Ltd. •www.suitecrm.com
Nombre del producto	•SuiteCRM
Módulos	• **Gestión de Ventas** •Gestión de cuentas y cuadro de mando • **Gestión de pagos** •Gestión de pagos y devoluciones •**Gestión de Marketing** •Gestión de campañas •**Gestión de la comunicación** •Gestión de soluciones, bug tracker •**Gestión del trabajo en grupo** •Documentos compartidos y chat
Puntos en los que destaca	•Integración con Facebook y otras redes sociales y páginas web •Producto muy flexible •Cuenta con un equipo de desarrolladores activo •Workflow •Seguridad

Tabla 2.5 Características de SuiteCRM
Fuente. Elaboración propia

2.10.4 Otras herramientas CRM Open Source

- OroCRM: una de las herramientas CRM más potentes del mercado. Dispone de dos versiones, Community y Enterprise, esta última con más funcionalidades y soporte técnico. Esta versión soporta integración con múltiples organizaciones y páginas web, Microsoft Outlook o Microsoft Exchange.
- Dolibarr ERP & CRM: destaca por su simplicidad. Incorpora múltiples idiomas y módulos como Google, Paypal, MemCache que acelera su uso a través de la caché, cliente de correo y como en el caso anterior, soporta integración con múltiples empresas.

- Fat Free CRM: proporciona características como listas de contactos, manejo de campañas de marketing y leads, y se caracteriza por proveer un código fuente fácil de extender para los desarrolladores.

3 Hipótesis de trabajo y objetivos concretos de investigación.

El método de autenticación *Mobile Connect*, se está adoptando por los operadores de telefonía de todo el mundo según se muestra en su sitio web. "Mobile Connect (2018). Recuperado de: https://mobileconnect.io/partner"

Debido a su amplio ámbito de aplicación, se puede emplear tanto para autenticarse en páginas web donde los datos que se tratan no son sensibles, como en la autenticación de aplicaciones de un banco donde se trata información personal y bancaria altamente sensible.

He elegido esta tecnología por la seguridad que aporta a la autenticación además de por su comodidad y agilidad, ya que con un solo clic y sin la necesidad de recordar nombre de usuario y contraseña podremos acceder al cualquier portal de cliente que ofrezca una organización a sus colaboradores simplemente introduciendo nuestro número de teléfono móvil. Una vez se verifica en *SuiteCRM* que el teléfono introducido corresponde a un colaborador, se proporciona acceso al área privada donde se dispone de todos los datos personales que pueden ser modificados, eliminados o introducir nuevos si es necesario evitando comunicárselos a la organización mediante otra vía menos ágil como el correo electrónico.

Lamentablemente hoy en día siguen existiendo compañías telefónicas que no ofrecen este servicio a sus usuarios por lo que no todo el mundo podrá autenticarse por esta vía, aunque será cuestión de poco tiempo cuando se unan el resto de operadores de red móvil a *GSMA* para ofrecer este servicio.

Actualmente, y sobre todo en el sector no lucrativo, existe un vacío tecnológico importante ya que la mayor parte de los fondos que se recaudan de sus colaboradores (particulares y/o empresas privadas) se destinan a ayudar a las diferentes causas para las que estas organizaciones trabajan. En este sector como en cualquier otro, se mueve una gran cantidad de información sensible como datos personales o datos bancarios, NIF/CIF, direcciones fiscales y datos de tarjetas, los cuales se envían a través de formularios web, aunque el método más utilizado por las organizaciones y sus colaboradores para el intercambio de información es el correo electrónico. Ofreciendo un método de autenticación como *Mobile Connect*, los colaboradores optarán por esta vía de acceso seguro para ejercer cualquiera de sus derechos como es acceder a sus datos personales.

Por otro lado, la organización tiene la obligación de emitir un certificado de donación que acredita que la persona o empresa, cuyos datos fiscales vienen descritos en éste, ha

realizado una aportación económica. El certificado es necesario para la contabilidad empresarial del donante o por un requerimiento por parte de la agencia tributaria. El envío de estos certificados, al igual que ocurre con los datos fiscales y bancarios, viajan desde el usuario hasta la organización, y viceversa, a través del correo electrónico. A partir de ahora, los colaboradores podrán obtener estos certificados dentro del portal de colaborador desarrollado accediendo con *Mobile Connect* al igual que para acceder a sus datos. Esta forma de acceder y que los colaboradores puedan ver toda la información relativa a su persona, es una muestra de confianza, seguridad y transparencia por parte de la organización.

El resultado que espero conseguir es la integración total entre la organización y sus colaboradores de forma que estos últimos no tengan que esperar a que la organización les envíe la información que necesitan periódicamente a través de una vía poco efectiva y manual, y crear una plataforma que les dé a los colaboradores la seguridad y facilidad de acceder sus datos sin esperas, lo que ayudará a las organizaciones con uno de los aspectos más importantes como es la fidelización de sus colaboradores.

3.1 Objetivos de la investigación

3.1.1 Acceso fácil y seguro al portal de clientes [O1]

Acceder a la plataforma sin recordar usuarios y contraseñas y en un solo clic.

Una de las formas más fáciles que puede tener un usuario de acceder a una plataforma es hacerlo sin la necesidad de recordar una contraseña y un usuario, y aún más en el sector no lucrativo donde una comunicación poco fluida con la organización puede hacer que el colaborador deje de ayudar a la causa. Aquí es donde toma fuerza la implementación del método de autenticación *Mobile Connect*, aunque la opción de usuario y contraseña también está disponible para aquellos usuarios que no puedan hacerlo con la opción móvil debido a que su proveedor de servicios de telefonía no dispone del servicio *Mobile Connect*. Con *Mobile Connect* se evita que un atacante pueda adivinar el usuario y contraseña y acceda al área privada del colaborador para modificar sus datos personales o bancarios en su beneficio.

Para autenticarse con *Mobile Connect* solo hay que registrarse en este servicio una única vez, posteriormente introducir nuestro número de teléfono móvil y esperar a que nuestro operador nos envíe un SMS que aceptaremos para terminar de logarnos al portal web.

El proceso de registro para empezar a usar el método de autenticación *Mobile Connect* es el siguiente:

1. Poseer una tarjeta SIM de un proveedor de telefonía que ofrezca este servicio
2. Acceder al sitio web del proveedor e introducir el número de teléfono en el acceso Mobile Connect para comenzar el proceso de activación
3. El siguiente paso será aceptar los términos y condiciones del servicio Mobile Connect
4. Posteriormente se crea un usuario automático con nuestro número de teléfono
5. El último paso es recibir un SMS del proveedor con un mensaje que debemos aceptar. Debemos estar en una zona con cobertura y el terminal móvil encendido

3.1.2 Cumplir con el Reglamento Europeo de Protección de Datos [O2]

El objetivo es que los colaboradores puedan tanto ingresar nuevos datos como actualizar los ya existentes, eliminarlos o directamente oponerse a facilitarlos por una vía segura y de acceso rápido.

RGPD	MEJORAS CON PORTAL WEB CON AUTENTICACIÓN MOBILE CONNECT
Tratamiento legal, leal y transparente	Los interesados tienen acceso ágil y seguro a sus datos y aportaciones económicas.
Limitación del fin, datos y almacenamiento	La solución permite que los interesados puedan cancelar cualquier tipo de comunicación tanto vía postal como por correo electrónico, limitando así alguno de los fines de la organización como son las campañas de marketing.
Derechos de los interesados	Los interesados podrán ejercer sus derechos ARCO, supresión y portabilidad sin ningún tipo de oposición por parte de la organización y sin esperas.
Violación de seguridad de datos personales	La base de datos donde se almacenan los datos, tiene limitación de acceso por roles y privilegios de los empleados. Se realizan copias de seguridad diarias.
Privacidad en el	Los datos están accesibles solamente por el interesado y los empleados y podrán cederse a terceros según las políticas de

diseño	privacidad firmadas en el proceso de alta como colaborador
Transferencia de datos	Los datos podrán ser cedidos a terceros previa aceptación del colaborador para llevar a cabo las tareas organizacionales
Delegado de Protección de Datos	Existe un DPO que será el responsable de que todos los datos se protejan y traten según lo establecido en la ley
Concienciación y formación	Todos los trabajadores de la organización se formarán y concienciarán para que se minimicen los riesgos de sufrir algún tipo de ataque

Un área privada con acceso ágil y seguro sin tener que recordar credenciales es la opción ideal para una organización de este sector. Al portal web desarrollado en este trabajo que solo podrá acceder el colaborador sin que sea suplantada su identidad usando bien usuario y contraseña o *Mobile Connect*. Su información está almacenada en la base de datos de la herramienta que utiliza la organización, *SuiteCRM*, y a la que solamente acceden sus empleados y que no implica ningún desarrollo propio para este trabajo, simplemente configuración y adaptación para integrarse con el portal web. El método que actualmente se utiliza en el sector para el intercambio de información sensible es el envío de correos electrónicos entre los colaboradores y la organización, para lo que se necesitan muchos recursos de personal y tiempo para poder realizar estas tareas.

Los empleados de la organización son los encargados de registrar los datos de los colaboradores la primera vez en *SuiteCRM* e ingresar manualmente cada donación que el colaborador realiza.

El portal web donde accederá el colaborador con autenticación segura *Mobile Connect* o usuario y contraseña, y la herramienta *SuiteCRM* usada por las organizaciones están integradas mediante la *API Rest* que usan este tipo de software y que es la encargada de registrar y actualizar datos en el sistema CRM.

3.1.3 Obtención de certificados de donación [O3]

El objetivo es emitir los certificados de donación por un medio seguro y que ahorre tiempo y recursos a la organización.

El tiempo que tiene que invertir la organización en generar los certificados que acreditan a los colaboradores como donantes es muy elevado. Estos certificados se emiten mensualmente y se envían por correo electrónico lo que hace que el intercambio de información sea lento y que por error se envíe un certificado a un destinatario incorrecto.

Dentro del portal web, el colaborador dispone de un apartado privado donde puede visualizar todas las donaciones que ha realizado a la organización y podrá descargar los certificados de donación que presentará a la agencia tributaria en caso de que ésta lo solicite.

La descarga del certificado de donación se produce en formato pdf y firmado para evitar que pueda ser modificado.

4 Desarrollo de la arquitectura

En este capítulo se diferenciarán dos partes, una es el desarrollo propio que incluye la creación de la página web de una fundación inventada como *Learn Technologies Foundation* con el portal web de acceso a los colaboradores donde tendrán disponibles dos métodos de autenticación, por un lado el método clásico de usuario y contraseña, y por otro *Mobile Connect*, esta última más segura y cómoda para los colaboradores que utilicen operadores de telefonía móvil que les permitan el uso de esta tecnología.

La otra parte la forma la herramienta CRM de software libre elegida, *SuiteCRM*, que se ha adaptado con los campos necesarios que la organización necesitaría para poder realizar sus funciones. He creado nuevos campos que no existían y que serán necesarios para la integración con la parte del portal web de desarrollo propio.

La integración de ambos sistemas se ha realizado con el desarrollo de la *API Rest* de *SuiteCRM* que lleva a cabo la comunicación entre el CRM y el portal web seguro con autenticación *Mobile Connect*. Esta API es común para la mayoría de las herramientas CRM Open Source disponibles en el mercado.

He elegido *SuiteCRM Open Source* ya que a día de hoy es difícil pensar que una organización del tercer sector pueda tener su propio sistema de gestión de bases de datos hecho a medida con la inversión económica que esto conlleva. Para contrarrestar este elevado gasto se hace uso de herramientas CRM de software libre adaptadas a este sector. Estas herramientas ya desarrolladas son por ejemplo *SuiteCRM* o *SugarCRM*, dos de las herramientas CRM por excelencia en el mercado.

Me he decantado finalmente por *SuiteCRM* porque existe un grupo de desarrolladores en activo para este proyecto, justo al contrario que SugarCRM que tiende al desuso ya que el equipo de desarrolladores que hacían posible este proyecto han dejado de prestar su apoyo aunando todos los esfuerzos en SuiteCRM.

El problema económico, es uno de los problemas dentro del tercer sector que se solventa usando herramientas *Open Source*, lo que implica que con una inversión mínima de alojamiento en un servidor web se puede tener un sistema CRM operativo para la organización.

Como comentaba en el capítulo 3.1 **Objetivos de la investigación**, otro de los problemas a solventar es la cantidad de tiempo y recursos empleados en la actualización de datos personales de los colaboradores y el continuo intercambio de información sensible por

medio de correo electrónico que facilite el proceso de fidelización de los colaboradores. Además, la continua necesidad de las empresas de obtener el certificado que acredite que ha realizado una donación a la ONG hace que el proceso sea tedioso.

La arquitectura de la tecnología desarrollada se representa en la siguiente imagen.

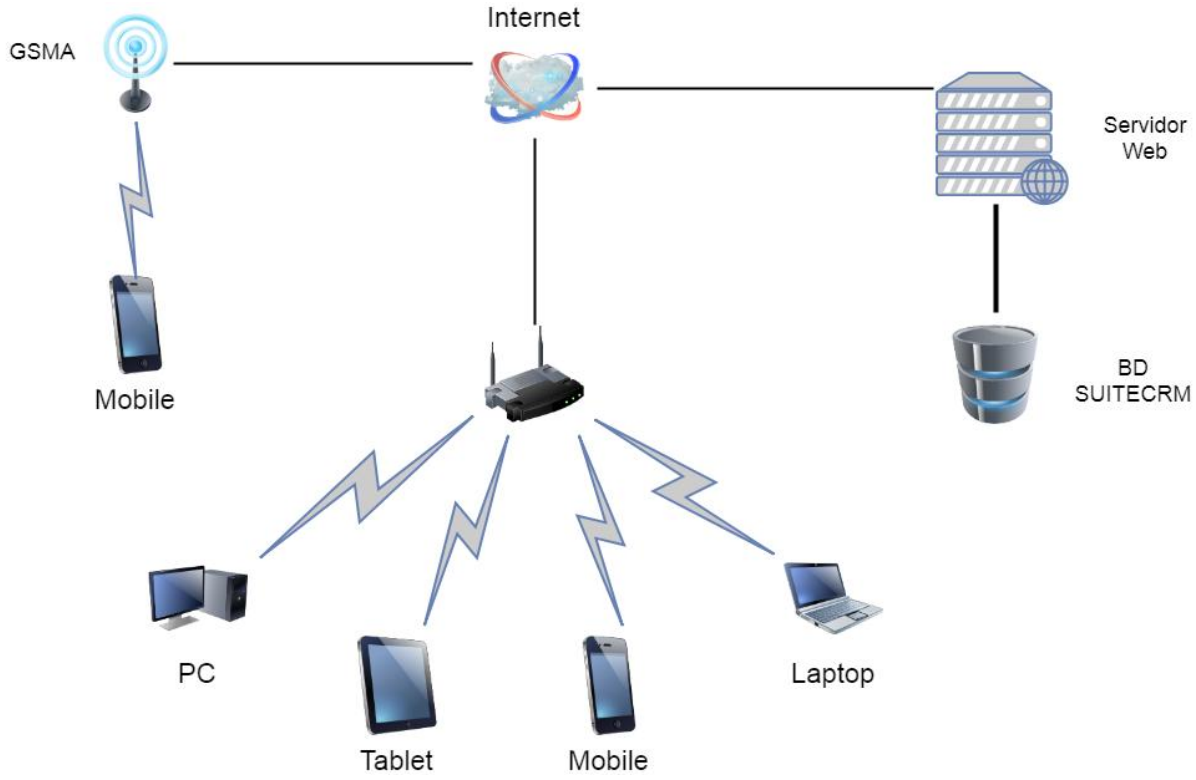

Ilustración 4.1 Arquitectura Web - SuiteCRM
Fuente. Elaboración propia

El diagrama de uso que representa el funcionamiento del sistema es el mismo que se desarrolla más abajo en el capítulo 4.2 **Acceso al portal Web mediante usuario y contraseña. Caso de uso.**

4.1 Desarrollo propio. Portal Web de colaboradores con acceso seguro

La creación de una página web corporativa de una organización ficticia donde estará el portal privado de colaboradores y desde donde podrán acceder a su área privada para actualizar datos personales y descargar el certificado de forma mucho más segura.

Esta es la parte de desarrollo propio en la que he creado las diferentes páginas que forman parte de la página web y la correspondiente *API Rest* para que se lleve a cabo la integración entre el portal web y la aplicación *SuiteCRM* de manera que mediante llamadas a ésta podamos obtener los campos necesarios que el colaborador necesita tener en su perfil privado de área de cliente.

Ilustración 4.2 Página web de la fundación ficticia
Fuente. Elaboración propia

El menú principal de navegación de la página web de la organización está formado por:

- Página de inicio: se muestra información sobre el trabajo de la organización.
- Portal: donde podrán acceder los colaboradores, registrarse y obtener la información personal que la organización tiene registrada en su base de datos.
- Contacto: donde podrán escribir los visitantes de la página web para realizar cualquier petición, queja o sugerencia.

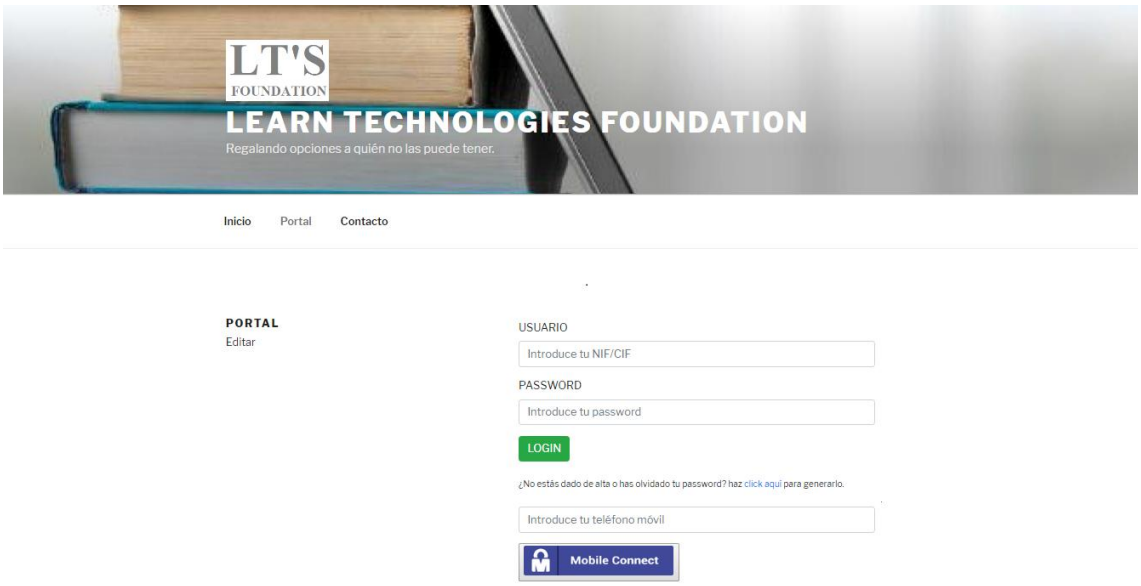

Ilustración 4.3 Portal web de la fundación
Fuente. Elaboración propia

El portal web se ha configurado para acceder por un lado, mediante usuario y contraseña y por otro lado de acceso con *Mobile Connect*.

Como se observa en la Ilustración 4.3 **Portal web de la fundación**, el campo usuario se corresponde con el NIF/CIF que tengamos registrado en *SuiteCRM*. Si es la primera vez que el colaborador accede al portal web, tendrá que registrarse para introducir una contraseña nueva que se registra en *SuiteCRM* y que será uno los dos campos que se contrastan y que aprueban el acceso a la zona privada.

El registro se realiza simplemente introduciendo el campo NIF/CIF. Posteriormente el usuario recibirá un correo electrónico en el que se incluye *token* con un único uso que se utiliza para elegir la contraseña nueva. El colaborador solo tendrá que hacer clic en un botón llamado *generar contraseña* que lo llevará de nuevo a la página web de la fundación donde puede elegir la contraseña.

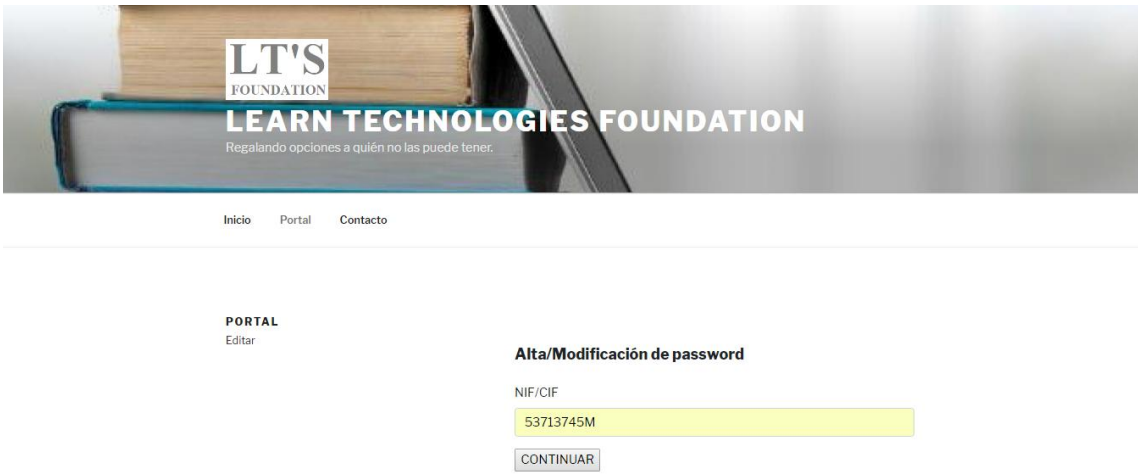

Ilustración 4.4 Formulario de alta/modificación de contraseña
Fuente. Elaboración propia

Ilustración 4.5 Confirmación de envío de contraseña
Fuente. Elaboración propia

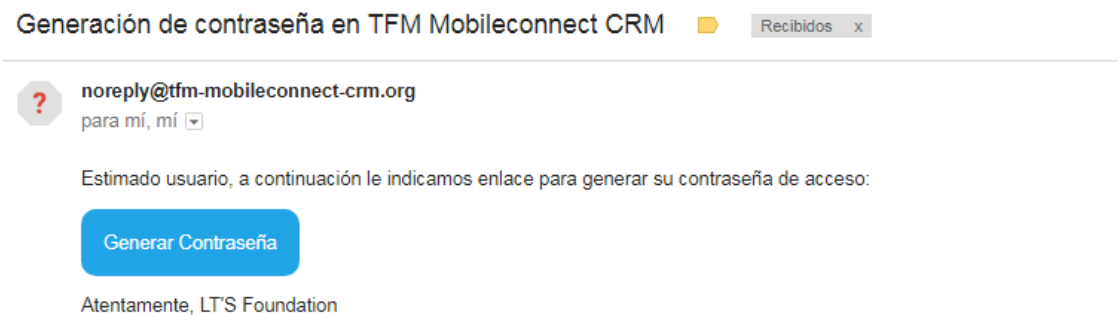

Ilustración 4.6 Correo electrónico de generación de contraseña
Fuente. Elaboración propia

La siguiente Ilustración 4.7 **Petición de nueva contraseña** muestra la pantalla a la que llegamos después de hacer clic en *generar contraseña* del correo electrónico recibido. Este *token* se valida una única vez e invalida si se produce un segundo intento de alta/modificación de contraseña, lo que enviará un nuevo correo electrónico con un nuevo *token*.

Se accede a una nueva página con el formulario donde se introduce la nueva contraseña con unas características de formato especificas entre la que se pide que contenga caracteres, números y símbolos.

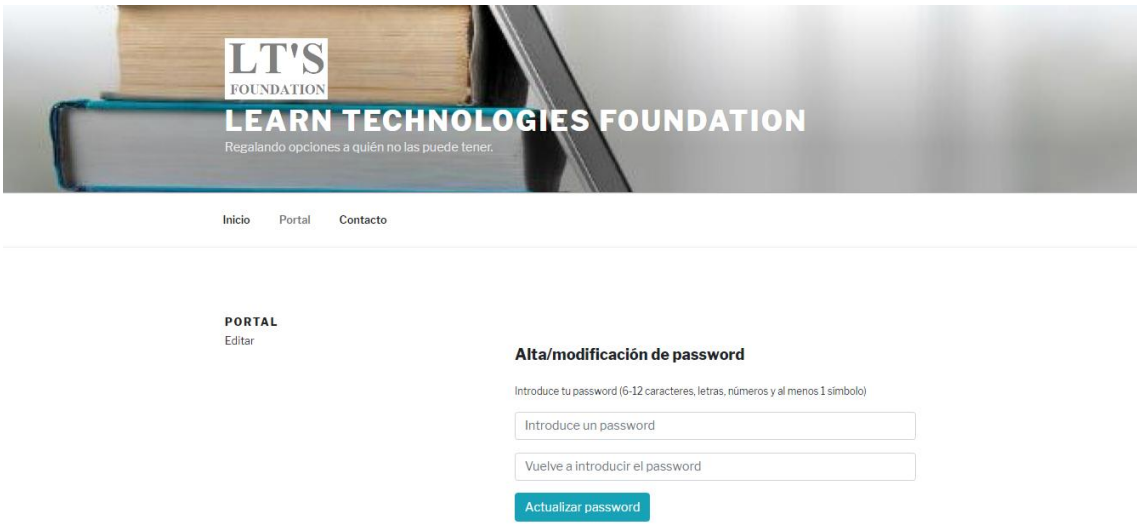

Ilustración 4.7 Petición de nueva contraseña
Fuente. Elaboración propia

Una vez realizada el alta/modificación correctamente, se puede acceder a los datos de colaborador donde tendrá dos pestañas, **mis datos** con los campos que aparecen en la Ilustración 4.8 **Formulario de datos del colaborador**, y una segunda pestaña llamada **certificados** donde se encuentran los pagos realizados a la organización y donde está la opción de descargar el correspondiente certificado de cada pago.

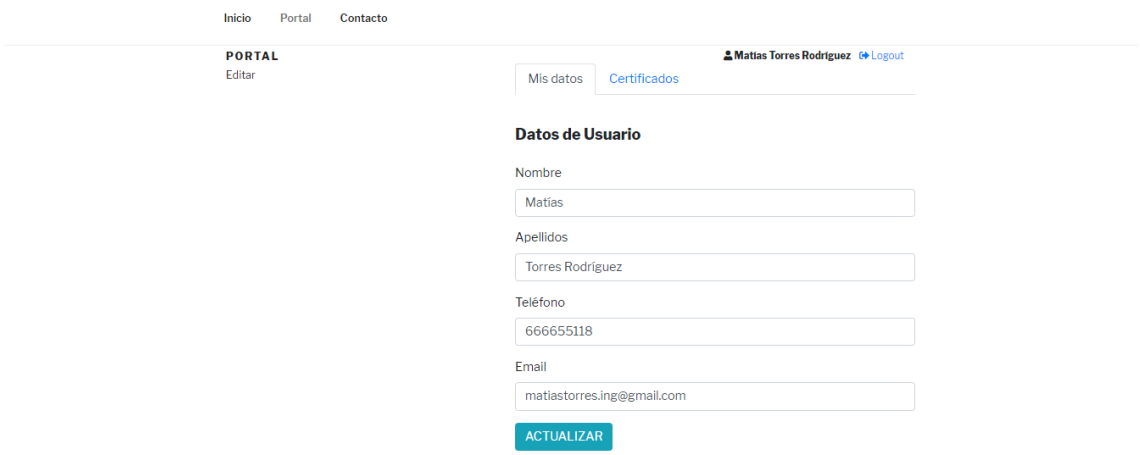

Ilustración 4.8 Formulario de datos del colaborador
Fuente. Elaboración propia

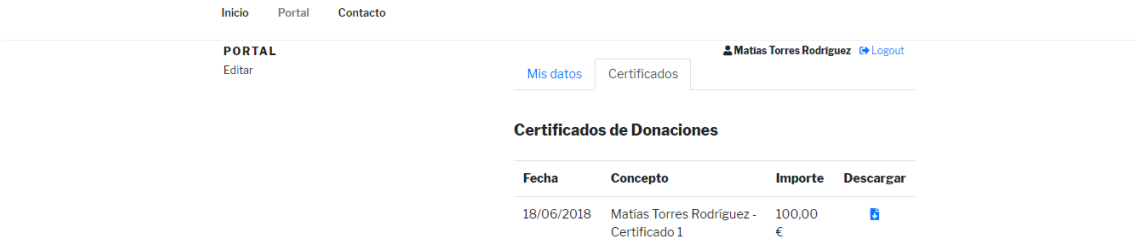

Ilustración 4.9 Pagos y certificados del colaborador
Fuente. Elaboración propia

El certificado de donación tiene una estructura como se muestra en la Ilustración 4.10 **Certificado de donación tipo** en la que incluye los datos fiscales de la organización, la información correspondiente al registro de fundaciones y su representante legal.

También se incluyen los campos que son obligatorios para que el certificado tenga validez, como son el nombre completo del colaborador, el NIF/CIF y la provincia de su dirección fiscal además de la fecha de realización de la donación.

LT'S
FOUNDATION

D. Matías Torres, Secretario de la **FUNDACIÓN LEARN TECNOLOGIES**, domiciliada en Madrid, clasificada de carácter asistencial por orden del Ministerio de Trabajo y Asuntos Sociales de 8-II-2006 y, actualmente, adscrita a la Consejería de Asuntos Sociales (CAM) por Resolución de 3-06-2013 de la Dirección General de Seguridad e Interior, Consejería de Presidencia, Justicia y Portavocía del Gobierno, (CAM). Inscrita en el Registro de Fundaciones de la Comunidad de Madrid con número de hoja personal 700, en el tomo CCXXVII, folios 201-215.

CERTIFICA

I.- Que el día **18/06/2018** la FUNDACIÓN LEARN TECNOLOGIES ha recibido de **MR. MATíAS TORRES RODRíGUEZ** con domicilio en **MADRID** y titular de **N.I.F 53713745M**, un total de **100,00 €**, en concepto de donativo irrevocable para cumplimiento de fines de la Fundación, al amparo del artículo 2º de nuestros Estatutos.

II.- Que la FUNDACIÓN LEARN TECNOLOGIES se encuentra incluida entre las entidades beneficiarias de mecenazgo, de acuerdo con lo establecido en Ley 49/2002, de 23 de diciembre, de régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo.

Y para que así conste y surtan los efectos oportunos donde fuere pertinente, expido la presente certificación en Madrid, a 02/07/2018 17:50.

Ilustración 4.10 Certificado de donación tipo
Fuente. Elaboración propia

4.1.1 Acceso al portal Web mediante usuario y contraseña. Caso de uso.

A continuación, se han diseñado tanto un diagrama de caso de uso como el correspondiente diagrama de secuencias del acceso mediante usuario y contraseña.

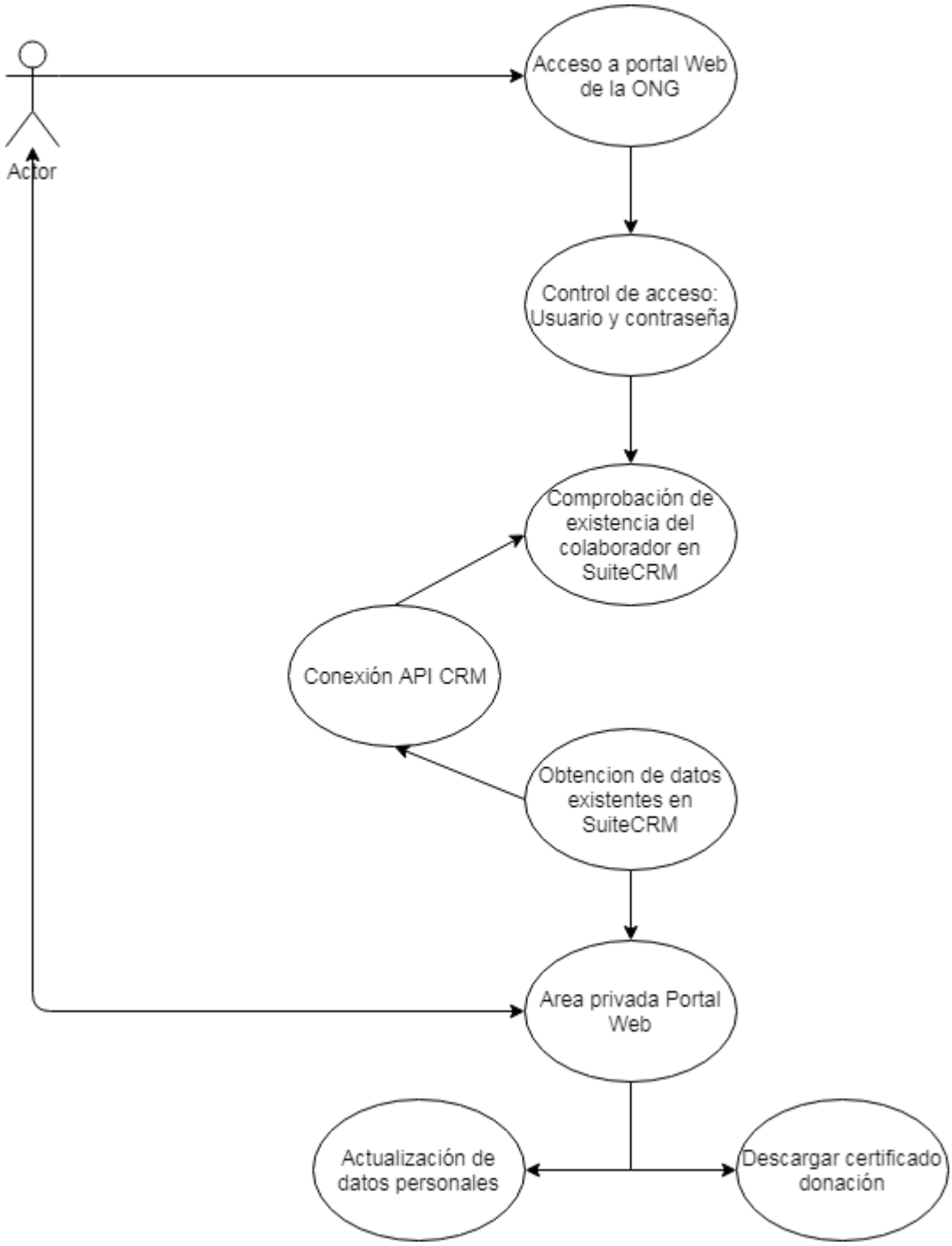

Ilustración 4.11 Interacción entre colaborador y sistema
Fuente. Elaboración propia

Descripción del caso de uso: Acceso al portal web con usuario y contraseña

Nombre: Acceso al portal web

Descripción: El sistema le solicita al usuario el ingreso de un nombre de usuario y contraseña (si está registrado) que previamente había introducido en el registro, para que lo valide el sistema y acceda a sus datos personales. Si no está registrado deberá hacerlo introduciendo su número de identificación fiscal, posteriormente recibirá un correo electrónico con un token para poder generar una nueva contraseña.

Propósito: Acceder al portal web para actualizar sus datos personales y/o descargar sus certificados de donación correspondientes a las donaciones realizadas.

Precondiciones: Que el usuario haya sido validado para que pueda acceder al portal web.

Post-condiciones: Que el usuario tendrá acceso al sistema si ha introducido la contraseña correcta.

Usuario	Sistema
1. Ingreso de usuario y contraseña	2. Conexión con API CRM
	3. Búsqueda del usuario en el sistema SuiteCRM
	4. Validación del usuario
	5. Validación de la contraseña
	6. Muestra la interfaz del usuario
7. El usuario puede modificar sus datos y/o descargar su certificado de donación	

Tabla 4.1 Caso de uso. Acceso al portal web con usuario y contraseña
Fuente. Elaboración propia

Una vez realizado el caso de uso y descrito para acceder al portal web mediante usuario y contraseña, se muestra el diagrama de secuencias.

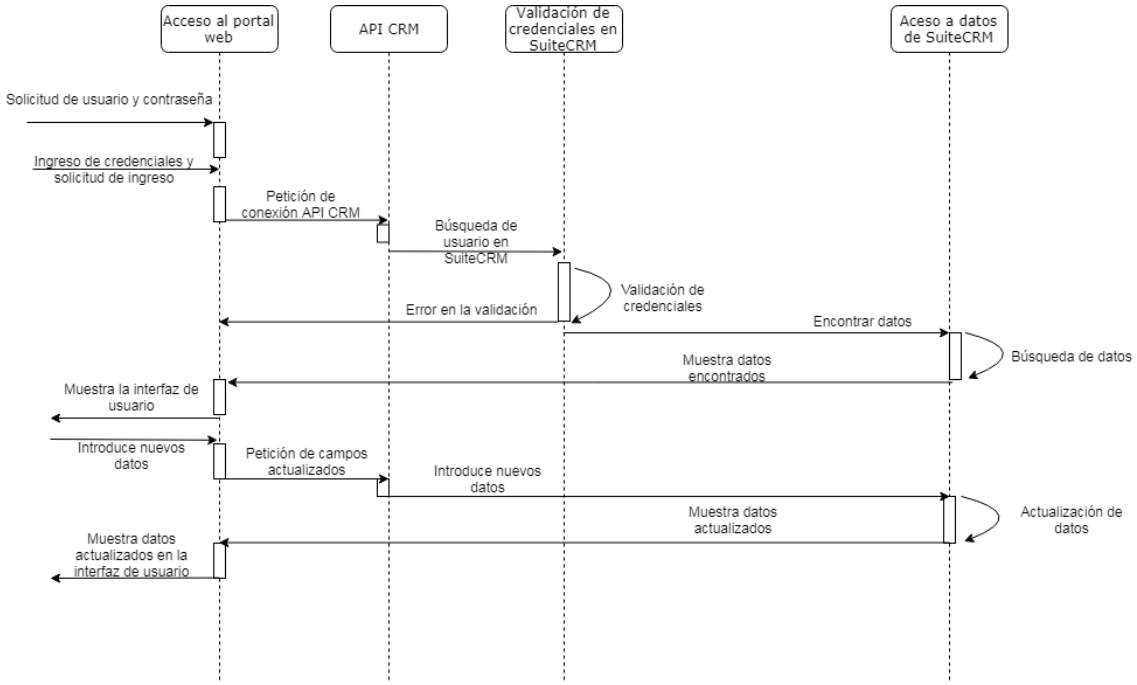

Ilustración 4.12 Diagrama de secuencias acceso portal web mediante usuario y contraseña
Fuente. Elaboración propia

4.1.2 Acceso al portal Web mediante Mobile Connect. Caso de uso.

Aquí se representa el acceso de un colaborador al portal Web mediante el método de autenticación *Mobile Connect*.

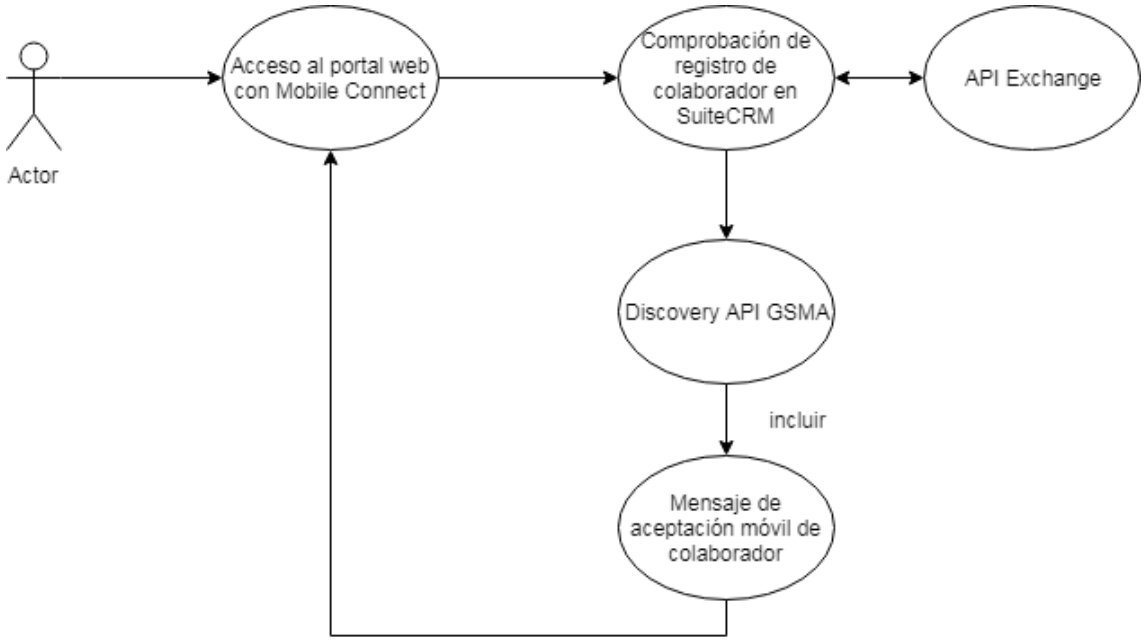

Ilustración 4.13 Caso de uso acceso a portal Web mediante Mobile Connect
Fuente. Elaboración propia

Descripción del caso de uso: Acceso al portal web mediante *Mobile Connect*

Nombre: Acceso al portal web con método seguro

Descripción: Una vez se hace clic en el botón de *Mobile Connect*, se solicita al colaborador su número de teléfono móvil. Este número deberá coincidir con el número registrado en el sistema *SuiteCRM* para que se pueda llevar a cabo la autenticación, en otro caso enviará un mensaje de error indicando que se registre en el sistema. Aquí el proceso será el mismo que en el punto anterior, deberá hacerlo introduciendo su número de identificación fiscal, posteriormente recibirá un correo electrónico con un token para poder generar una nueva contraseña.

Propósito: Acceder al portal web para actualizar sus datos personales y/o descargar sus certificados de donación correspondientes a las donaciones realizadas.

Precondiciones: Que el usuario haya sido validado para que pueda acceder al portal web y además utilice una tarjeta SIM compatible con el método de autenticación utilizado.

Post-condiciones: Que el usuario tendrá acceso al sistema si ha introducido la contraseña correcta.

Usuario	Sistema
1. Ingreso de número de teléfono móvil compatible	2. Conexión con API CRM
	3. Búsqueda del usuario en el sistema SuiteCRM
	4. Validación del usuario
	5. Conexión con API Exchange
	6. Conexión con Discovery API GSMA
	7. Recepción de SMS al móvil del colaborador para aceptar conexión
8. El usuario puede modificar sus datos y/o descargar su certificado de donación	

Tabla 4.2 Caso de uso. Acceso al portal web mediante Mobile Connect
Fuente. Elaboración propia

El diagrama de secuencias correspondiente al acceso a la aplicación web con *Mobile Connect* quedaría como muestra la Ilustración 4.14 **Discovery GSMA con portal web**.

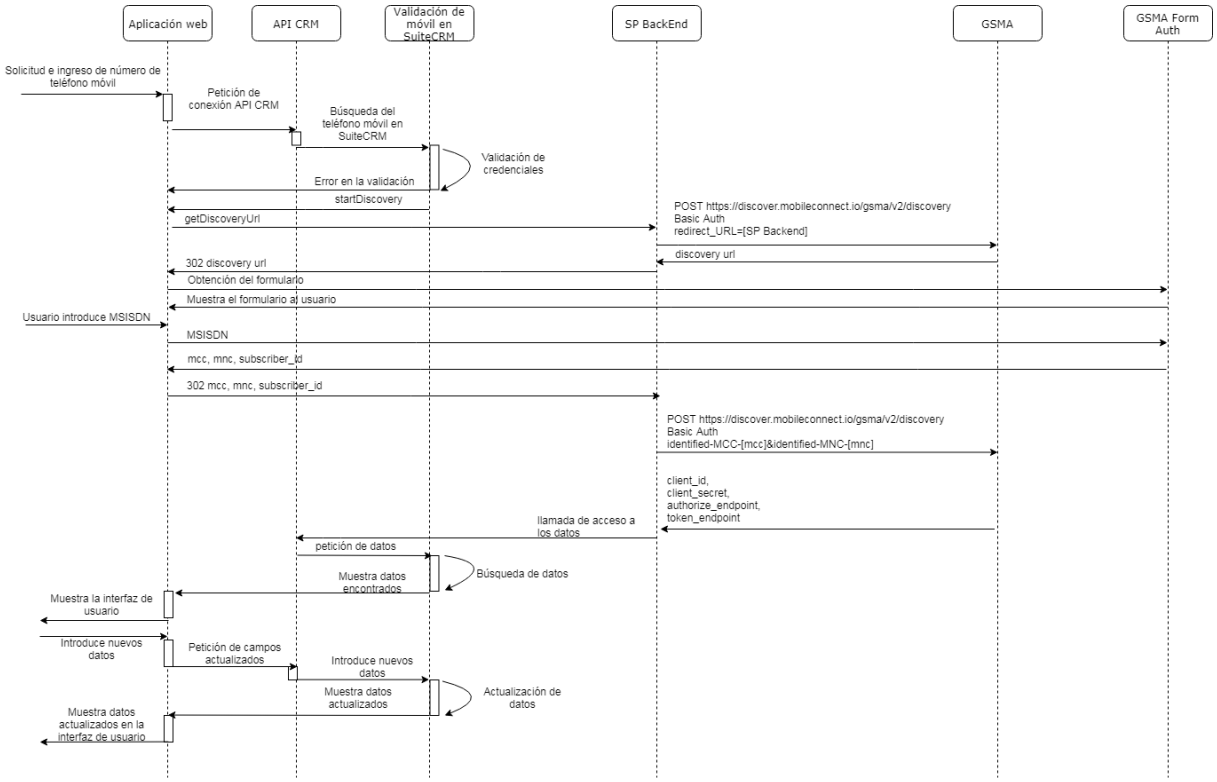

Ilustración 4.14 Discovery GSMA con portal web
Fuente. Elaboración propia

4.1.3 Registro de usuario en SuiteCRM. Caso de uso.

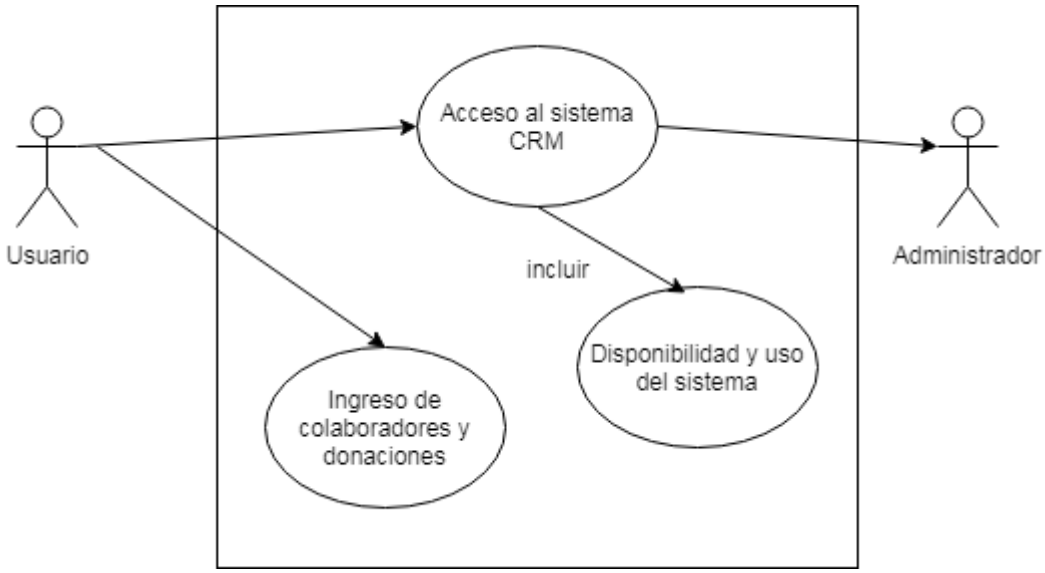

Ilustración 4.15 Caso de uso Registro de nuevo usuario en SuiteCRM
Fuente. Elaboración propia

Descripción del caso de uso: registro de nuevo usuario en el sistema *SuiteCRM* por parte del administrador del sistema.

Nombre: Registro de nuevo empleado en *SuiteCRM*

Descripción: El administrador del sistema registra el nuevo empleado con un identificador y contraseña de acceso. Una vez éste tiene acceso, ya podrá introducir nuevos contactos y dar de alta nuevos donativos que estos hayan realizado para que puedan obtener sus certificados una vez accedan al portal web.

Propósito: que el empleado pueda registrar tanto donantes como sus respectivos donativos.

Precondiciones: el empleado ha sido dado de alta por el administrador del sistema.

Post-condiciones: Que el usuario tendrá acceso al sistema si ha introducido la contraseña correcta y realice tareas según rol concedido.

Administrador	Empleado
1. Registra identificador y contraseña del empleado	2. Validación del usuario
	3. Validación de la contraseña
	4. Muestra la interfaz del sistema SuiteCRM
	5. Empleado registra nuevos donantes
	6. Empleado registra nuevos donativos del los colaboradores

Tabla 4.3 Caso de uso. Registro de nuevo usuario en el sistema SuiteCRM
Fuente. Elaboración propia

4.1.4 Registro y recuperación de contraseña de colaborador en portal Web. Caso de uso.

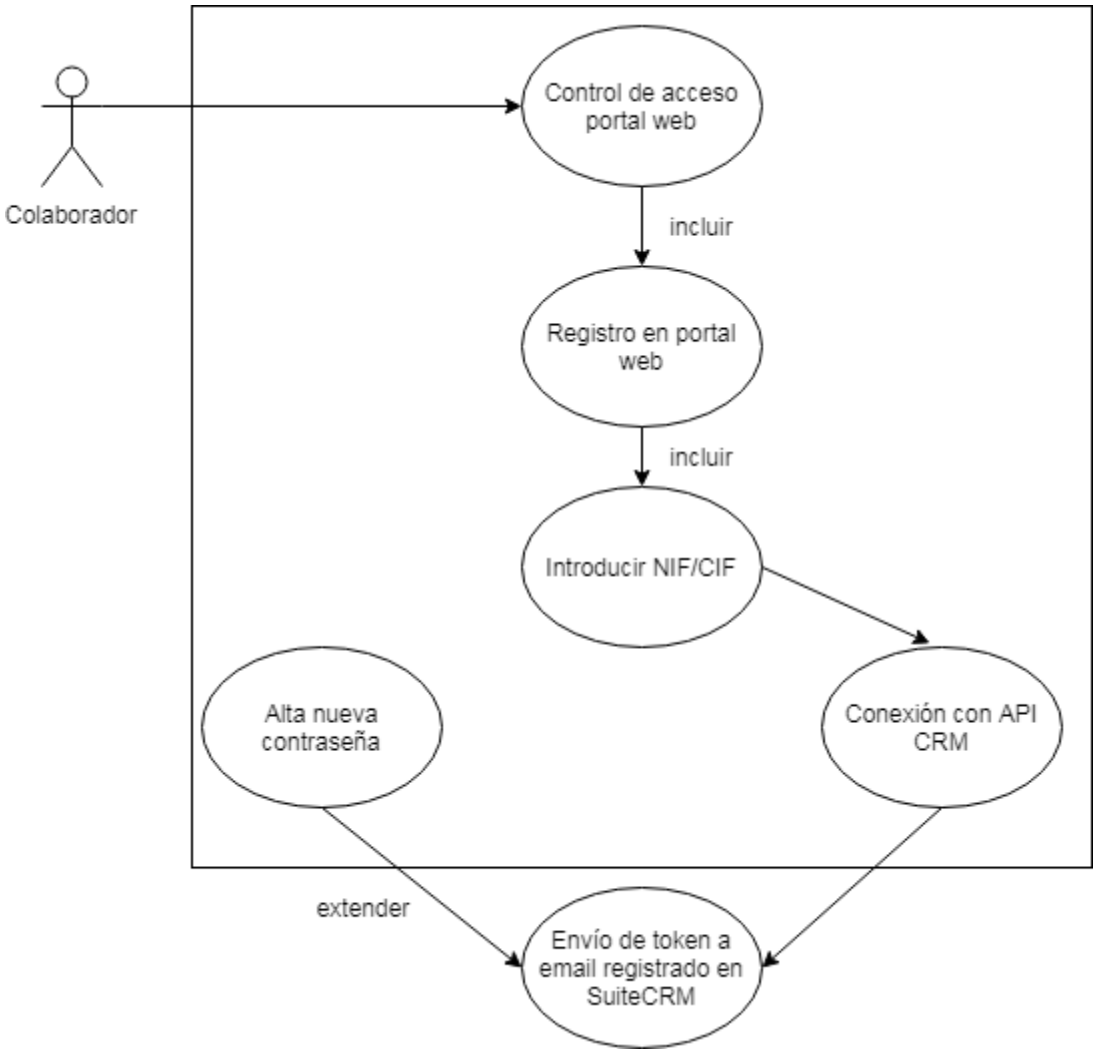

Ilustración 4.16 Caso de uso registro y recuperar contraseña portal web
Fuente. Elaboración propia

Descripción del caso de uso: registro de nuevo colaborador y/o recuperación de contraseña para acceder al portal web.

Nombre: Alta y recuperación de contraseña de acceso al portal web.

Descripción: El colaborador se registrará en el sistema, aquí introducirá su número de DNI/CIF y recibirá un *token* vía el correo electrónico que tengamos registrado en *SuiteCRM*, con ese token nos invitará a introducir una contraseña. A partir de aquí podemos acceder. El mismo proceso para recuperar contraseña.

Propósito: que el colaborador pueda acceder a sus datos personales y certificados de donación.

Precondiciones: que el colaborador esté registrado en el sistema *SuiteCRM* con su DNI/CIF.

Post-condiciones: Que el usuario tendrá acceso al sistema si ha introducido la contraseña correcta.

Colaborador	Sistema
1. Introduce su NIF/CIF	2. Envía token al correo electrónico registrado en la base de datos
3. Usando el token recibido introduce nueva contraseña	
	4. Guarda la nueva contraseña
5. Introduce usuario y contraseña	
	6. Valida usuario y contraseña
7. Accede al área privada del portal web	

Tabla 4.4 Caso de uso. Registro de nuevo colaborador y/o recuperación de contraseña
Fuente. Elaboración propia

4.1.5 Actualización de datos personales y registro del número de teléfono móvil. Caso de uso.

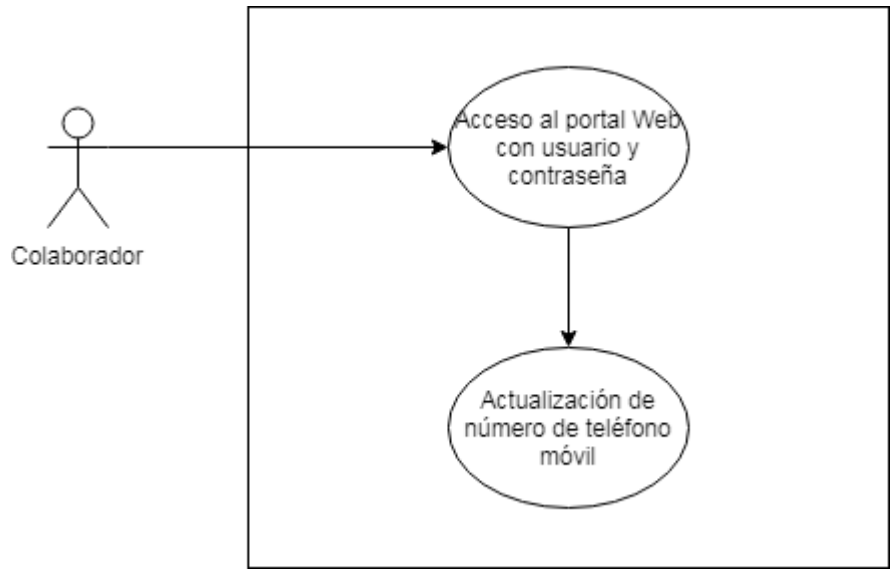

Ilustración 4.17 Registro de número de teléfono móvil en sistema
Fuente. Elaboración propia

Descripción del caso de uso: registro de número de teléfono móvil en la base de datos.

Nombre: registro de número de teléfono móvil en sistema.

Descripción: el colaborador accede al portal web por primera vez mediante usuario y contraseña. Una vez dentro, el colaborador deberá introducir un teléfono móvil con el que le habilitará para poder acceder al portal Web mediante *Mobile Connect.*

Propósito: que el colaborador pueda acceder a sus datos personales y certificados de donación mediante autenticación *Mobile Connect.*

Precondiciones: que el colaborador esté registrado en el sistema *SuiteCRM* con su DNI/CIF.

Post-condiciones: Que el usuario tendrá acceso al sistema con *Mobile Connect* si ha introducido el número de teléfono móvil correcto.

Colaborador	Sistema
1. Introduce su NIF/CIF y contraseña	2. Valida las credenciales y da acceso al portal web
3. Actualiza el campo Teléfono móvil en el portal web	
	4. Guarda el campo teléfono móvil
5. Accede nuevamente con Mobile Connect	

Tabla 4.5 Caso de uso. Registro de número de teléfono móvil en el sistema
Fuente. Elaboración propia

4.2 Configuración de entorno existente SuiteCRM

La instalación y configuración de *SuiteCRM* se ha realizado sobre un servidor cloud gestionado. El *servidor cloud gestionado* tiene instalados una base de datos *MySql, Php 7* y preinstalación de *SuiteCRM*.

Para poder acceder públicamente he reservado el dominio *https://www.tfm-mobileconnect-crm.org* donde estará alojada la herramienta y a través del cual podrán acceder los empleados de la organización mediante autenticación de usuario y contraseña. Para la configuración de *SuiteCRM* comenzamos accediendo al portal del proveedor de servicios de internet donde tenemos contratado nuestro servidor, en este caso se trata de *1and1*.

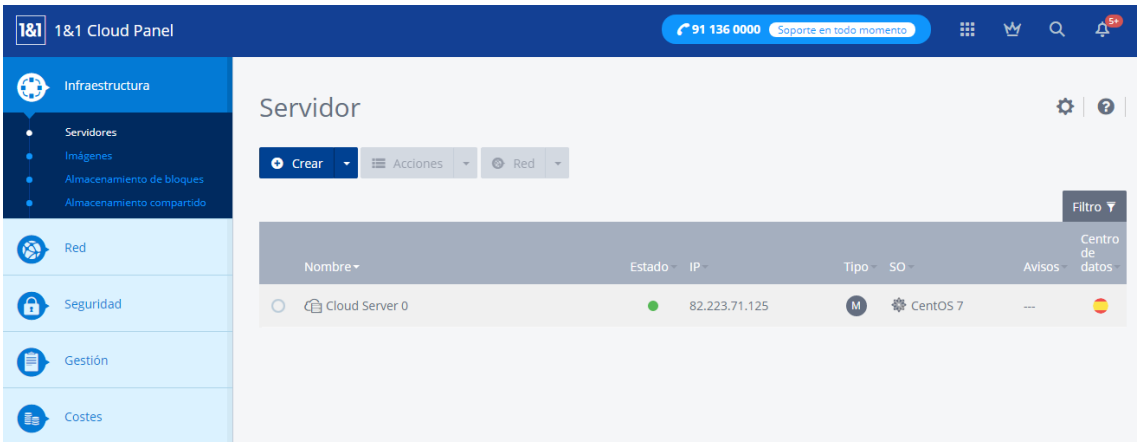

Ilustración 4.18 Portal de administración servidor cloud 1and1
Fuente. Elaboración propia

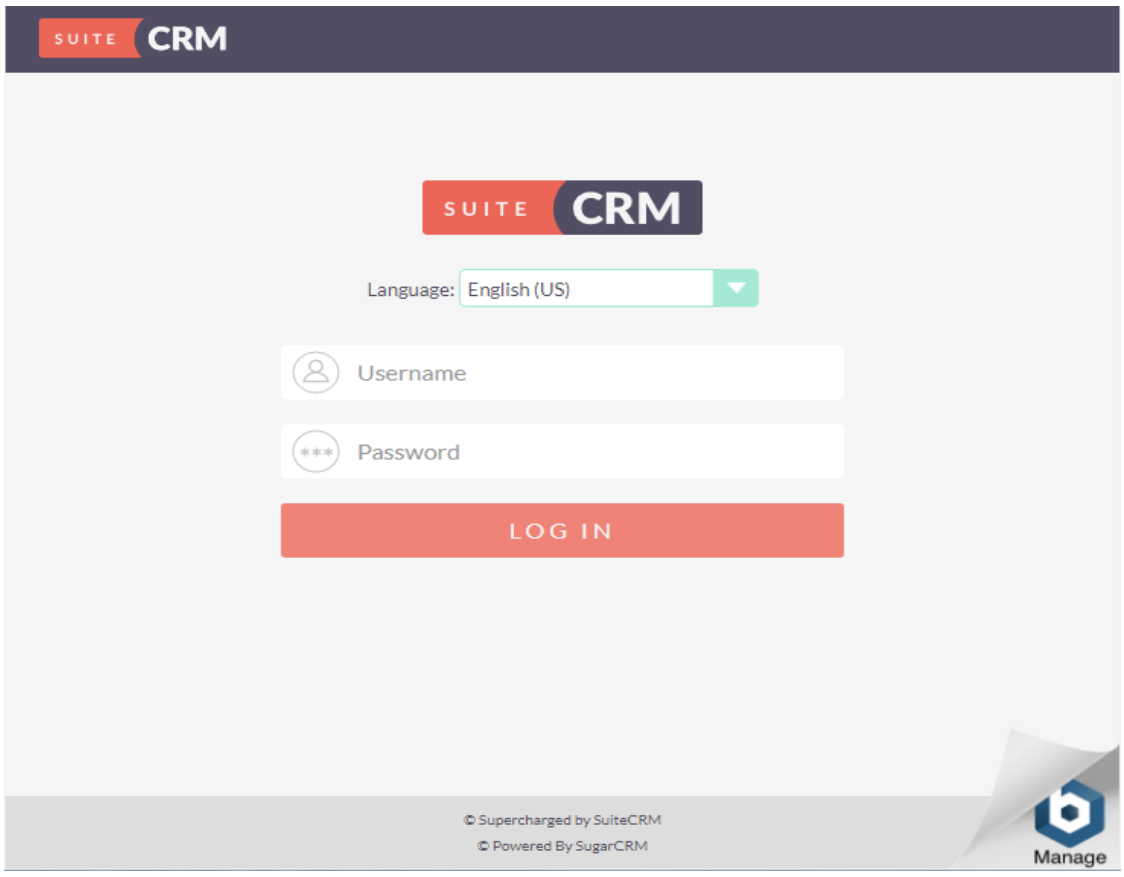

Ilustración 4.19 Herramienta de software libre SuiteCRM
Fuente. Elaboración propia

SuiteCRM cuenta con módulos específicos para controlar todas las donaciones realizadas (*invoices*), las cuales se muestran dentro del portal de colaboradores.

Entre los módulos que cuenta están:

- Contacts: se refiere al módulo de personas tanto físicas como jurídicas que van a tener alguna relación con la fundación bien sean socios recurrente como puntuales, u otro tipo de relación como puede ser simplemente seguidor y no colabora económicamente.
- Accounts: este módulo es el de las empresas, al igual que las personas podremos tener tanto empresas que colaboran económicamente o bien otro tipo de colaboración que no implica un intercambio monetario.
- Invoices: este es el módulo de los donativos. Aquí quedarán registrados todos los donativos realizados bien sea por contacts o accounts.
- Otros módulos: la herramienta dispone de otros muchos módulos relacionados con otro tipo de actividades que puede llevar a cabo la fundación, como es el módulo de envío de campañas de marketing, el de informes que permitirá crear como su nombre indica informes para realizar *data mining*[16] dentro de nuestra base de datos y poder saber si estamos cumpliendo con el objetivo de la organización.

Ilustración 4.20 Módulo de contactos de SuiteCRM
Fuente. Elaboración propia

[16] Data mining: exploración de datos en grandes volúmenes.

Además de las funcionalidades que ofrece por defecto, dispone de un panel de administración que permite desarrollar tanto módulos, como paneles y campos que sean necesarios. En mi caso adapté varios de los campos que hemos utilizado en el portal de colaboradores como son los campos NIF/CIF y contraseña, este último oculto y cifrado para que no pueda ser modificado.

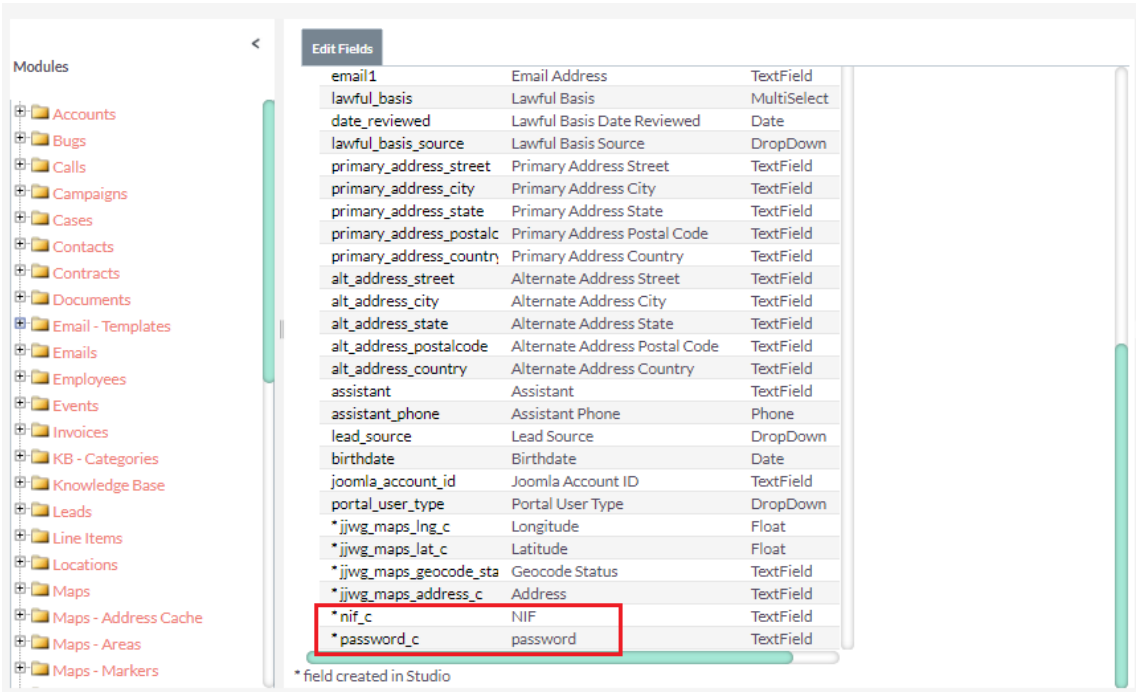

Ilustración 4.21 Campos NIF y Password creados
Fuente. Elaboración propia

Dentro del panel de administración se puede controlar todo lo relacionado con la creación de nuevos empleados, gestionar sus contraseñas y otro punto importante dentro de la seguridad de la herramienta es que contiene un módulo de administración de roles y privilegios. Para realizar una estructura de la organización dentro de *SuiteCRM*, se crean grupos y roles por empleados que realizan las mismas tareas y que solo podrán acceder a ciertas funciones de la herramienta.

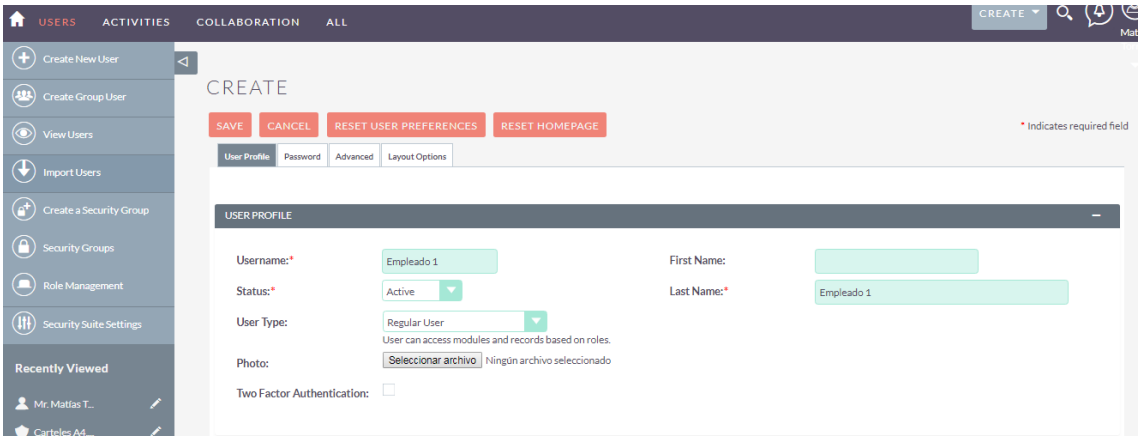

Ilustración 4.22 Creación de empleados y contraseñas
Fuente. Elaboración propia

4.3 ¿Cómo se ha implementado la integración Portal Web y SuiteCRM?

La integración del portal de colaboradores de la página web con la herramienta *SuiteCRM* se ha realizado a través de la *API Rest* de *SuiteCRM*. Esta API consta de varías partes que se describen a continuación.

Por un lado tenemos el fichero **APICRM.php** donde se han declarado las distintas funciones que vamos a necesitar para establecer una comunicación e intercambio de datos entre el portal y *SuiteCRM*. Dentro de *SuiteCRM* siempre vamos a trabajar en base a dos módulos diferentes como son el módulo de personas (*contacts)* y el módulo de empresas (*accounts*), y además de estos, en base a una serie de campos que son únicos dentro de la base de datos de la herramienta, estos son:

- Id: este campo contiene un número aleatorio único dentro del sistema de base de datos que identifica bien sea una persona como una empresa.
- NIF: Número de identificación fiscal de la persona.
- CIF: Código de identificación fiscal de la empresa.
- Correo electrónico: este campo se utilizará tanto para el registro de alta como en la modificación de contraseña .Se envía un email con el enlace que contiene el *token* que se utilizará para crear una nueva contraseña.

4.3.1 Desarrollo API Rest para SuiteCRM

La API Rest contiene todas las clases y funciones necesarias para la comunicación entre el portal y *SuiteCRM*, se encarga de la integración entre ambos sistemas. A continuación se detallan las funciones responsables de esta integración y que permitirá tanto registrar nuevos datos en el sistema CRM como actualizar información ya existente.

La función **UpdateItem** será la encargada de actualizar los valores de los campos que hemos seleccionado para mostrar al colaborador.

La función **GetUser** tiene la tarea de obtener la información de la herramienta. Como se puede ver, dependiendo de si se introduce un número de CIF o de NIF, esta función buscará en SuiteCRM en los diferentes módulos, bien sea el módulo de personas (*contacts*) o el de empresas (*accounts*).

La función **GetUsebyNif** se encarga de obtener la información del colaborador en base a su NIF. Esta función va a ser útil cuando se proceda al alta y la recuperación de contraseña.

La función **GetUserByToken** se encarga de recuperar un usuario en base al token que se envía al correo electrónico para generar una nueva contraseña.

La función **LoadUserById** se encargará de recuperar el perfil del colaborador en base a su ID único de registro de la base de datos.

La función **GetInvoices** tiene como función obtener los pagos que se han realizado a la fundación y que serán mostrados en el área privada del colaborador para su posterior emisión del certificado de donación.

Las funciones **GetModules** y **GetFields** se encargan de conseguir los diferentes parámetros que lo forma y su contenido.

4.3.2 Desarrollo archivo INDEX.PHP

El archivo index.php contiene toda la programación relativa a la primera pantalla de acceso al portal web donde se lleva a cabo el *login* al área privada del colaborador mediante dos opciones, usuario y contraseña, y *Mobile Connect*.

En esta primera parte se hace la validación de las credenciales que nos facilitar el usuario que, mediante una llamada a la API Rest de *SuiteCRM* va a tratar de localizar los campos NIF/CIF y la contraseña para ver si coinciden, de ser así dará acceso a la parte privada, en otro caso emitirá un mensaje avisando al usuario de que las credenciales facilitadas son erróneas.

La validación de las credenciales de usuario se realiza con la siguiente función:

if(isset($_REQUEST['action']) && $_REQUEST['action']=='login'){

esta nos devolverá el permiso de acceso al portal o en su defecto un mensaje diciendo que el usuario no existe.

4.3.3 Desarrollo archivo DASHBOARD.PHP

El archivo Dashboard.php contiene toda la programación relativa al área privada del colaborador donde se podrán observar dos partes bien diferenciadas. Por un lado tenemos una página con los campos del formulario de datos personales que como decíamos pueden ser completados y actualizados mediante llamadas a las distintas funciones de la API Rest como,

```
<div class="form-group">
        <label>Nombre</label>
        <input type="text" class="form-control" name="name" value="<?php print getValue('name');?>">
    </div>
```

y por el otro la página de pagos realizados a la fundación con la opción de descargar el certificado con llamadas a la función detallada en el capítulo **Desarrollo archivo DESCARGA.PHP**. También nos encontramos la opción de *logout* de sesión.

4.3.4 Desarrollo archivo PASSWORD-GENERATE.PHP

En este archivo se ha implementado la función de generar una nueva contraseña mediante un token de un único uso formado por la unión del id de usuario, el tiempo de la petición en

milisegundos y un conjunto de caracteres aleatorios que le dan robustez frente a un ataque de descubrimiento de contraseña.

```
$token = md5($user->id.$user->name_value_list->email1-
        >value.time().nvpsipowrpowefp);
        $params = [
                'id'=>$user->id,
                'password_c'=>$token,
        ];
```

Cuando se realiza la petición desde el formulario web, se debe introducir el NIF/CIF y automáticamente mediante una llamada a la API Rest de *SuiteCRM* se localiza el colaborador y se envía un correo electrónico a la dirección que está registrada en la herramienta con el *token* que lo llevará a generar la nueva contraseña.

4.3.5 Desarrollo archivo SET-PASSWORD.PHP

En este archivo se desarrolla toda la parte posterior a la recepción del email y recepción del token para establecer la nueva contraseña.

Esta contraseña tiene que tener una estructura en la que contenga entre 6-12 caracteres, mayúsculas, minúsculas y un número. De no ser así fallará la generación de la clave.

```
if(strlen($clave) < 6){
        $error_clave = "La clave debe tener al menos 6 caracteres";
          return false;
  }
```

Haciendo uso de la función **GetUserbyToken**, accederá a *SuiteCRM* para localizar si realmente el colaborador existe, si no es así, mostrará un mensaje advirtiendo de su no existencia en la base de datos.

```
if(isset($_REQUEST['t']) && $_REQUEST['t']!=''){
        $token = filter_var($_REQUEST['t'],FILTER_SANITIZE_STRING);

        if(!$user = $api->getUserByToken($token,'Contacts')){
                if(!$user = $api->getUserByToken($token,'Accounts')){
                        array_push($errores,'El usuario no existe');
                }
        }
}
```

Finalmente si el usuario existe, los datos se actualizarán en *SuiteCRM*.

4.3.6 Desarrollo archivo DESCARGA.PHP

Es en este archivo donde se ha desarrollado la descarga de los certificados de donación en .pdf en base a los pagos (módulo *invoices* en *SuiteCRM*) que se vean reflejados en el área privada del colaborador. Si no existen pagos, se recibirá un mensaje informando de que no se ha localizado ningún pago.

Para ello se hace uso de varios campos pertenecientes al módulo de invoices como son el nombre y apellidos, importe de la donación, fecha de la donación, NIF/CIF y código postal del colaborador como mostraba anteriormente en ilustración Ilustración 4.10 **Certificado de donación tipo**.

Para generar el certificado en formato pdf, se hace uso de la clase **dompdf** que se encargará de renderizar de formato html a pdf.

```
use Dompdf\Dompdf;

$dompdf->render();
```

4.3.7 Desarrollo archivo LOGOUT.PHP

El archivo *logout* se encarga como su propio nombre indica de cerrar la sesión de usuario abierta.

```
session_start();
unset($_SESSION['USER']);
```

4.3.8 ¿Cómo se ha integrado el método de autenticación Mobile Connect?

Para poder integrar la tecnología *Mobile Connect* en nuestro portal web ha sido necesario realizar los siguientes pasos:

Se han registrado dos aplicaciones, una en el portal de *GSMA* (https://developer.mobileconnect.io) y la otra en el portal de desarrolladores de *Orange* (https://developer.orange.com).

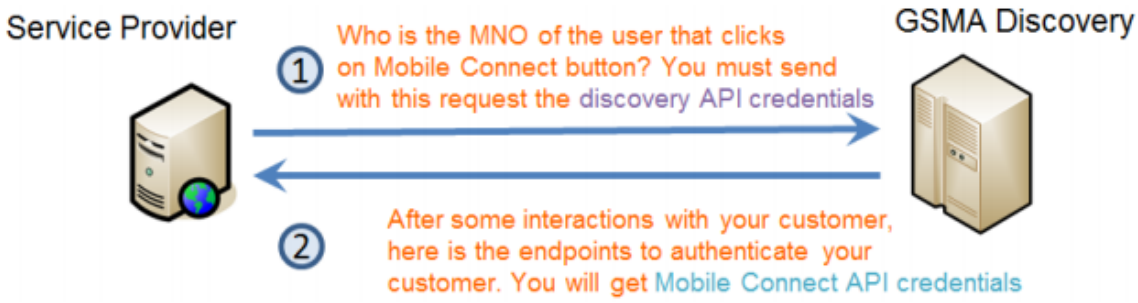

Ilustración 4.23 Petición GSMA Discovery
Fuente. Guía de implementación Mobile Connect (2017)

Una vez realizado el registro de la aplicación dentro del portal de *GSMA*, se queda establecida la dirección URL de la aplicación.

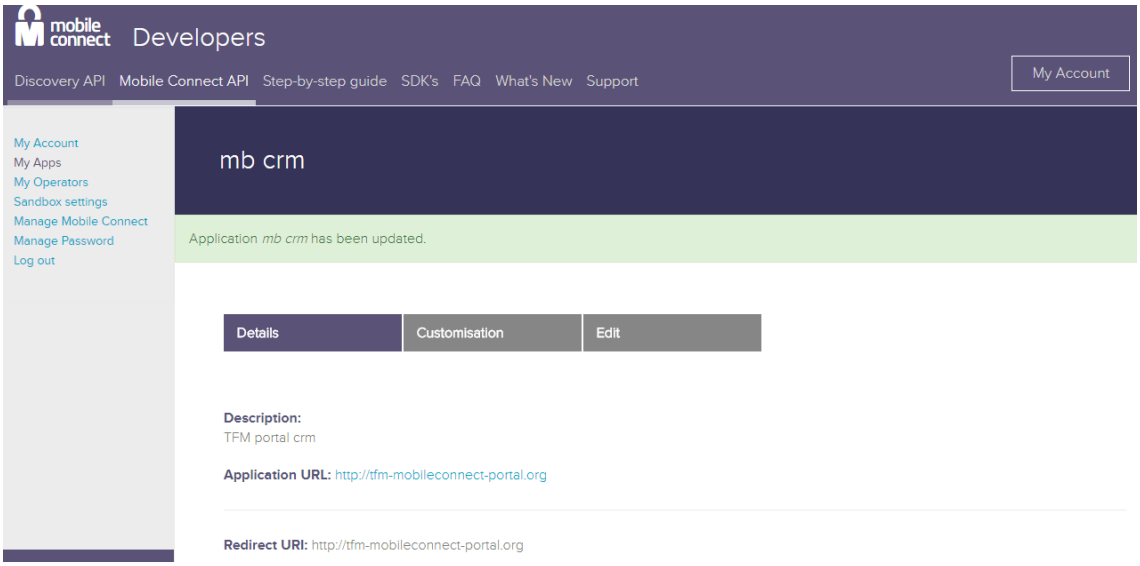

Ilustración 4.24 Registro de la aplicación web dentro de GSMA
Fuente. https://mobileconnect.io/account (2018)

En el portal de desarrolladores de Orange queda realizar los mismos pasos, registrar la aplicación a fin de obtener las credenciales necesarias para poder establecer la conexión correctamente.

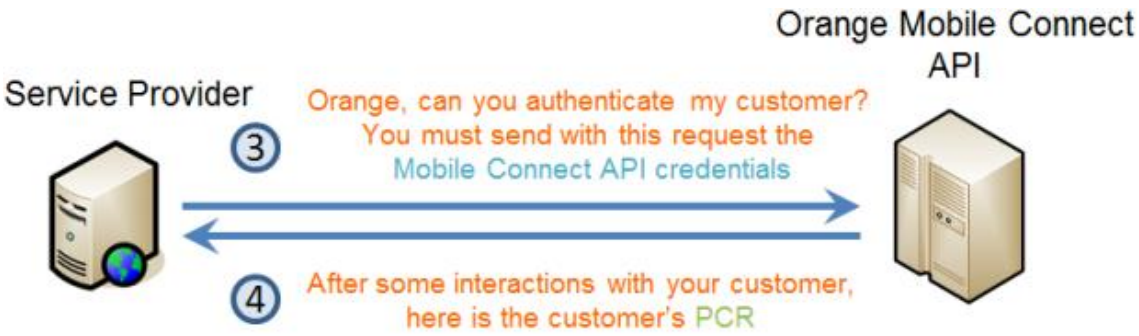

Ilustración 4.25 Petición de autenticación a API Orange Mobile Connect
Fuente. Guía de implementación Mobile Connect (2017)

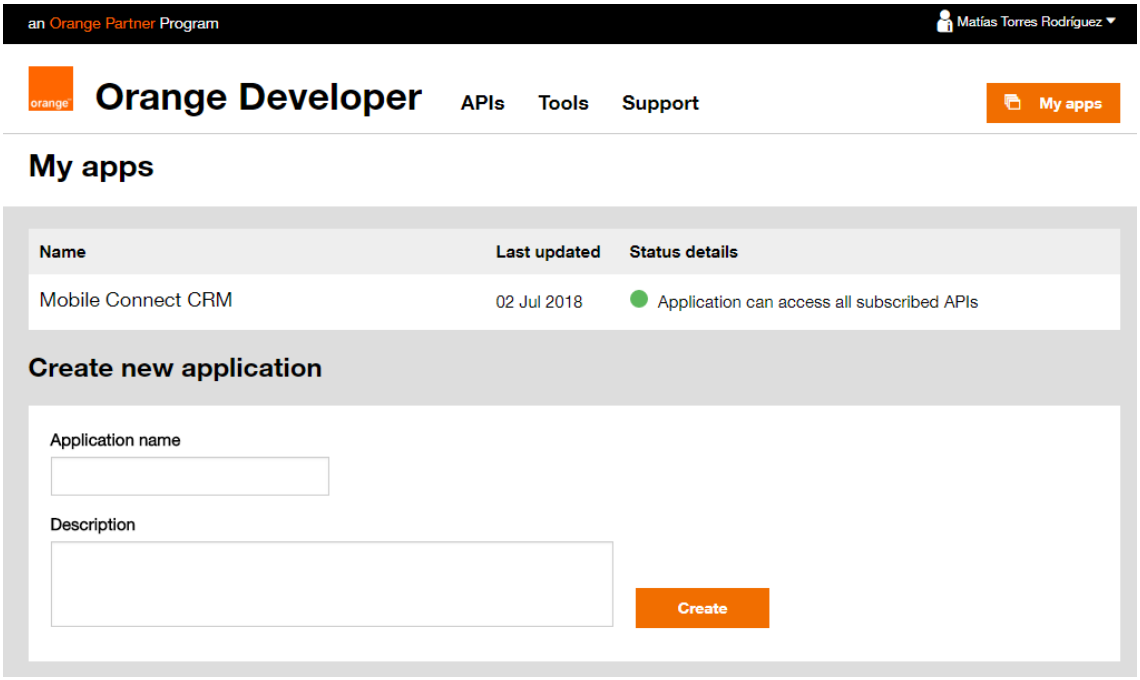

Ilustración 4.26 Mi App Mobile Connect CRM de Orange
Fuente. https://orange.developers.com/myapps (2018)

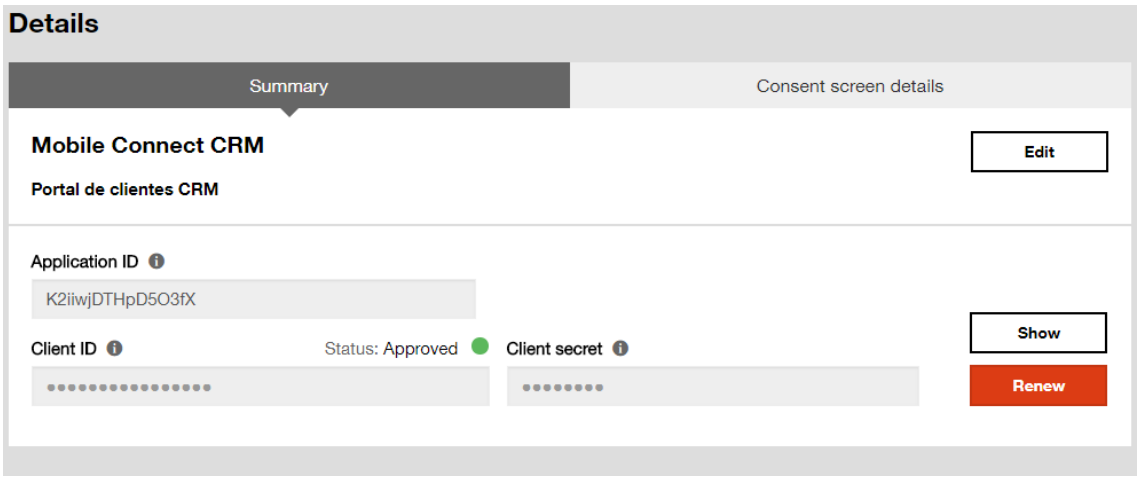

Ilustración 4.27 ID de mi App Orange
Fuente. https://orange.developers.com/myapps (2018)

Tanto el cliente **ID** como el **client secret** serán facilitados automáticamente por *Discovery API* de *GSMA*, lo único que hay que tener en cuenta es no renovarlos para mantener activa la sesión.

Los niveles de seguridad *LoA* van desde 1-4 aunque hay que indicar que solo el 2 es gratuito que es el que he utilizado para el trabajo fin de máster.

El primer punto de esta parte de desarrollo ha sido registrar la dirección de la aplicación web en el portal de Orange y esperar la aceptación de la aplicación por parte de los administradores de Orange.

Una vez tenemos todo aprobado por las partes (GSMA y Orange) se procede a integrar el botón de *Mobile Connect* en nuestra aplicación eligiendo una de las opciones de botón que nos ofrece la propia página *https://mobileconnect.io*.

Una vez el usuario hace clic en el botón de *Mobile Connect*, seguidamente se llamará a la función **StartDiscovery** que tiene la estructura que se muestra a continuación:

```
public function StartDiscovery($msisdn = "", $mcc = "", $mnc = "") {
    $msisdn = $this->input->get('msisdn', true);
    $mcc = $this->input->get('mcc', true);
    $mnc = $this->input->get('mnc', true);

    $response = $this->_mobileConnect->AttemptDiscovery($this->input, $msisdn, $mcc, $mnc, true, new MobileConnectRequestOptions());
    return $this->CreateResponse($response);
}
```

Ilustración 4.28 Función StartDiscovery

Fuente. Guía de implementación Mobile Connect (2017)

Esta función va a descubrir desde nuestra aplicación creada en el portal de *GSMA* los ID mediante una llamada a *DiscoveryURL* con un método POST.

La *GSMA* a continuación devolverá la *DiscoveryURL* para usar con HTTP 302.

A partir de aquí el usuario introducirá su número de teléfono (MSISDN) que se enviará a *GSMA* que nos devolverá **mcc (mobile connect code), mnc (mobile network code)** y **subscriber_id**. Subscriber_id contiene el MSISDN[17] encriptado que se usará para encriptar al colaborador.

Nuevamente se hace una llamada a GSMA discovery desde la parte del usuario con la intención de conseguir los endpoints de la *API Mobile Connect* de Orange y las credenciales de la misma.

Una vez conseguidos los endpoints, subscriber_id y las credenciales, estas se utilizarán para llamar a la *API Mobile Connect* de Orange.

Los endpoints son un punto muy importante de la ciberseguridad, estos son los equipos de usuario finales que deberían estar también protegidos para evitar robos de información.

Tanto el subscriber_id como las credenciales las proporciona el servicio de Orange donde se registró la aplicación.

Llegado este punto nos podemos encontrar con que GSMA nos devuelve algún tipo de error como:

- MSISDN pertenece a un operador que no soporta Mobile Connect con un código de error **404**.
- Invalid_Request, este error se mostraría cuando al realizar una redirección URI esta no se encuentra, el código que se muestra es **400 Bad Request**

En la parte de la *API Mobile Connect* de Orange se llevaría a cabo la autorización de la petición para permitir el acceso al portal web. En la siguiente imagen se muestra el diagrama de caso de uso del proceso:

[17] MSISDN: Mobile Station Integrated Services Digital Network

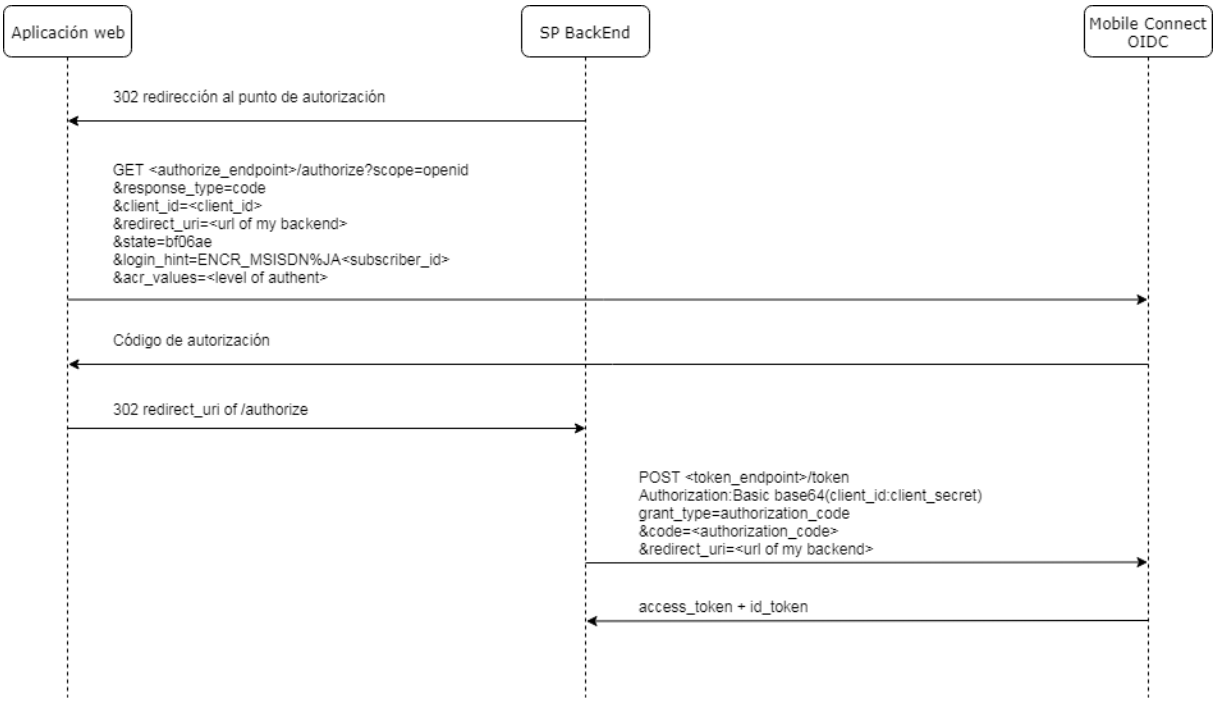

Ilustración 4.29 Autorización Mobile Connect con Portal Web
Fuente. Elaboración propia

Esta parte comenzará diciéndole al navegador del colaborador que haga una llamada para autorizar el endpoint usando una redirección del tipo 302.

Si se produce un error, los siguientes parámetros se añadirían al componente de petición de la redirección URI.

```
"Location:
<redirect_uri>?error=<code>&error_description=<description>&state=<state>"
```

Ilustración 4.30 Error de autorización endpoint
Fuente. Guía de implementación Mobile Connect (2017)

En el caso de que la petición se realice correctamente, *Mobile Connect* devolverá un código de autorización tipo **code = OES-5G52DA64SD64SD6FD62DSZXG**

Posteriormente se realiza la petición del token de acceso y del id_token junto con el código anteriormente obtenido.

Mobile Connect devuelve ambos tokens los cuales son un JWT. "*JWT se trata de un estándar basado en JSON que permiten la propagación de identidad y privilegios*". (*Wikipedia, 2018*).

Finalmente, habrá que leer el payload de id_token. Es necesario coger el segundo segmento de id_token, cada segmento está separado por punto (.).

El valor de PCR (Pseudonymous Customer Reference), es el valor que *Mobile Connect* utiliza para referenciar al usuario final. Se trata del un ID único que siempre representa al usuario.

El valor de amr (Authentication Methods References) claim especifica el método de autenticación y el acr (Authentication Context Class Reference) claim especifica el nivel de seguridad de autenticación. El valor de acr puede ser 2-3 y amr SIM_PIN, OK o SMS OTP.

5 Evaluación de la herramienta

Cuando se realiza la evaluación de un sistema web, lo que realmente se está evaluando es la usabilidad o lo que es lo mismo, la facilidad de uso de la herramienta. *"Usabilidad se refiere a la facilidad con que las personas pueden utilizar una herramienta particular o cualquier otro objeto fabricado por humanos con el fin de alcanzar un objetivo concreto*. (*Wikipedia, 2018)."*

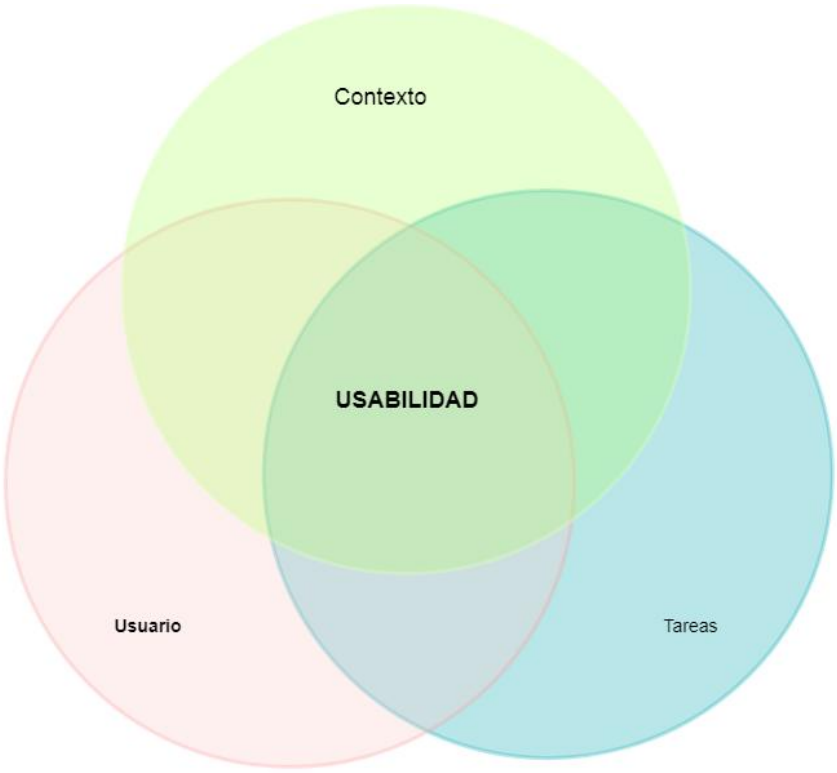

Ilustración 5.1 Representación de las partes esenciales de la usabilidad
Fuente. Elaboración propia

Lo que se pretende en este apartado es detectar errores que deban ser mejorados en cuanto a usabilidad. Hay que señalar que en muchas ocasiones aun habiendo realizado varias evaluaciones, podrían seguir apareciendo errores o fallos. Después de cada evaluación lo más probable es que haya que rediseñar la herramienta con el fin de corregir los fallos detectados, lo que se define como integración continua.

Para llevar a cabo la técnica de integración continua se utilizan Devops que mediante el uso de herramientas, metodologías y prácticas buscan poder adaptarse de forma ágil, seguro y eficiente a un cambio en el sector.

Dentro de los distintos métodos que pueden existir para evaluar la herramienta, yo voy a escoger la evaluación con usuarios, y para ello he escogido a cuatro personas de mi entorno con perfiles distintos como son un colaborador real de una organización, otro usuario que no colabora con entidades no lucrativas, un informático y un último perfil con poca experiencia en tecnología. La evaluación consiste en probar la herramienta y devolver un feedback de su experiencia con respecto a la usabilidad y seguridad del desarrollo. Para ello he preparado varias preguntas que me ayudarán a obtener las posibles mejoras.

Los perfiles de usuario quedan definidos por las siguientes etiquetas:

- Colaborador real: [Colaborador]
- Informático: [Informático]
- Usuario normal no colaborador: [Usuario]
- Usuario poco frecuente no colaborador: [Inexperto]

5.1 Cuestionario a los usuarios

¿Te ha resultado fácil y clara la navegación por la página web de la organización?

Colaborador: me ha resultado tanto fácil como clara, se observa rápidamente donde se encuentra cada sección que quería encontrar.

Informático: muy sencilla la página web. Al ser un piloto obviamente el contenido no es amplio pero la usabilidad bastante buena.

Usuario: la página web es muy fácil de seguir y el menú superior también muy visible.

Inexperto: se entiende todo correctamente, es fácil de leer y seguir.

¿Has llegado al portal de colaboradores de forma rápida?

Colaborador: sí, se visualiza rápidamente en la parte superior de la página web, muchas organizaciones lo ponen en la parte superior derecha.

Informático: sí, al estar en la parte superior se ve nada más entrar.

Usuario: sí, nada más acceder a la página web he visto que tenía la opción del portal en la parte superior.

Inexperto: sí, es lo primero que he visto nada más entrar a la página web.

Una vez entraste al área privada, ¿tenías claro cómo registrarte e introducir tus datos?

Colaborador: muy sencillo, simplemente recibir el correo electrónico para después registrar la contraseña. Nada más entrar tienes toda la información personal a introducir o modificar si es necesario. Me ha encantado poder descargar los certificados de donación tan sencillo.

Informático: no hay mucho que objetar, el proceso típico de registro y al acceder todo está súper claro y sencillo.

Usuario: sí, la forma de registrarse parece la normal que se usa en otros portales, una vez dentro simplemente rellenar los campos que se piden, aunque no son obligatorios. Luego en la parte de certificados (aunque no se para que sirven), es simplemente pulsar en el icono de descargar, resulta fácil.

Inexperto: para registrarme me parece complicado tener que ir al correo electrónico para meter la contraseña nueva, me resultaría más fácil hacerlo todo desde la página web. Después de registrarme, acceder ya me parece mucho más sencillo e intuitivo.

¿Te ha resultado sencillo acceder con autenticación Mobile Connect?

Colaborador: sin duda me ha resultado sencillo y algo novedoso, no sabía de esta posibilidad y sobretodo me encanta que no necesite usuario y contraseña.

Informático: no había escuchado sobre esta tecnología, no tengo un proveedor de servicios que me permita acceder con Mobile Connect, pero en la demostración hecha me parece un proceso sencillo, me encanta.

Usuario: he accedido al portal con Mobile Connect y aún sin saber cómo funcionaba, su sencillez me parece un punto muy a favor que invita a entrar y probarlo.

Inexperto: no puedo entrar con mi teléfono móvil, pero entrar con este método como me has enseñado, hace que sin dudo me decante por entrar con Mobile Connect en vez de usuario y contraseña. Estas tecnologías acercan a personas que no están tan familiarizadas con la informática a desenvolverse mejor.

En cuanto al proceso de acceso, ¿te ha resultado un proceso seguro?

Colaborador: totalmente seguro, a menos que me roben el teléfono móvil no encuentro otra forma para que alguien pueda acceder y hacerse con mis datos personales. Por sencillez, transparencia y seguridad sería un motivo para continuar colaborando.

Informático: sí, es un proceso seguro ya que utilizar los factores como son algo que conocemos y algo que poseemos. La fuerza bruta para adivinar la contraseña no es una vía de intrusión. El robo del terminal sería facilitaría el acceso a todos los portales en los que estuviera registrado, si debería elevar la seguridad introduciendo un código.

Usuario: súper seguro, además de cómodo el hecho de tener que poseer mi teléfono móvil para poder entrar aporta la confianza de que nadie más que yo puede acceder a mis datos personales.

Inexperto: sí, me gusta mucho que se piense en las personas que no tenemos facilidad para la tecnología. Solo metiendo mi número de teléfono y aceptando en mi móvil puedo entrar, lo veo muy seguro.

¿Has tenido dificultad para descargar el certificado de donación?

Colaborador: no, la descarga es muy simple. Disponer de los certificados en todo momento me da confianza.

Informático: ninguna, es un proceso muy sencillo.

Usuario: para nada, no existe bajo mi punto de vista dificultad alguna.

Inexperto: no, se observa claramente el icono de descarga, me ha resultado fácil.

La sencillez y seguridad de la aplicación, ¿invita a colaborar / seguir colaborando con la organización?

Colaborador: Sin duda alguna, me inspira confianza saber que puedo acceder a mis datos en cualquier momento y tan sencillo. Colaboraría mientras mis posibilidades me lo permitieran.

Informático: Claramente ofrece agilidad a un proceso de intercambio de información que a veces puede ser pesado, esto es un plus que invita a colaborar.

Usuario: cuando una organización te ofrece la oportunidad de poder gestionar tus propios datos, hace que el nivel de confianza aumente. Si además el proceso de acceso a la plataforma es simple, incentiva que la relación entre los colaboradores y la organización sea más duradera.

Inexperto: en mi caso me gusta que sea simple llegar a mi información. Creo que así se ha pensado en todos los perfiles de colaboradores y por lo tanto sí colaboraría en este caso.

5.2 Resolución del problema inicial

Recordando el problema inicial, teníamos que para el tercer sector, es decir, el sector no lucrativo las formas de recaudar fondos son mediante donaciones de particulares y empresas privadas.

Para todas las organizaciones no lucrativas pequeñas y medianas, el acceso de sus colaboradores a su información privada es un proceso largo y pesado, donde estos pueden terminar frustrándose y abandonando la colaboración. En este sector, un aspecto importante es la fidelización de los colaboradores, y sin duda este trabajo contribuye a que sigan colaborando durante largos periodos de tiempo.

Dentro de la necesidad de los colaboradores por acceder a sus datos personales incluye la obtención de un certificado de donación que lo certifica como donante de la organización. La necesidad de ingresar nuevos datos, actualizar otros ya existentes, eliminarlos y pedir la cancelación de la colaboración se suele hacer a través de contacto telefónico o mediante correo electrónico.

Ahora, con el uso del portal web cuyo dominio estaría protegido con un certificado de seguridad SSL (protocolo https) y el acceso al mismo mediante *Mobile Connect*, se añade un extra de seguridad y agilidad en el proceso de acceso a la información personal.

Los colaboradores pueden ver toda su información en dos simples pasos y sin la necesidad de escribir un correo electrónico o llamar a la organización, y lo que es más importante, sin esperas y con la sensación de que el lugar al que están accediendo es un lugar seguro y transparente donde sus datos están accesibles y a salvo en cualquier momento.

6 Conclusiones y propuesta de futuro

Una vez que se ha concluido la elaboración del trabajo, es el momento de reflexionar sobre el desarrollo realizado.

En el presente trabajo fin de máster, lo que se ha pretendido es aplicar conocimientos aprendidos durante el curso a un caso práctico. Para ello, en un principio lo que se ha realizado es profundizar en los distintos métodos de autenticación, los ataques a los que están expuestos y cómo *Mobile Connect* podría mitigarlos. También he hablado de las distintas opciones de sistemas CRM *Open Sou*rce que existen ya que son las que la mayoría de las organizaciones sin ánimo de lucro utilizan y he hecho hincapié en el cumplimiento del nuevo reglamento general de protección donde los derechos de los afectados deben cumplirse y se cumplen en este desarrollo.

Como ya comentaba a lo largo del desarrollo del trabajo, mantener una buena relación entre la organización y sus colaboradores es fundamental para que estos últimos mantengan su aportación económica durante un largo periodo de tiempo. Los sistemas CRM proporcionan a la organización gran cantidad de información que los trabajadores deberán interpretar, pero la parte más importante es proporcionar a los colaboradores un área privada donde accedan a su información personal de la forma más ágil y segura posible, en este caso usando *Mobile Connect*.

El sistema CRM que suelen utilizar las organizaciones no lucrativas es tanto *SugarCRM* como *SuiteCRM* por la gran cantidad de funcionalidades que ofrecen. Yo he elegido finalmente *SuiteCRM* ya que es un proyecto que cuenta con un equipo de desarrolladores en activo, al contrario que *SugarCRM* que se encuentra en una vía muerta.

El portal web desarrollado, y que es el pilar más importante del trabajo está integrada con *SuiteCRM* mediante una API Rest que es común para integrar la mayoría de los sistemas CRM con cualquier aplicación web, cuyo objetivo principal es agilizar y securizar el proceso de acceso a información personal.

En cuanto a su utilidad, como hemos podido destacar y comprobar de forma práctica, el portal web es clave para mantener y fidelizar a los colaboradores con un acceso rápido y de confianza mediante *Mobile Connect*, mostrando al mismo tiempo la sensación de seguridad.

Así, en la actualidad, este método de autenticación *Mobile Connect* conforma uno de los métodos de autenticación más ágiles sin necesidad de recordar usuario y contraseña que favorece la interacción entre organización y colaboradores.

Para llegar a esta conclusión, me he apoyado en mi experiencia en el sector, y es que por cada nuevo proceso que se introduce entre el colaborador y la organización, bien sea para realizar una donación o para comunicar cualquier cambio en el tipo de colaboración, se pierden más del 50% de los colaboradores, siendo este uno de los objetivos a cubrir en este trabajo, facilitar el intercambio de información entre las partes y fidelizar a los colaboradores.

Tras finalizar la parte más teórica, comenzamos a desarrollar el enfoque práctico. Para ello, lo primero que se hizo fue recopilar información sobre *SuiteCRM*, ver los módulos que de los que está compuesto, sus campos y etiquetas que serían necesarios para la integración con el portal web. Para esto he consultado foros de desarrolladores de la herramienta.

La información introducida en *SuiteCRM* ha sido inventada simulando lo que sería la información personal de un colaborador y sus donaciones realizadas, información que mediante la API Rest se mostrará en el portal web del colaborador.

Por último, una vez conocidas las necesidades que quería cubrir, comencé el desarrollo de la aplicación web mediante lenguaje *php* hasta conseguir la funcionalidad deseada. También he contratado un servidor web y dos dominios donde se alojarán tanto la herramienta CRM como la página web corporativa.

En resumen, pienso que el resultado obtenido ha sido muy satisfactorio, destacando que se han cumplido los objetivos inicialmente marcados, siguiendo paso a paso cada uno de ellos.

A continuación, se muestra el grado de cumplimiento de los objetivos marcados al inicio de este proyecto:

Para dar cumplimiento al objetivo [O1] hice un desarrollo teórico de la tecnología empleada como método de autenticación Mobile Connect, otros métodos de autenticación conocidos y, cuáles son los ataques a los que están expuestos y como mitigarlos.

"Definición de los distintos métodos de autenticación, tipos de ataques que le pueden afectar y cómo *Mobile Connect* puede mitigarlos"

Se han descrito los métodos de autenticación que existen. En una tabla he resumido los ataques posibles sobre la autenticación y cómo *Mobile Connect* puede mitigarlos. Tabla 2.2 **Ataques y mitigación con Mobile Connect**

"Aproximación teórica al concepto *Mobile Connect y Sistema de Gestión de los Clientes (CRM)*".

Para la aproximación al concepto, he desarrollado un capítulo recogiendo los aspectos más importantes de los mismos. Capítulo 2.7 **GSMA y la tecnología Mobile Connect**

"Descripción de las partes implicadas en la conexión como son el proveedor de servicios de telefonía móvil y *GSMA*"

He descrito los agentes que forman parte de la autenticación y los factores de los que depende la tecnología Mobile Connect para una autenticación exitosa. Capítulo 2.7.7 **¿Qué son los autenticadores?**

Tras realizar una entrevista a cuatro usuarios todos ellos con un perfil diferente, se contestaron a una serie de preguntas en cuanto a usabilidad, agilidad y, confianza y seguridad al facilitar sus datos personales, que dan una idea de la mejora que supone para el sector y la relación con sus colaboradores. Capítulo 5.1 **Cuestionario a los usuarios**

"Entrevista a los siguientes perfiles: colaborador, informático, usuario habitual y usuario poco habitual"

Finalmente he diseñado un caso práctico, diseñando una página web corporativa ficticia con un portal web para los colaboradores usando autenticación *Mobile Connect* y usuario y contraseña, además de la opción de registro.

Para dar respuesta al objetivo [O2], el portal web desarrollado ofrece a los colaboradores mayor facilidad para acceder a sus datos y ejercer sus derechos sobre los mismos según indica el nuevo reglamento de protección de datos RGPD.

En el apartado 2.1 **Ley Orgánica de Protección de datos (LOPD) y Reglamento General de Protección de datos (RGPD)** , he descrito cuáles son los derechos que tienen los afectados y cómo con la herramienta desarrollada pueden ejercer cada uno de ellos en cualquier momento.

Para dar respuesta al objetivo [O3], dentro del portal web existe una sección donde el colaborador puede visualizar todas sus aportaciones económicas a la fundación y con un simple clic descargar su correspondiente certificado de donación.

El certificado de donación se descarga en formato PDF y firmado para que su modificación sea más complicada.

En cuanto al *software* seleccionado para la parte de la organización he elegido *SuiteCRM*. *SuiteCRM* como ya se ha comentado en anteriores capítulos, es un *software* de código

abierto por lo que gracias a ello me ha permitido reducir el coste *software* del proyecto. Es el software que la gran mayoría de las organizaciones en el tercer sector.

En resumen, el resultado de este TFM es una Aplicación Web integrada con el *Sistema de Gestión de las Relaciones con los Clientes (CRM)* que ayudará a la organización a mantener a sus colaboradores activos durante más tiempo debido a su agilidad usando la tecnología d autenticación *Mobile Connect* y que facilitará el trabajo a los empleados de la organización debido al intercambio de información diario con los colaboradores y la emisión de los certificados de donación de los mismos.

En cuanto a las conclusiones que se pueden extraer, hay que destacar:

- Las organizaciones deben hacer uso de métodos que faciliten cualquier operación a los colaboradores para que estos se mantengan activos durante más tiempo.
- El uso de tecnología *Mobile Connect* aumenta la agilidad en el proceso de autenticación y mejora la confianza de los usuarios en cuanto a seguridad.
- Poner un portal web a disposición de los colaboradores donde puedan ver su información privada, mejora las relaciones y disminuye la carga de trabajo para la organización.
- La opción de que los propios colaboradores puedan acceder, rectificar, cancelar y oponerse además de posibilitar la limitación del tratamiento, derecho al olvido y portabilidad de sus datos, da cumplimiento al nuevo reglamento general de protección de datos de reciente entrada en vigor.
- Al usar casi todas las organizaciones del sector el mismo tipo de software *Open Source CRM*, la integración del portal desarrollado se estandariza para todo el sector.

Como mejora de este desarrollo, sería de gran avance poder añadir una nueva combinación de factores al método de autenticación *Mobile Connect.*

Idealmente una combinación de acceso mediante *Mobile Connect* con el factor biométrico hace que la seguridad en el acceso se multiplique ante la probabilidad de que nuestro terminal móvil sea sustraído o alguien consiguiera un duplicado de la tarjeta SIM de nuestro teléfono mediante técnicas de ingeniería social.

El acceso combinado con nuestra huella dactilar por ejemplo es algo que difícilmente se pueda robar.

Por otro lado, sería interesante utilizar *Mobile Connect* en otras vías de colaboración para colaboradores recurrentes como, rellenar un formulario de datos personales que permitan

realizar donaciones sin necesidad de introducir la información cada vez que se accede al formulario, lo que mejoraría el tedioso proceso de rellenar los formularios todo el tiempo.

También, conectar la solución realizada a *Blockchain*[18] sería interesante para la parte de obtención del certificado de donación mencionado. El certificado quedaría registrado y cifrado con una huella digital única y que puede ser comprobado en cualquier momento accediendo a un enlace proporcionado.

Finalmente, las organizaciones podrían hacer uso de *Mobile Connect* como método de autenticación para acceder a la herramienta CRM por parte de los empleados.

[18] Blockchain: estructura de datos en bloques formando una cadena y cuyo bloque contiene metainformación de los bloques anteriores.

7 Bibligrafía

Wikipedia (2018): Definición de Autenticación. Disponible en: https://es.wikipedia.org/wiki/Autenticaci%C3%B3n. [Consultado 21-04-2018]

Eset (2017): Origen de la contraseña. Disponible en: https://www.welivesecurity.com/la-es/2017/05/04/dia-de-la-contrasena-origen/. [Consultado 22-04-2018]

Eset (2014): Amenazas contra las contraseñas. Disponible en: https://www.welivesecurity.com/la-es/2014/08/14/amenazas-atentan-contra-contrasenas/. [Consultado 22-04-2018]

Hipertextual (2014): Qué es un ataque Man In The Middle. Disponible en: https://hipertextual.com/archivo/2014/06/ataque-man-in-the-middle/ [Consultado 15-09-2018]

Wikipedia (2018): Ataque de intermediario. Disponible en: https://es.wikipedia.org/wiki/Ataque_de_intermediario [Consultado 15-09-2018]

Wikipedia (2018): JSON Web Token. Disponible en: https://es.wikipedia.org/wiki/JSON_Web_Token [Consultado 15-09-2018]

Xataka (2013): Autenticación en dos pasos. Disponible en: https://www.xataka.com/seguridad/autenticacion-en-dos-pasos-que-es-como-funciona-y-por-que-deberias-activarla. [Consultado 27-04-2018]

OSI (2017): Verificación en dos pasos. Disponible en: https://www.osi.es/es/actualidad/blog/2017/01/17/verificacion-en-dos-pasos-que-es-y-como-me-puede-ayudar. [Consultado 04-05-2018]

Security Advisor (2016): Vulnerabilidades encontradas. Disponible en: http://www.sadvisor.com/ar/2016/10/21/con-que-vulnerabilidades-nos-estamos-encontrando/. [Consultado 05-05-2018]

Underc0de (2014): Ataques de autenticación. Disponible en: https://underc0de.org/foro/hacking/ataques-de-autenticacion/. [Consultado 07-05-2018]

EcuRed (2018): Ataque de autenticación. Disponible en: https://www.ecured.cu/Ataque_de_autenticaci%C3%B3n. [Consultado 07-05-2018]

Blog Micayael (2011): Método GET frente a POST. Disponible en: http://blog.micayael.com/2011/02/09/metodos-get-vs-post-del-http/. [Consultado 15-05-2018]

Junta de Andalucía (Sin fecha de publicación): Autenticación y autorización. Disponible en: http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.1/contenido-libro-pautas-110.html. [Consultado 21-05-2018]

GCN (2013): Niveles de autenticación. Disponible en: https://gcn.com/Articles/2013/02/12/4-levels-mobile-authentication.aspx. [Consultado 21-05-2018]

ElevenPaths (2015): Mobile Connect: el nuevo estándar en autenticación digital. Disponible en: http://blog.elevenpaths.com/2015/09/mobile-connect-el-nuevo-estandar-en.html. [Consultado 25-05-2018]

Mobile Connect Developers (2017): Implementación Mobile Connect. Disponible en: https://developer.mobileconnect.io. [Consultado 02-06-2018]

Orange Developers (2017): Programa de desarrollo de Orange. Disponible en: https://developer.orange.com. [Consultado 16-06-2018]

Blog de Silvia Barrera (2018): El ataque a Telegram muestra que la verificación en dos pasos también es vulnerable. Disponible en: https://sbarrera.es/el-ataque-a-telegram-muestra-que-la-verificacion-en-dos-pasos-tambien-es-vulnerable/. [Consultado 15-07-2018].

AEPD (2016): Guía del reglamento general de protección de datos. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf. [Consultado 16-07-2018].

El Derecho.com (2018): El reglamento UE sobre protección de datos. Disponible en: https://www.elderecho.com/tribuna/civil/Reglamento-UE-Proteccion-Datos-Comunidades-Propietarios_11_1232305005.html. [Consultado 16-07-2018].

UNIR (2017): Temario asignatura Aspectos Legales y Regulatorios. Disponible en: https://campusvirtual.unir.net. [Consultado 17-07-2018].

Openbiz (2009): Definición de Open Source. Disponible en: http://www.openbiz.com.ar/Open%20Source.pdf. [Consultado 18-07-2018].

Vtiger: La empresa y su negocio CRM. Disponible en: http://www.vtiger.com. [Consultado 29-07-2018].

SugarCRM: La empresa y su negocio CRM. Disponible en: http://www.sugarcrm.com. [Consultado 29-07-2018].

SuiteCRm: La empresa y su negocio CRM. Disponible en: https://www.suitecrm.com. [Consultado 29-07-2018].

OroCRM: La empresa y su negocio CRM. Disponible en: https://oroinc.com/orocrm/. [Consultado 29-07-2018].

Delibarr ERP & CRM: La empresa y su negocio CRM. Disponible en: https://www.dolibarr.org/ . [Consultado 29-07-2018].

Fat Free CRM: La empresa y su negocio CRM. Disponible en: http://www.fatfreecrm.com/ . [Consultado 29-07-2018].

Grupo Ático34: Protección de datos. Disponible en: https://protecciondatos-lopd.com/empresas/derechos-arco-que-son/. [Consultado 22/08/2018].

Smart Insights: Ecommerce conversion funnel. Disponible en: https://www.smartinsights.com/ecommerce/ecommerce-analytics/ecommerce-conversion-rates/ [Consultado 18/09/2018]

Mr. Benchmarks: BenchMarks 2018. Disponible en: https://mrbenchmarks.com/# [Consultado 18/09/2018]