2023

Trabajo Fin de Grado

DEMO ITERACCIÓN LOGS EN QRADAR

HENAR ALCOLEA LOPEZ

Tutor Centro Educativo: Carlos Rufiangel Garcia
Tutor Centro Trabajo: Alejandro Castaneyra

Intencionadamente en blanco

Resumen

Trabajo de Fin de Grado presentado en el centro de estudios superiores profesionales IMF, con prácticas realizadas en el centro de trabajo Deloitte, en la parte de Ciberseguridad para la obtención del título de formación profesional superior en Desarrollo de Aplicaciones Web.

El TFG está basado en la combinación de los conocimientos obtenidos en el grado superior de desarrollo web, así como en las prácticas realizadas en la parte de Ciberseguridad.

Se presenta una maqueta realizada, íntegramente por la alumna Henar Alcolea López, tanto en la parte front como back end, de un sistema de gestión de logs en el entorno Qradar.

Abstract

Final degree Project submitted at Higher Education Centre IMF, based on a project done in a workplace, Deloitte in his cybersecurity centre. To have access to academic degree “Web development application”.

This final degree Project is based on merge academic knowledge and work experience obtained in Deloitte cybersecurity centre.

The presentation is about an mock-up of log management done 100%, front and back end by Henar Alcolea López student.

Agradecimientos

En primer lugar, dedicar este TFG a mi Hermana quien ha sido mi referente en muchos aspectos de la vida , pero sobre todo en el mundo IT. Ella me hizo ver este mundo desde dentro, en todos sus puntos, desde el punto inicial, el académico, como toda la progresión laboral que se pueda desarrollar, incluyendo el aplicar los conocimientos y experiencia a la docencia. Sin ella, mi trayectoria hubiera sido muy diferente.

En segundo lugar, aunque dentro del primer puesto, están y siempre estarán, mis padres. Ellos son el motor que me impulsa cada día, mi gran apoyo.

Carlos Rufiangel Garcia, no necesita puesto, ni presentación. Es bien conocido entre todos los alumnos y docentes del centro de estudios. No es de extrañar, pues su entrega, dedicación y sus grandes dotes docentes, superan cualquier expectativa que se pueda tener ante un tutor. Carlos ha estado a mi lado en las asignaturas con mayor carga académica durante los dos años de estudio, además de tener la suerte de ser mi tutor para este TFG.

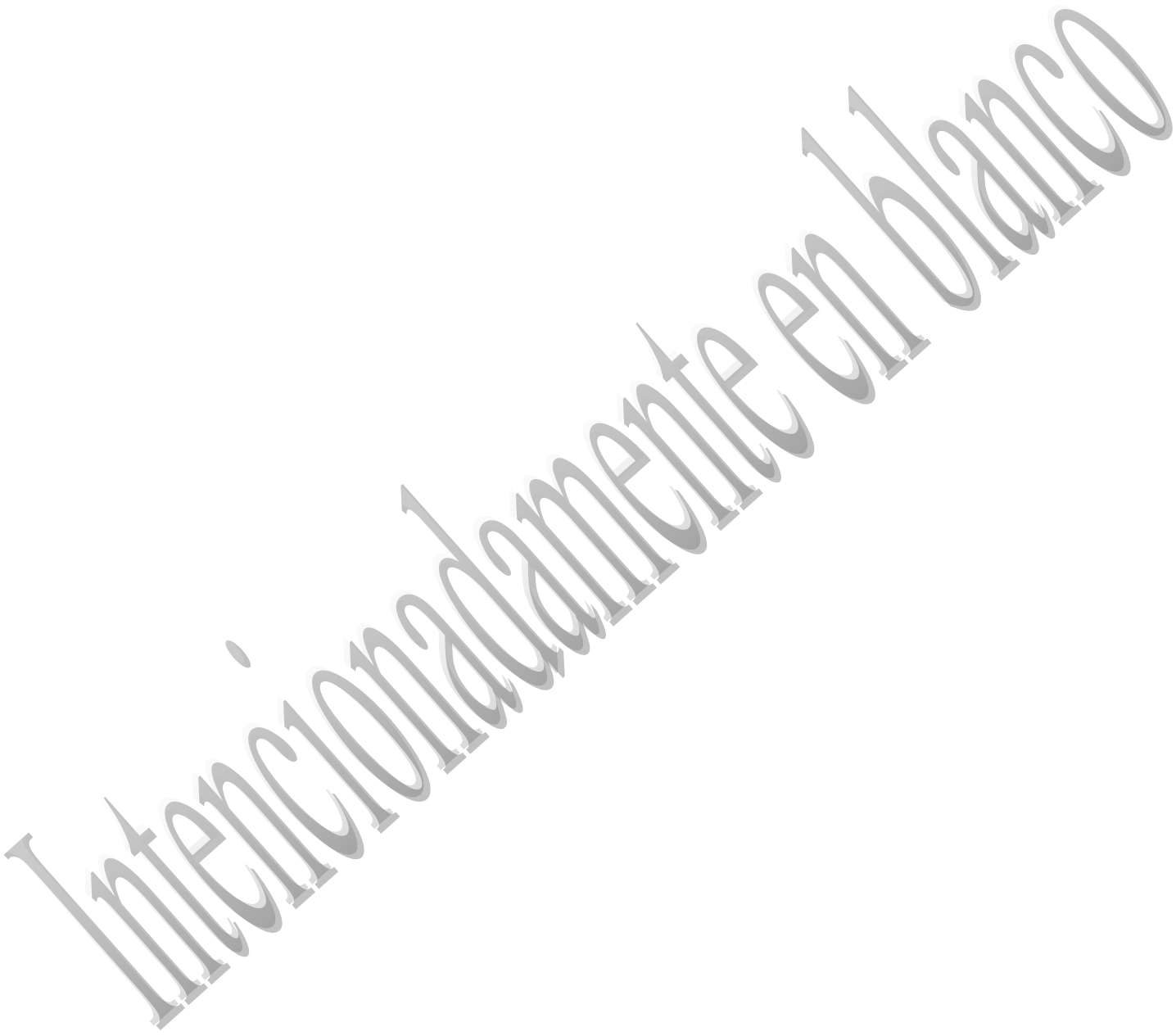
Mi mayor agradecimiento a Carlos es el saber sacar de mi el máximo, cuando sentía que no podía más, que no llegaba, él sabía tirar de mí, para obtener los mejores resultados posibles. Gracias por esas tutorías, donde sin yo saberlo, en ese momento, me estabas levantando y mejorando.

Último, pero no menos importante a mi tutor en las prácticas, Alejandro Castaneyra. Gracias a él, he descubierto el apasionante mundo de la ciberseguridad. Alejandro me ha ayudado y ha estado pendiente en todo momento de mi progreso, también me ha motivado para continuar en su increíble equipo.

Nota: Para evitar que el TFG sea secreto y mantener los datos de la empresa a salvo, se usará un nombre genérico para la empresa a la cual se les realizó este proyecto, llamándolos "cliente".

Puede que algunos nombres y configuraciones se vean modificados con el fin de mantener la confidencialidad de los datos y el proyecto.

Índice


Intencionadamente en blanco

Capítulo 1. Introducción

1.1 Motivación

El crecimiento de las conexiones a internet se ha visto incrementado de manera exponencial. Esto supone una exposición masiva de los usuarios a potenciales ataques, debido a las vulnerabilidades de los cientos de protocolos, aplicaciones e incluso a las producidas por fallos humanos.

Actualmente, la integración de las tecnologías, en todos sus ámbitos dentro de las empresas está en aumento. En esta misma línea, crecen los delincuentes informáticos que poseen máquinas y herramientas cada vez más capaces.

Es por esto, por lo que, la ciberseguridad es una pieza fundamental en cualquier empresa.

Debido a estos factores, la motivación de este proyecto es mostrar, en pequeña escala, la gestión de los reportes que llegan a una empresa dedicada a la ciberseguridad.

1.2 Objetivos

La importancia actual de los sistemas de seguridad que permitan proteger equipos y redes corporativas enteras se hace cada vez más evidente, a medida que cada vez la información más relevante está expuesta, y que el número de ataques, así como su sofisticación aumenta.

Así pues, dada la importancia de desarrollar herramientas de ciberseguridad, resulta imprescindible que los titulados en todas las ramas de tecnologías de la información tengan la máxima preparación disponible para que puedan trabajar de acuerdo con las mejores prácticas posibles, limitando la exposición tanto a nivel corporativo como personal.

Por estos motivos, el objetivo final de este TFG es juntar en un solo proyecto las competencias, nivel desarrollo web obtenidas en el grado superior con las tareas realizadas en la parte de ciberseguridad en las prácticas de dicho grado superior.

1.3 Justificación del proyecto

Como bien se ha desarrollado en los puntos anteriores, la ciberseguridad es una rama sumamente importante para todo aquel que esté en contacto con redes, más aún a nivel empresarial. Pues un ataque cibernético causaría una merma, no solo económica a la empresa afectada, sino a nivel de confianza para sus clientes y los datos almacenados que pudieran verse afectados.

Cierto es que, a pesar del valor que tiene la protección de datos, no se imparte en el módulo estudiado.

Es por esto que, la gran causa de la realización de este proyecto sea, ya no solo mostrar la importancia de tener conocimientos en ciberseguridad, sino que un técnico no especializado ni titulado en ciberseguridad, pero sí con manejo cotidiano de datos altamente sensibles en sus labores profesionales, pueda desarrollar un sistema/ programa para la protección de estos datos que maneja.

1.4 Conclusión

En relación con lo antes expuesto, podríamos finalizar este apartado resumiendo que el titulado en Desarrollo de aplicaciones web, obtiene una polivalencia importante, pues es capaz de manejar y proteger datos altamente significativos, tanto para una empresa como para su cliente.

1.5 Estructura de la memoria

1.2.1 Capítulo 1 Introducción

Se presenta un contexto para comprender la situación actual relativa a el área de ciberseguridad, haciendo hincapié en la importancia que tiene en relación con el grado superior, aun no siendo objeto de estudio ni evaluación en dicho grado.
Además, se presenta una motivación al desarrollo y estudio del presente trabajo, así como también una presentación de los objetivos.
Se da también un apartado en el cual se especifica la estructura del documento.

1.2.2 Capítulo 2. Desarrollo

Sirve para introducir, de manera breve y a modo de contextualización, todas las tecnologías que guardan una relación directa con el presente trabajo.

1.2.3 Capítulo 3. Exposición

Mostraremos el funcionamiento del proyecto realizado, mediante capturas de pantalla, casos de uso y control de errores.

1.2.4 Capítulo 4. Especificaciones

En este capítulo se pretende describir las especificaciones y restricciones (funcionales y no funcionales) del proyecto que se va a desarrollar.

1.2.5 Capítulo 5. Metodología

Se expone y desarrolla la metodología empleada para la elaboración de este proyecto.

1.2.6 Capítulo 6. Implementación

Breve resumen de las tecnologías utilizadas y empleadas en el proyecto.

1.2.7 Capítulo 7. Referencias

Se muestran las referencias utilizadas para la elaboración del proyecto, tanto código como memoria.

1.2.8 Capítulo 8. Conclusiones

Resumen y conclusiones finales del proyecto.

Capítulo 2. Desarrollo

2.1 Contexto

Como bien se ha detallado en la introducción, el mundo IT (Information Technology) está en constante crecimiento y esto genera un crecimiento de los activos a proteger por la seguridad informática de una empresa.

La ciberseguridad es un área de análisis de alto rendimiento y en tiempo real que puede ser fundamental para la toma de decisiones, ya que los ataques se cometen cada vez con más frecuencia y en menos tiempo. Surgen amenazas nuevas todos los días.

En combinación con técnicas de analítica predictiva, se podrían identificar patrones y tendencias de comportamiento, lo que otorga la capacidad de anticiparse a multitud de ataques, que están caracterizados por ser relativamente aleatorios, espontáneos y fuera de lo común.

El software que normalmente se utiliza para analizar la información relacionada con los eventos de seguridad en una organización (SOC) se llama Security Intelligence and Event Management (SIEM).

Un **SOC** (Security Operation Center) es un equipo que monitoriza y analiza comportamientos extraños y amenazas, con el objetivo de detectarlas, y dado el caso de detección correcta, tiene la potestad de pedir o realizar acciones contraofensivas.

Un **SIEM** (Security Information and Event Management) es un sistema centralizado que se encarga del almacenamiento y la interpretación de los datos relevantes en un entorno de seguridad informática. Estos datos son transmitidos por medio de mensajes llamados ‘logs’. El SIEM es el “el cerebro” capaz de correlar distintos eventos y extraer así información útil para el SOC.

El software SIEM recibe alertas de seguridad en tiempo real de aplicaciones de software (tanto en la red como en la nube) y equipos de redes inteligentes. Estos sistemas permiten almacenar y analizar la información obtenida a partir de eventos de seguridad (logs) originados a partir de los datos que se van registrando desde diferentes fuentes.

2.2 Elección SIEM

Hay una amplia variedad de SIEM en el mercado, tanto de pago como SIEMs gratuitos.

En la empresa donde se realizaron las prácticas del grado superior, hacían uso tanto de Splunk, como de ArcSight, sin embargo, el SIEM elegido es Qradar, ya que fue en este SIEM donde se desarrollaron la mayor parte de las tareas realizada en las prácticas.

2.3 Qradar

Primero explicaremos las funciones que realiza el SIEM Qradar, para posteriormente ahondar en las distintas arquitecturas disponibles y saber la adecuada para el entorno de trabajo del cliente

2.3.1 Funciones Qradar

- Collector and parser: esta función es la que se encarga de recoger los logs y "parsearlos", esto es, analizar sintácticamente, ordenar y clasificar la información de los logs que llegan al Qradar como texto o JSON de las distintas fuentes y darles una estructura para almacenarlas e indexarlas de forma eficiente.

- Correlator: Es la "inteligencia" de Qradar. Se encarga de correlar los eventos y en función de las alertas/casos de uso/procedimientos marcados crea ofensas u otros eventos.

- Console and apps: es la parte en la cual se pueden visualizar los logs, realizar búsquedas y tratar con los datos recibidos. Existen aplicaciones que se incorporan en esta capa y hacen que estas tareas se faciliten.

2.3.2 Arquitecturas

En el caso particular de Qradar, las arquitecturas de la solución se pueden dividir en tres tipos agrupados a su vez en dos clases:

- Qradar on premise: Este Qradar se instala físicamente en las instalaciones del cliente o en un CPD que pertenezca al mismo. Pueden ser uno o varios dipositivos que interatuen entre sí como un ente único. Existen principalmente dos tipos:

    - All-in-one: como su propio nombre indica, es un dispositivo en el que todas las partes que componen un Qradar se integran en un único dipositivo, o como se suele llamar en la jerga de seguridad, un único "appliance".

    - Various appliances: Cada una de las funciones que componen el Qradar se lleva a cabo en un dispositivo diferente, con lo que tenemos varios dispositivos y una sola consola de control. A ojos del usuario es indistinguible de la primera opción, y se puede pasar de la primera a esta opción más avanzada en caso de que el proyecto así lo necesitara.

- Qradar on cloud: En este tipo de instalación, la empresa no posee ningún hardware, de modo que los logs se envían a internet y no tiene que comprar o alquilar ningún dispositivo.

2.4 Elección tipo Qradar

Como bien se ha comentado en puntos anteriores, el motivo de la elección de Qradar es ser el utilizado en el desarrollo de las prácticas.

Es por este mismo motivo que la elección final del tipo de Qradar es on permise "All-in-One".

2.5 Implementación

IBM Qradar cuenta con un periodo de prueba gratuita con funcionalidad limitada que nos permite introducirnos en el manejo de dicha aplicación, así como entrenarnos en caso de que seamos profesionales y queramos aprender a usar dicha tecnología, pero para poder usar la aplicación en una compañía, el precio de Ibm Qradar varía en función de la funcionalidad y los paquetes que necesitemos.

Para implementar Qradar en el cliente, la primera operación debe ser instalarlo físicamente, se aplicó la instalación "Appliance installation" mencionada en la guía de instalación de Qradar, apartado dos, configurando los parámetros básicos como la IP de ingesta y la IP de gestión, también el DNS, contraseñas y usuario root.

Las IPs de gestión e ingesta son distintas, y el funcionamiento es diferente: la de gestión se usa para controlar la consola, mientras que la de ingesta es la que se utiliza para recibir los distintos logs y poder analizarlos sintácticamente.

Con esta instalación tenemos acceso mediante SHH a la consola y acceso mediante web.

2.5.1 Configuración usuarios

Una vez que se puede acceder mediante web a Qradar, estamos preparados para configurar los usuarios. Estos usuarios pueden ser tanto locales en el sistema, (opciónmenos habitual) como la opción que se suele emplear en las empresas que disponen de Active Directory, que es la de usar usuarios de dominio.

2.5.2 Implementar aplicaciones

Qradar dispone de multitud de aplicaciones que se pueden implementar o no. En este TFG nos centraremos exclusivamente en la aplicación Log Source Managment.

2.5.3 Wincollect

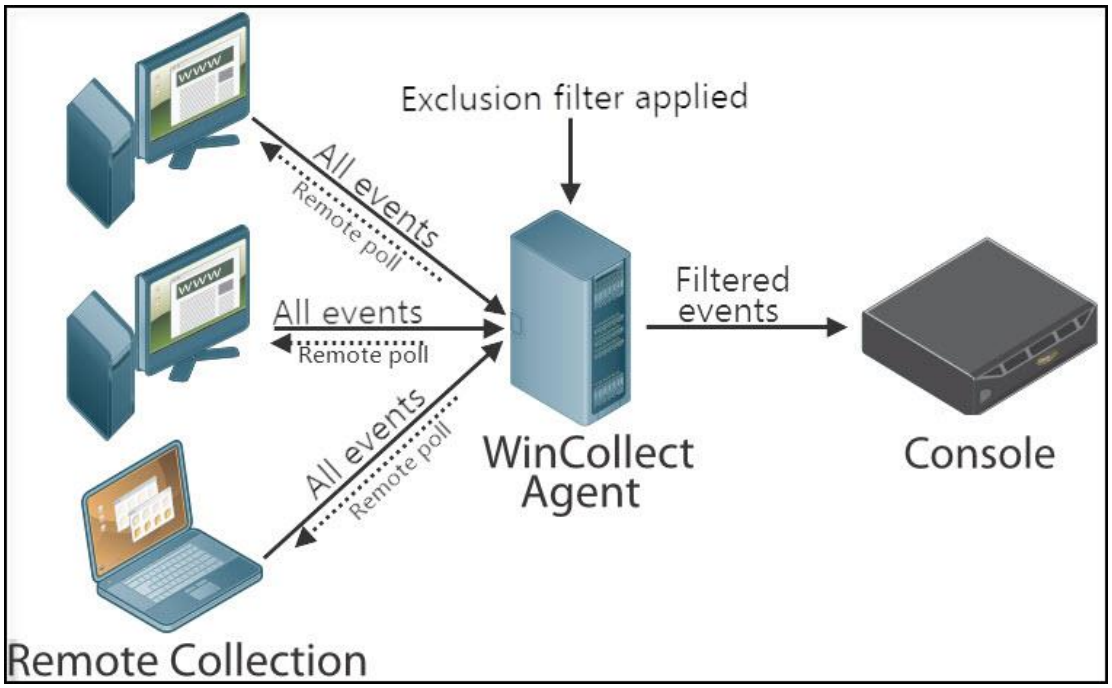
Para integrar distintas fuentes en Qradar, existe un procedimiento estándar que se encuentra en la propia web de IBM.

Antes de realizar acciones en el Qradar para la integración de la fuente, es importante configurar un agente de Wincollect. Este agente es un pequeño programa que permite a Qradar recolectar información del sistema Windows (WINdows COLLECTor) y transferirla por un protocolo propietario al SIEM. WinCollect es un reenviador de sucesos que los administradores pueden utilizar para reenviar sucesos de los registros de Windows a QRadar. Las instrucciones de instalación de este agente se les deben

transmitir al departamento de arquitectura de red o departamento IT. Las instrucciones y los archivos necesarios para ello se encuentran disponibles en el propio repositorio de información de IBM.

Cuando se instala un wincollect, éste intenta conectarse con la dirección IP que se le ha proporcionado en los parámetros que se le han dado al instalarse.

A continuación, se muestra una imagen representativa del funcionamiento de un Wincollect, donde cosole se entiende por la consola de QRadar.



Fuente: https://www.ibm.com/support/pages/wincollect-event-filtering

Es importante entender la función de un WinCollect, pues este será el encargado de almacenar los log y enviárselos a QRadar, para posteriormente un usuario pueda gestionar dichos logs.

Es este último punto, la gestión de los log en la que se desarrolla la maqueta realizada y que será explicada en puntos siguientes.

Capítulo 3. Exposición

3.1 Prefacio

En este capítulo se expondrá el funcionamiento de la maqueta realizada, a la hora de la creación, modificación y eliminación de una fuente/log en Qradar, con capturas de pantalla sobre el entorno original y una exposición previa, mediante casos de usos.

3.2 Configuraciones iniciales

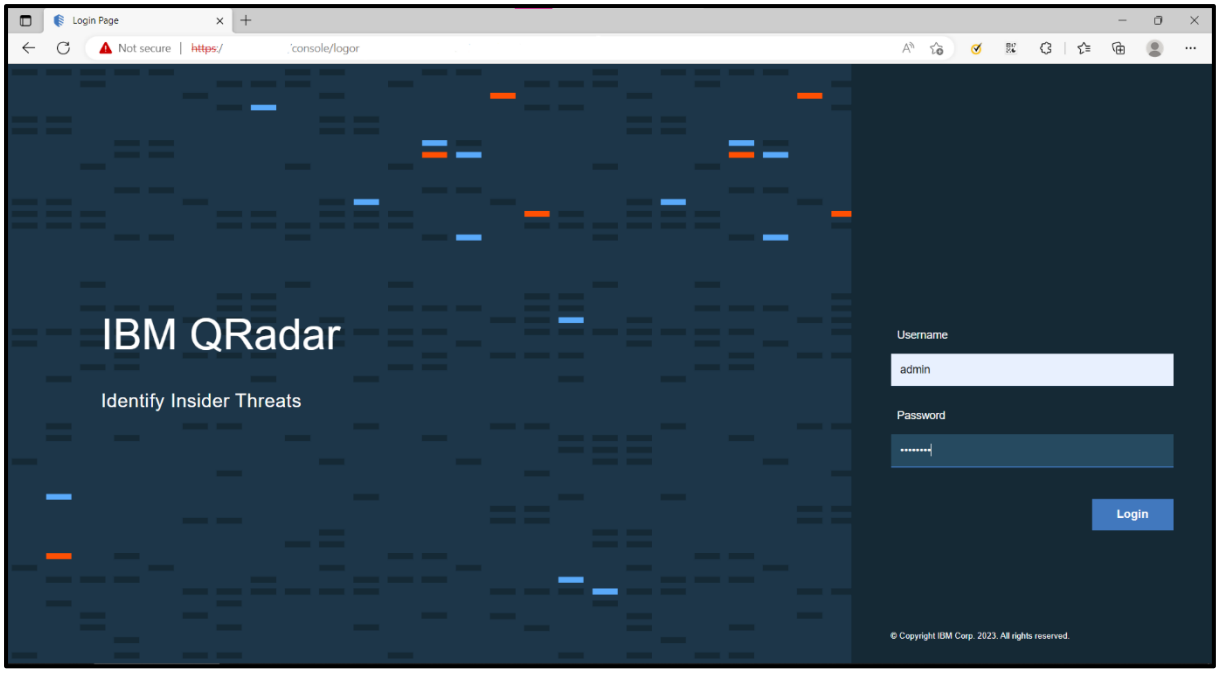
Para poder visualizar y llevar a cabo los siguientes puntos es necesario tener en cuenta las especificaciones que se detallan en el Capítulo 4. Especificaciones.

3.3 Acceso al entorno QRadar

En esta primera página mostrada a través de capturas de pantalla sobre un entorno real de IBM QRadar, tenemos el acceso a este entorno mediante un nombre de usuario y una contraseña asociada.

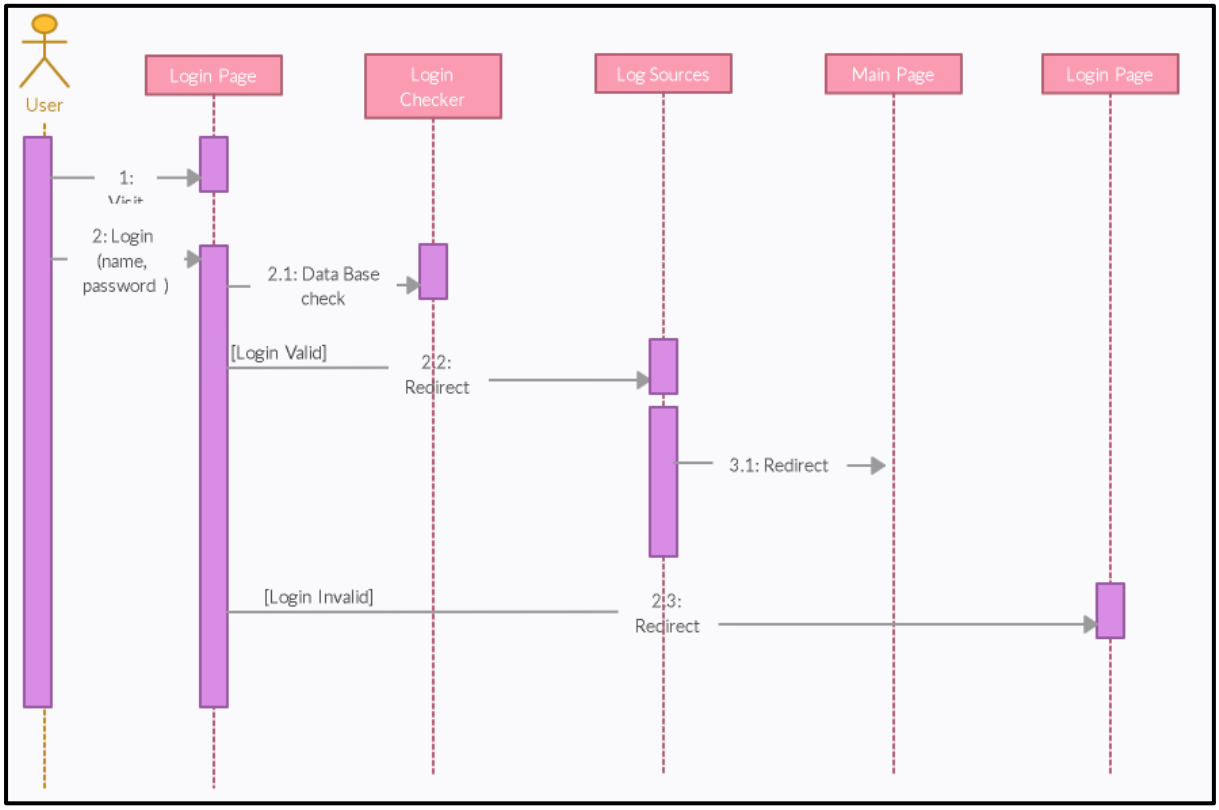
En la maqueta realizada para este proyecto se han añadido diversos usuarios y contraseñas repetidos, pero no en la misma relación unos con otros, para así poder comprobar el correcto flujo y funcionamiento de la validación de datos. Chequeando que el usuario introducido coincida con la contraseña que tiene asociado.

En esta página mostrada en este punto, el usuario sólo tiene opción de poner su usuario, contraseña y acceder al entorno QRadar. Aunque en el punto 3.3.3.1 Control de errores - Maqueta se detalla que se ha añadido dicha opción en a maqueta realizada



Entorno Real 1

3.3.1 Caso de Uso



Caso de Uso 1

3.3.1.1 Explicación – Caso de Uso

- **Descripción**: El usuario debe de ir al la dirección URL del log in. El sistema permite ingresar al usuario, la información de usuario y contraseña, en sus campos correspondientes.
- **Actores**: Usuario
- **Pre-condiciones**: Para Poder acceder al sistema el usuario debe de estar registrado en la base de datos.
- **Flujo normal**:
  1) El caso se inicia en el momento en que el usuario ingresa su usuario y contraseña.
  2) El sistema valida que ambos datos estén en conjunto en la base de datos.
  3) Fin de este caso de uso.
- **Flujo alternativo**:
  1) Si el usuario no ha ingresado correctamente su usuario y contraseña, el sistema le redirige de nuevo a la misma página de log in.
- **Pos-condiciones**: El usuario ingresa a la página principal del sistema.

3.3.2 Diagrama Base de Datos

La autenticación nos permite identificar a un usuario, cuando este presente su nombre de usuario y contraseña. En general estos datos son guardados por el servidor en una base de datos como MySQL y se utilizan para validar los datos ingresados en el momento del Login.

La tabla necesario para lograr la autenticación está compuesta por dos columnas de Usuario y contraseña.

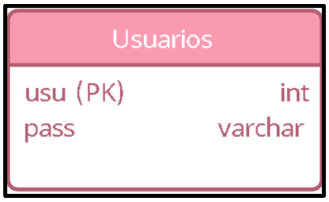
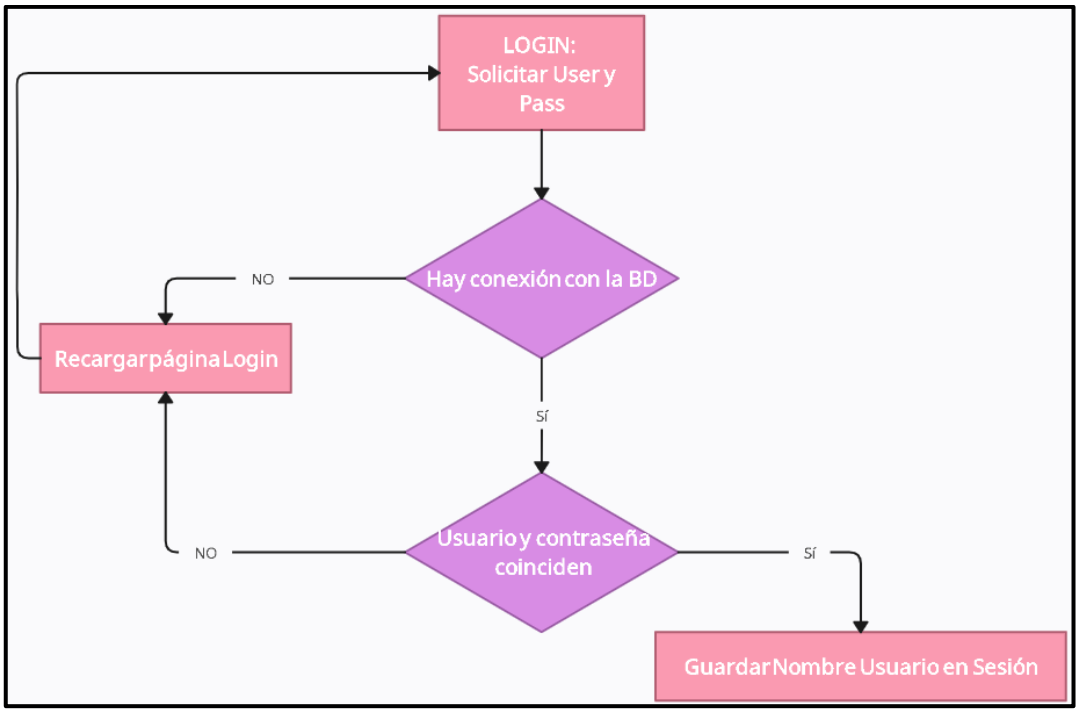


Tabla 1

Una vez realizado el Login exitoso, se registra el login en la sesión. Esto nos permite en la maqueta realizada, no en la página real, mantener el nombre de usuario en la parte superior derecha, en todas las páginas de la maquete.

La siguiente imagen muestra un diagrama dónde se representa el flujo antes explicado.



Flujo BD 1

3.3.3 Control de errores - Maqueta

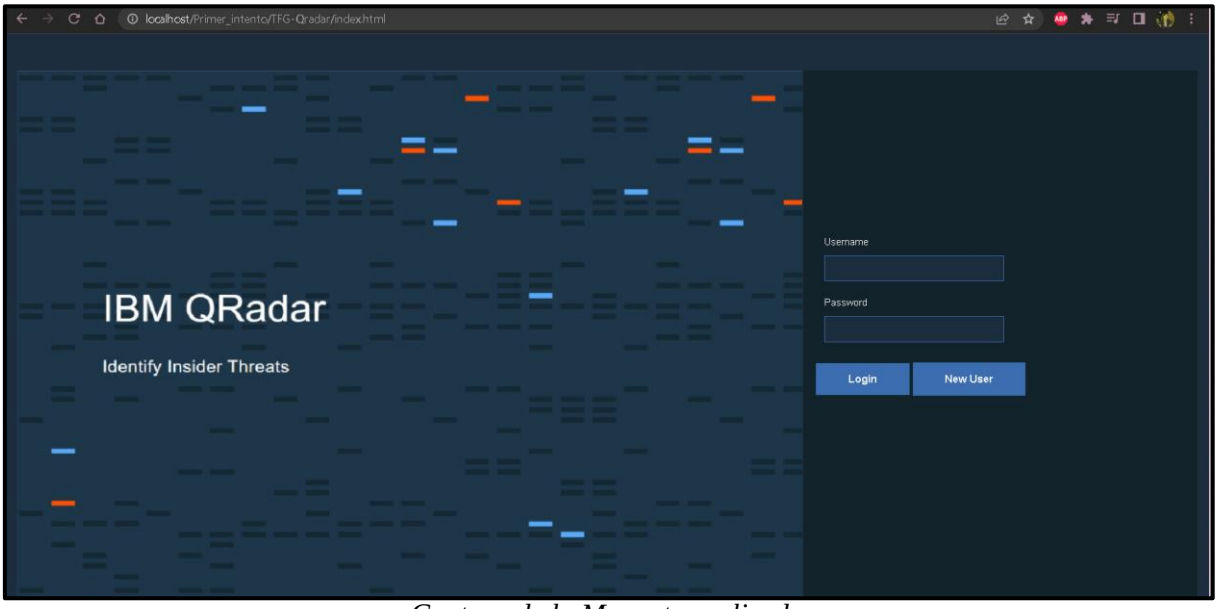
El proyecto presente, no deja de ser una maqueta para la muestra de un control de logs en el área de ciberseguridad de una empresa, es por esto que algunas funcionalidades que podría tener el programa en la versión original, no se ha implementado en esta maqueta.

1. **Sí** se informa al usuario si hay fallo de conexión con la base de datos.
2. Si el usuario introduce mal su usuario y/o contraseña, no se le informa de ello, simplemente se le recarga la página del login de nuevo.
3. No se le informa al usuario si el usuario introducido existe o no en la base de datos en caso de introducir una contraseña errónea.
4. No se le informa al usuario si no coinciden el usuario y/o contraseña.
5. No se controla el número de intentos fallidos.
6. No se bloquea al usuario tras un número de intentos incorrectos.
7. No se le da al usuario la opción de recuperar su contraseña, en caso de introducir su contraseña errónea.
8. **Sí** existe la opción de crear un usuario nuevo, aunque NO existe esta opción en la plataforma real.

3.3.3.1 Control de errores - Maqueta

En esta primera página, se ha añadido en la maqueta realizada la opción de crear un nuevo usuario, a pesar de que en la versión real, no exista dicha opción.

A continuación, expondremos de manera breve esta pequeña modificación:



Captura de la Maqueta realizada

El Usuario tras ingresar un número de usuario y una contraseña presiona en el botón New User, donde automáticamente el sistema guardará su contraseña encriptada en la base de datos.

```
MariaDB [pro_tfg]> select * from usuarios;
+--------+--------------------------------------------------------------+
| usu    | pass                                                         |
+--------+--------------------------------------------------------------+
|  11111 | $2y$10$aLKy5P8k3LIRLG7.RmPYW.kVktGWsYttaHnLgytAvq7Tu0egwV7PC |
|  12456 | $2y$10$7vpJlSEjEAW1vcdXvFjPy.PKMcwS12rOfJKZJaUytSqw1f/TF5zh6 |
| 888777 | $2y$10$YHg996Bv1N.ubp9wYFzmAuSwG5Tr.YebQa4U8sDkAfyMSSonP4r9C |
+--------+--------------------------------------------------------------+
3 rows in set (0.000 sec)
```

Ejemplo encriptación en bbdd de la contraseña

Caso de Uso

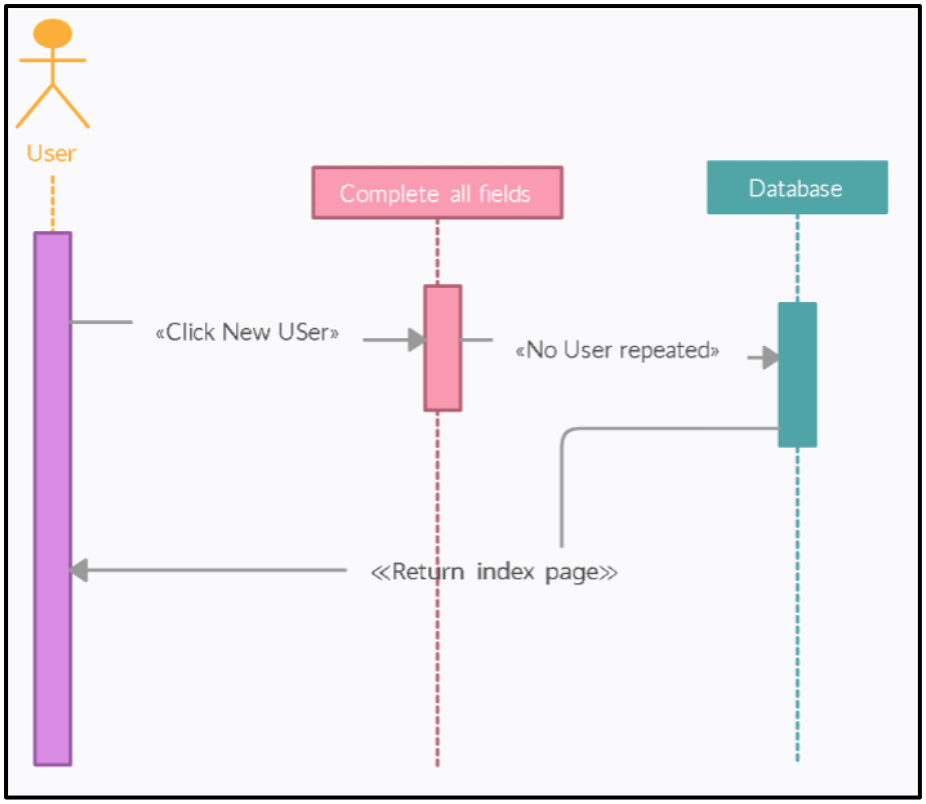
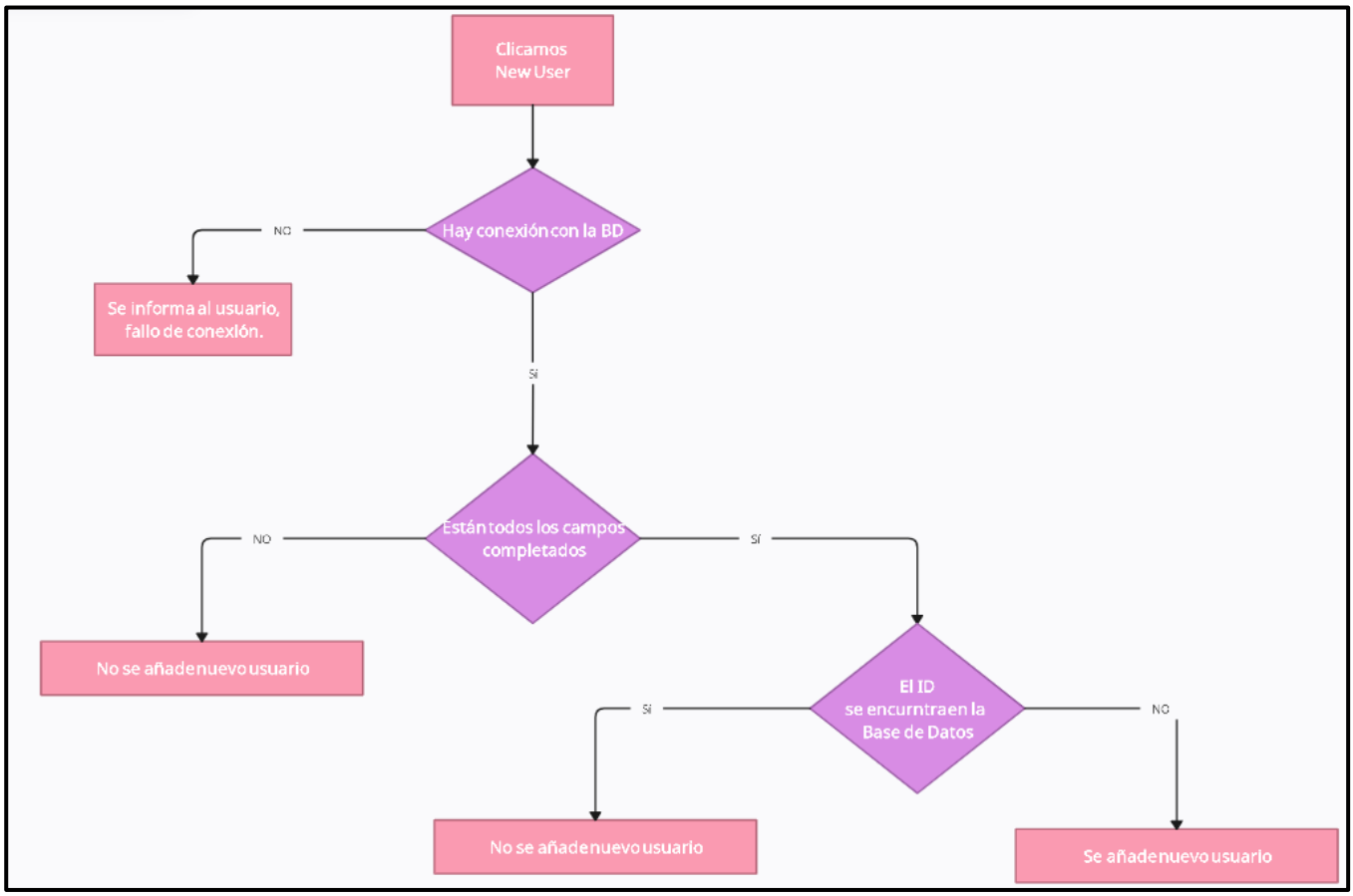


Diagrama Base de Datos



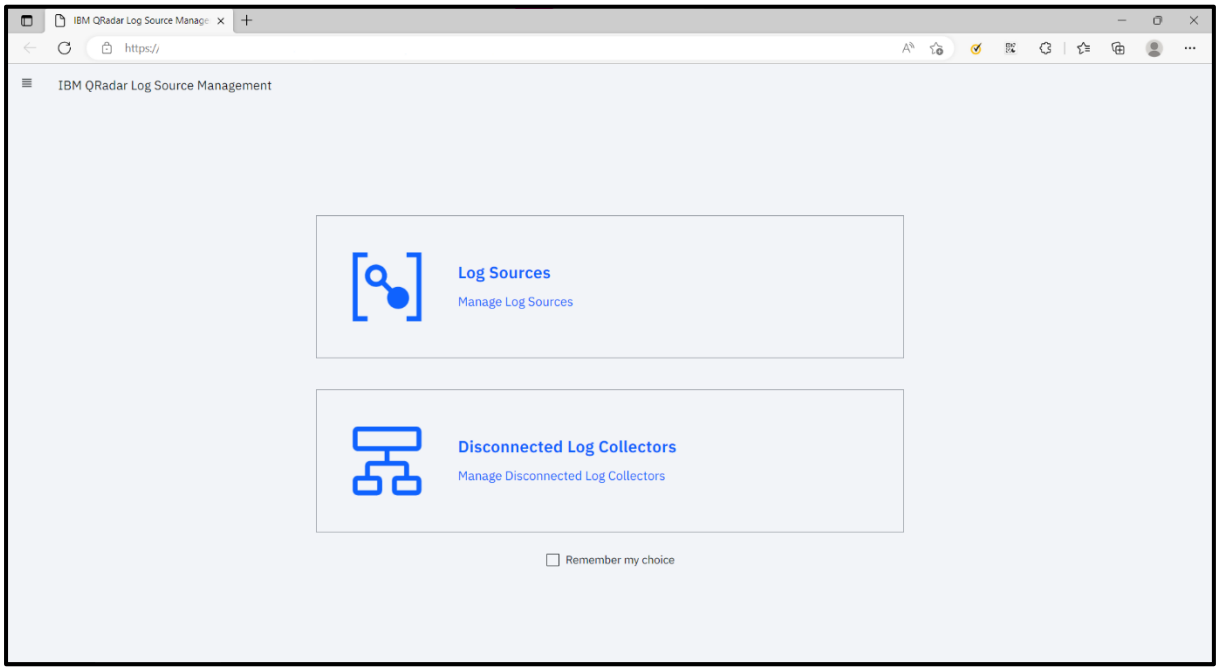
3.4 Acceso a la aplicación Log Source Management

Tras la validación del usuario y contraseña en un entorno real, QRadar nos ofrece multitud de opciones dentro de su SIEM, más allá de las detalladas en puntos anteriores. Sin embargo, debido a información altamente delicada, se suprime la muestra de los pasos a seguir hasta llegar a la aplicación interna de Log Source Management, ya que en este proyecto nos estamos centrando únicamente en esta función y aplicación de QRadar.

En un entorno real, antes de llegar a la aplicación Log Source Management, tenemos la opción de acceder a la aplicación de Qradar Manage Disconnected Log Collector.

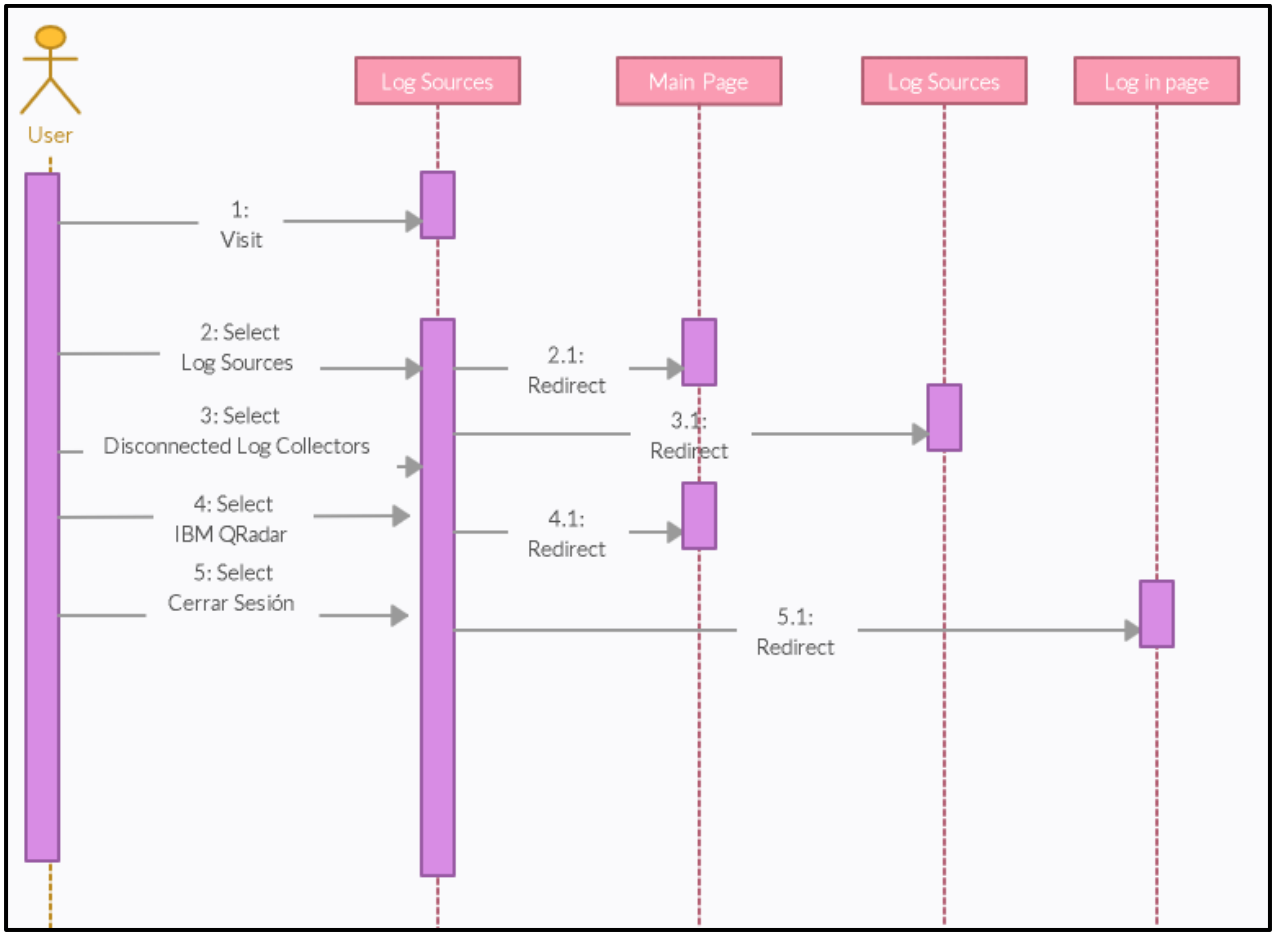
Es importante recordar el punto 2.5.3 Wincollect en el que se explicaba la función de este. Es en esta última aplicación mencionada, donde se puede gestionar los wincollectors desconectados.

En la maqueta realizada, esta aplicación no está implementada, por lo que al usuario no se le redirige a ninguna página. La última función, <<Remember my choice>> tampoco está habilitada en la maqueta realizada.



Entorno Real 2

3.4.1 Caso de Uso



Caso de Uso 2

3.4.1.1 Explicación – Caso de Uso

- **Descripción**: El usuario, tras ingresar de manera correcta su usuario y contraseña, se le redirige a la página de Log Sources para así acceder a la página correspondiente.
- **Actores**: Usuario
- **Pre-condiciones**: Para Poder acceder a esta página el usuario ha sido redirigido por el sistema, tras haber validado su usuario y contraseña
- **Flujo normal**:

1) El usuario selecciona Log Source – Manage Log Sources.
2) El sistema Le redirige a la página de Log Source Managment.
3) Fin de este caso de uso.

- **Flujo alternativo**:

  1) El usuario selecciona Disconnected Log Collectors.
  2) El sistema no redirige al usuario a ninguna página

  ---

  1) El usuario selecciona Cerrar Sesión
  2) El sistema redirige al usuario a la pagina de log in principal

  ---

  1) El usuario selecciona la pestaña superior izquierda
  2) El sistema Le redirige a la página de Log Source Managment

- **Pos-condiciones**: El usuario ingresa a la página correspondiente

3.4.2 Diagrama Base de Datos

En este paso no se realiza interacción con la base de datos.

3.4.3 Control de Errores - Maqueta

1. El botón para acceder a la aplicación Disconected Log Collectors **SÍ** contiene enlace, para comunicar al usuario que no está operativo.
2. El botón <<Remember my choice>> es estático, su clicado no interfiere en sucesivos accesos por parte del usuario.

3.5 Detalles página principal

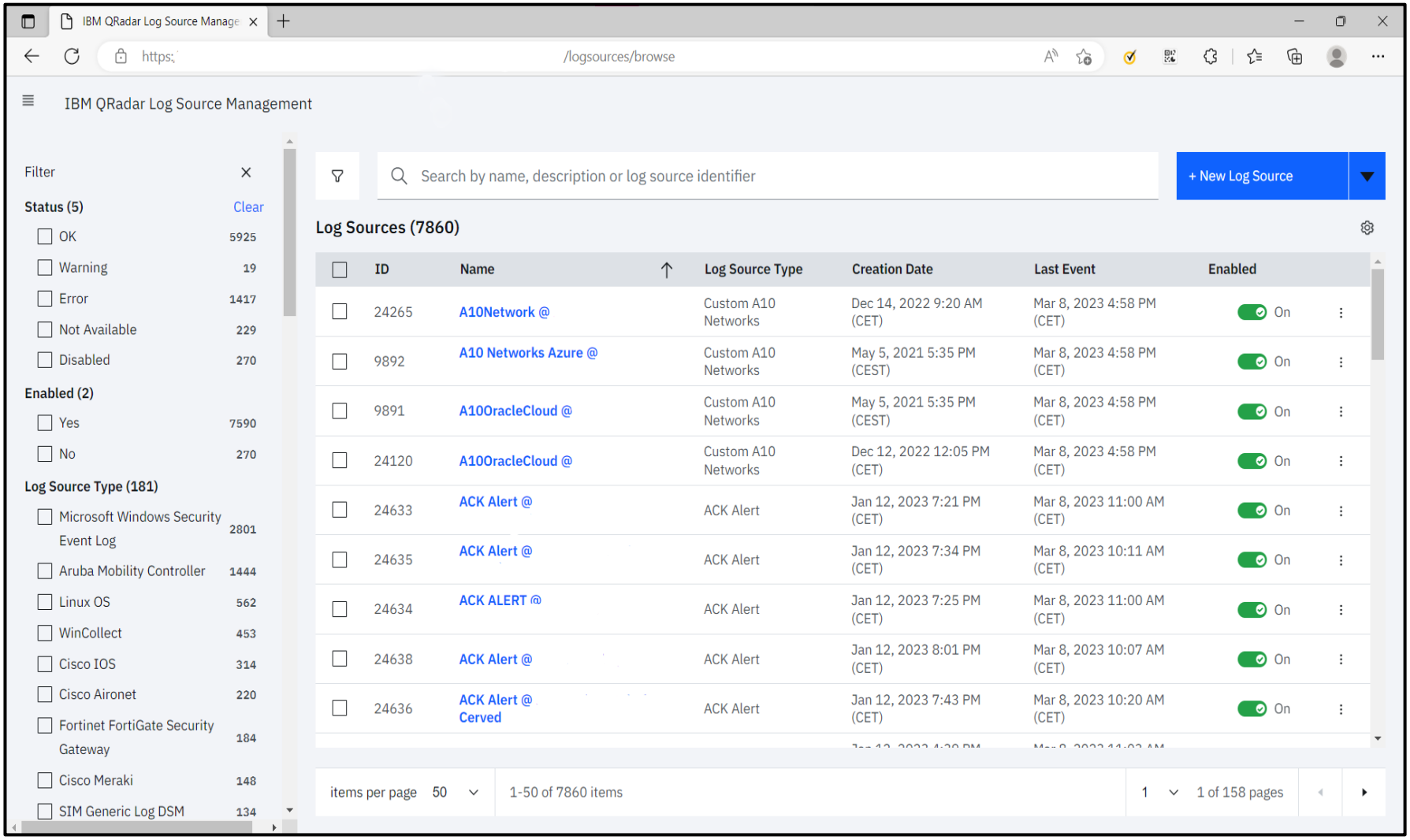
Cómo se puede apreciar en la siguiente página, donde encontramos la captura de pantalla de la página principal de QRadar Log Source Management, observamos en la parte derecha un menú deslizante para seleccionar los filtros deseados, y así encontrar más rápidamente los log sources en los que estemos interesados. Otra opción que nos ofrece IBM en QRadar es su buscador, por el cual podemos filtrar los log sources disponibles por su nombre, o identificador. Este buscador se encuentra en la parte superior central de la página principal

En la maqueta realizada en este proyecto, dicho menú desplegable y buscador no tienen ninguna funcionalidad.

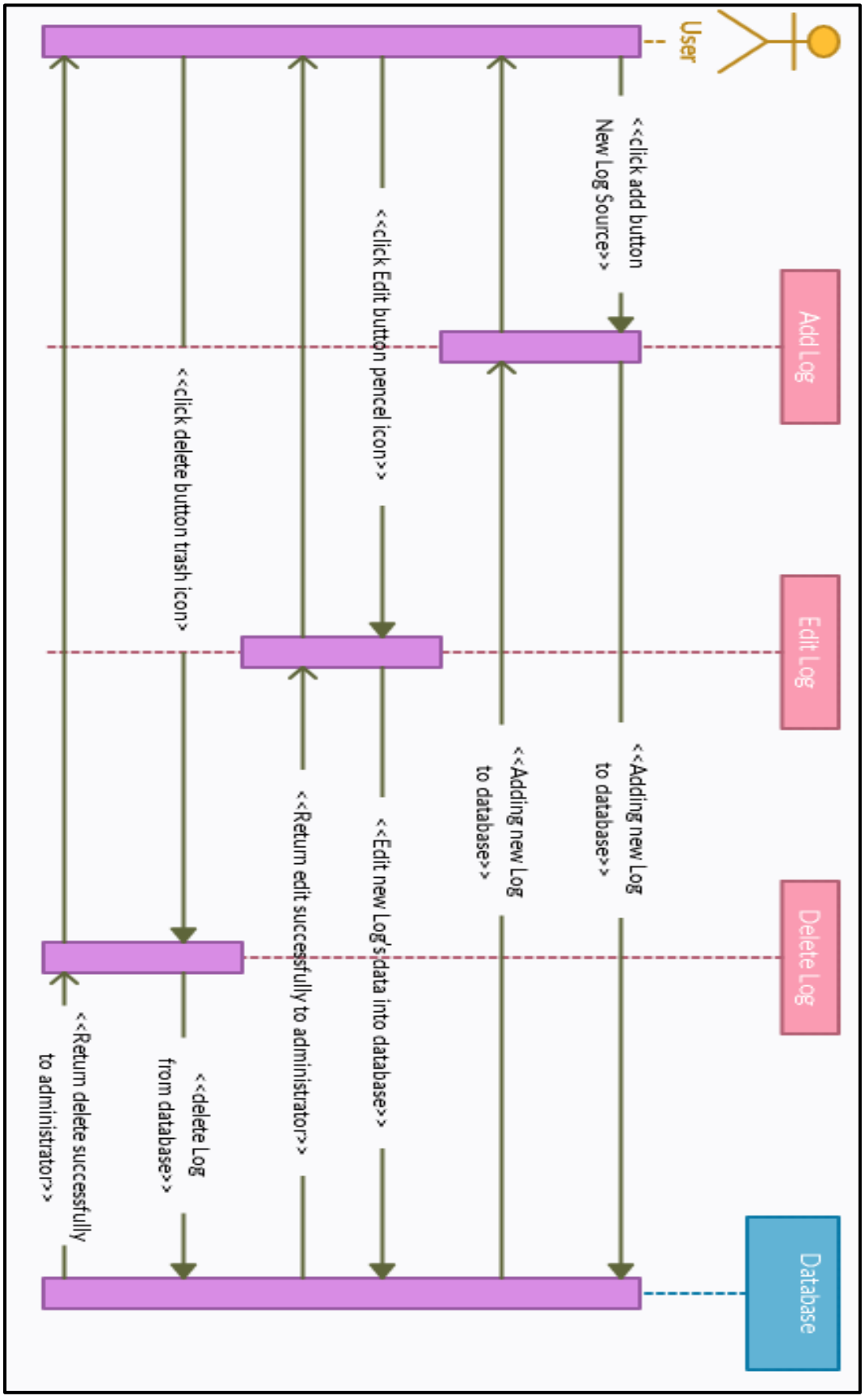
Como bien se ha señalado, en la siguiente página encontramos la captura de pantalla de la página principal de QRadar Log Source Managment. Página principal también de la maqueta de este proyecto.

Desde esta página principal se realiza la modificación, eliminación y añadido de un log en QRadar. Para añadir una nueva fuente se efectúa a través del botón azul situado en la parte derecha. La edición y eliminación de una fuente será clicando los tres puntos horizontales que se encuentran a la derecha de cada log source dentro de la tabla que se muestra.

El proceso de eliminación, modificación y añadido se explica más detalladamente en los próximos puntos.


IBM QRadar Log Source Manage
https:
/logsources/browse
IBM QRadar Log Source Management
Filter
Status (5)
Clear
OK 5925
Warning 19
Error 1417
Not Available 229
Disabled 270
Enabled (2)
Yes 7590
No 270
Log Source Type (181)
Microsoft Windows Security Event Log 2801
Aruba Mobility Controller 1444
Linux OS 562
WinCollect 453
Cisco IOS 314
Cisco Aironet 220
Fortinet FortiGate Security Gateway 184
Cisco Meraki 148
SIM Generic Log DSM 134
Search by name, description or log source identifier
+ New Log Source
Log Sources (7860)
ID
Name
Log Source Type
Creation Date
Last Event
Enabled
24265 A10Network @ Custom A10 Networks Dec 14, 2022 9:20 AM (CET) Mar 8, 2023 4:58 PM (CET) On
9892 A10 Networks Azure @ Custom A10 Networks May 5, 2021 5:35 PM (CEST) Mar 8, 2023 4:58 PM (CET) On
9891 A10OracleCloud @ Custom A10 Networks May 5, 2021 5:35 PM (CEST) Mar 8, 2023 4:58 PM (CET) On
24120 A10OracleCloud @ Custom A10 Networks Dec 12, 2022 12:05 PM (CET) Mar 8, 2023 4:58 PM (CET) On
24633 ACK Alert @ ACK Alert Jan 12, 2023 7:21 PM (CET) Mar 8, 2023 11:00 AM (CET) On
24635 ACK Alert @ ACK Alert Jan 12, 2023 7:34 PM (CET) Mar 8, 2023 10:11 AM (CET) On
24634 ACK ALERT @ ACK Alert Jan 12, 2023 7:25 PM (CET) Mar 8, 2023 11:00 AM (CET) On
24638 ACK Alert @ ACK Alert Jan 12, 2023 8:01 PM (CET) Mar 8, 2023 10:07 AM (CET) On
24636 ACK Alert @ Cerved ACK Alert Jan 12, 2023 7:43 PM (CET) Mar 8, 2023 10:20 AM (CET) On
items per page 50
1-50 of 7860 items
1
1 of 158 pages

3.5.1 Caso de Uso



Caso de Uso 3

3.5.1.1 Explicación – Caso de Uso

- **Descripción**: Tras el ingreso de sus credenciales en la página de login y llegar a la página previa a la aplicación donde ha seleccionado Log Sources, llega a la aplicación para la gestión de los logs.
- **Actores**: Usuario
- **Pre-condiciones**: Credenciales validados y conocimiento de los pasos hasta llegar a esta aplicación.
- **Flujo normal**:
    1) El caso se inicia en el momento en que el usuario clica en una de las tres opciones:
        a) Add Log
        b) Edit Log
        c) Delete Log
    2) El sistema redirige al usuario a la página correspondiente.
    3) Tras la gestión realizada correcta o incorrectamente, el sistema redirige al usuario a la página principal
    4) Fin de este caso de uso.
- **Flujo alternativo**:
    1) El usuario selecciona uno de los filtros mostrados en el panel izquierdo deslizante o escribe en el buscador central.
    2) El sistema no realiza ningún tipo de filtro solicitado.

    ---

    3) El usuario selecciona Cerrar Sesión
    4) El sistema redirige al usuario a la página de log in principal

    ---

    3) El usuario selecciona la pestaña superior izquierda
    4) El sistema Le redirige a la página de Log Source Managment
- **Post-condiciones**: El usuario ingresa a la página solicitada en el caso de flujo normal.

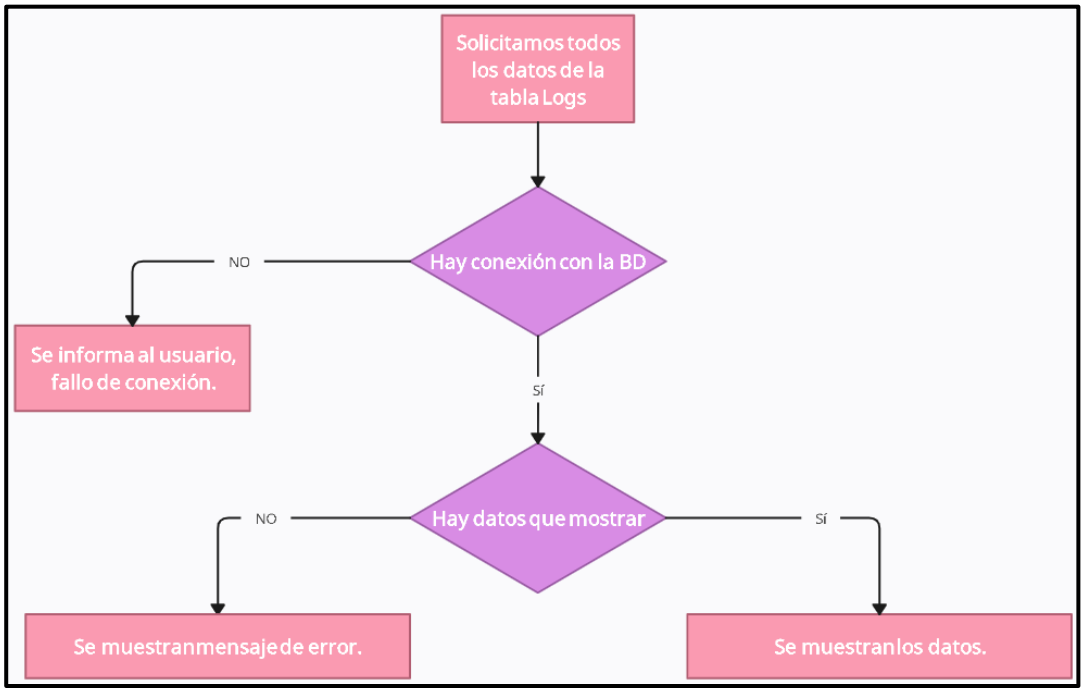
3.5.2 Diagrama Base de Datos

La interacción de la Base de datos para la creación, edición y eliminación de los logs se realiza en las siguientes páginas. En esta página se consulta a la base de datos, con el fin de obtener todos los campos de la tabla LOGS, para así mostrarlos al usuario, este tenga a simple vista los logs y sus datos visibles y accesibles si desase realizar alguna modificación, eliminación o añadido de nuevo log.

Logs	
id (PK)	int
Name	varchar
logSourceType	varchar
protocolType	varchar
extension	varchar
creationDate	Datetime
lastEvent	Datetime
internal	Bit
enabled	Bit

Tabla 2

La siguiente imagen muestra el flujo con la base de datos, explicado en este apartado.



Flujo BD 2

3.5.3 Control de Errores - Maqueta

1. Si no hay datos para mostrar, se muestra un mensaje de error.
2. Los únicos botones con funcionalidad en la maqueta son para la edición, eliminado y añadido de fuentes en la base de datos.
3. No se puede realizar filtros para la búsqueda de logs
4. El buscador sí **está operativo**.

3.6 Añadir nueva Fuente

QRadar nos ofrece la opción de añadir una nueva fuente / log para así recibir eventos de nuestros dispositivos de red.

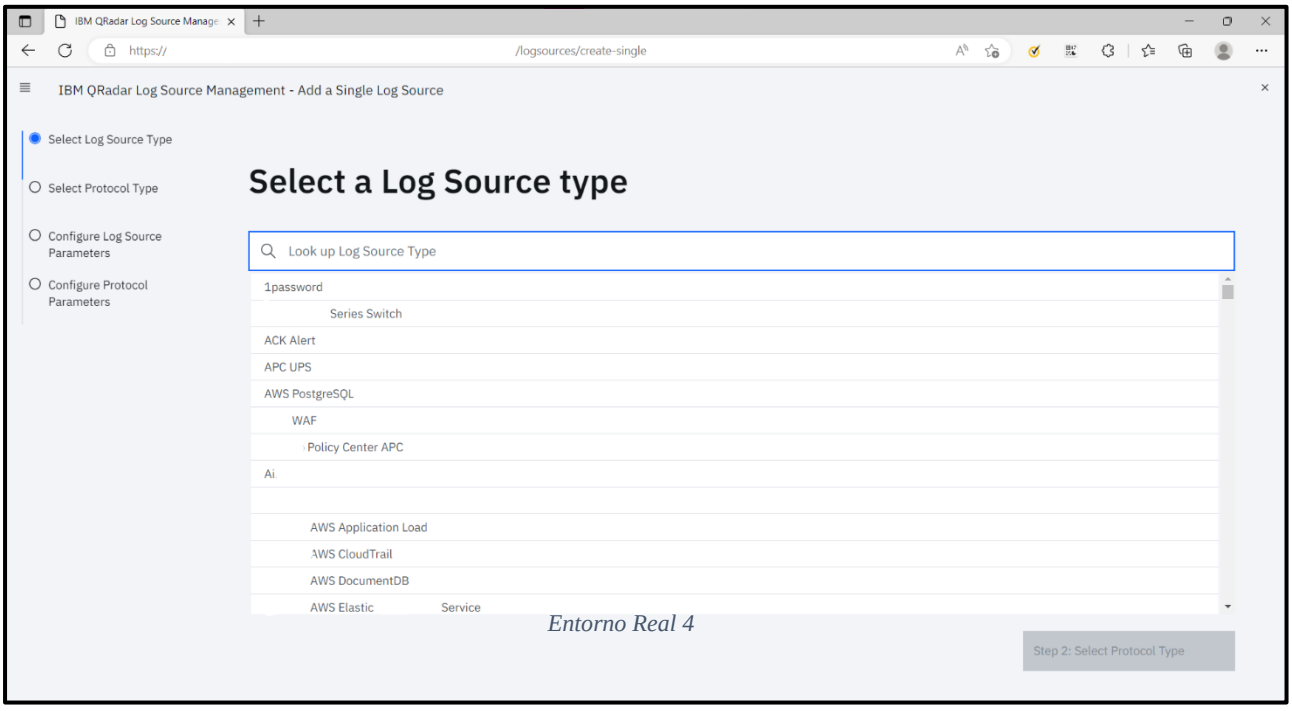
Añadir una nueva fuente en un entorno real requiere de mayores parámetros que en la maqueta realizada. QRadar solicita, el tipo de fuente, así como el protocolo utilizada para la transferencia de datos, también los parámetros y el protocolo relacionado.

En la API de QRadar encontramos el procedimiento para esta acción en entorno real. https://www.ibm.com/docs/es/dsm?topic=management-adding-log-source

Para mayor detalle de este paso, se puede visitar el siguiente enlace, donde explica paso a paso, con referencia del entono real, todos los parámetros que son necesarios para añadir una nueva fuente.

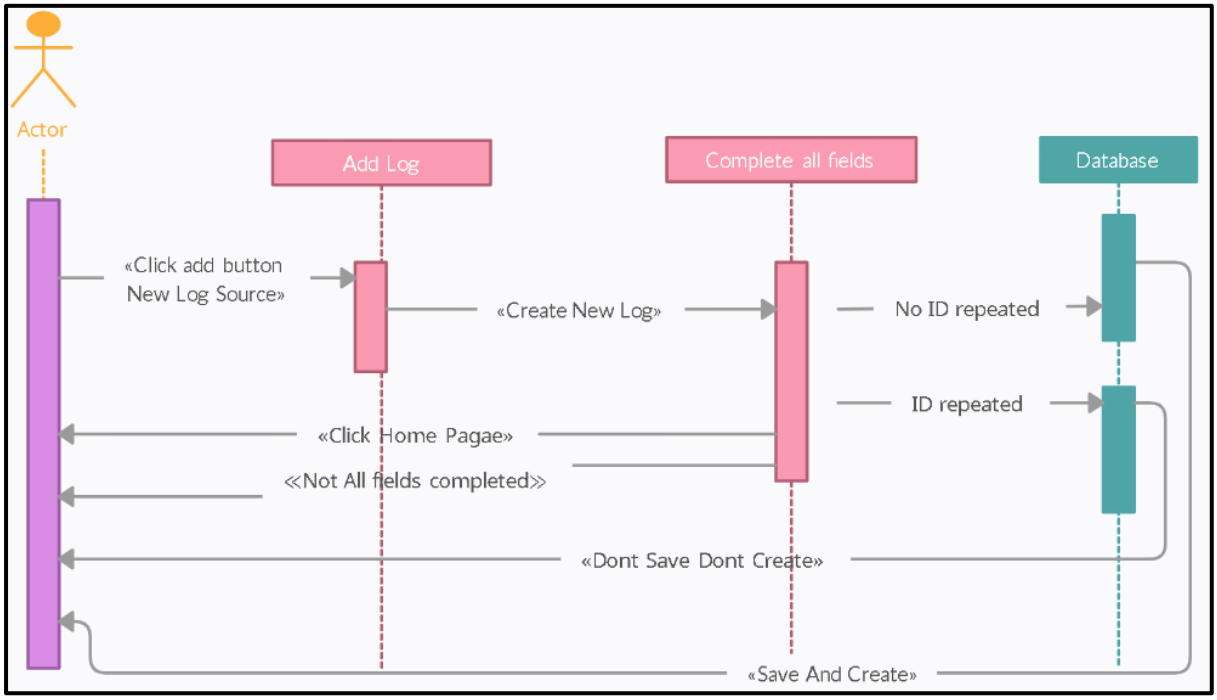
https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/General/IBM_security_QRadar_DSM.html

En la maqueta realizada los parámetros que se solicicitan al usuario son los mismos que contiene la tabla Logs en la base de datos, es decir; ID, Name, Log Source Type, Creation Date, Last Event y si se encuentra activado.



Entorno Real 4

3.6.1 Caso de Uso



Caso de Uso 4

3.6.1.1 Explicación – Caso de Uso

- **Descripción**: Una vez el usuario, tras ingreso de credenciales y acceso a la aplicación de Log Sources Management, el usuario clica en el botón <<+ New Log Source>>.
- **Actores**: Usuario
- **Pre-condiciones**: Credenciales validados y conocimiento de los pasos hasta llegar a esta aplicación, para cliclar en el botón <<+ New Log Source>>.
- **Flujo normal**:

  1) El caso se inicia en el momento en que el usuario clica en el botón <<+ New Log Source>>:
  2) El sistema redirige al usuario a la página correspondiente.
  3) El usuario ha de completar todos los campos, sin introducir un ID ya existente en la base de datos.
  4) El Usuario clicla en <<Guardar Log>>
  5) Si el ID no está repetido, se redirige al usuario a la pégina principal con mensaje satisfactorio.
  6) Fin de este caso de uso.

- **Flujo alternativo**:

  1) El usuario No completa todos los campos.

  2) El sistema redirige al usuario a la página principal con mensaje erróneo informando que todos los campos han de estar completados.

  ---

  3) El usuario selecciona Cerrar Sesión
  4) El sistema redirige al usuario a la página de log in principal

  ---

  3) El usuario selecciona la pestaña superior izquierda
  4) El sistema Le redirige a la página de Log Source Managment

- **Pos-condiciones**: El usuario ingresa a la página solicitada en el caso de flujo normal.

3.6.2 Diagrama Base de Datos

En este apartado se añade una nueva fuente/log a la tabla previamente creada.

Todos los campos de la tabla son NOT NULL, por lo que es necesario que el usuario complete todos los campos antes de añadir la fuente, en caso contrarío no se podrá realizar el ingreso de la nueva fuente. Tampoco se podrá añadir la nueva fuente si el ID introducido ya existe en la BD, pues este campo es Primary Key, por lo que no se puede encontrar repetido dentro de la tabla.

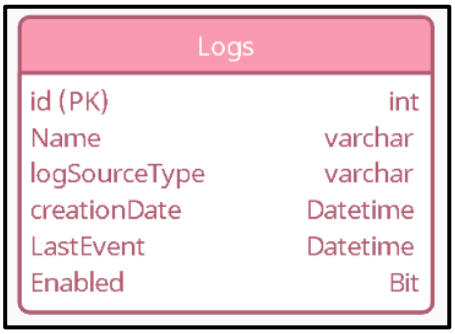
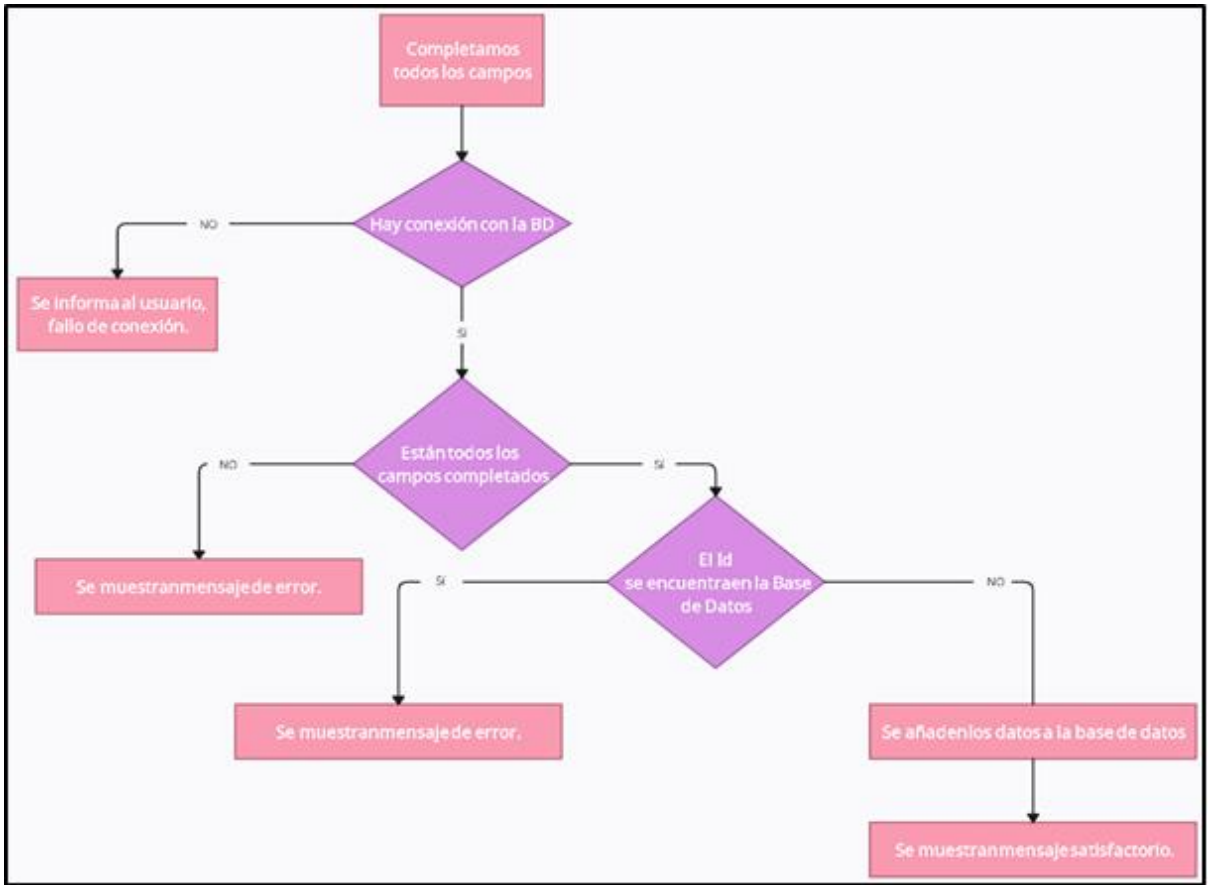


Tabla 3

En la siguiente imagen se muestra el flujo con la base de datos, explicado en este apartado.



Flujo BD 3

3.5.3 Control de Errores – Maqueta

1. Si un campo no se ha completado, salta mensaje de error.
2. **Sí** se informa qué campo es el faltante/incorrecto.
3. Si todos los campos están correctos, salta mensaje satisfactorio.
4. Si el id se encuentra ya en la base de datos, se informa al usuario.

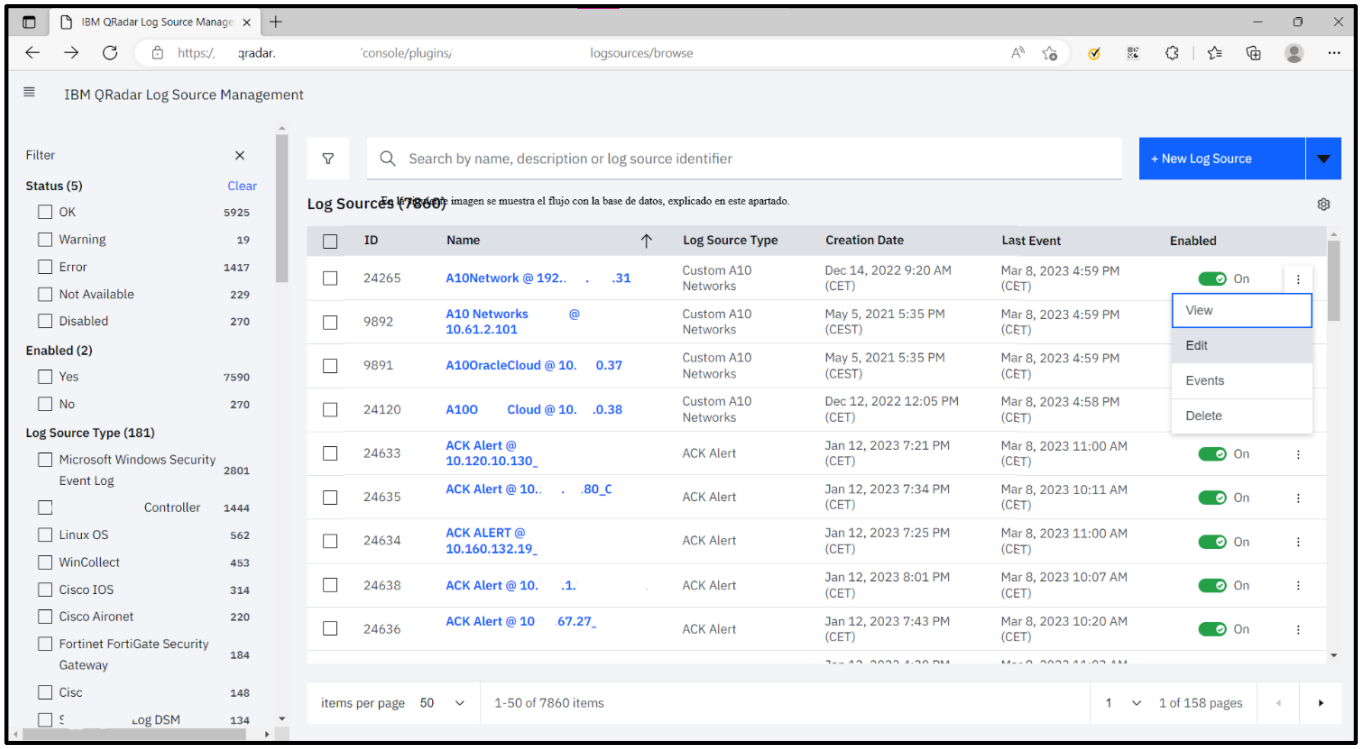
3.7 Editar fuente

En el entorno real de QRadar se ofrece la opción de modificar una fuente ya existente.

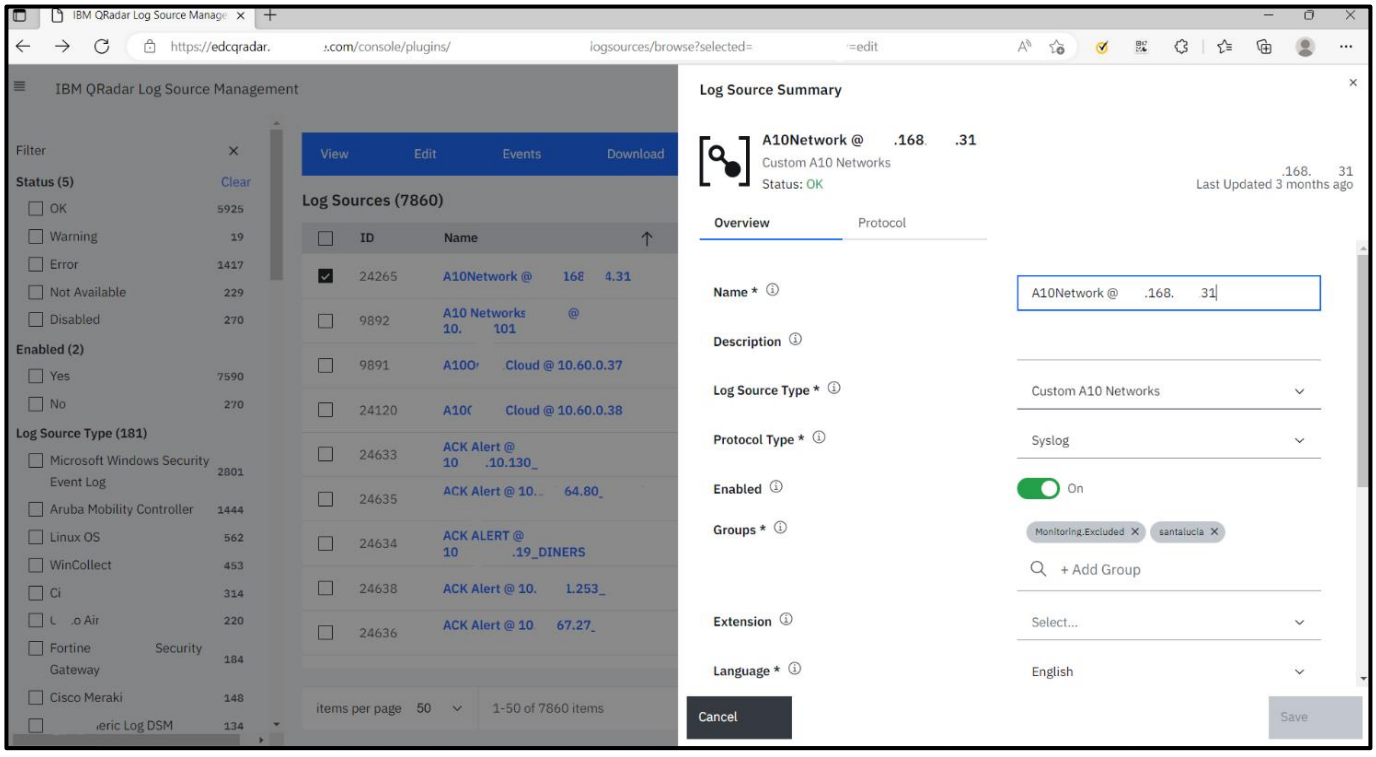
En este caso, el primer paso es bastante similar a la maqueta realizada, el botón para editar la fuente se encuentra en la parte derecha de la tabla mostrada, sin embargo, en el entorno real los campos para editar la fuente se realizan en una ventana modal, dejando la página principal de fondo.

En la maqueta realizada no se ha implementado ventanas modales, ya que no fueron objeto de estudio en el curso.

En la API de QRadar encontramos el procedimiento para esta acción en entorno real.
https://www.ibm.com/docs/en/dsm?topic=management-editing-bulk-log-sources

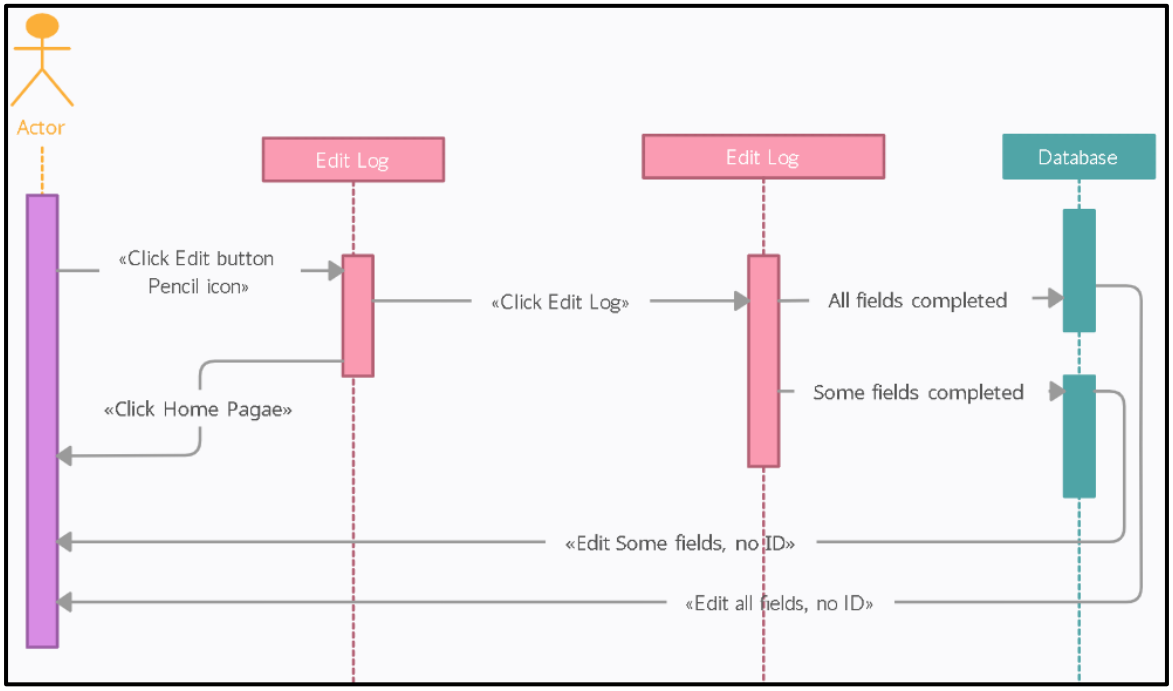


Entorno Real 5



Entorno Real 6

3.7.1 Caso de Uso



Caso de Uso 5

3.7.1.1 Explicación – Caso de Uso

- **Descripción**: Una vez el usuario, tras ingreso de credenciales y acceso a la aplicación de Log Sources Management, el usuario clica en el icono del lápiz.
- **Actores**: Usuario
- **Pre-condiciones**: Credenciales validados y conocimiento de los pasos hasta llegar a esta aplicación, para clicar en el icono del lápiz.
- **Flujo normal**:
  1) El caso se inicia en el momento en que el usuario clica en el icono del lápiz:
  2) El sistema redirige al usuario a la página correspondiente.
  3) El usuario ha de completar los campos que desee modificar. El ID, no puede ser modificado, así como la fecha de creación.
  4) El Usuario clica en <<Editar Log>>
  5) Se redirige al usuario a la página principal con mensaje satisfactorio.
  6) Fin de este caso de uso.
- **Flujo alternativo**:

1) El usuario selecciona Cerrar Sesión
2) El sistema redirige al usuario a la página de log in principal

---

1) El usuario selecciona la pestaña superior izquierda
2) El sistema Le redirige a la página de Log Source Managment

3.7.2 Diagrama Base de Datos

En este apartado estamos modificando una fuente, previamente añadida a nuestra tabla Logs.

Todos los campos de la tabla son NOT NULL, es por este motivo que en caso de no completar un campo, el programa se queda con el valor previo a la modificación.

Al ser una modificación no se permite ni modificar el ID, ya que este campo es Primary Key, ni la fecha de la creación.

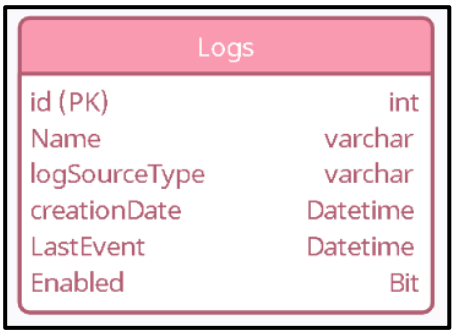
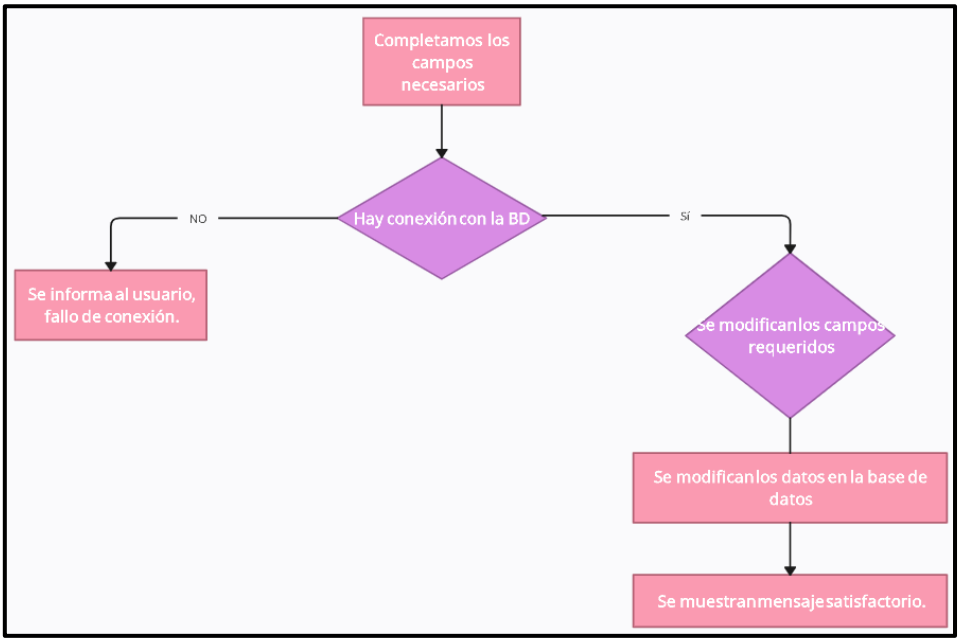


Tabla 4

En la siguiente imagen se muestra el flujo con la base de datos, explicado en este apartado.



Flujo BD 4

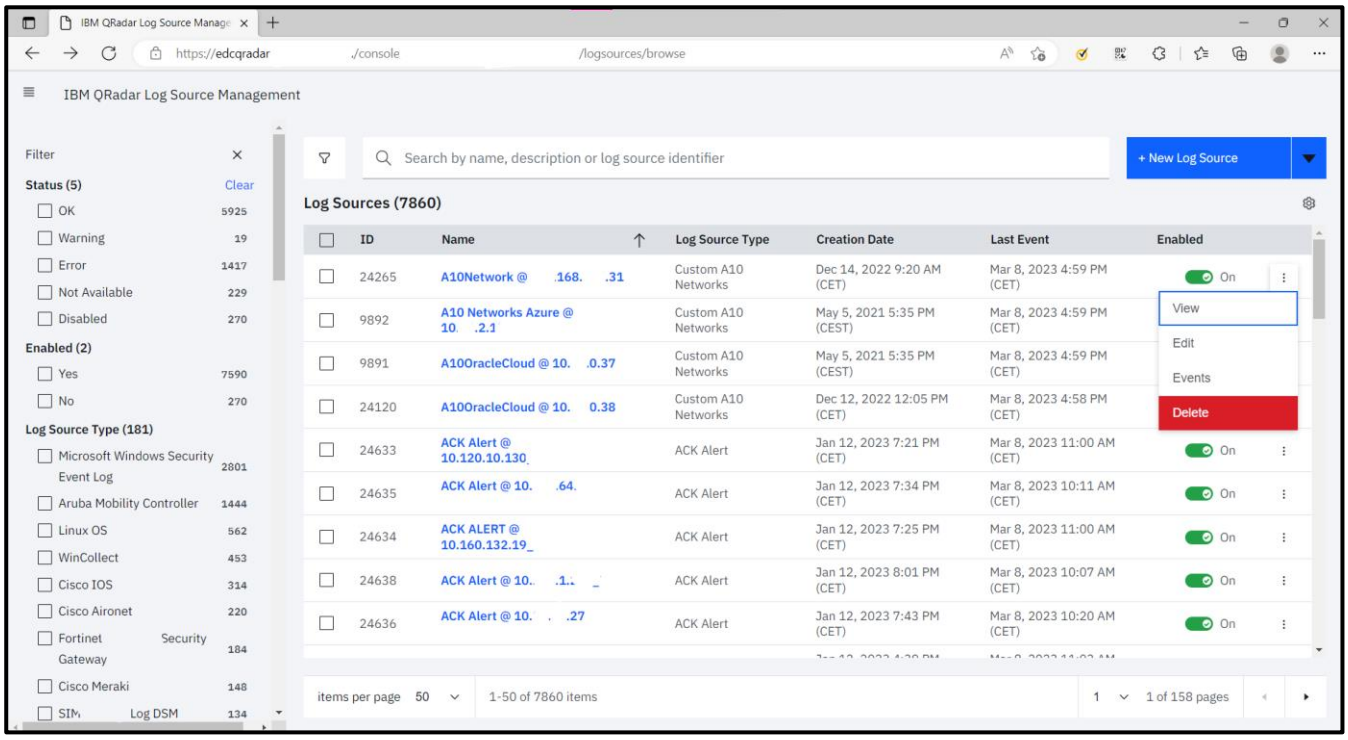
3.7.3 Control de Errores – Maqueta

1. Si un campo no se ha completado, permanece el valor anterior.
2. No se informa qué campo ha sido modificado.
3. El botón de Enabled no modifica el valor en la tabla de la BD.
4. La fecha del último evento es la actual a la modificación, no pudiéndola poner de forma manual.

3.8 Eliminar fuente

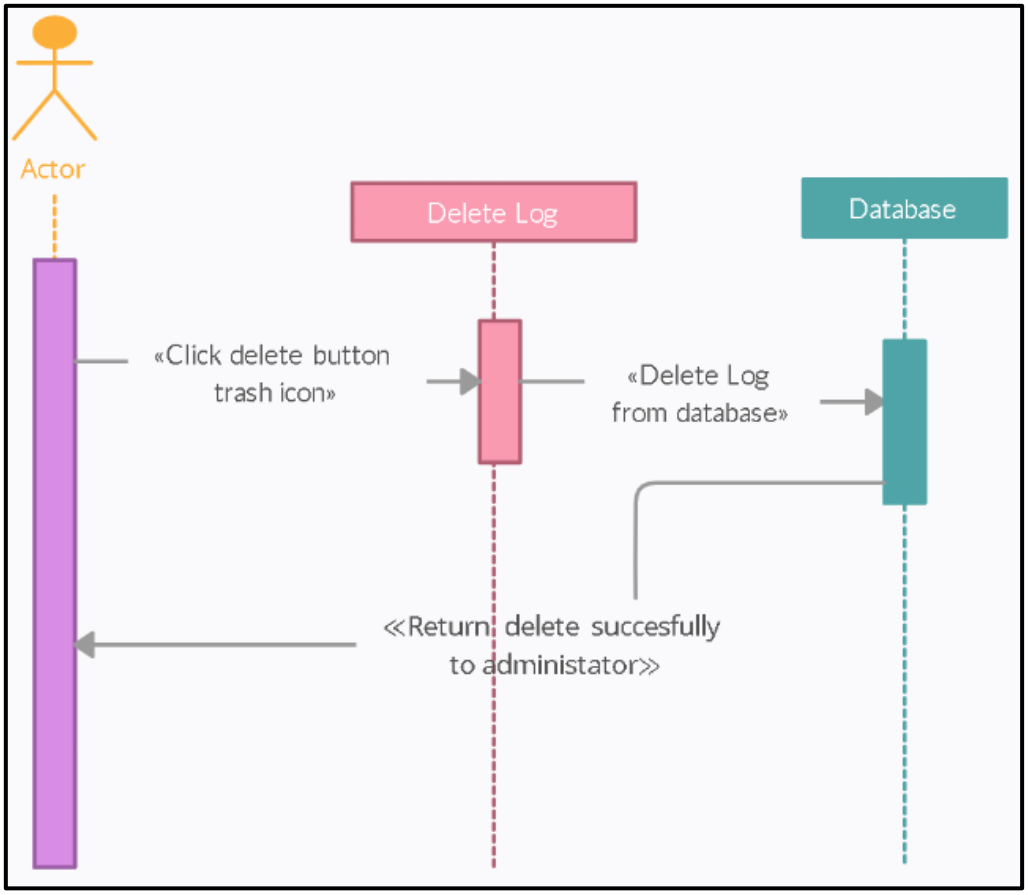
QRadar ofrece la opción de eliminar una fuente, bien por fallo a la hora de ser utilizada, o bien por su falta de uso.

La eliminación en el entorno real es igual de sencilla que en la maqueta realizada. El usuario ha de pulsar el botón <<Delete>> situado a la derecha de cada Log, dentro de la tabla.



Entorno Real 7

3.8.1 Caso de Uso



Caso de Uso 6

- **Descripción**: Una vez el usuario, tras ingreso de credenciales y acceso a la aplicación de Log Sources Management, el usuario clica en el icono de la papelera.
- **Actores**: Usuario
- **Pre-condiciones**: Credenciales validados y conocimiento de los pasos hasta llegar a esta aplicación, para clicar en el icono de la papelera.
- **Flujo normal**:

  1) El caso se inicia en el momento en que el usuario clica en el icono de la papelera:
  2) Se muestra mensaje de eliminación satisfactorio.
  3) Fin de este caso de uso.

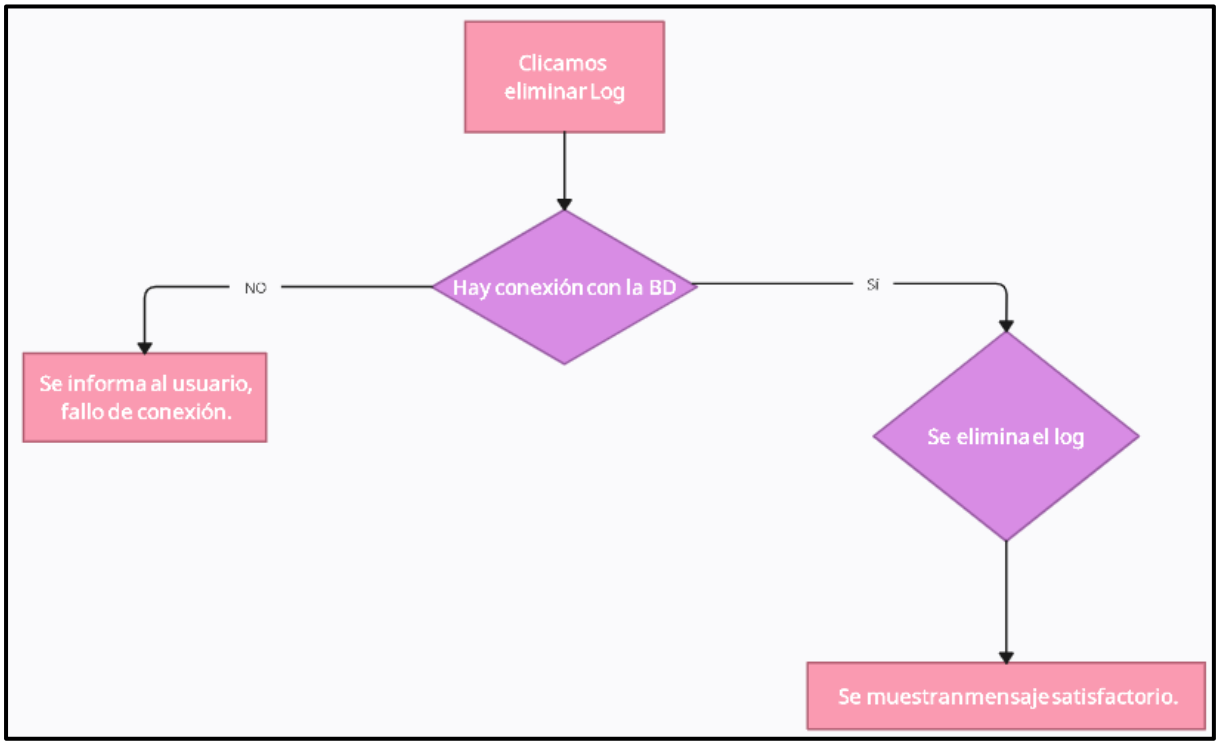
- **Flujo alternativo**:

  1) El usuario selecciona Cerrar Sesión
  2) El sistema redirige al usuario a la página de log in principal.

3.8.2 Diagrama Base de Datos

En este apartado la interacción con la base de datos es simple. Tan solo se hace una query de eliminación de la fuente con el ID seleccionado.

En la siguiente imagen se muestra el flujo con la base de datos, explicado en este apartado.



Flujo BD 5

3.8.3 Control de Errores – Maqueta

1. No se le pregunta al usuario si está seguro de la eliminación de la fuente.
2. No se informa al usuario del riesgo que tiene perder todos los datos.
3. Se informa al usuario de la eliminación de la fuente seleccionada.

Capítulo 4. Especificaciones

En este capítulo se exponen tanto las especificaciones como las restricciones a la hora de poder visualizar y ejecutar el proyecto.

4.1 Especificaciones

- Para la lectura del código se ha de tener un **lector/editor de código**.

  Aunque los editores de texto que vienen por defecto con el sistema operativo, como pueden ser NotePad o TextEdit, pueden abrir y leer todos los archivos de código, es altamente recomendable tener un editor de código que incorpore el lenguaje principal utilizado en este TFG, PHP, así como HTML.

- **Navegador web.** Para poder visualizar la maqueta realizada, es necesario cargar los archivos de código en un navegador web.

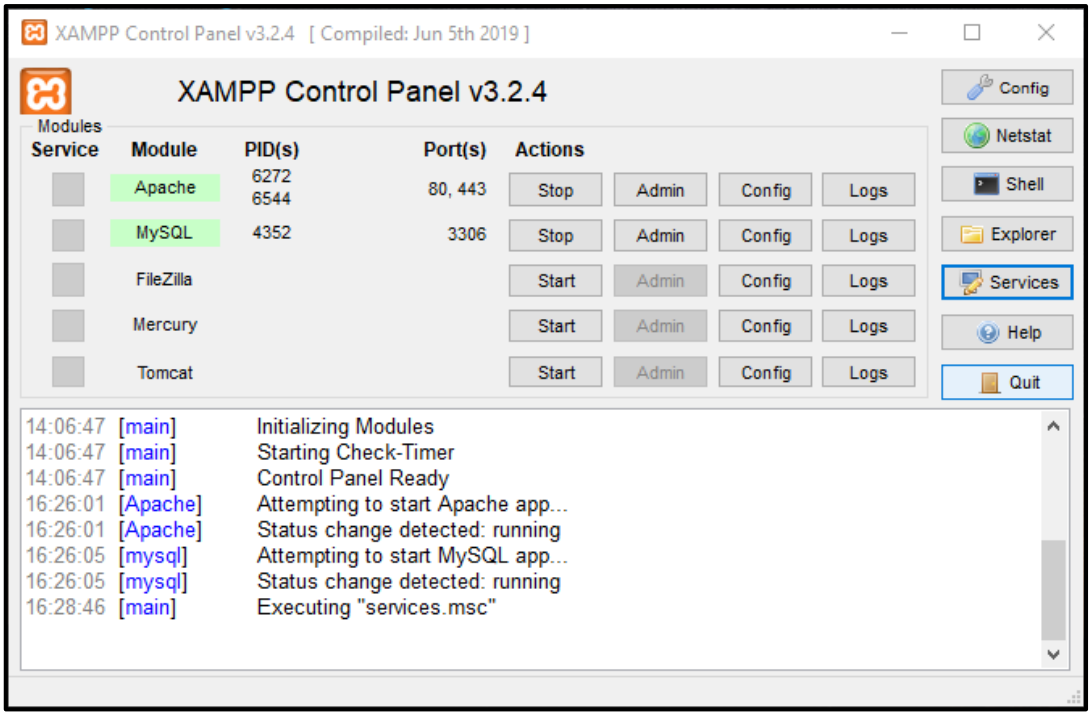
  al igual que su funcionalidad.

- **Servidor Local.** Este ha de tener, principalmente, un sistema de gestión de base de datos Mysql, servidor web Apache y los intérpretes para lenguajes de script PHP.

  Se recomienda el uso de XAMPP.

  A continuación, se detalla de manera breve el uso de XAMPP para la correcta visualización del proyecto.

  - Una vez descargado e instalado XAMPP se ha de poner en funcionamiento Apache y MySQL, haciendo clic en el botón <<Start>> correspondiente. Si el arranque del módulo tiene éxito, el panel de control mostrará el nombre del módulo con fondo verde, su identificador de proceso, los puertos abiertos (http y https), el botón <<Start>> se convertirá en un botón “Stop” y en la zona de notificación se verá el resultado de las operaciones realizadas.

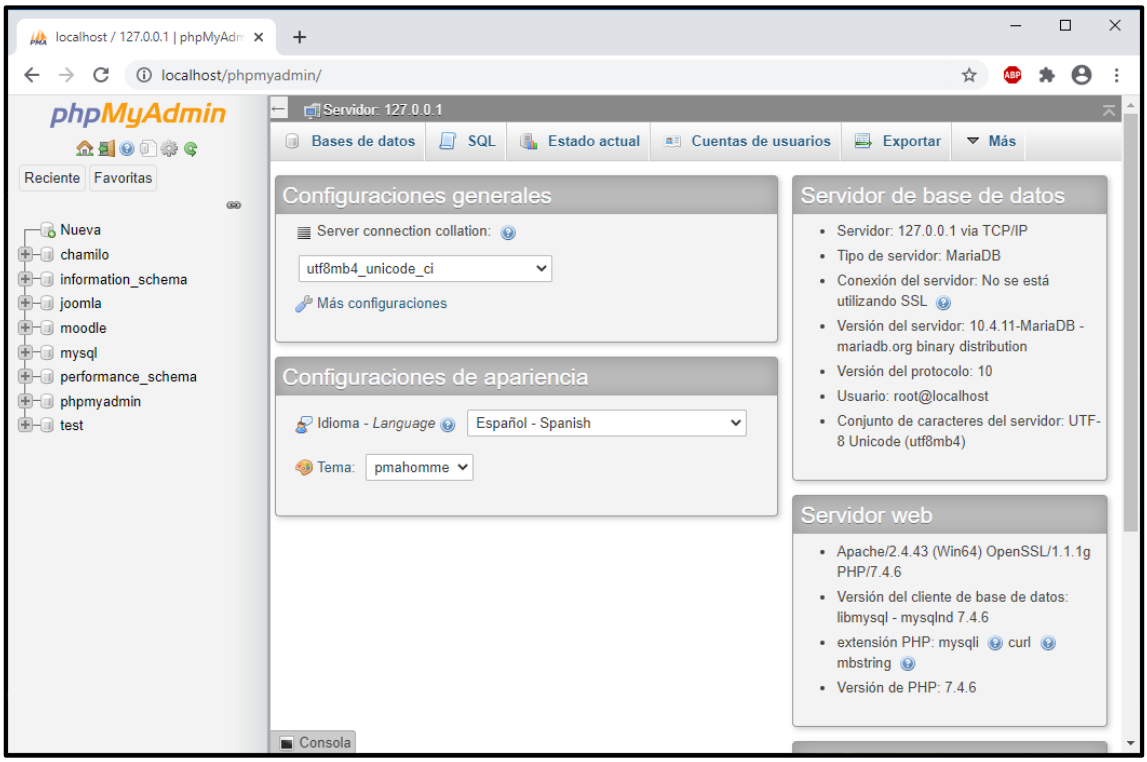


Especificaciones 1

- Si se ha iniciado el servidor Apache, para comprobar que todo funciona correctamente, hay que escribir en el navegador la dirección http://localhost. XAMPP abrirá el nuevo panel de administración web (dashboard).

Especificaciones 2

- Si se ha iniciado el servidor Apache y MySQL, para comprobar que todo funciona correctamente, hay que escribir en el navegador la dirección http://localhost/phpmyadmin/. XAMPP abrirá el nuevo panel de administración de base de datos phpMyAdmin.



Especificaciones 3

- Para subir y probar el proyecto web en Xammp, nos vamos al directorio de Xampp, después ingresamos a la carpeta htdocs, es aquí donde pegamos el proyecto.
- Ahora regresamos al navegador web y escribimos la dirección del localhost seguido del nombre proyecto.

  http://localhost /TFG-Qradar/

4.2 Restricciones

- No es necesario el acceso a internet, ya que se utiliza un servidor local.
- Al igual que en la página original de la aplicación Log Source Managment de Qradar, no es 100% responsive. Es por esto que se ha de utilizar unas dimensiones de pantalla fijas. (1289 x 882)

Capítulo 5. Metodología

En este capítulo se exponen la Metodología empleada para la realización del proyecto, así como su organización y desarrollo.

La metodología utilizada para el desarrollo de este proyecto ha sido una basada en un modelo secuencial, es decir cada fase de este proyecto es una continuación de la anterior

5.1 Modelo en Cascada

Cabe destacar un dato interesante antes de desarrollar y comentar este modelo. Este enfoque de cascada originalmente fue propuesto en 1970 por Winston W. Royce, es también conocido como modelo lineal o modelo de ciclo de vida.

El motivo de su nombre. En simples palabras, se debe a la manera en la que se dividen y se llevan a cabo cada una de las fases de su proceso, de manera escalonada, siguiendo una secuencia ordenada desde la primera hasta la última etapa.

5.2 Fases del modelo en cascada

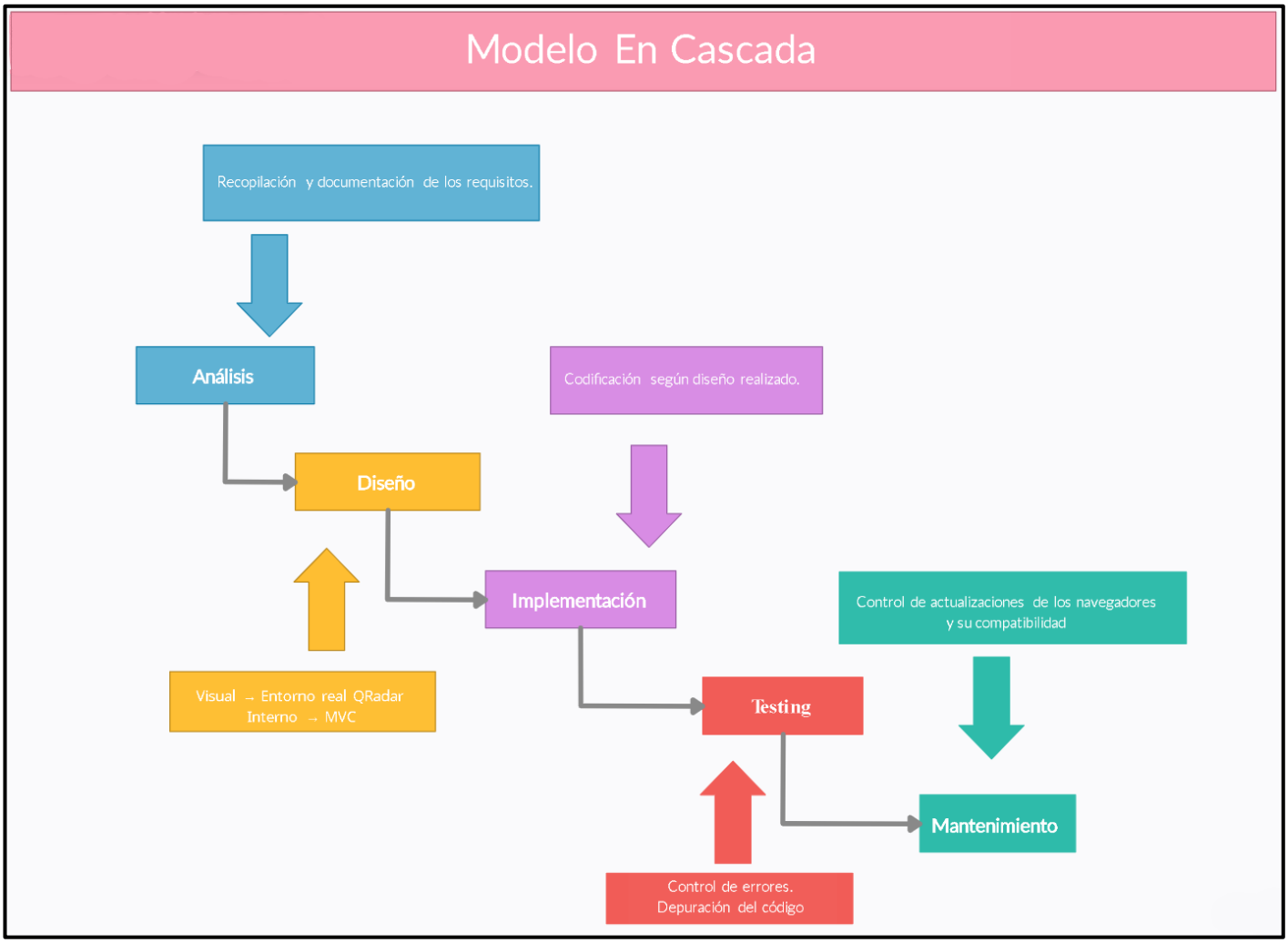
Aunque originalmente este modelo constaba de 7 fases;

1. Análisis de Requisitos
2. Diseño del sistema.
3. Diseño del programa
4. Codificación
5. Pruebas
6. Implementación o verificación del programa
7. Mantenimiento

Actualmente es más común encontrar una variación más reducida, ya que algunas de las etapas se fusionaron en una sola, quedando 5 fases de desarrollo;

1. Análisis
2. Diseño
3. Implementación
4. Verificación
5. Mantenimiento

En cualquier caso, para el desarrollo de este proyecto se ha utilizado una combinación de ambas fases.



5.2.1 Análisis

En primer lugar, fue necesario contactar con el tutor del centro de estudios para poder realizar una correcta recopilación y documentación de los requisitos para la elaboración de este TFG.

En esta fase hubo interacción entre el tutor y la alumna, mediante correos electrónicos en los que el tutor detalló a la alumna los requisitos mínimos junto con un modelo. La alumna planteó una propuesta de TFG con el lenguaje principal a utilizar y el entorno gráfico con el que se trabajaría.

El tutor dio el Ok y con ello se pudo pasar a la siguiente fase.

5.2.2 Diseño

La parte de diseño visual del programa se basó en la estructura original del programa QRadar, teniendo como referente los trabajos realizados durante las prácticas en el centro de trabajo.

Por otra parte, nos encontramos con el diseño del programa. Se tomó como modelo y referente el modelo Vista/Controlador para la implementación de un CRUD, ya que fue objeto de estudio en ciclo formativo, en la asignatura DWES.

5.2.3 Implementación

En esta fase se realizó la codificación. Se utilizaron los elementos obtenidos en el diseño para permitir la elaboración del proyecto. Con la fase de diseño ya terminada, se produjo a realizar el código con su estructura interna en Modelo Vista Controlador, aplicando el diseño gráfico del entorno real de QRadar.

5.2.4 Verificación

Esta fase se centró en la comprobación del correcto funcionamiento del código. Se realizaron un control de errores que han quedado reflejados en esta memoria.

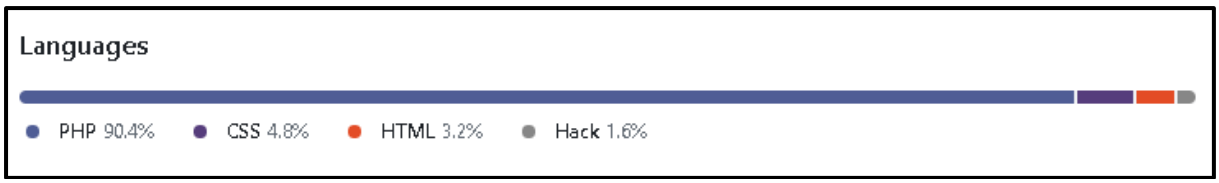
5.2.5 Mantenimiento

Se realizan chequeos, diarios y semanales, con el fin de comprobar que el programa sigue siendo compatible con los navegadores y sus actualizaciones.

Capítulo 6. Implementación

En este capítulo se detallan las tecnologías utilizadas en el desarrollo del proyecto.

De manera visual y esquemática podemos apreciar en la siguiente imagen el porcentaje del lenguaje empleado en el código.



Porcentaje lenguajes empleados

6.1 HTML

Aunque presenta un 3.2% del total del código, se expone en primer lugar, ya que es la base del proyecto y donde se emplea el lenguaje prepoderante de este proyecto, PHP.

HTML, siglas de HyperText Markup Language (Lenguaje de Marcado de Hipertexto), es el lenguaje de marcado predominante para la elaboración de páginas web. El lenguaje HTML es un estándar reconocido en todo el mundo y cuyas normas define un organismo sin ánimo de lucro llamado World Wide Web Consortium, más conocido como W3C. Como se trata de un estándar reconocido por todas las empresas relacionadas con el mundo de Internet, una misma página HTML se visualiza de forma muy similar en cualquier navegador de cualquier sistema operativo. El propio W3C define el lenguaje HTML como "un lenguaje reconocido universalmente y que permite publicar información de forma global". Por convención, los archivos de formato HTML usan la extensión .htm o .html.

6.2 CSS

Las hojas de estilo en cascada (Cascading Style Sheets, CSS) son un lenguaje formal usado para definir la presentación de un documento estructurado escrito en HTML. El W3C es el encargado de formular la especificación de las hojas de estilo que servirá de estándar para los agentes de usuario o navegadores.

La idea que se encuentra detrás del desarrollo de CSS es separar la estructura de un documento de su presentación. La información de estilo puede ser adjuntada tanto como un documento separado o en el mismo documento HTML.

En este proyecto se ha utilizado dos hojas de estilo común para todas las páginas que compartían misma cabecera y pie de página.

Dentro de CSS tenemos la tecnología BootStrap, la cual ha sido empleada para los cuerpos de cada página, así como sus tablas.

6.3 PHP

PHP es un lenguaje interpretado de propósito general ampliamente usado, diseñado especialmente para desarrollo web y que puede ser incrustado dentro de código HTML. Generalmente se ejecuta en un servidor web, tomando el código en PHP como su entrada y creando páginas web como salida. Puede ser desplegado en la mayoría de los servidores web y en casi todos los sistemas operativos y plataformas sin costo alguno. Es también el módulo Apache más popular entre las computadoras que utilizan Apache como servidor web.

Cuando el cliente hace una petición al servidor para que le envíe una página web, el servidor ejecuta el intérprete de PHP. Éste procesa el script solicitado que generará el contenido de manera dinámica (por ejemplo, como es el caso de este proyecto, obteniendo información de una base de datos). El resultado es enviado por el intérprete al servidor, quien a su vez se lo envía al cliente.

Permite la conexión a diferentes tipos de servidores de bases de datos tal como MySQL.

6.4 SQL

El lenguaje de consulta estructurado (SQL Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones sobre las mismas. Una de sus características es el manejo del álgebra y el cálculo relacional permitiendo lanzar consultas con el fin de recuperar de una forma sencilla información de interés de una base de datos, así como también hacer cambios sobre la misma.

```php
public function CompruebоDato($tabla,$campo, $dato){
    try {
        //ejecutamos una query para comprobar si el dato se encuentra en la bbdd
        $sentencia ="select * from ".$tabla." where ".$campo."='$dato'";
        $sql = $this->conec->query($sentencia);
        // captamos los posibles errores
        $this->conec->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
        //ejecutamos la consulta sql
        $sql->execute();
        //Contamos el número de filas devueltas en la consulta sql
        $total =$sql->rowCount();
        if($total ==1){
            //Si devuelve una fila el dato se encuentra en la bbddd
            return true;
        }else{
            return false;
        }
    } catch (PDOException  $e) {
        echo "<h3>Failed: </h3>" ."<h3>". $e->getMessage()."</h3>";
    }
```

Ejemplo empleo SQL en código

6.5 MySQL

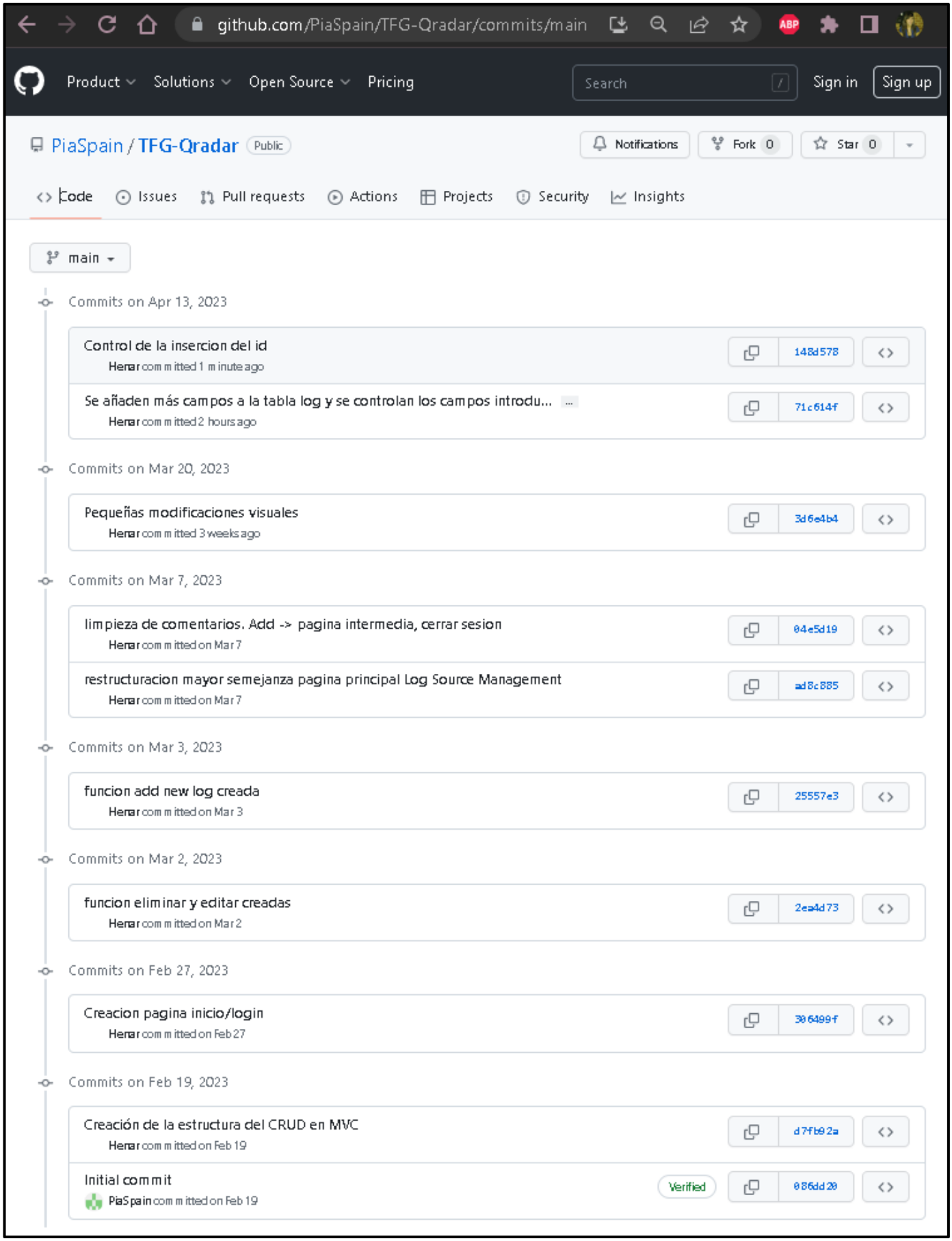
MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones. Su popularidad como aplicación web está muy ligada a PHP.

6.6 PhpMyAdmin

PhpMyAdmin es una herramienta escrita en PHP con la intención de manejar la administración de MySQL a través de páginas web, utilizando Internet. Actualmente puede crear y eliminar bases de datos, crear, eliminar y alterar tablas, borrar, editar y añadir campos, ejecutar cualquier sentencia SQL, administrar claves en campos, administrar privilegios, exportar datos en varios formatos y está disponible en 50 idiomas.

6.7 Control de Versiones – Git Hub

El control de versiones es un sistema que ayuda a rastrear y gestionar los cambios realizados en un archivo o conjunto de archivos. Utilizado principalmente por ingenieros de software para hacer un seguimiento de las modificaciones realizadas en el código fuente, el sistema de control de versiones permite analizar todos los cambios y revertirlos sin repercusiones si se comete un error.
GitHub es un servicio basado en gestión y organización de proyectos almacenados en la nube que aloja un sistema de control de versiones (VCS) llamado Git. Es decir que todos los usuarios de GitHub pueden rastrear y gestionar los cambios que se realizan en el código fuente en tiempo real, a la vez que tienen acceso a todas las demás funciones de Git disponibles en el mismo lugar.



Pantallazo Git Hub https://github.com/PiaSpain/TFG-Qradar

5.3 Diagrama de Gantt.

Más abajo, se muestra mediante un diagrama de Gantt el tiempo empleado en cada tarea del proyecto, así como de cada parte y su complejidad con el código.

Este diagrama está dividido y subdividido en grupos, claramente diferenciados por su id y color en el diagrama.

Como se ha explicado en el Capítulo 5. Metodología, la metodología empleada ha sido en modelo en cascada, por lo que al acabar cada tarea /parte del código se pasaba a la siguiente, solo volviendo atrás en caso de error.

Digrama de Gantt

ID	Tarea	Duración
1.0	Planteamiento	2h
2.0	Organización MVC	6h
2.1	Creación Base de Datos	1h
2.2	Estructura Controlador.php	1h
2.3	estructura Modelo.php	30 min
2.3.1	Sesiones.php	1h
2.3.1	exit.php cerrar.php	1h
2.3.2	Conexión BD -> Modelo	20 min
2.3.3	Index.html	2h
2.3.4	login.php	1h
2.3.5	Controlador -> existe	30 min
2.3.6	Modelo -> CompruebоUsu	1h
2.4	Vista -> CCS Headaer y Footer	1h30min
3	LogSources.php	1h
4	app.php	16h
4.1	Controlador -> buscoLog	1h
3.1	Modelo -> CompruebоDato	1h
4	addLog.php	2h
4.1	saveLog.php	4h
4.2	Controlador -> buscoLog	——
4.3	Modelo -> CompruebоDato	——
4.5	Controlador -> add	1h
4.6	Modelo -> saveLog	2h
5	editLog.php	2h
5.1	Controlador -> muestro	1h
5.2	Modelo -> muestroDatos	2h
5.3	saveLog.php	4h
5.4	Controlador -> edit	2h
5.6	Modelo -> editLog	2h
6	deleteLog.php	1h
6.1	Controlador -> delete	1h
6.2	Modelo -> deleteLog	1h
7	Organización Memoria	2h
7.1	Desarrollo Memoria	10h
7.2	Casos de Uso	2h
7.3	Diagrama BD	2h
Tiempo total		**78:40**

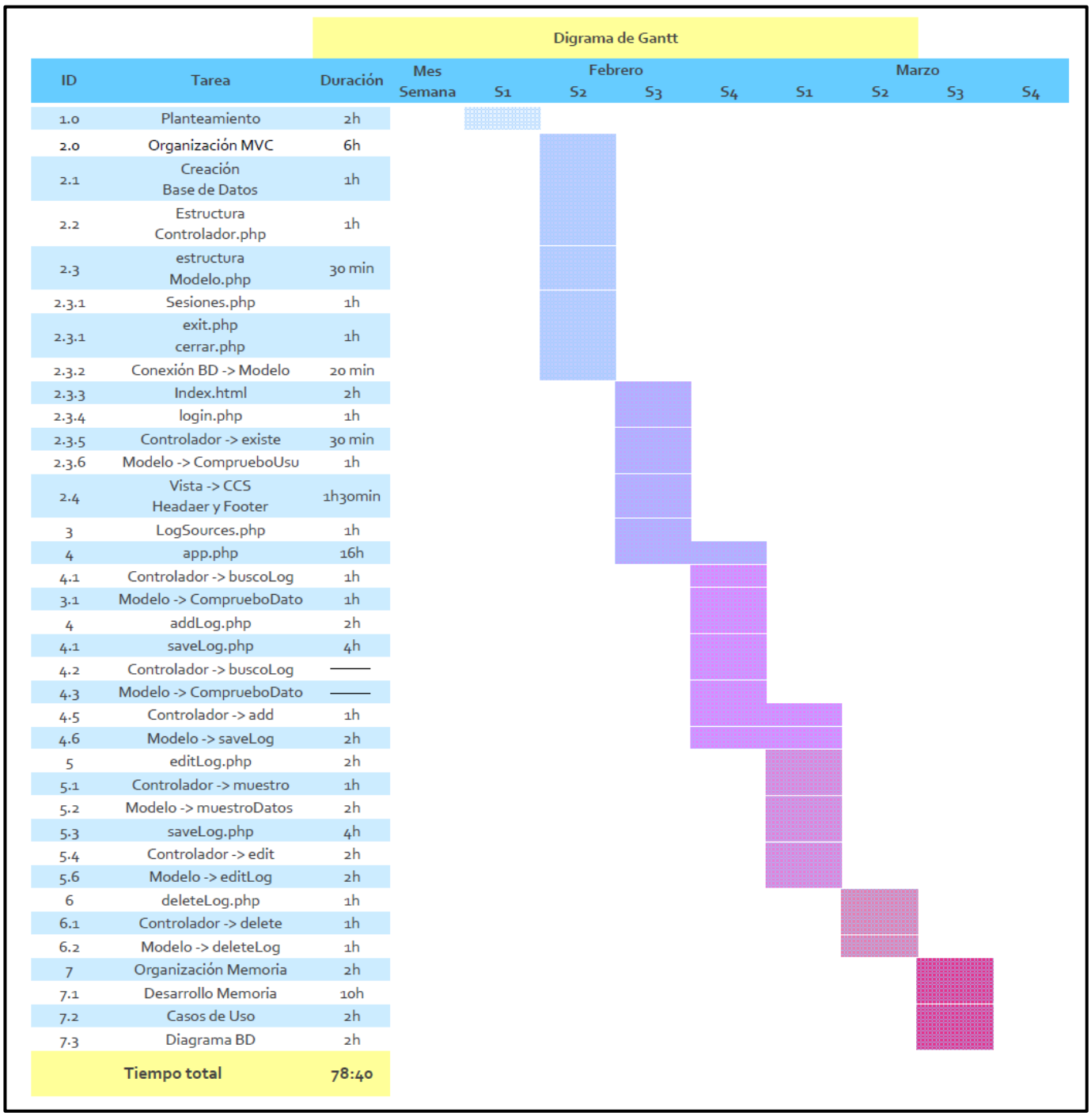


Diagrama de Gantt

Capítulo 7. Referencias

En este capítulo se hace un recorrido sobre el proyecto, tanto memoria, como código, para destacar aquellos puntos de donde se ha tomado referencia para poder realizar el proyecto de manera satisfactoria.

7.1 Código

- Se tomó como referencia un trabajo final de la misma alumna en la asignatura DEWS

Entrega de dicho trabajo final

- Se utilizo el siguiente video para recordar la estructura MVC https://www.youtube.com/watch?v=pn2v9lPakHQ&t=1817s
- Se ha utilizado BootStrap 5.6 para el diseño, tomando como referencia el entorno real de Qradar.
- Se utilizados iconos de: https://fontawesome.com/
- El código se encuentra perfectamente explicado, cada acción. Aún así, puede que algunas partes se haya tomado algunas páginas de internet como referencia. Podemos destacar;
    - https://developer.mozilla.org/es/
    - https://www.php.net/docs.php
    - https://www.w3schools.com/
    - https://lenguajehtml.com/
    - https://www.anerbarrena.com/programacion/php/
- También se consultó la página https://es.stackoverflow.com/ aunque no siempre con los resultados esperados.

7.2 Memoria

- En la elaboración del Capítulo 2. Desarrollo se consultaron diversas páginas web, para poder complementar junto con los conocimientos y nociones adquiridas en las prácticas los términos y sus definiciones de las siguientes páginas:
  - https://eniit.es/big-data-para-deteccion-de-intrusiones-en-proyectos-de-ciberseguridad/
  - https://www.ibm.com/es-es/topics/security-operations-center
  - https://revistasic.es/sic146/revistasic146.pdf

- En 2.5 Implementación se tomó de referencia la Api de IBM
  - https://www.ibm.com/es-es/products/qradar-siem
  - https://www.ibm.com/docs/es/qsip/7.4?topic=installations-installing-qradar-console
  - https://www.ibm.com/docs/es/qradar-on-cloud?topic=installations-installing-wincollect-agent-from-command-prompt
  - https://www.ibm.com/docs/es/qradar-common?topic=wincollect-communication-between-agents-qradar

- En el Capítulo 6. Implementación donde se desarrollan los lenguajes y tecnologías implementadas se tomaron las siguientes páginas de referencia:
  - 6.1 HTML → https://developer.mozilla.org/es/docs/Web/HTML
  - 6.2 CSS → https://developer.mozilla.org/es/docs/Web/CSS
  - 6.3 PHP → https://www.php.net/manual/es/intro-whatis.php
  - 6.4 SQL → https://www.ibm.com/docs/es/db2woc?topic=reference-sql
  - 6.5 MySQL → https://es.wikipedia.org/wiki/MySQL
  - 6.6 PhpMyAdmin → https://es.wikipedia.org/wiki/PhpMyAdmin
  - 6.7 Control de Versiones – Git Hub → https://www.hostinger.es/tutoriales/que-es-github

Capítulo 8. Conclusiones

A continuación, se realiza un resumen del trabajo realizado y las conclusiones a las que se han llegado una vez finalizado. También se presenta unas posibles ampliaciones al trabajo efectuado.

8.1 Resumen

El primer paso que se tomó fue establecer los requisitos que debía cumplir el proyecto con el tutor del centro educativo. Posteriormente presenté una propuesta al tutor quien me dio el OK.

Una vez, tenía la idea y el visto bueno, procedí a organizar el código y repasar los conocimientos obtenidos del grado, pues había pasado casi un año desde el último examen realizado.

La estructuración del código y su desarrollo en un principio fue un tanto rígido y lento, ya que se había perdido práctica, pero a medida que fue avanzando el proyecto la fluidez fue en aumento.

Podría dividir el proyecto en 7 etapas:

1. Planificación
2. Creación Base de Datos y PhpMyAdmin
3. Estructura MVC
4. Diseño / CSS
5. Añadir – Editar – Eliminar
6. Planteamiento y desarrollo memoria
7. Revisión y mejoras

He de decir que las partes que más tiempo me llevaron, sin ser tan productivas, fueron el punto 2 y 3, por lo que se ha comentado más arriba y es que por temas laborales el TFG, así como las practicas fueron aplazadas a casi un año desde la finalización de la parte teórica del módulo, lo que produjo que en un principio fuera más costoso y menos productivo algunas fases.

8.1.1 Validación personal del trabajo realizado

Durante la realización del proyecto he podido comprobar lo útiles que son los conocimientos adquiridos durante el grado en asignaturas como Base de Datos, Entornos de Desarrollo, Lenguaje de Marcas, Programación, Diseño de interfaces Web y Desarrollo Web en entorno Cliente, pero sobre todo a la hora de realizar las prácticas en un centro de trabajo, donde en un principio parecía no estar en relación con el módulo, asignaturas como Sistemas Informáticos o Despliegue de Aplicaciones Web, me dieron los conocimientos suficientes como para poder afrontar ciertas desventajas que podría suponer en un primer momento, en cuanto a nivel técnico.

8.2 Conclusión

Como bien se mencionó en Motivación, la ciberseguridad es una pieza fundamental en cualquier empresa. También se dijo, dentro del mismo capitulo que resulta imprescindible que cualquier titulado en todas las ramas de la tecnología tenga la máxima preparación en ciberseguridad, tanto a nivel corporativo como personal.

En 1.4 Conclusión ya se dio una pequeña pincelada de la conclusión final de este TFG. Es por esto, que desde este punto continuamos el desarrollo y la motivación del proyecto estableciendo que lo que se ha mostrado tanto en la memoria como en el código es la gran polivalencia que tiene un titulado en Desarrollo de Aplicaciones Web, pues este es capaz de crear y gestionar un sistema de seguridad para una empresa dedicada a la ciberseguridad, pues no solo puede crear, editar o eliminar una fuente que nos está dando datos importantes de un servidor, sino que es lo suficientemente competente como para crear dicho programa y ejecutarlo.

Dando por finalizada la conclusión, se ha de destacar y resumir la ya mencionada polivalencia del titulado en Desarrollo de Aplicaciones Web.

8.3 Posibles ampliaciones

Lo ya expuesto y explicado en este TFG ha sido una maqueta con funcionalidades ajustadas a los requisitos del proyecto.

A continuación, se listan una serie de ampliaciones que pudieran implementarse sobre el prototipo:

- Mejora en el control de acceso e información al usuario en la página del login.
- Implementar la aplicación de Disconected Log Collectors.
- Dar funcionalidad al botón <<Remember my choice>> en la página Log Management.
- Dar funcionalidad tanto a los posibles filtros en la página principal de Log Source Management.
- Modificar la página de añadir nueva fuente que sea más semejante a la original.
- Modificar las páginas de edición y eliminación de fuentes, a ventanas modales, para así ser más similares al entorno real.

Intencionadamente en blanco