KeyPaX, Barbaro Software

Propuesta técnica y económica del proyecto

22 de febrero de 2021

Índice

1. Resumen Ejecutivo

2. Objetivos del sistema

KeyPaX permite gestionar una colección de contraseñas de manera segura y remota. Permite almacenar los nombres de usuario y claves de acceso a distintos servicios, además de otra información adicional como URL y descripciones de texto. Estas contraseñas se pueden organizar en categoría y realizar búsquedas según sus campos. El sistema puede generar contraseñas robustas y configurables por el usuario. El usuario accederá a su colección de contraseñas mediante una contraseña maestra y realizará 2FA en las ocasiones requeridas. Se accederá al sistema mediante una interfaz web o una aplicación móvil.

2.1. Análisis de requisitos preliminar

Código	Descripción
RF-1	El sistema permite almacenar contraseñas
RF-1.1	El sistema permite almacenar pares que constan de nombre de usuario y contraseña
RF-1.2	El sistema permite asociar a las contraseñas una URL del sitio web al que corresponden
RF-1.3	El sistema registra la fecha de creación y actualización de la contraseña
RF-2	El sistema permite organizar las contraseñas por categorías
RF-3	El sistema permite realizar una búsqueda entre las contraseñas por categoría, fecha de creación y actualización
RF-4	El sistema permite generación de contraseñas pseudoaleatorias
RF-4.1	El sistema permite seleccionar la longitud de la contraseña a generar
RF-4.2	El sistema permite seleccionar el conjunto de caracteres que compone la contraseña a generar
RF-4.3	El sistema mostrará el grado de robustez de la contraseña al ser generada
RF-5	El sistema permite al usuario acceder a sus contraseñas únicamente a través de la contraseña maestra
RF-6	El sistema requiere 2FA para iniciar sesión desde un dispositivo nuevo, distinto a los utilizados con anterioridad
RF-7	El usuario se registra en el sistema mediante un correo electrónico y una contraseña maestra
RF-7.1	El registro de sesión se deberá confirmar, para verificar la identidad, mediante un correo al usuario registrado
RF-8	Se accede al sistema mediante una aplicación móvil
RF-9	Se accede al sistema mediante una interfaz web

3. Descripción técnica

3.1. Aspectos técnicos de relevancia para los usuarios

El acceso al repositorio de contraseñas de KeyPaX requiere de conexión a internet. Las contraseñas no son guardadas en el dispositivo del usuario para evitar desajustes de versionado y limitar la posibilidad de pérdida/*leaking* de las contraseñas.

El sistema KeyPaX permite a los usuarios acceder al repositorio mediante dos interfaces:

- Navegador web. El sistema funcionará al 100 % de sus capacidades en los siguientes navegadores web: Google Chrome, Firefox, Safari. En el resto de navegadores, el sistema puede no cargar ciertos componentes.
- Aplicación Android. La versión del sistema debe ser al menos 6.0 "Marshmellow".

3.2. Aspectos técnicos de relevancia para los clientes

El sistema está diseñado para ser desplegado en un entorno de contenedores Docker. Se ha escogido esta tecnología de despliegue por su alto aprovechamiento de los recursos de la máquina host y portabilidad a través de distintas máquinas. Dicho esto, a término del plazo de desarrollo del producto, el sistema quedará desplegado en un clúster remoto accesible vía internet por los usuarios. Dicho clúster remoto será de propiedad ajena a la empresa y los clientes deberán acarrear los costes de mantenimiento y alquiler de las máquinas que imponga el proveedor de cloud. Sin embargo, el código fuente completo del producto junto con manuales de despliegue serán entregados al cliente, por tanto, este puede decidir migrar el despliegue del sistema a máquinas propias que cumplan con los requisitos establecidos en los manuales.

Despliegue

El producto será desplegado en distintos componentes dockerizados:

- Front-end: Constituye la interfaz de usuario. Se separa en dos componentes, front-end para la aplicación móvil y front-end para la interfaz web.
- Back-end: Constituye el çerebro"del sistema, se encargará de atender todos los aspectos necesarios para que el sistema desarrolle el comportamiento diseñado.
- Base de datos: Almacenará la información de los usuarios y aquella necesaria para el funcionamiento del sistema.

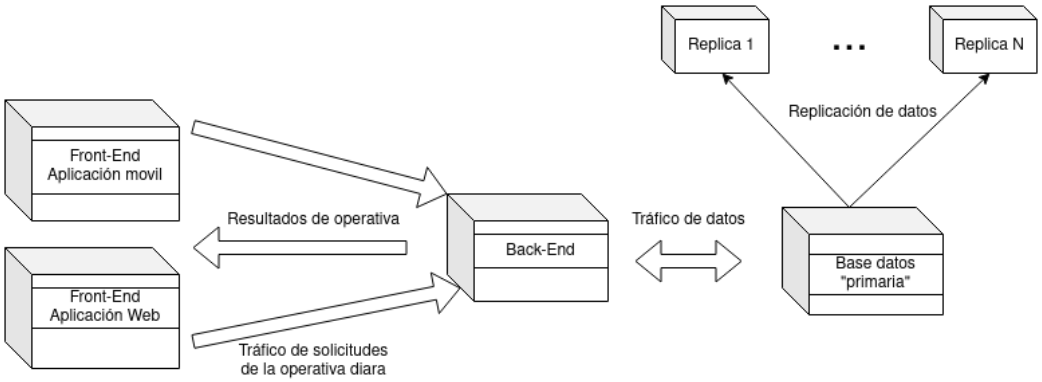

Figura 1: Primera versión del diagrama de despliegue

Análisis de riesgos y planes de contingencia

El mayor riego en el que incurre el sistema es la exposición de los datos de los usuarios a causa de una ataque a la base de datos. Para reducir el impacto y ocurrencia de este posible evento se propone limitar el acceso al componente de base de datos mediante contraseñas robustas, autentificación del origen de las peticiones a la base de dato y cifrado de la información.

Para prevenir ataques de tipo *ransomware* o el borrado malicioso de la información, se replicará la información de la base de datos a lo largo de un conjunto de replicas, lo cual permite disponer de un *back-up* de los datos para permitir el funcionamiento del sistema si ocurriese alguno de estos eventos.

En cuanto ataques contra la disponibilidad del sistema, se implementarán los cortafuegos necesarios para asegurar la disponibilidad en todo momento.

4. Plan de trabajo

A continuación se va a presentar un primer boceto de plan de trabajo con fechas importantes para los clientes.

Fecha	Descripción
22/02/2021	Presentación de la propuesta técnica y económica.
02/03/2021	Reunión de feedback con los clientes para aprobación/negociación de la propuesta técnica y económica anteriormente presentada. Comienzo de la redacción del plan de gestión, análisis y diseño.
15/03/2021	Presentación de la primera versión del plan de proyecto.
22/03/2021	Reunión de seguimiento con los clientes.
14/04/2021	Presentación de la segunda versión del plan de proyecto.
15/04/2021	Demostración a los clientes de la primera versión desplegada. Entrega de documentación generada hasta el momento y transferencia del código de la versión primera del sistema.
03/05/2021	Segunda reunión de seguimiento con los clientes.
21/05/2021	Demostración a los clientes de la segunda versión desplegada. Entrega de documentación generada hasta el momento y transferencia del código de la versión segunda del sistema.
01/06/2021	Entrega final del producto. Consistirá en la entrega del código fuente final, manuales de usuario en formato video y texto y delegación de control del producto ya instalado en servidores de acceso públicos.

5. Equipo técnico encargado del proyecto

Barbaro Software Inc. cuenta con tres años de permanencia en el mercado, que han proporcionado una amplia experiencia en el mundo empresarial y nos avala como una empresa referente en el sector. La empresa se caracteriza por tener una filosofía basada en el trabajo coordinado en grupo, con especialistas en distintos campos del sector que unificados forman un equipo de trabajo altamente sofisticado. Los servicios y capacidades que nuestros clientes han podido destacar entre los más importantes son:

- Experiencia en desarrollo móvil en dispositivos Android.
- Veteranía en el *framework* de JavaScript React para Web y Móvil.
- Destreza en el entorno de ejecución NodeJS con el *framework* Express.
- Práctica en Bases de Datos relacionales (Oracle, Postgresql, MySql...).
- Conocimiento en Base de Datos no relacionales (MongoDB).
- Alta uso de diferentes lenguajes de programación (Java, JavaScript, C, C++, GoLang).
- Estudio de metodología de despliegue de Proyectos con Docker y Kubernetes.
- Maestría en el uso de *IaaS* (Microsoft Azure, Amazon AWS).
- Prácticas de *testing* con PostMan.
- Altos conocimientos en gestión de versiones a través del Software Git.

Nuestro nombre proviene de Barbara Liskov, científica de la computación estadounidense reconocida con la medalla John von Neumann (2004) y el premio Turing (2008).

6. Presupuesto

Anexo I. Glosario

2FA *Two-Factor Authentication*. Método de autentificación que requiere dos tipos de información del usuario. Normalmente una contraseña y un código enviado al correo electrónico o teléfono móvil.

API *Application Programming Interface*. Conjunto de procedimientos que ofrece cierta biblioteca o sistema para ser utilizado por otro *software* e interaccionar con él abstrayendo ciertos aspectos.

Contraseña Clave alfanumérica y que puedo contener además símbolos para identificarse en un servicio o cuenta de internet.

Framework Plataforma para desarrollar aplicaciones software que ofrece una estructura inicial en la que los desarrolladores pueden construir para una plataforma específica.

IaaS *Infrastructure as a Service*. Servicios en línea, generalmente *cloud*, que proporcionan APIs de alto nivel que permiten abstraer detalles de infrastructura.

URL *Uniform Resource Identifier*. En este contexto, la dirección de la página web (www.example.com)

Anexo II. Estimación de costes