DARG (DATA ADMINISTRATION REVOLUTION GARAGE).

MANUAL DE USUARIO.

DESARROLLADORES:

- ADRIANA PAOLA MEJÍA MÉNDEZ
- MELANIE JACKELINE MARTÍNEZ RAMÍREZ
- EMILY GUADALUPE MURILLO ARGUETA
- DANIEL ALEJANDRO CORTEZ QUINTANILLA
- AXEL GABRIEL GARCÍA RAMÍREZ

PORTADA: Melanie

Índice

Introducción

¡Bienvenido al Manual de Usuario del Garage de Administración de Datos (DARG)!

Este documento está diseñado para guiarte en el uso eficiente y efectivo de nuestro software administrativo, creado específicamente para satisfacer las necesidades de gestión de talleres. Nuestro software tiene como objetivos facilitar la comprensión de nuestro proyecto, conocer las diferentes funcionalidades disponibles y permitirte indagar en todo el sistema sin ningún problema. Está dirigido a personas que estarán administrando el taller del proyecto, como empleados, y busca ayudarles a optimizar sus operaciones y mejorar la organización.

Este manual ofrece una guía paso a paso sobre cómo utilizar cada una de las funcionalidades del proyecto. Desde la instalación inicial, encontrarás instrucciones claras y capturas de pantalla que te ayudarán a aprovechar al máximo todas las funciones disponibles.

Emily (Ponelo en tercera persona wt)

Manejo de usuarios.

Daniel

Mantenimientos.

Melanie

Lógica del negocio.

Axel

Gráficos y reportes.

Gráficos que se muestran en la aplicación

Gráficos Automáticos

- **1**
- **2**
- **3**
- **4**

Gráficos Parametrizados

- **1**
- **2**
- **3**
- **4**

Gráficos Predictivos.

- **Adriana**
- **Adriana**

Reportes que se muestran en la aplicación

Reportes Automáticos

- **1**
- **2**
- **3**

- **4**

Reportes Parametrizados

- **1**
- **2**
- **3**
- **4**

Reportes Predictivos.

- **Adriana**
- **Adriana**

Seguridad.

En el presente apartado se describen las medidas que se han implementado para proteger la información y asegurar el control de acceso dentro del sistema. A continuación, se detallan los principales aspectos de seguridad que se han tenido en cuenta para ofrecer un entorno confiable y seguro para los usuarios:

01. Restauración y Cambio de Contraseña

- **Restauración de contraseña**: El usuario puede restaurar su contraseña en caso de haberla olvidado o perdido, a través de un apartado disponible en la pantalla de inicio de sesión. Para iniciar el proceso, debe hacer clic en el botón "Cambiar contraseña". El procedimiento consta de varios pasos:

    1. Primero, se le pedirá que ingrese el correo electrónico con el que registró su cuenta, para enviarle un código de verificación.

    2. A continuación, el usuario deberá ingresar dicho código en un campo específico dentro del apartado en el que se encuentre.

    3. Si el código coincide con el enviado al correo, se le solicitará que ingrese una nueva contraseña, diferente a la anterior, y que la confirme.

    4. Finalmente, si la nueva contraseña cumple con los requisitos de seguridad (como el mínimo de caracteres, inclusión de mayúsculas, minúsculas, etc.), podrá hacer clic en el botón "Aceptar", y su contraseña será restablecida exitosamente.

- **Cambio de contraseña**: El usuario puede cambiar su contraseña después de haber iniciado sesión si desea una diferente. Para ello, debe acceder al apartado de "Usuario" y seleccionar la opción "Cambiar contraseña". En esta sección, encontrará tres campos: uno para ingresar la contraseña actual, otro para ingresar la nueva

contraseña y un último para confirmar.Una vez que haya completado los tres campos y hecho clic en "Aceptar", se realizarán varias validaciones, como comprobar que la nueva contraseña sea diferente de la actual, que cumpla con los requisitos mínimos de seguridad (como la cantidad de caracteres, mayúsculas, minúsculas, etc.). Si todo está correcto, la contraseña se actualizará con éxito.

02. Cierre de Sesión

- **Cierre de sesión manual:** **Axel**

- **Cierre de sesión por inactividad:** Con el fin de prevenir accesos no autorizados en dispositivos compartidos o desatendidos, se ha implementado un cierre de sesión automático por inactividad. Este mecanismo desconecta al usuario tras 5 minutos sin interacción del usuario.

03. Intentos fallidos de inicio de sesión

- Con el fin de brindar transparencia al usuario y permitir un seguimiento efectivo de los problemas de seguridad, el sistema implementa una medida de bloqueo de cuenta después de 3 intentos fallidos de inicio de sesión. Al alcanzar este límite, la cuenta se bloqueará temporalmente y el usuario no podrá acceder al sistema hasta transcurridas 24 horas.

04. Visualización de Errores (403 y 404)

- **Error 403 (Prohibido):** **Axel**

- **Error 404 (No encontrado):** **Axel**

05. Sesiones Expiradas

- Con el fin de asegurar que las contraseñas permanezcan seguras y proteger mejor la información del usuario frente a posibles amenazas, el sistema forzará el cierre de

sesión si la contraseña no ha sido actualizada dentro del periodo configurado (90 días). Antes de permitirle iniciar sesión nuevamente, se solicitará el cambio de contraseña. Para realizar este proceso, el usuario debe hacer clic en el botón "Cambiar contraseña" en la pantalla de inicio de sesión y seguir el mismo procedimiento que se detalla en la sección de restauración de contraseña.

06. Cifrado de Datos

- **Axel**

Mensajería.

Daniel y Emily