



ContraSegur

Manual de Usuario

Versión: 0100

Fecha: 21/04/2025

Versión δ (con Base de Datos)

ContraSegur © 2025 por Gemma Semley-Dyne está licenciado bajo Creative Commons Reconocimiento 4.0 Internacional

	ContraSegur Manual de Usuario	IES Bendinat
---	---	---------------------

HOJA DE CONTROL

Organismo	IES Bendinat		
Proyecto	ContraSegur		
Entregable	Manual de Usuario		
Autor	Gemma Semley-Dyne		
Versión/Edición	0100	Fecha Versión	21/04/2025
Aprobado por	Pere Miquel Rosselló Espases	Fecha Aprobación	DD/MM/AAAA
		Nº Total de Páginas	67

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
0100	Primera versión del manual	Gemma Semley-Dyne	21/04/2025

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos
Pere Miquel Rosselló Espases

ÍNDICE

<u>1 DESCRIPCIÓN DEL SISTEMA</u>	4
1.1 Objeto.....	4
1.2 Alcance.....	4
1.3 Funcionalidad.....	4
<u>2 MAPA DEL SISTEMA</u>	6
2.1 Modelo Lógico.....	6
2.1.1 Flujograma.....	6
2.1.2 Estructuras de datos.....	6
2.1.3 Modelo relacional de la base de datos.....	8
2.2 Navegación.....	10
<u>3 DESCRIPCIÓN DEL SISTEMA</u>	13
3.1 Subsistema 1.....	13
3.1.1 Pantalla 1.....	13
3.1.2 Pantalla 2.....	32
3.1.3 Pantalla 3.....	35
3.1.4 Mensajes de error.....	39
3.1.5 Ayudas contextuales.....	39
3.2 Subsistema 2.....	40
3.2.1 Pantalla 1.....	40
3.2.2 Mensajes de error.....	51
3.2.3 Ayudas contextuales.....	51
<u>4 FAQ</u>	52
4.1 ¿Qué significa que este trabajo está licenciado bajo Creative Commons Reconocimiento 4.0 Internacional?.....	52
4.2 ¿Cuál es el propósito de este proyecto?.....	52
4.3 ¿Qué hace que una contraseña sea fuerte?.....	52
4.4 ¿Puedo usar esta herramienta para administrar mis contraseñas reales?.....	52
4.5 ¿Es confiable el generador de contraseñas?.....	52
4.6 ¿Cuál es la diferencia entre "score" y la puntuación "zxcvbn"?.....	53
4.7 ¿Cómo debe ser el formato del fichero?.....	53
4.8 ¿Qué ocurre si el formato del fichero es incorrecto?.....	54
4.9 ¿Cómo maneja el sistema los caracteres no latinos (como cirílico o emojis) en las contraseñas?.....	54
4.10 ¿Qué se incluirá en versiones posteriores de este proyecto?.....	55
<u>5 ANEXOS</u>	56
5.1 Fichero contraseñas comunes.....	56
5.2 Fichero patrones comunes.....	56
5.3 Cálculos internos y externos de la robustez.....	56
<u>6 GLOSARIO</u>	58
<u>7 BIBLIOGRAFÍA Y REFERENCIAS</u>	60

1 DESCRIPCIÓN DEL SISTEMA

1.1 Objeto

Este proyecto consiste en una aplicación web cuyo objetivo principal es facilitar la creación, evaluación y gestión de contraseñas seguras mediante una interfaz gráfica intuitiva y visualmente clara. La herramienta evalúa contraseñas ingresadas según criterios de seguridad establecidos, proporcionando métricas comprensibles como el tiempo estimado para ser descifradas mediante ataques de fuerza bruta o su coincidencia con patrones comunes. Asimismo, ofrece recursos educativos sobre ciberseguridad y permite la localización en varios idiomas, favoreciendo su adopción global. Para complementar esta funcionalidad, el sistema utiliza una base de datos editable con SQLite Studio, que permite al usuario gestionar directamente los idiomas, patrones y diccionarios de contraseñas desde una interfaz externa sencilla, ampliando así la personalización y adaptabilidad del entorno.

1.2 Alcance

Aunque esta herramienta está diseñada para ser universal, su propósito principal es servir como recurso educativo en el entorno escolar. Está pensada específicamente para los estudiantes del IES Bendinat como una forma de aprender sobre ciberseguridad de forma práctica y accesible. Está dirigida a usuarios que desean proteger su información personal creando contraseñas seguras, sin necesidad de tener conocimientos técnicos avanzados.

1.3 Funcionalidad

La herramienta "Contraseñas Seguras" cuenta con un amplio conjunto de funcionalidades:

- Validación dinámica de contraseñas ingresadas, comprobando en tiempo real que cumplan con criterios básicos como longitud mínima, inclusión de letras mayúsculas, minúsculas, números y caracteres especiales.
- Análisis exhaustivo de la robustez de las contraseñas mediante el uso combinado de cálculos propios y del algoritmo zxcvbn, que detecta patrones comunes, secuencias, repeticiones.
- Visualización interactiva de la seguridad de la contraseña mediante una barra de progreso que se actualiza conforme el usuario escribe, ofreciendo retroalimentación visual e intuitiva.
- Estimación del coste computacional que supondría descifrar la contraseña mediante fuerza bruta, incluyendo el tiempo aproximado necesario y una clasificación del nivel de seguridad.
- Generación automática de contraseñas seguras utilizando combinaciones aleatorias de caracteres con alta entropía, que pueden ser usadas directamente por el usuario.
- Soporte multilingüe, permitiendo traducir la interfaz y los mensajes del sistema a varios idiomas como inglés, catalán, francés y español.
- Integración con ficheros externos para identificar contraseñas comunes o patrones de palabras frecuentes, que puedan comprometer la seguridad.
- Ofrecer la posibilidad de manipular la base de datos para añadir un nuevo idioma



junto con su conjunto específico de contraseñas comunes, ampliando así la capacidad del sistema para adaptarse a diferentes contextos lingüísticos y culturales.

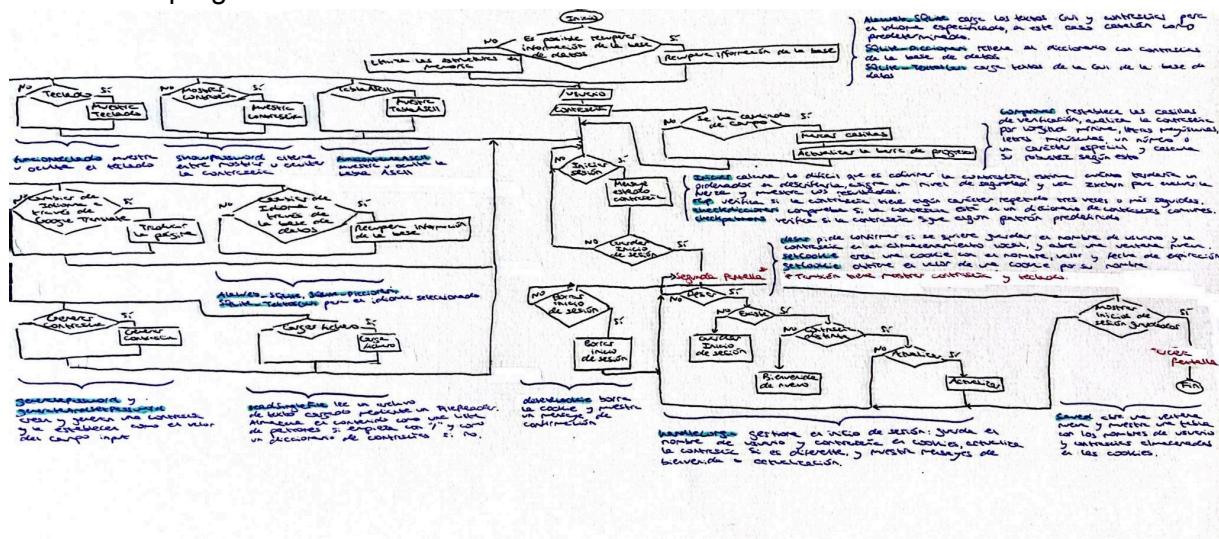
- Incorporación de elementos de ayuda como teclados virtuales, tabla ASCII, y enlaces informativos para que los usuarios puedan entender mejor cada componente de la herramienta.
- Capacidad para almacenar y gestionar contraseñas dentro del sistema incluyendo funciones para visualizarlas, eliminarlas o actualizarlas, siempre de forma segura.

2 MAPA DEL SISTEMA

2.1 Modelo Lógico

2.1.1 Flujograma

En este apartado se incluirá un flujograma de la aplicación web enfocado en los aspectos técnicos del programa.



2.1.2 Estructuras de datos

En esta sección se presenta una tabla de estructuras de datos utilizadas.

Estructura de datos	Por qué se utilizó	Nombre en código	Ejemplo en el código
Array	Almacena listas de contraseñas comunes (diccionarialt) y patrones de expresiones regulares (patrones).	diccionarialt, patrones	javascript var diccionarialt = ["password", "123456", "qwerty"];
Set	Comprueba de forma eficiente si existe una contraseña en un diccionario (búsqueda más rápida que en un array).	diccionari	javascript var diccionari = new Set(diccionarialt);

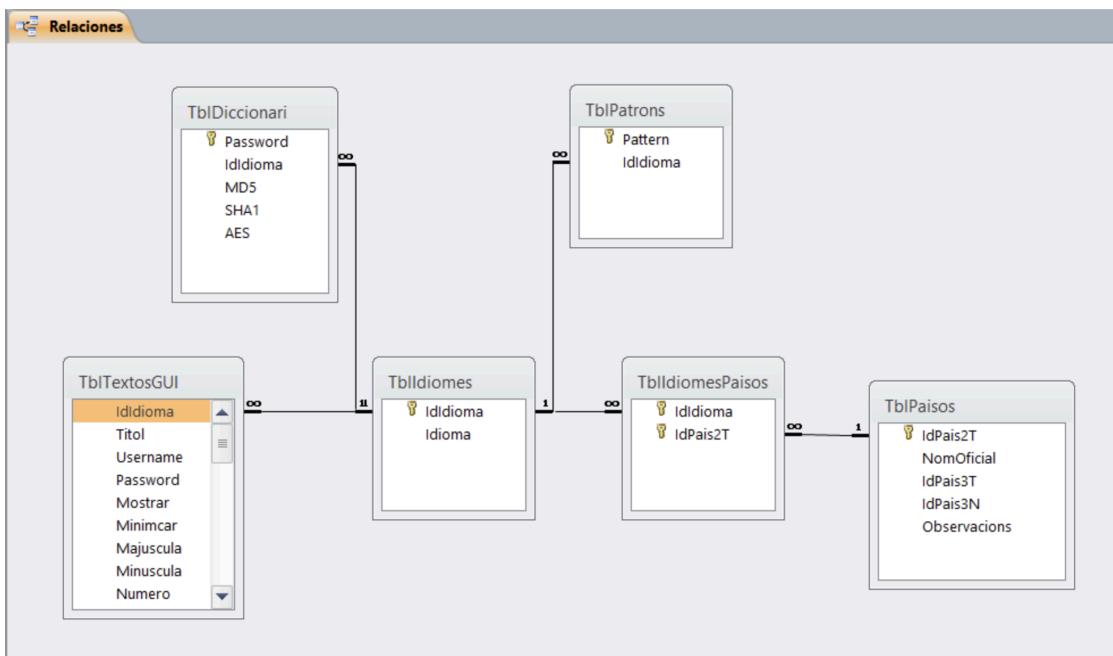
Regular Expression (RegEx)	Almacena patrones comunes que se encuentran en las contraseñas.	patrons, repmult	javascript var patrons = [/123/, /abc/, /(.)\1{2,}/];
LocalStorage	Guarda el nombre de usuario y la contraseña entre sesiones (para mayor comodidad).	localStorage	javascript localStorage.setItem("Username", "user123");
Object	Almacena traducciones de idiomas (por ejemplo, inglés, español, catalán).	Idioma, Idiomes_dft	javascript var Idioma = { "Username": "Usuari" };
SQLite (via alasql)	Obtiene contraseñas comunes y traducciones de una base de datos.	AlaWeb_SQLite()	javascript alasql('SELECT * FROM TblTextosGUI');
Cookies	Almacena los datos de inicio de sesión del usuario (nombre de usuario + contraseña) de forma persistente en el navegador.	document.cookie	javascript document.cookie = "user=pass; expires=...";
Date Object	Establece el tiempo de expiración de las cookies.	new Date()	javascript d.setTime(d.getTime() + (days * 24 * 60 * 60 * 1000));
Array	Almacena pares clave-valor de cookies divididas.	ca (cookie array)	javascript let cookies = decodedCookie.split(',');
Window Object	Abre una ventana emergente para mostrar los inicios de sesión guardados.	window.open()	javascript const myWindow = window.open(...);
DOM Manipulation	Alterna la visibilidad de la contraseña de los elementos de la interfaz de usuario.	getElementById() , hidden	javascript x.type = "text";

2.1.3 Modelo relacional de la base de datos

La base de datos de Contraseñur está diseñada para soportar un entorno completamente multilingüe. Su estructura modular permite integrar fácilmente nuevos idiomas, así como sus patrones de validación y listas de contraseñas comunes.

La tabla central, **TblIdiomes**, almacena los distintos idiomas disponibles en el sistema. A partir de ella se articulan las siguientes funcionalidades:

- **TblTextosGUI** permite definir las etiquetas e instrucciones de la interfaz gráfica en múltiples idiomas. Cada idioma tiene su conjunto completo de textos, lo que garantiza una experiencia de usuario completamente localizada.
- **TblDiccionari** almacena contraseñas comunes, cifradas mediante distintos algoritmos (MD5, SHA1, AES), clasificadas por idioma. Esto permite adaptar los controles de seguridad y advertencias a las particularidades lingüísticas y culturales de cada comunidad.
- **TblPatrons** define patrones de validación personalizados (como expresiones regulares), también vinculados a idiomas específicos. Así, se pueden implementar requisitos distintos según el idioma, como el uso de ciertos caracteres o formatos.
- **TblPaisos** y su tabla relacional **TblIdiomesPaisos** permiten asociar idiomas a países concretos.



A continuación se detallará las tablas y sus campos:

TblIdiomes representa el núcleo del sistema multilingüe.

- IdIdioma (clave primaria): Identificador único del idioma. Usado como referencia externa.
- Idioma: Nombre completo del idioma (ej. "Español", "English", "Català").

TblTextosGUI contiene las traducciones de los textos usados en la interfaz gráfica.

- IdIdioma (clave foránea → TblIdiomes): Vincula el conjunto de textos con su idioma.
- Titol: Título principal de la aplicación o ventana inicial.

- Username: Etiqueta del campo donde se introduce el nombre de usuario o correo electrónico.
- Password: Etiqueta del campo de introducción de la contraseña.
- Mostrar: Texto para el botón u opción de mostrar/ocultar la contraseña.
- Minimcar: Advertencia sobre la longitud mínima exigida de la contraseña.
- Majuscula: Requisito de contener al menos una letra mayúscula.
- Minuscula: Requisito de contener al menos una letra minúscula.
- Numero: Requisito de incluir al menos un número.
- Carespecial: Requisito de incluir al menos un carácter especial (como @, #, \$, etc.).
- Robustesa: Indicadores de robustez de la contraseña según su análisis.
- Inisessio: Texto del botón para iniciar sesión.
- Massacomu: Advertencia cuando se detecta una contraseña presente en diccionarios comunes.
- Nopatrons: Mensaje cuando se detectan patrones predecibles.
- Norepmult: Mensaje cuando hay demasiadas repeticiones.
- Majminnum: Recordatorio de los requisitos mínimos básicos para una contraseña segura.
- Almcaresp: Requisito de incluir un carácter no alfanumérico.
- Almmincar: Advertencia cuando no se alcanza la longitud mínima.
- Contrarob: Mensaje cuando la contraseña cumple con todos los requisitos.
- Computacional: Introducción al análisis de coste computacional para romper la contraseña por fuerza bruta.
- Maquina: Continuación del análisis: estima el tiempo requerido por una máquina con cierta capacidad.
- Processament: Convierte el cálculo anterior en años.
- Nivell: Traduce a días y añade el nivel de robustez asociado.
- Score: Presenta la puntuación total obtenida por la contraseña.
- Voldesar: Mensaje de confirmación para guardar las credenciales.
- Diccionari: Etiqueta que introduce los resultados de análisis por diccionario de contraseñas.
- Patrons: Etiqueta que introduce los resultados de análisis de patrones.
- Mostrartaula: Texto del botón para mostrar la tabla de resultados detallados.
- Amagartaula: Texto del botón para ocultar dicha tabla.

TblDiccionari gestiona contraseñas comunes inseguras por idioma.

- Password (clave primaria): Contraseña en texto plano (preferiblemente normalizada o anonimizada).
- IdIdioma (clave foránea → TblIdiomes): Idioma al que pertenece la contraseña.
- MD5 / SHA1 / AES: Cifrado de la contraseña con distintos algoritmos. Permite detectar contraseñas inseguras en diversos formatos de seguridad.

TblPatrons define patrones de validación para contraseñas.

- Pattern (clave primaria): Expresión regular o formato de validación.
- IdIdioma (clave foránea → TblIdiomes): Idioma con el que se relaciona el patrón.

TblPaisos contiene los datos de cada país, incluyendo su identificación estandarizada.

- IdPais2T (clave primaria): Código ISO alfa-2.
- NomOficial: Nombre oficial del país.
- IdPais3T: Código ISO alfa-3.
- IdPais3N: Código numérico ISO.
- Observaciones: Campo libre para notas, dialectos o características particulares del país.

TblIdiomasPaisos es una tabla intermedia que relaciona idiomas y países. Permite múltiples idiomas por país y viceversa.

- IdIdioma (clave foránea → TblIdiomas): Idioma hablado en el país.
- IdPais2T (clave foránea → TblPaisos): País donde se habla ese idioma.

2.2 Navegación

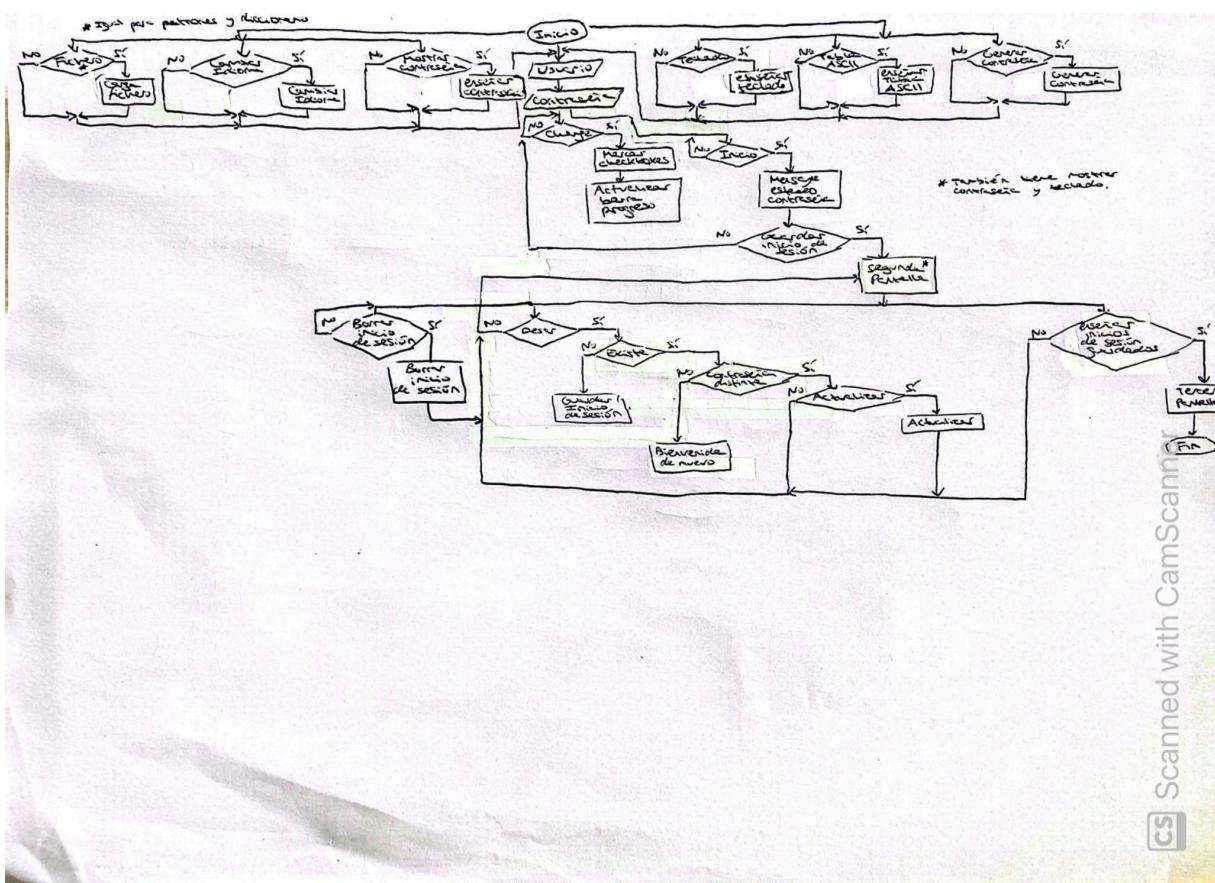
A continuación describiré el flujograma de navegación de la aplicación web. Este diagrama de flujo es una versión muy simplificada del programa con el propósito de entender el flujo lógico del mismo. La aplicación ContraSegur ha sido diseñada con una estructura de navegación clara y accesible, que permite al usuario desplazarse de forma intuitiva entre sus distintas funcionalidades. Desde el momento en que se accede a la pantalla de inicio, el sistema guía al usuario a través de diversas acciones que lo conducen a otras secciones, cada una diseñada con funciones específicas y bien delimitadas.

Al iniciar, tiene la opción de utilizar un teclado en pantalla, consultar una tabla ASCII con los caracteres disponibles, generar una contraseña aleatoriamente, mostrar u ocultar la contraseña a medida que se escribe, cambiar el idioma mediante un menú desplegable o iconos con banderas representativas, y agregar archivos externos para un análisis más exhaustivo de la contraseña, como contraseñas o patrones comunes. Además, puedes introducir tu nombre de usuario y contraseña. Al hacerlo, las casillas con los requisitos básicos de una contraseña segura y la barra de progreso que indica su nivel de seguridad se completarán según corresponda.

Al pulsar el botón "Iniciar sesión", el sistema realiza un análisis de la contraseña proporcionada y muestra un mensaje emergente que detalla el nivel de seguridad de la misma, el coste computacional estimado para descifrarla y si existen coincidencias con contraseñas o patrones comunes. A continuación, podrás decidir si deseas guardar tus datos de inicio de sesión. Si lo haces, accederás a una segunda pantalla orientada a la gestión de credenciales. En este apartado, podrás visualizar las credenciales que ya has guardado, eliminar entradas existentes, actualizar contraseñas previamente almacenadas y volver a hacer uso del teclado virtual o del botón para mostrar la contraseña.

Si aún no has guardado tus datos, se almacenarán. De lo contrario, se te dará la bienvenida de nuevo. Si el nombre de usuario ya está guardado pero con una contraseña distinta, el sistema solicitará confirmación para actualizarla. En esta vista, también es posible eliminar la entrada correspondiente, y el sistema confirma todas las acciones mediante mensajes emergentes.

Desde esta segunda pantalla se puede acceder a una tercera vista, donde se presenta una tabla con todas las credenciales almacenadas: nombres de usuario y contraseñas. Durante toda la navegación, la aplicación ContraSegur mantiene una comunicación constante con el usuario a través de mensajes contextuales. Estos mensajes informan del estado de las contraseñas, las acciones ejecutadas (como guardar, borrar o actualizar), y la robustez de las combinaciones introducidas, ofreciendo así una experiencia fluida, comprensible y segura.



Por otra parte, el usuario puede navegar por SQLite Studio, una herramienta gráfica externa que permite al usuario interactuar con la base de datos del sistema ContraSegur y realizar modificaciones personalizadas. Este entorno está pensado para usuarios con un mínimo de familiaridad con bases de datos, y facilita la edición directa del archivo ContraSegur.db.

Al acceder a la plataforma (<https://sqlitesudio.netlify.app>), el usuario puede arrastrar y soltar el archivo de base de datos o seleccionarlo manualmente mediante el botón habilitado para ello. El archivo a cargar debe ser el ContraSegur.db, que contiene todas las tablas necesarias para el funcionamiento multilingüe del sistema.

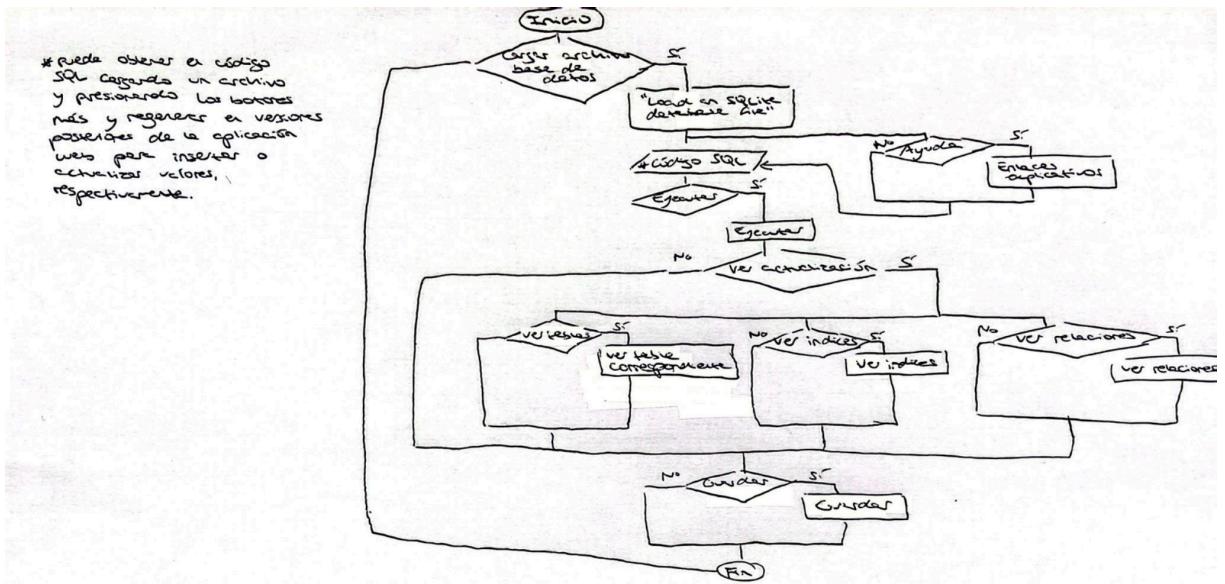
Una vez cargado el archivo, el sistema mostrará visualmente las tablas contenidas en la base de datos, como TblIdiomes, TblTextosGUI, TblDiccionari y TblPatrons. Desde aquí,

insertar los nuevos valores en la tabla que desea el usuario mediante una instrucción INSERT INTO o actualizar datos mediante una instrucción UPDATE. Este código debe seguir la estructura establecida para que el sistema los reconozca correctamente.

Una vez escrito el código SQL, el usuario debe pulsar el botón "Execute" para aplicar los cambios. Si la instrucción es correcta, los nuevos datos se insertarán y podrán visualizarse al volver a consultar la tabla correspondiente mediante el botón "Tables".

Para finalizar el proceso, es imprescindible guardar los cambios realizados presionando el botón "Save the db". Esto asegura que las nuevas entradas permanezcan registradas en el archivo y puedan ser utilizadas por la aplicación web.

A lo largo de esta navegación, el sistema ofrece una interfaz clara con paneles visuales para ver resultados, escribir código SQL y consultar datos existentes, lo que facilita la modificación directa de las funcionalidades lingüísticas del sistema.





ContraSegur
Manual de Usuario

IES Bendinat

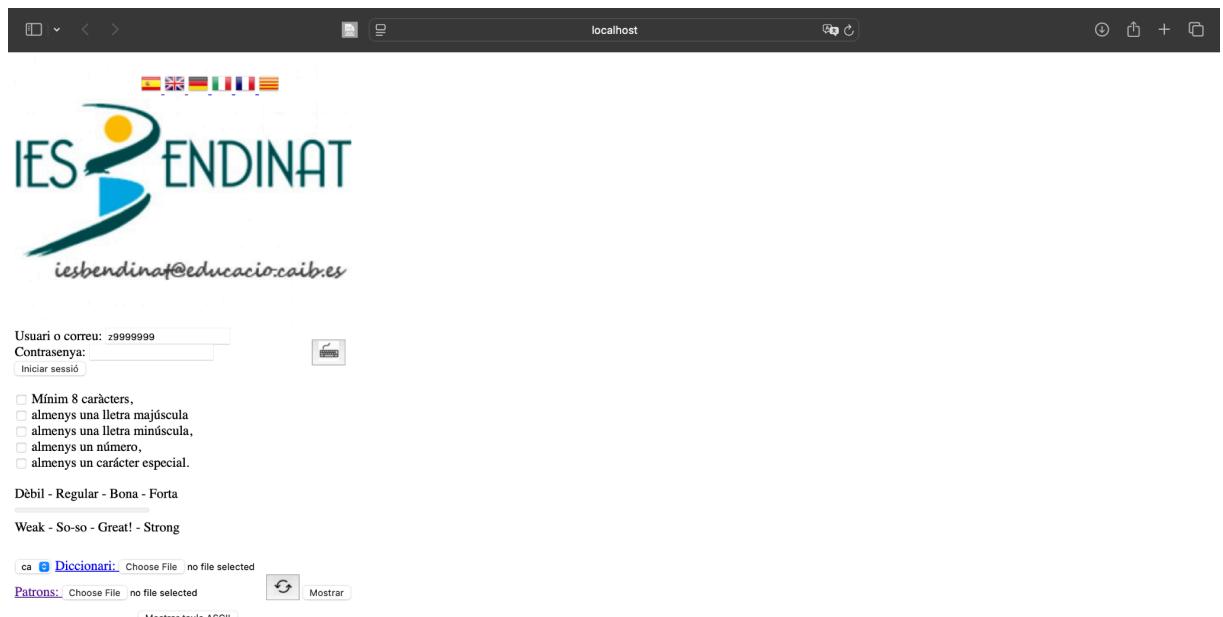
3 DESCRIPCIÓN DEL SISTEMA

Esta sección describe el funcionamiento del sistema ContraSegur, detallando sus subsistemas, la estructura de la aplicación desde la perspectiva del usuario, su interacción con la base de datos y el recorrido por la interfaz. Mediante capturas de pantalla y explicaciones, se busca ofrecer una visión clara de cómo actúa el sistema en cada fase.

3.1 Subsistema 1

El subsistema 1 es la aplicación web. A continuación mostraré todos los caminos que puede tomar el usuario, explicando cada paso.

3.1.1 Pantalla 1



Esta es la pantalla que se muestra al cargar la aplicación web por primera vez. Como puede ver, en la parte superior se encuentran las banderas de los países (de izquierda a derecha: España, Reino Unido, Alemania, Italia, Francia y Cataluña). Justo debajo, el logotipo del IES Bendinat. A continuación, hay dos cuadros de texto para introducir un nombre de usuario o correo electrónico y la contraseña. A la derecha, un botón de teclado. Debajo, un botón de inicio de sesión. Además, hay cinco casillas de verificación que corresponden a los requisitos de una contraseña segura: un mínimo de 8 caracteres, al menos una letra mayúscula, al menos una letra minúscula, al menos un número y al menos un carácter especial. Justo debajo, una barra de progreso (de izquierda a derecha), que indica la robustez de la contraseña. Es importante mencionar que, al crear este manual, surgieron dificultades técnicas con esta barra de progreso, por lo que no es representativa en las



siguientes capturas de pantalla. Debajo, a la izquierda, se encuentra un menú desplegable con los idiomas catalán (ca), español (es), inglés (en) y francés (fr). Posteriormente, tenemos dos lectores de archivos: uno para contraseñas comunes (Diccionari) y otro para patrones comunes (Patrons). También tenemos un botón para generar una contraseña aleatoria y otro para mostrar la contraseña mientras se escribe. Finalmente, un botón para mostrar la tabla ASCII.

Usuari o correu: z9999999
Contrasenya:
Iniciar sessió

Mínim 8 caràcters,
almenys una lletra majúscula
almenys una lletra minúscula,
almenys un número,
almenys un caràcter especial.

Dèbil - Regular - Bona - Forta
Weak - So-so - Great! - Strong

ca Diccionari: Choose File no file selected
Patrons: Choose File no file selected

Mostrar

Mostrar taula ASCII

Aquí podemos ver lo que sucede cuando presionamos el botón del teclado, proporciona un teclado en pantalla con letras minúsculas.



Screenshot of the ContraSegur login page for IES Bendinat. The page includes the school's logo and contact email (iesbendinat@educacio.caib.es). It features a password strength meter from 'Dèbil' to 'Strong'. A large ASCII character map is displayed, with the top section showing standard characters and the bottom section showing accented characters (À, È, Ì, Ò, Ú, À, È, Ì, Ò, Ú, À, È, Ì, Ò, Ú).

Aquí podemos ver lo que sucede cuando presionamos el botón de ↑, que nos muestra las letras en mayúsculas.

Screenshot of the ContraSegur login page for IES Bendinat, identical to the previous one but with the ASCII character map showing only uppercase characters (À, È, Ì, Ò, Ú, À, È, Ì, Ò, Ú, À, È, Ì, Ò, Ú).

Aquí podemos ver lo que sucede cuando presionamos el botón de [^], que nos muestra más caracteres como, por ejemplo, con acentos diacríticos.

ca [Diccionari](#): Choose File no file selected

Patrons: Choose File no file selected

[Mostrar](#)

Mostrar taula ASCII

\	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F															
0	♦	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤															
1	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤															
2	!	!	#	\$	%	&	*	()	*	+	-	-	/																	
3	o	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?															
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O															
5	P	Q	R	S	T	U	V	W	X	Y	Z	[l]	^	-															
6	.	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o															
7	p	q	r	s	t	u	v	w	x	y	z	())	-																
8	€	▀	,	f	,	..	+	+	+	‰	ſ	<	Œ	▀	▀	▀															
9	▀	,	*	*	*	*	-	-	-	*	»	ø	▀	z	ÿ																
A	i	ɛ	ɛ	ɛ	ɛ	ɛ	ɛ	ɛ	ɛ	ɛ	ɛ	ɛ	ɛ	ɛ	ɛ	ɛ															
B	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ	ɔ															
C	À	Á	Ã	À	Ã	À	Ã	À	Ã	À	Ã	À	Ã	À	Ã	À															
D	Đ	Ñ	Ó	Ó	Ó	Ó	Ó	Ø	Ù	Ù	Ù	Ù	Ù	Ù	Ù	Ù															
E	È	À	À	À	À	À	À	à	à	à	à	à	à	à	à	à															
F	ñ	ñ	ñ	ñ	ñ	ñ	ñ	ñ	ñ	ñ	ñ	ñ	ñ	ñ	ñ	ñ															
##Char																															
000:	♦ 001;	¤ 002;	¤ 003;	¤ 004;	¤ 005;	¤ 006;	¤ 007;	¤ 008;	¤ 009;	¤ 010;	¤ 011;	¤ 012;	¤ 013;	¤ 014;	¤ 015;	¤															
016:	¤ 017;	¤ 018;	¤ 019;	¤ 020;	¤ 021;	¤ 022;	¤ 023;	¤ 024;	¤ 025;	¤ 026;	¤ 027;	¤ 028;	¤ 029;	¤ 030;	¤ 031;	¤															
032:	¤ 033;	¤ 034;	¤ 035;	¤ 036;	¤ 037;	¤ 038;	¤ 039;	¤ 040;	(041;) 042;	* 043;	+ 044;	, 045;	- 046;	. 047;	/															
048:	¤ 049;	¤ 050;	¤ 051;	¤ 052;	¤ 053;	¤ 054;	¤ 055;	¤ 056;	¤ 057;	¤ 058;	¤ 059;	; 060;	< 061;	= 062;	> 063;	?															
064:	¤ 065;	¤ 066;	¤ 067;	¤ 068;	¤ 069;	¤ 070;	¤ 071;	¤ 072;	¤ 073;	¤ 074;	¤ 075;	¤ 076;	¤ 077;	¤ 078;	¤ 079;	¤															
080:	¤ 081;	¤ 082;	¤ 083;	¤ 084;	¤ 085;	¤ 086;	¤ 087;	¤ 088;	¤ 089;	¤ 090;	¤ 091;	¤ 092;	¤ 093;	¤ 094;	¤ 095;	¤															
096:	¤ 097;	¤ 098;	¤ 099;	¤ 100;	¤ 101;	¤ 102;	¤ 103;	¤ 104;	¤ 105;	¤ 106;	¤ 107;	¤ 108;	¤ 109;	¤ 110;	¤ 111;	¤															
112:	¤ 113;	¤ 114;	¤ 115;	¤ 116;	¤ 117;	¤ 118;	¤ 119;	¤ 120;	¤ 121;	¤ 122;	¤ 123;	(124;) 125;	¤ 126;	- 127;	¤															
128:	¤ 129;	¤ 130;	,	131;	¤ 132;	,	133;	,	134;	+	135;	,	136;	,	137;	,	138;	¤ 139;	,	140;	¤ 141;	¤ 142;	¤ 143;	¤							
144:	¤ 145;	,	146;	,	147;	,	148;	,	149;	,	150;	,	151;	,	152;	,	153;	,	154;	,	155;	,	156;	,	157;	¤ 158;	,	159;	ÿ		
160:	,	161;	,	162;	,	163;	,	164;	,	165;	,	166;	,	167;	,	168;	,	169;	,	170;	,	171;	,	172;	,	173;	,	174;	,	175;	,
176:	,	177;	,	178;	,	179;	,	180;	,	181;	,	182;	,	183;	,	184;	,	185;	,	186;	,	187;	,	188;	,	189;	,	190;	,	191;	,

Aquí podemos ver lo que sucede cuando presionamos el botón de tabla ASCII, proporciona una tabla ASCII en pantalla.

A screenshot of a web browser window showing the ContraSegur login page. The page includes the IES Bendinat logo and email address. It has fields for "Usuari o correu:" and "Contraseña:", with a "Mostrar" (Show) button next to the password field. Below these are several checkboxes for password complexity rules. At the bottom, there are links for "Diccionari:" and "Patrons:", a "Mostrar" button, and a link to "Mostrar taula ASCII".

Aquí podemos ver qué sucede al presionar el botón para generar contraseña. También es importante ver cómo se visualiza la contraseña inicialmente, ya que está oculta por motivos de privacidad.



Usuari o correu: z9999999
Contrassenya: qY*È%Q<6;FèX
Iniciar sessió

Mínim 8 caràcters,
 almenys una lletra majúscula,
 almenys una lletra minúscula,
 almenys un número,
 almenys un caràcter especial.

Dèbil - Regular - Bona - Forta
Weak - So-so - Great! - Strong

ca Choose File no file selected
Patrons: Choose File no file selected

Mostrar taula ASCII

Aquí podemos ver lo que sucede al presionar el botón "Mostrar contraseña". Ahora ya no está oculto y podemos ver la contraseña generada en la captura de pantalla anterior y cómo cumple con todos los requisitos.



localhost

IES BENDINAT
iesbendinat@educacio.caib.es

Usuari o correu: z9999999
Contrasenya: q*ÈQ<6;FèX
Iniciar sessió

Mínim 8 caràcters,
 almenys una lletra majúscula
 almenys una lletra minúscula,
 almenys un número,
 almenys un caràcter especial.

Dèbil - Regular - Bona - Forta
Weak - So-so - Great! - Strong

ca Diccionari: Choose File no file selected
es Choose File no file selected
en Choose File no file selected
fr Mostrar taula ASCII

Aquí podemos ver el menú desplegable de idiomas.

localhost

IES BENDINAT
iesbendinat@educacio.caib.es

Usuari o correu: z9999999
Contrasenya: q*ÈQ<6;FèX
Iniciar sessió

Mínim 8 caràcters,
 almenys una lletra majúscula
 almenys una lletra minúscula,
 almenys un número,
 almenys un caràcter especial.

Dèbil - Regular - Bona - Forta
Weak - So-so - Great! - Strong

ca Diccionari: Choose File no file selected
es Patrons: Choose File no file selected
fr Mostrar taula ASCII

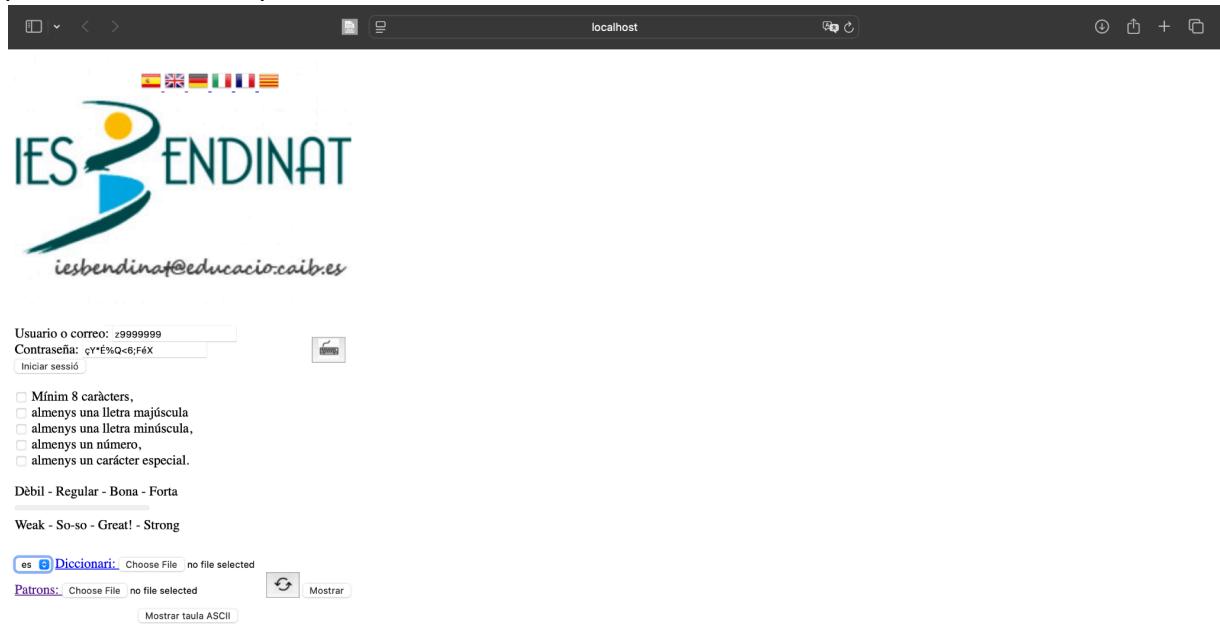
Canviar idioma(es). Versión con Base de Datos Contraseñas Seguras

[Close](#)

Una vez que cambiamos a otro idioma, en este caso español, muestra un mensaje en

	ContraSegur Manual de Usuario	IES Bendinat
---	--	---------------------

pantalla indicando que ha cambiado de idioma.



The screenshot shows a web browser window with the following details:

- Header:** ContraSegur Manual de Usuario, IES Bendinat
- Page Content:**
 - IES Bendinat logo and email address: iesbendinat@educacio.caib.es
 - Language selection: Spanish (España) is selected, with other European flags available.
 - Login fields: "Usuari o correu: z9999999" and "Contraseña: q%é%Q-6;FéX".
 - Checkboxes for password complexity: "Mínim 8 caràcters", "almenys una lletra majúscula", "almenys una lletra minúscula", "almenys un número", and "almenys un caràcter especial".
 - Strength meter: "Débil - Regular - Bona - Forta" (Weak - So-so - Great! - Strong).
 - File upload fields: "Diccionari" (Choose File) and "Patrons" (Choose File), both currently set to "no file selected".
 - Buttons: "Iniciar sessió" (Start session), "Mostrar" (Show), and "Mostrar taula ASCII".

Al cerrar el mensaje anterior, podemos ver cómo se han traducido los textos de nombre de usuario y contraseña, y si tuviéramos otra pestaña abierta, también podríamos ver cómo cambia el título de la página web. Las traducciones se limitan a algunos elementos debido a limitaciones de tiempo. Estas traducciones se cargan desde una base de datos que, como usuario, puede manipular para incluir más idiomas si desea agregar un nuevo idioma.



Google Translate Catalan → English

Translation ▾ ⋮ ×


IES BENDINAT
iesbendinat@educacio.caib.es

Username or email: z9999999
Password:

Log in

Minimum 8 characters.
 at least one capital letter
 at least one lowercase letter
 at least one number,
 at least one special character.

Weak - Regular - Good - Strong

Weak - So-so - Great! - Strong

ca Choose File no file selected

Patterns: no file selected

Show ASCII table

Open "https://translate.google.com/website?sl=ca&tl=en&hl=en&client=webapp&u=https://glistening--faloodeh--c6e49b-netlify-app.translate.goog/?_x_tr_slf%3Dca%26_x_tr_tf%3Den%26_x_tr_h%3Den%26_x_tr_plo%3Dwapp" in a new tab

Si en cambio deseas recibir la traducción de la página completa, proporcionada por Google Translate, esto ocurrirá al presionar las banderas de las respectivas naciones.

localhost


IES BENDINAT
iesbendinat@educacio.caib.es

Usuari o correu: z9999999
Contraseña:

Iniciar sessió

Mínim 8 caràcters,
 almenys una lletra majúscula
 almenys una lletra minúscula,
 almenys un número,
 almenys un caràcter especial.

Débil - Regular - Bona - Forta

Weak - So-so - Great! - Strong

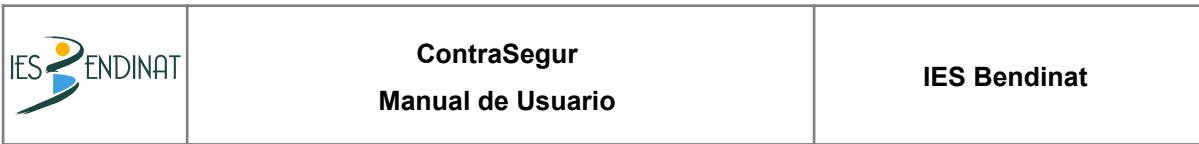
ca Choose File no file selected

Patrons: no file selected

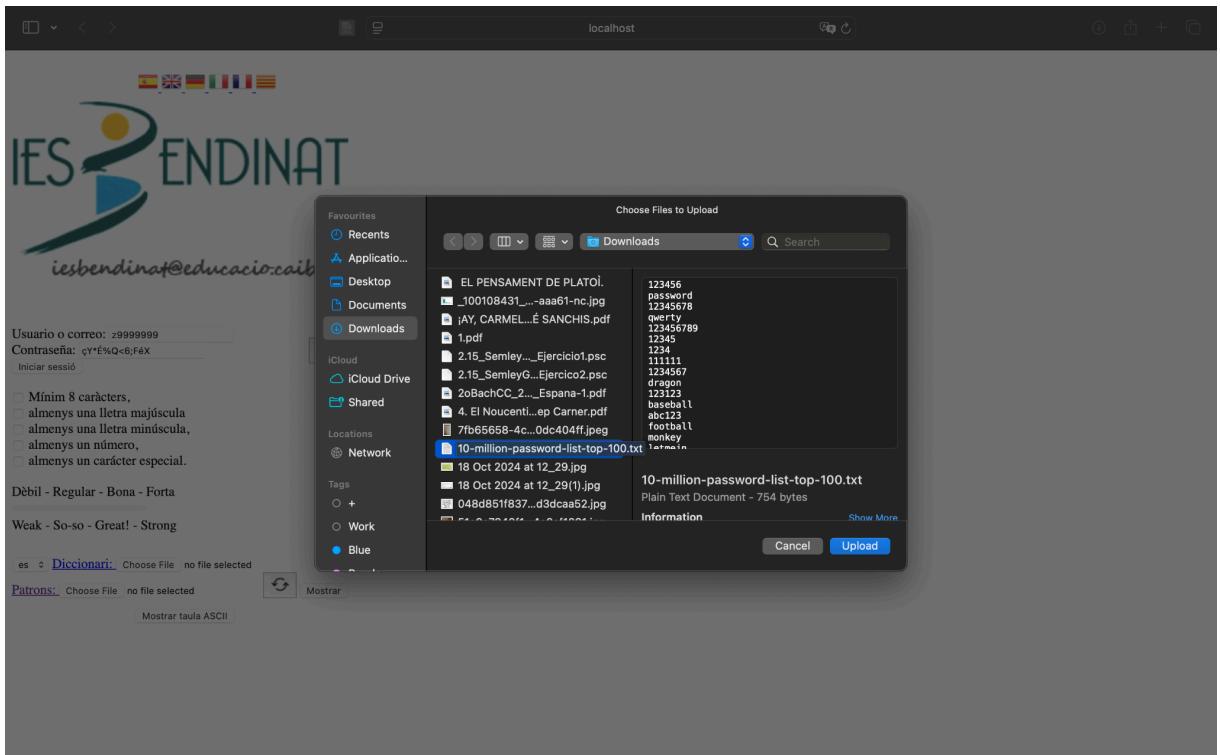
Mostrar

Mostrar taula ASCII

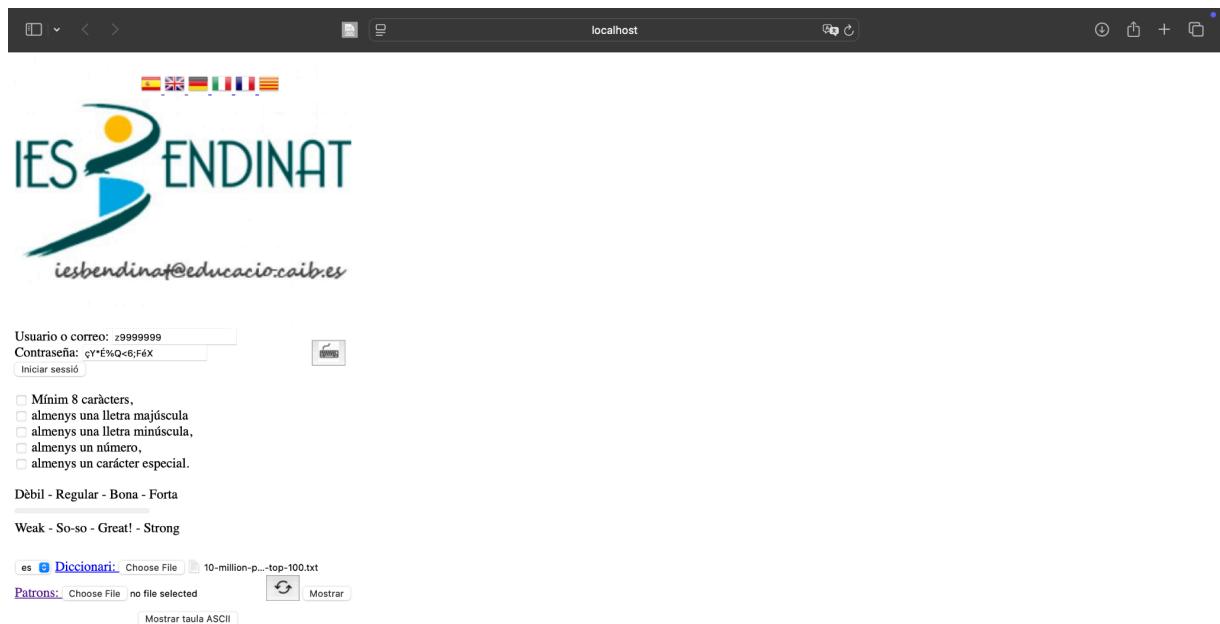
Open "https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-Password-list-top-100.txt" in a new tab



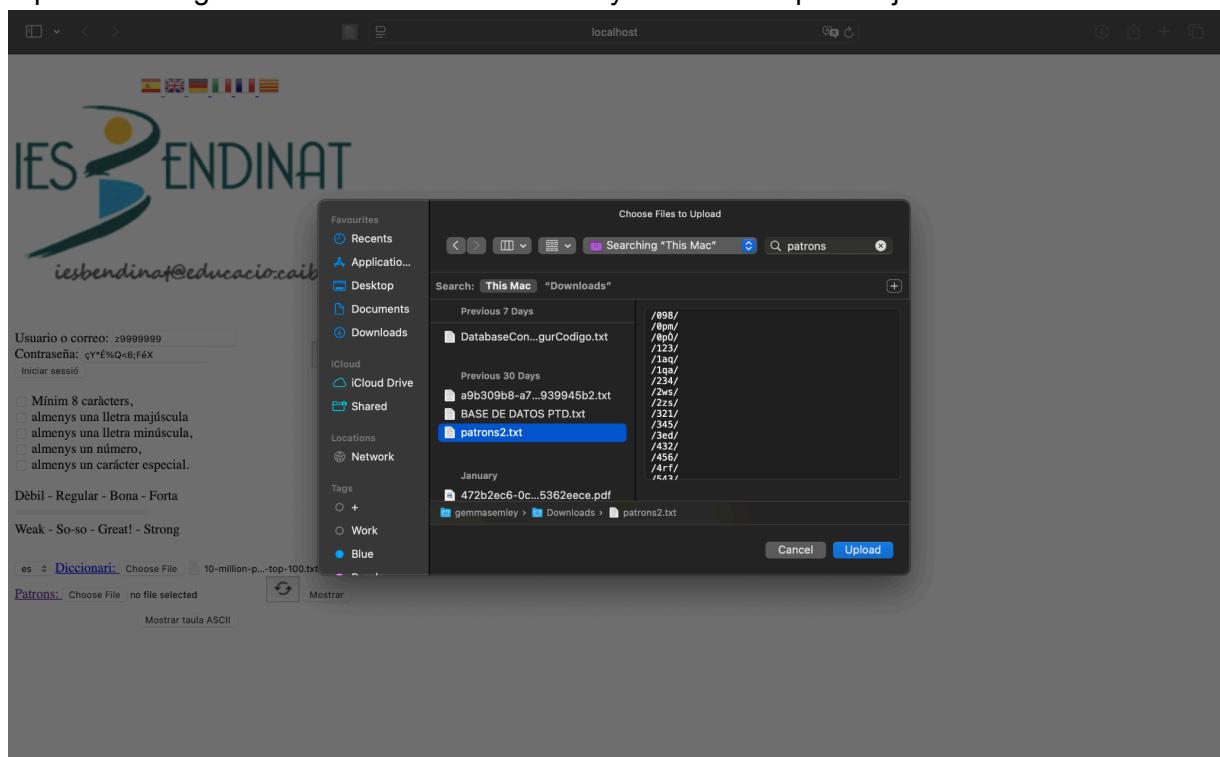
Los enlaces con las palabras ‘Diccionari’ y ‘Patrons’ te darán acceso, respectivamente, a una lista de 10.000 contraseñas comunes y patrones comunes.



Esto es lo que sucede al presionar el botón de carga de archivo, específicamente para las contraseñas comunes. En este caso, cargo las 100 contraseñas más comunes, que se encuentran en el [Anexo 1](#).



Aquí se ha cargado el archivo de contraseñas y su nombre aparece junto al botón.



Ahora, repito el proceso anterior para los patrones. En este caso, cargo un archivo de

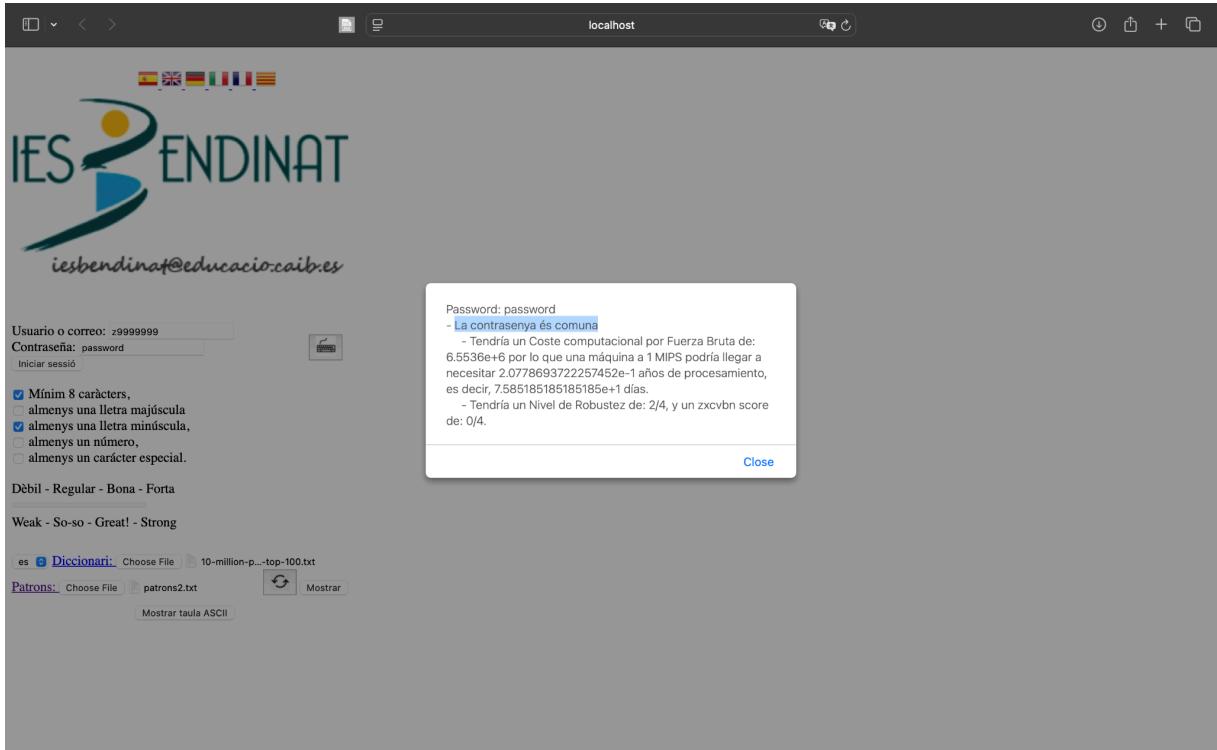


patrones comunes que se encuentra en el [Anexo 2](#).

Como antes, el archivo de patrones se ha cargado y su nombre aparece junto al botón.



A continuación, detallaré los diferentes niveles de seguridad de contraseña considerados. Primero, introduce la contraseña "password" y presioné el botón "Mostrar". Al salir del cuadro de texto, se mostrarán los requisitos que cumple y la barra de progreso debería actualizarse según corresponda.



Esto es lo que sucede al presionar el botón de inicio de sesión. Se muestra un mensaje en pantalla con los detalles de la contraseña introducida. A continuación, se muestra el estado de la contraseña, que en este caso es común (texto subrayado). A continuación, se muestra su coste computacional por fuerza bruta, que se traduce en años y días que una máquina de 1 mip necesitaría para procesarla. Finalmente, se puntúa primero según nuestros cálculos y luego según los cálculos de zxcvbn. En el [anexo 3](#) se detallan los cálculos internos y externos realizados. Es importante mencionar que si se traduce la página con la base de datos, se traducirá todo el contenido de este mensaje, excepto el estado.



This screenshot shows a web-based login form for 'IES Bendinat'. The form includes fields for 'Usuari o correu:' (with value 'z9999999') and 'Contrasenya:' (with value 'qwert'). Below the password field is a link 'Iniciar sessió' with a small key icon. To the right of the password field is a strength meter consisting of a series of colored squares (green, yellow, red) followed by the text 'Dèbil - Regular - Bona - Forta'. Underneath the meter, it says 'Weak - So-so - Great! - Strong'. Further down, there are two file selection fields: 'Diccionari:' (choose file) and 'Patrons:' (choose file), both currently set to 'no file selected'. Next to these fields are 'Mostrar' (Show) and 'Mostrar taula ASCII' buttons. A small note at the bottom left says 'ca ☰ Diccionari: Choose File no file selected'. A tooltip for the 'Patrons:' field states: 'La contrasenya conté patrons'.

Ahora he repetido el proceso anterior, esta vez introduciendo la contraseña "qwert".

This screenshot is similar to the previous one but includes a tooltip for the 'Patrons:' field. The tooltip contains the following text:

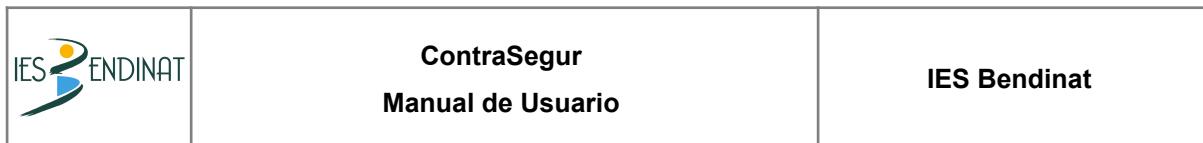
```

Password: qwert
- La contrasenya conté patrons
- Tendria un Cost Computacional per Força Bruta de:
  4.096e+3 pel que una màquina a 1 MIPS podria arribar a
  necessitar 1.2986683576410906e-4 anys de processament,
  es a dir, 4.7407407407405e-2 dies.
- Tendria un Nivell de Robustesa de: 1/4, i un zxcvbn score
  de: 0/4.

```

The rest of the interface is identical to the first screenshot, showing the login form and the password strength meter.

En este caso podemos ver que el estado de la contraseña es que incluye patrones (texto



subrayado).

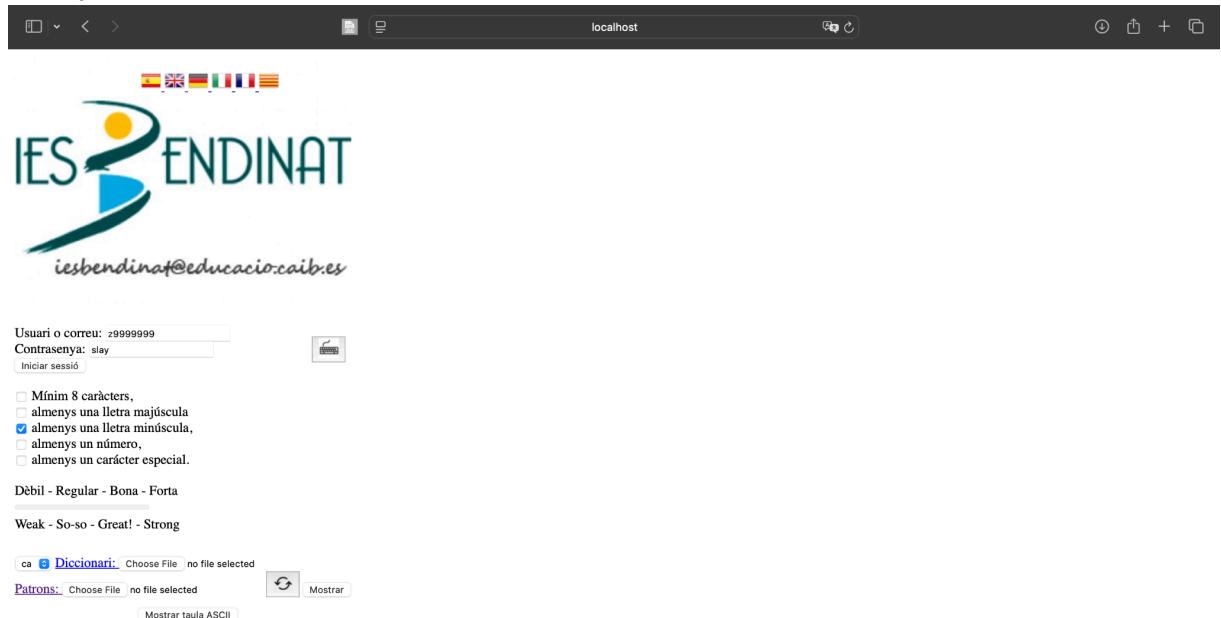
A screenshot of a web-based password strength checker. At the top, there are input fields for "Usuari o correu:" (29999999) and "Contraseña:" (111111). Below these are several checkboxes for password complexity rules, with the last one checked. Underneath the checkboxes are two strength indicators: "Débil - Regular - Bona - Forta" and "Weak - So-so - Great! - Strong", both showing "Weak". Further down, there are file upload fields for "Diccionari:" and "Patrons:", a "Mostrar" button, and a link to "Mostrar taula ASCII". A modal dialog box is open, displaying the password "111111" and a warning message: "La contraseña conté repeticions" followed by a detailed explanation of the password's weaknesses.

Ahora he repetido el proceso anterior, esta vez introduciendo la contraseña "111111".

A screenshot of the same password strength checker interface, but this time the password "Contraseña:" is set to "111111". The modal dialog box now shows a "Close" button and a small inset image in the bottom right corner showing a screenshot of a mobile device displaying the IES BENDINAT website.

	ContraSegur Manual de Usuario	IES Bendinat
---	--	---------------------

En este caso podemos ver que el estado de la contraseña es que incluye repeticiones (texto subrayado).



localhost

IES BENDINAT
iesbendinat@educacio.caib.es

Usuari o correu: z9999999

Contrasenya: slay

Iniciar sessió

Mínim 8 caràcters,
 almenys una lletra majúscula
 almenys una lletra minúscula,
 almenys un número,
 almenys un caràcter especial.

Dèbil - Regular - Bona - Forta

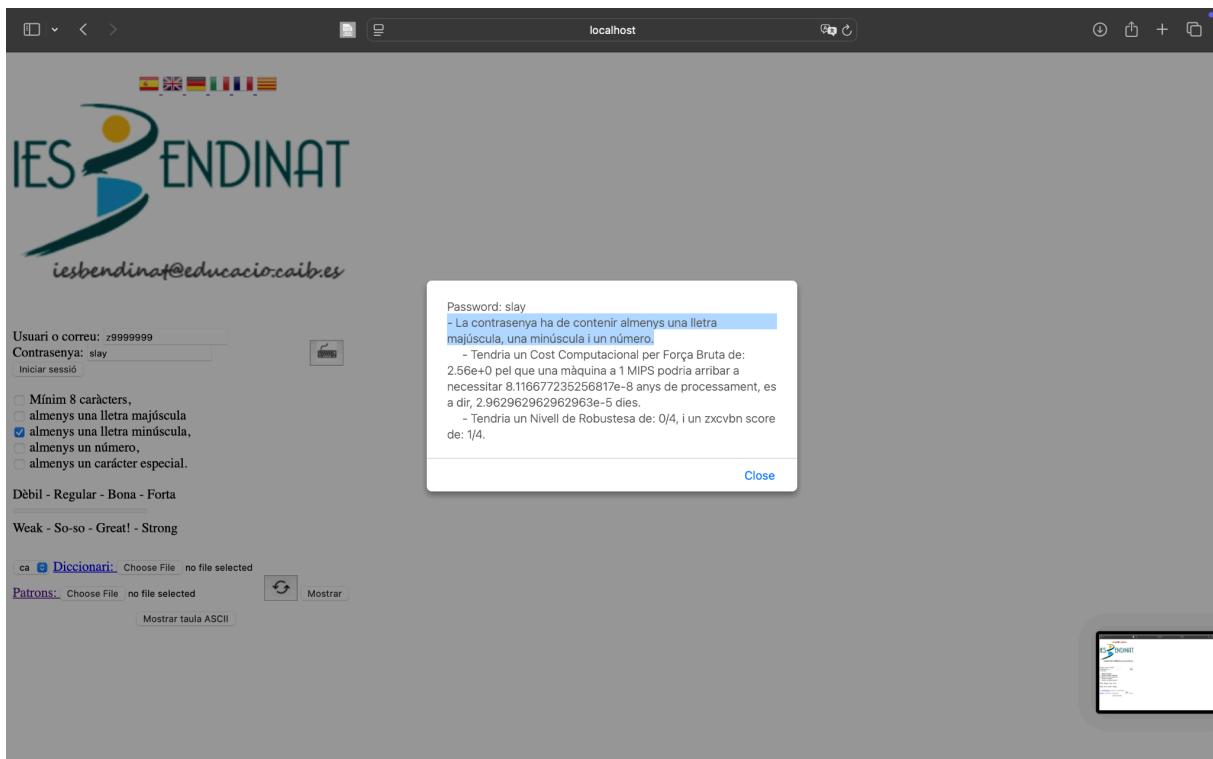
Weak - So-so - Great! - Strong

ca Choose File no file selected

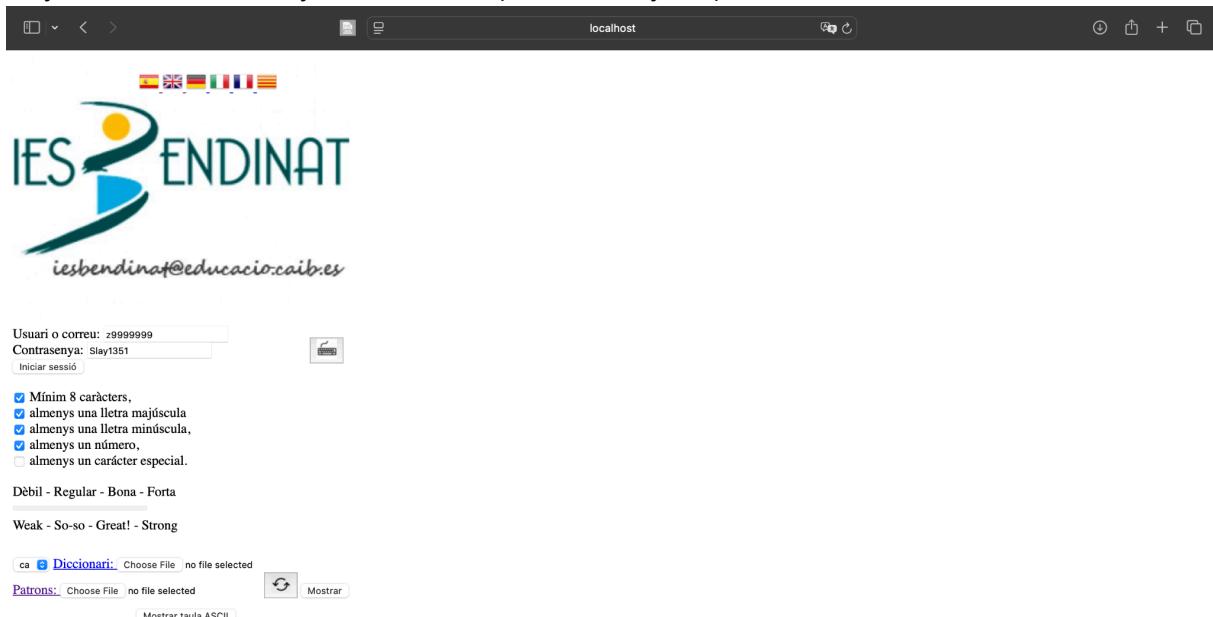
Patrons: Choose File no file selected

Mostrar taula ASCII

Ahora he repetido el proceso anterior, esta vez introduciendo la contraseña "slay".

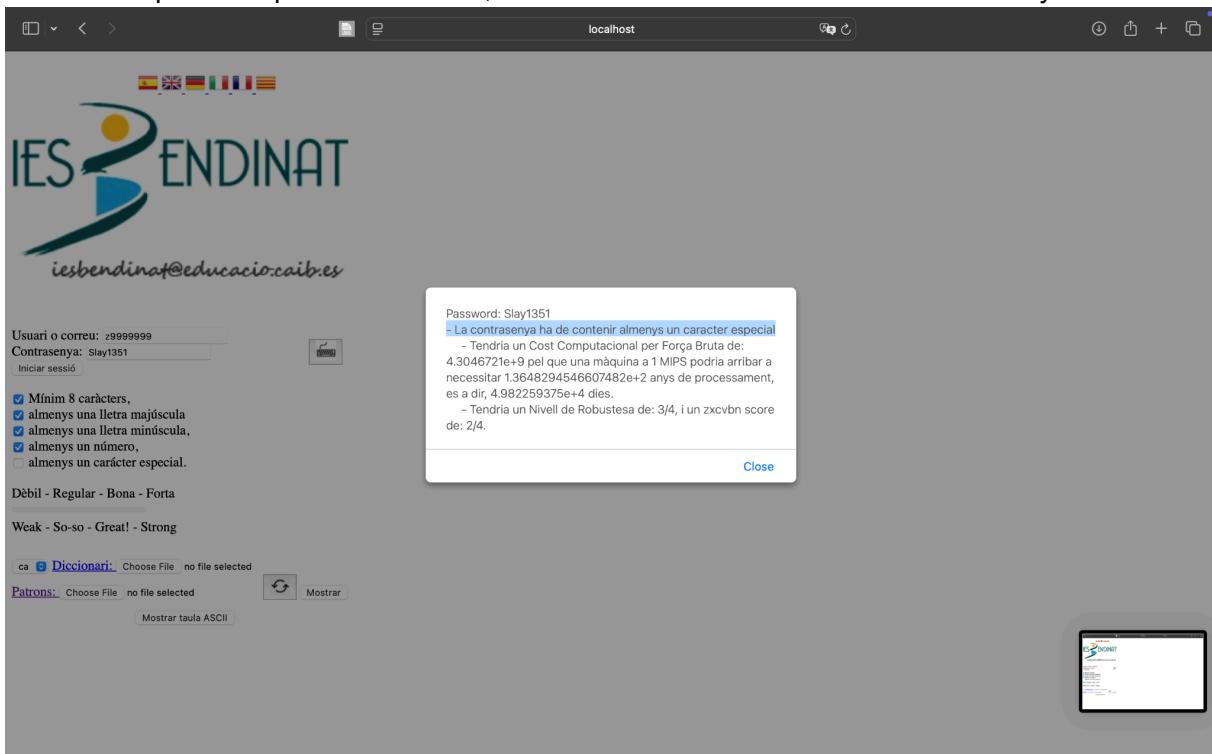


En este caso podemos ver que el estado de la contraseña es que le falta una letra mayúscula, minúscula y/o un número (texto subrayado).



	ContraSegur Manual de Usuario	IES Bendinat
---	--	---------------------

Ahora he repetido el proceso anterior, esta vez introduciendo la contraseña "Slay1351".



En este caso podemos ver que el estado de la contraseña es que le falta un carácter especial (texto subrayado).



localhost

IES BENDINAT
iesbendinat@educacio.caib.es

Usuari o correu: z9999999
Contrasenya: Slay@1
Iniciar sessió

Mínim 8 caràcters,
 almenys una lletra majúscula
 almenys una lletra minúscula,
 almenys un número,
 almenys un caràcter especial.

Dèbil - Regular - Bona - Forta

Weak - So-so - Great! - Strong

ca Choose File no file selected
Patrons: no file selected
Mostrar taula ASCII

Ahora he repetido el proceso anterior, esta vez introduciendo la contraseña "Slay@1".

localhost

IES BENDINAT
iesbendinat@educacio.caib.es

Usuari o correu: z9999999
Contrasenya: Slay@1
Iniciar sessió

Mínim 8 caràcters,
 almenys una lletra majúscula
 almenys una lletra minúscula,
 almenys un número,
 almenys un caràcter especial.

Dèbil - Regular - Bona - Forta

Weak - So-so - Great! - Strong

ca Choose File no file selected
Patrons: no file selected
Mostrar taula ASCII

Password: Slay@1

- La contrasenya ha de contenir almenys 8 caràcters
- Tendria un Cost Computacional per Força Bruta de:
5.053913144281e+6 pel que una màquina a 1 MIPS podria
arribar a necessitar 1.602382100279328e-1 anys de
processament, es a dir, 5.8494365095844906e+1 dies.
- Tendria un Nivell de Robustesa de: 2/4, i un zxcvbn score
de: 1/4.

[Close](#)

En este caso podemos ver que el estado de la contraseña es que no llega al mínimo de 8



caracteres (texto subrayado).

Usuari o correu: 29999999
Contraseña: Slay@1589
Iniciar sessió

Mínim 8 caràcters,
 almenys una lletra majúscula,
 almenys una lletra minúscula,
 almenys un número,
 almenys un caràcter especial.

Débil - Regular - Bona - Forta
Weak - So-so - Great! - Strong

ca Choose File no file selected
Patrons: no file selected

[Mostrar taula ASCII](#)

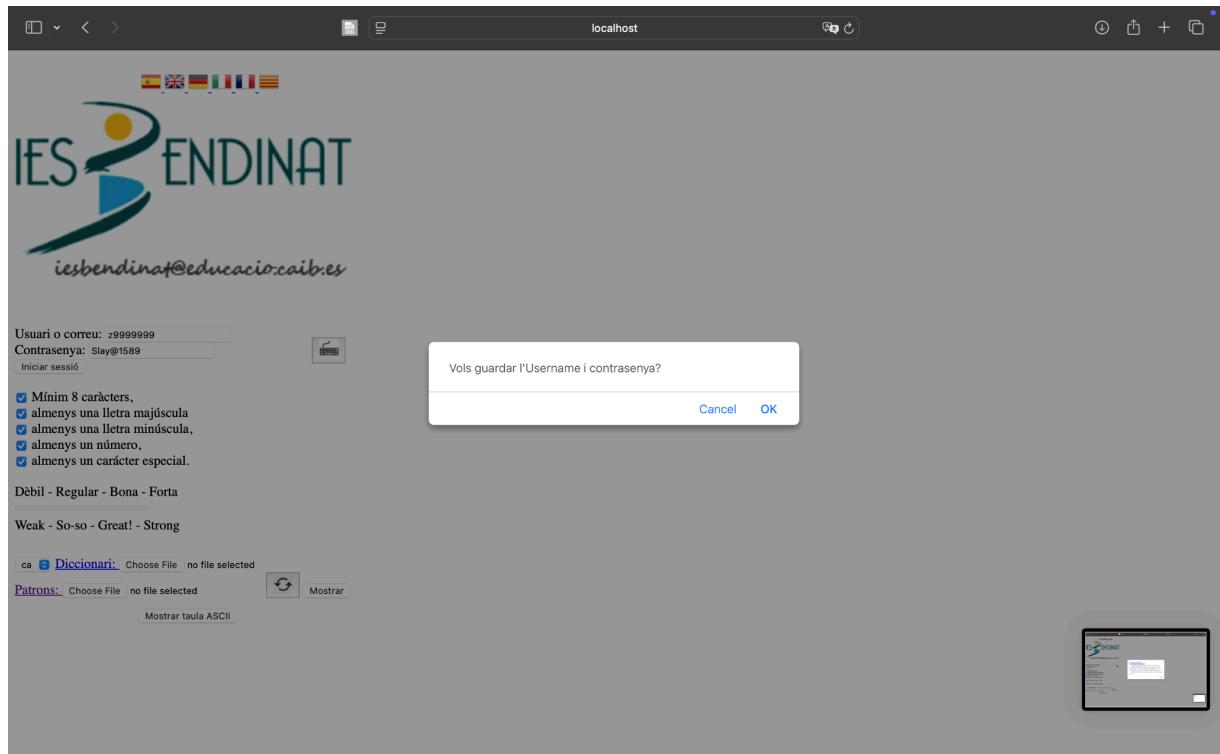
Ahora he repetido el proceso anterior, esta vez introduciendo la contraseña "Slay@1589".

Password: Slay@1589
La contrasenya és robusta!
- Tendria un Cost Computacional per Força Bruta de:
1.1361656654439816e+13 pel que una màquina a 1 MIPS
podria arribar a necessitar 3.602300778199054e+5 anys de
processament, es a dir, 1.3150065572268306e+8 dies.
- Tendria un Nivell de Robustesa de: 4/4, i un zxcvbn score
de: 3/4.

[Close](#)



En este caso podemos ver que el estado de la contraseña es que es robusta (texto subrayado).



En todos estos casos, después de cerrar el mensaje sobre la contraseña, le pregunta si desea guardar sus datos de inicio de sesión. Si presiona cancelar, se actualizará la página.

3.1.2 Pantalla 2

Vols desar l'inici de sessió a ContraSegur?

Usuari o correu: 29999999

Contrasenya: *****

Desar

No Desar

 Password

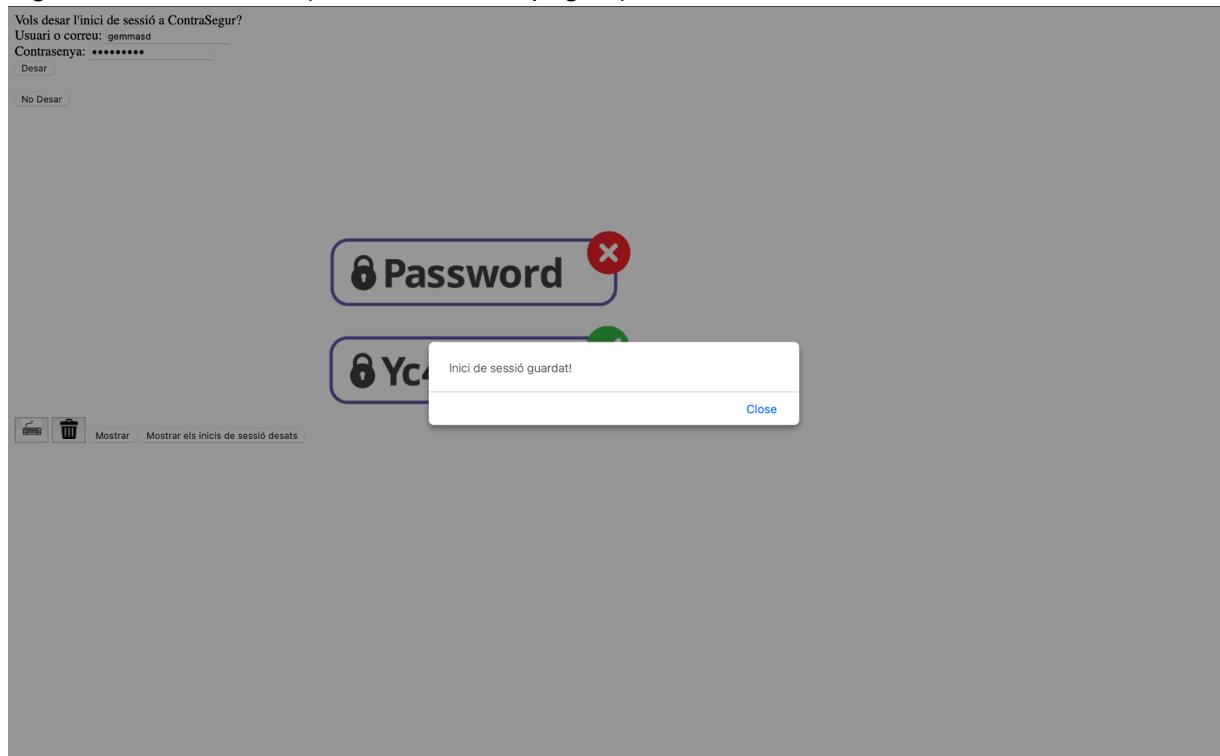
 Yc4gwy8@

  Mostrar Mostrar els inicis de sessió desats

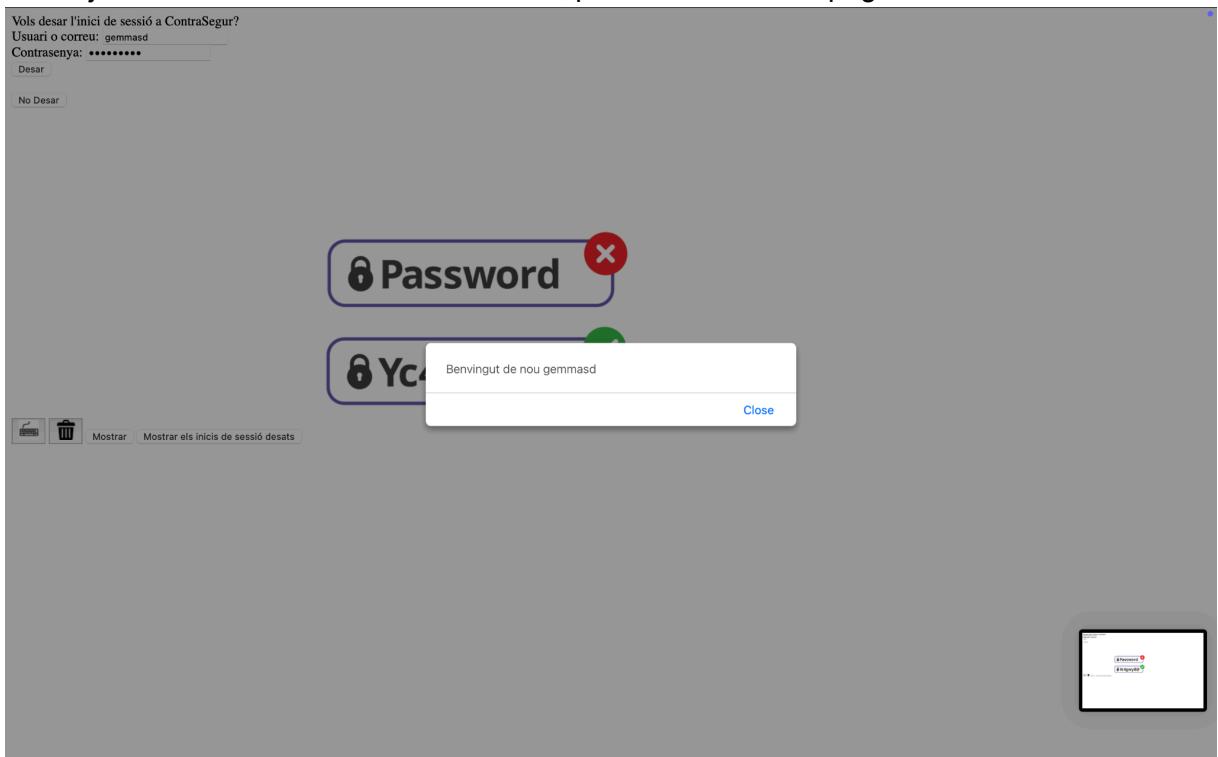
Por el contrario, si pulsa Aceptar, accederá a una segunda página para gestionar los inicios de sesión. Aquí es donde vemos el uso de cookies. Arriba de todo vemos el título “Vols desar l'inici de sessió a ContraSegur?”. Más abajo vemos dos cuadros de texto donde se pueden editar el nombre de usuario o correo electrónico y la contraseña introducidas en la primera pantalla. Luego vemos botones de “Desar” y “No desar”. También, observamos una foto representativa de una contraseña segura y otra que no. Debajo de esto, vemos botones para las funciones de la primera página, como ver la contraseña y el teclado. Además de esto, un botón de papelera para borrar las credenciales y otra de “Mostrar els inicis de sessió guardats”.

A screenshot of a web browser showing the ContraSegur login page for IES Bendinat. The page features the IES Bendinat logo and email address at the top. Below is a form with fields for 'Usuari o correu:' and 'Contraseña:', both containing placeholder text. A 'Iniciar sessió' button is next to the password field. Below the fields are several checkboxes for password complexity rules. Underneath the checkboxes are two sets of strength indicators: 'Dèbil - Regular - Bona - Forta' and 'Weak - So-so - Great! - Strong'. Further down are file upload fields for 'Diccionari:' and 'Patrons:', a 'Mostrar' button, and a link to 'Mostrar taula ASCII'. The browser's address bar shows 'localhost'.

Si presiona el botón "no desar", su información de inicio de sesión no se guardará y regresará al comienzo (actualización de página).



Si presiona el botón “desar” sus datos de inicio de sesión se guardarán y recibirá un mensaje de confirmación. Una vez cerrado, permanecerá en la página actual.

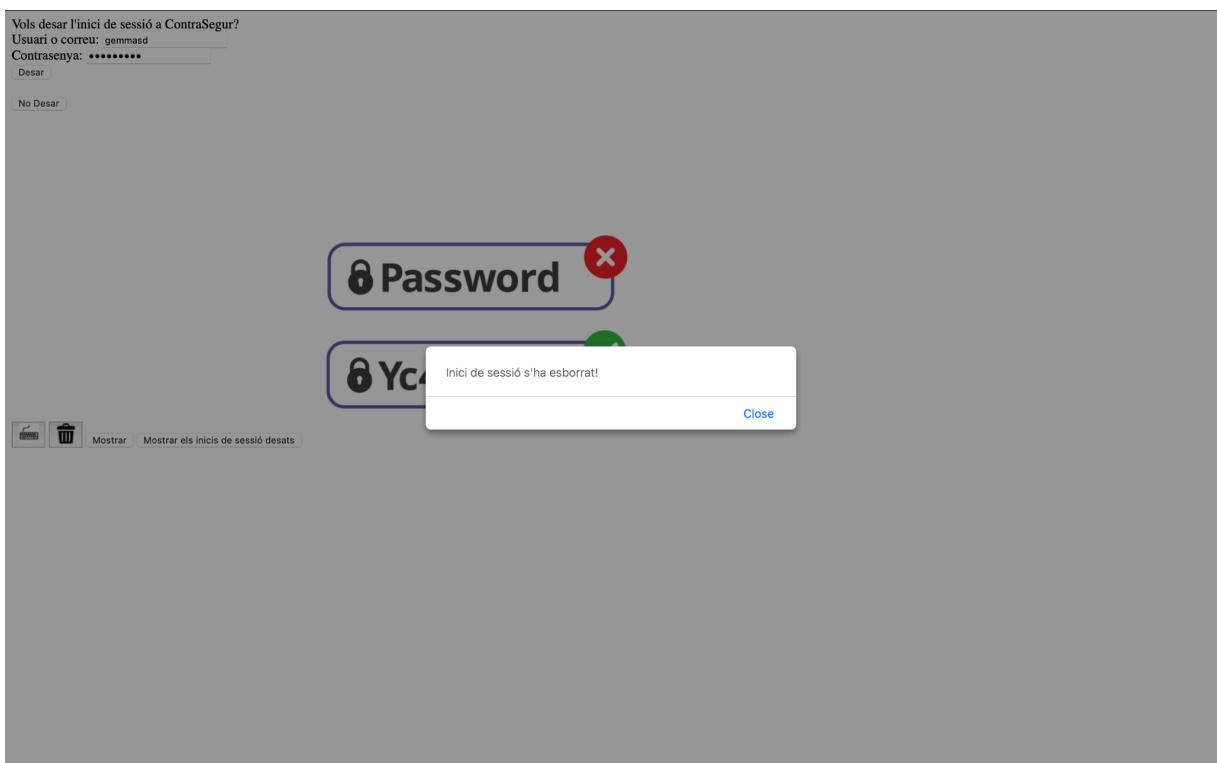


Si presiona nuevamente el botón "desar" con la misma información de inicio de sesión, verá un mensaje de bienvenida. Una vez cerrado, permanecerá en la página actual.

3.1.3 Pantalla 3

Usuari o correu:	Contraseña:
gemmasd	Slay@1589
z9999999	hhh
gem	1

Si pulsa el botón para ver los inicios de sesión guardados, accederá a una tercera página con una tabla de nombres de usuario y contraseñas. Aquí puede ver que se han guardado sus datos de inicio de sesión (usuario: gemmasd y contraseña: Slay@1589).



Si pulsa el botón de la papelera, eliminará el inicio de sesión anterior y recibirá un mensaje de confirmación. Una vez cerrado, permanecerá en la página actual.



ContraSegur
Manual de Usuario

IES Bendinat

Usuari o correu:	Contrasenya:
z9999999	hhh
gem	1

Aquí puedes ver que la información de inicio de sesión ya no se guarda.

Vols desar l'inici de sessió a ContraSegur?

Usuari o correu:

Contrassenya:

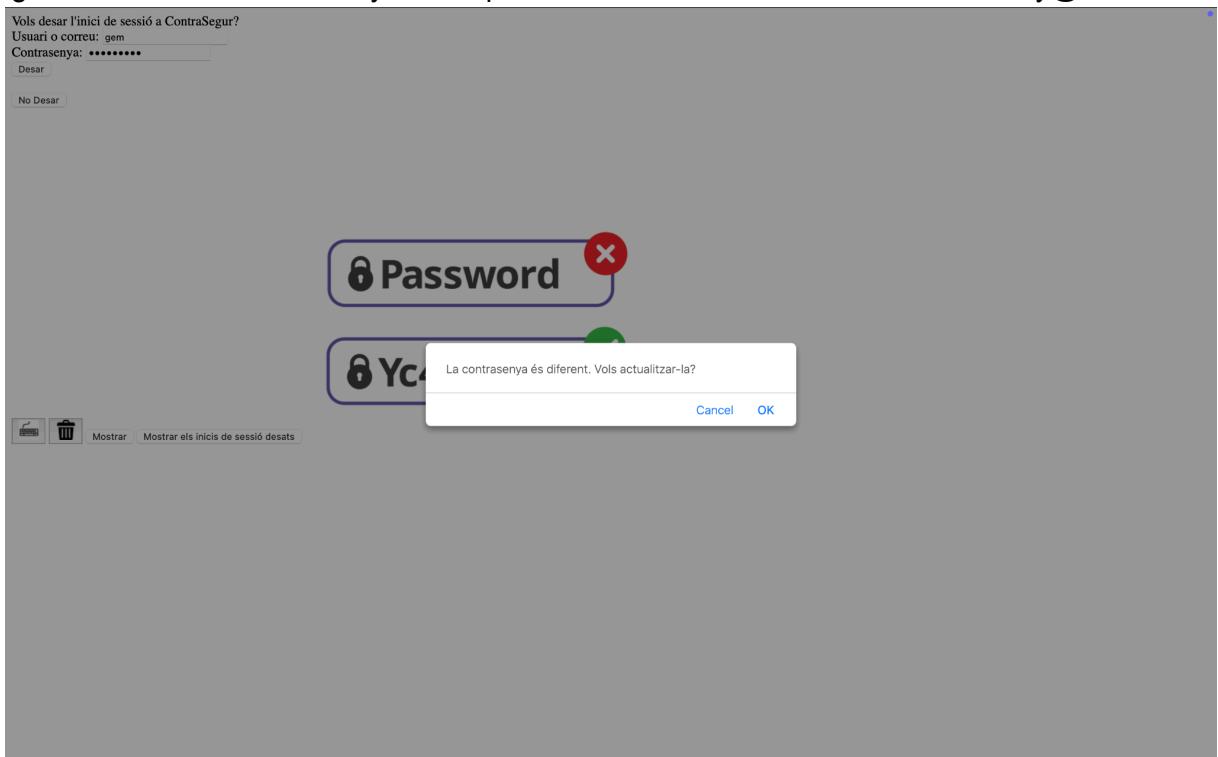
6 Password

6 Yc4gwy8@

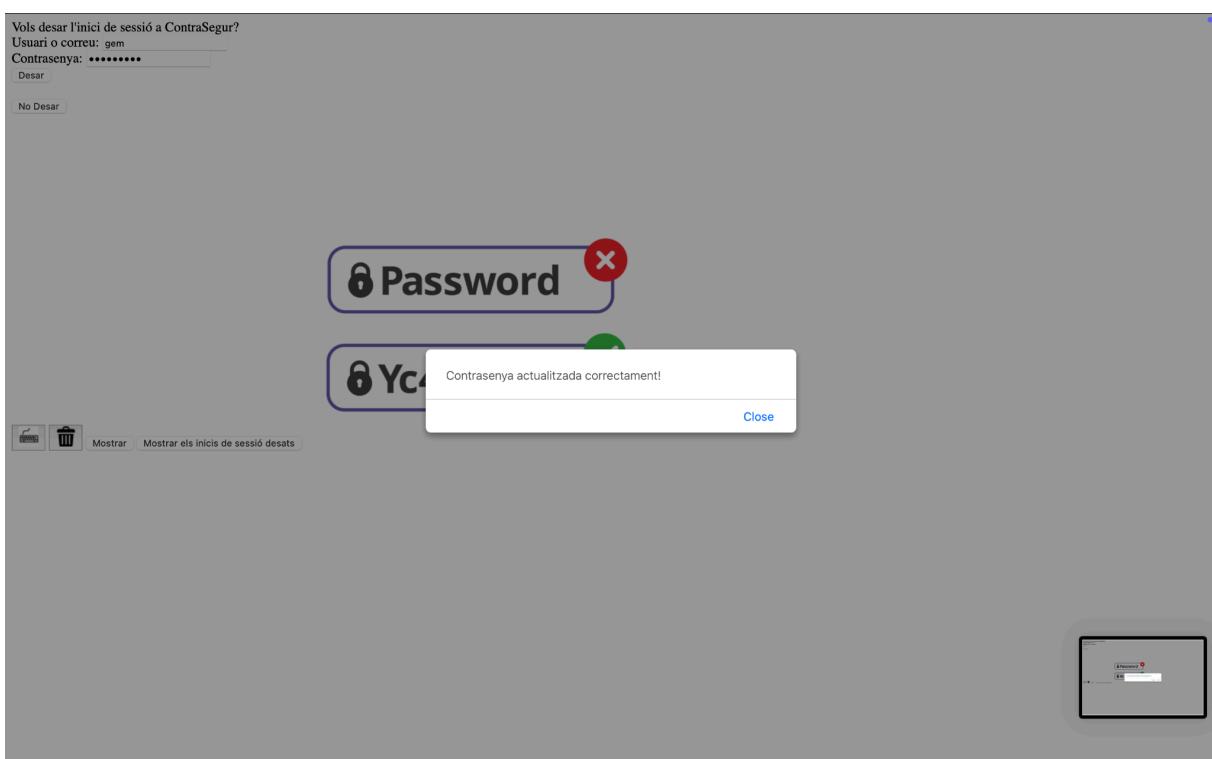
Mostrar Mostrar els inicis de sessió desats

Para demostrar la función de actualización de contraseña, intento iniciar sesión con un

nombre de usuario ya guardado, "gem", pero con una contraseña diferente. Tengo guardado "gem" con la contraseña "1" y ahora quiero iniciar sesión con la contraseña "Slay@1589".



Una vez que haya presionado el botón "desactivar", aparecerá un mensaje que le preguntará si desea actualizar la contraseña de ese usuario. Si presiona cancelar, la información de inicio de sesión no se actualizará y permanecerá en la misma página.



Sin embargo, si pulsa OK su contraseña se actualizará y recibirá un mensaje de confirmación de dicha acción.

Usuari o correu:	Contrassenya:
gem	Slay@1589
z9999999	hhh



Aquí podemos ver que el nombre de usuario "gem" ahora está guardado con la nueva contraseña "Slay@1589".

3.1.4 Mensajes de error

Los mensajes de error de este subsistema se activan en condiciones específicas relacionadas con datos faltantes:

1. Si el diccionario de contraseñas comunes proveniente de la base de datos está vacío, muestra una alerta: "Idioma sense contrasenyes / Idioma sin contraseñas / Language without passwords!". Esto significa que para el idioma seleccionado no hay contraseñas de la base de datos disponibles.
2. Si el ID del idioma seleccionado no existe en la lista de idiomas disponibles, se muestra una alerta: "No s'han trobat textos de la GUI / Textos de la GUI no encontrados / GUI texts not found". Esto significa que el sistema no pudo encontrar los textos de la interfaz de usuario para el idioma elegido.

En ambos casos, cuando se cumplen estas condiciones de error, la aplicación recurre al uso de una estructura predeterminada almacenada en memoria.

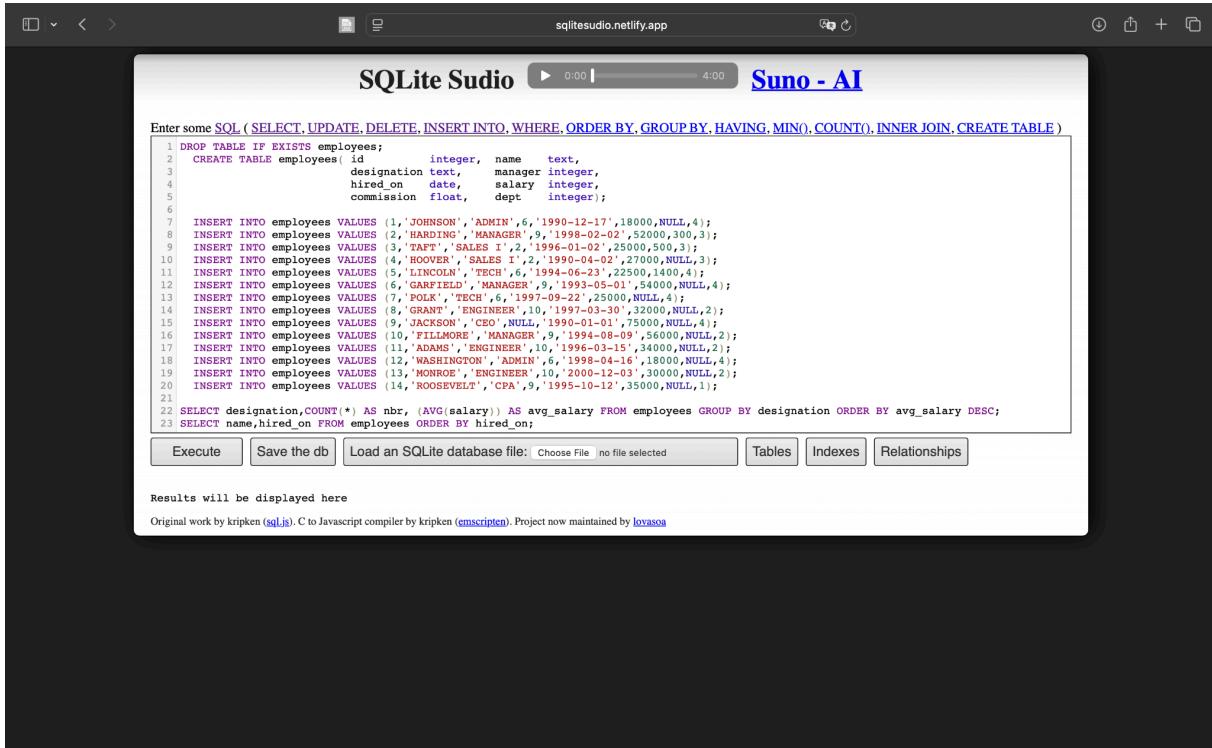
3.1.5 Ayudas contextuales

En la versión actual del programa no hay ayuda contextual. Sin embargo, se incorporará un botón de información que llevará a nuestra página web y un chatbot de AI para cualquier duda de la aplicación.

3.2 Subsistema 2

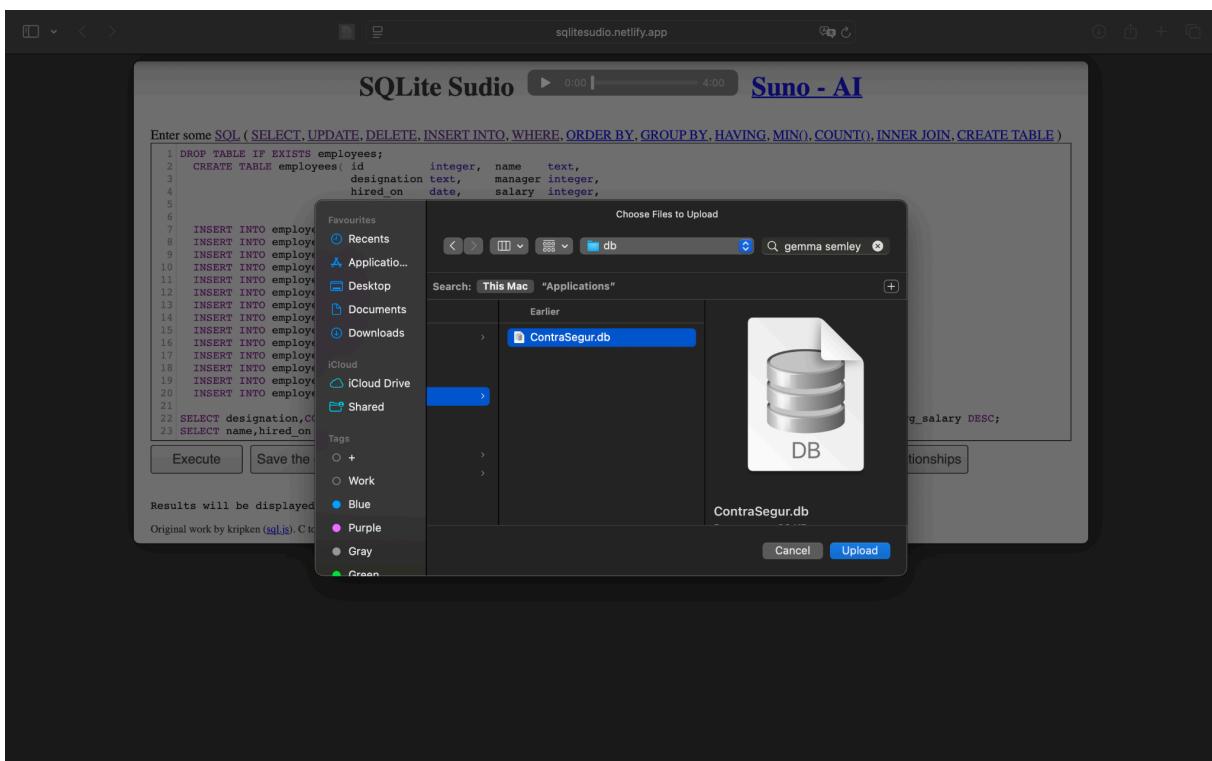
El subsistema 2 es el SQLite Studio. A continuación mostraré cómo el usuario puede manipular la base de datos para añadir idiomas o contraseñas.

3.2.1 Pantalla 1

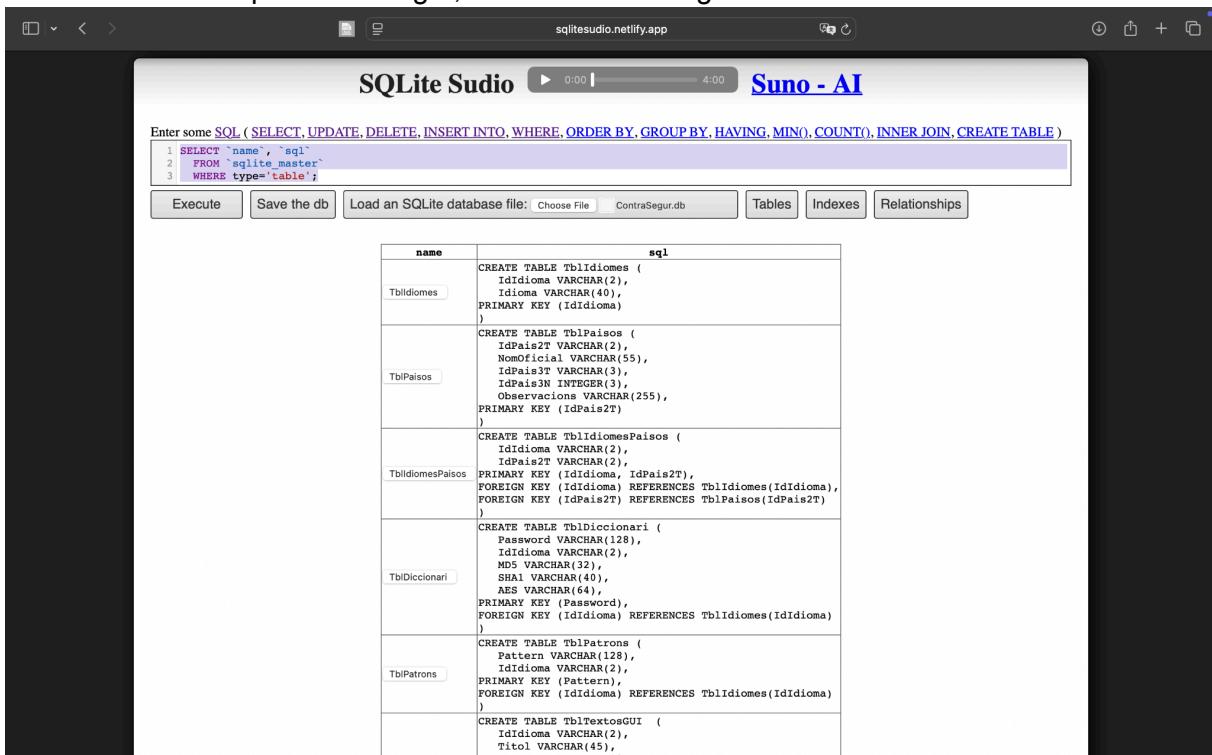


Cuando abra SQLite Studio (<https://sqlitesudio.netlify.app>) esto es lo que verá. En esta pantalla, encuentra un cuadro del editor de código donde se escriben los comandos SQL. En la parte superior de la página, justo encima del editor SQL, hay una lista de palabras clave SQL en las que se puede hacer clic, presentadas como enlaces. Estos enlaces son: SELECT, UPDATE, DELETE, INSERT INTO, WHERE, ORDER BY, GROUP BY, HAVING, MIN(), COUNT(), INNER JOIN, CREATE TABLE. En la sección inferior de la interfaz de SQLite Studio, varios botones permiten interactuar con el entorno SQL. El botón "Ejecutar" ejecuta el código SQL escrito en el editor y muestra los resultados justo debajo. El botón "Guardar la base de datos" permite descargar y guardar el estado actual de la base de datos SQLite, incluyendo todas las tablas y datos. El botón "Cargar un archivo de base de datos SQLite" permite cargar un archivo .db existente para trabajar con él dentro de la interfaz. El botón "Tablas" muestra una lista de todas las tablas de la base de datos, lo que facilita la navegación por su estructura. El botón "Índices" muestra los índices definidos, cruciales para optimizar las consultas y mejorar el rendimiento. Por último, el botón "Relaciones" revela las relaciones de clave externa entre las tablas, lo que permite visualizar y comprender cómo se conectan las diferentes partes de la base de datos.

Para empezar, debe soltar y arrastrar o seleccionar el archivo mediante el botón.



Este es el archivo que debe cargar, titulado ContraSegur.db.



Una vez cargado, se mostrarán las tablas. Para actualizar la base de datos, debe eliminar el código predeterminado. Para explicar cómo actualizar los textos de la interfaz gráfica de

usuario, voy a añadir nuevos valores (los textos en ucraniano) a TblTextosGUI.

El código debe seguir esta estructura:

```
INSERT INTO TblTextosGUI VALUES (
    "es",
    "Versión con Base de Datos Contraseñas Seguras",
    "Usuario o correo: ",
    "Contraseña: ",
    "Mostrar: ",
    "Mínimo 8 caracteres",
    "al menos una letra mayúscula",
    "al menos una letra minúscula",
    "al menos un número",
    "al menos un carácter especial",
    "Débil - Regular - Buena - Fuerte",
    "Iniciar sesión",
    "La contraseña es demasiado común. Por favor, elige una contraseña más fuerte.",
    "La contraseña no puede contener patrones previsibles",
    "La contraseña no puede contener múltiples repeticiones de caracteres",
    "La contraseña debe contener al menos una letra mayúscula, una minúscula y un número",
    "La contraseña debe contener al menos un carácter especial",
    "La contraseña es demasiado corta. Debe tener al menos 8 caracteres",
    "¡Contraseña robusta!",
    "\n - Tendría un Coste Computacional por Fuerza Bruta de: ",
    "por lo que una máquina a 1 MIPS podría llegar a necesitar ",
    "años de procesamiento, es decir, ",
    "días.\n - Tendría un Nivel de Robustez de: ",
    "/4, y un zxcvbn Score de: ",
    "¿Quiere guardar el inicio de sesión?",
    "Diccionario: ",
    "Patrones: ",
    "Mostrar tabla ASCII-HTML",
    "Esconder tabla ASCII-HTML",
    "¿Quieres guardar el inicio de sesión en ContraSegur? ",
    "¡Inicio de sesión guardado! ",
    "Bienvenido de nuevo ",
    "¿Quiere cambiar la contraseña? ",
    "¡Inicio de sesión borrado! ",
    "Mostrar los inicios de sesión guardados ",
    "Guardar ",
    "No guardar");
```

The screenshot shows the SQLite Studio interface with the title "Suno - AI". The main area contains the following SQL code:

```

Enter some SQL ( SELECT, UPDATE, DELETE, INSERT INTO, WHERE, ORDER BY, GROUP BY, HAVING, MIN(), COUNT(), INNER JOIN, CREATE TABLE )
1. INSERT INTO TblTextosGUI VALUES (
2.   "ok",
3.   "Версія з базою даних Безпечних Паролів",
4.   "Користувач або електронна пошта: ",
5.   "Пароль: ",
6.   "Показати: ",
7.   "Мінімум 8 символів",
8.   "принаймані один спеціальна літера",
9.   "принаймані одна мала літера",
10.  "принаймані один цифра",
11.  "принаймані один спеціальний символ",
12.  "Слайдики - Задовільний - Dobryj - Nadijnyj",
13.  "Увійти",
14.  "Пароль занадто поширеній. Будь ласка, виберіть надійніший пароль.",
15.  "Пароль не може містити передбачувану шаблони",
16.  "Пароль не може містити повторення символів",
17.  "Пароль має містити принаймані одну велику літеру та одну цифру",
18.  "Пароль має містити принаймані один спеціальний символ",
19.  "Пароль занадто короткий. Повинен містити щонайменше 8 символів",
20.  "Надійні паролі",
21.  "\n\n - Має бути обчислювану Варіті при Атакі Перебором: ",
22.  "тому комп'ютеру зі швидкістю 1 MIPS може знадобитися",
23.  "років обробки, тобто ",
24.  "днів.\n\n - Має Рівень Надійності: ",
25.  "/\n, та оцінку з хесьвом: ",
26.  "Бажаєте зберегти вхід?",
27.  "Словник: ",
28.  "",
29.  "Показати таблицю ASCII-HTML",
30.  "Словники таблиця ASCII-HTML",
31.  "Бажаєте зберегти вхід у ContraSegur? ",
32.  "Вхід збережено",
33.  "Ласкаво просимо назад",
34.  "Бажаєте змінити пароль?",
35.  "Вхід видалено!",
36.  "Показати збережені входи",
37.  "Зберегти",
38.  "Не зберигати");

```

Below the code are several buttons: Execute, Save the db, Load an SQLite database file (with "Choose File" and "ContraSegur.db" options), Tables, Indexes, and Relationships.

A table below the buttons shows the following data:

IdIdioma	Titol	Username	Password	Mostrar	Minimcar
ca	Versió amb Base de Dades Contraseyenes Segures	Usuari o correu:	Contrasenya:	Mostrar:	Minim 8 caracters, almenys

Aquí se puede ver el código con los textos GUI en el idioma correspondiente, ucraniano.

The screenshot shows the SQLite Studio interface with the title "Suno - AI". The main area contains the following SQL code:

```

Enter some SQL ( SELECT, UPDATE, DELETE, INSERT INTO, WHERE, ORDER BY, GROUP BY, HAVING, MIN(), COUNT(), INNER JOIN, CREATE TABLE )
1. SELECT `name` , `sql` 
2. FROM `sqlite_master` 
3. WHERE type='table';

```

Below the code are several buttons: Execute, Save the db, Load an SQLite database file (with "Choose File" and "ContraSegur.db" options), Tables, Indexes, and Relationships.

A table below the buttons shows the following data:

name	sql
TblIdiomes	CREATE TABLE TblIdiomes (IdIdioma VARCHAR(2), Idioma VARCHAR(40), PRIMARY KEY (IdIdioma))
TblPaisos	CREATE TABLE TblPaisos (IdPais2T VARCHAR(2), NomOficial VARCHAR(55), IdPais3T VARCHAR(3), IdPais3N INTEGER(3), Observacion VARCHAR(255), PRIMARY KEY (IdPais2T))
TblIdiomesPaisos	CREATE TABLE TblIdiomesPaisos (IdIdioma VARCHAR(2), IdPais2T VARCHAR(2), PRIMARY KEY (IdIdioma, IdPais2T), FOREIGN KEY (IdIdioma) REFERENCES TblIdiomes(IdIdioma), FOREIGN KEY (IdPais2T) REFERENCES TblPaisos(IdPais2T))
TblDiccionari	CREATE TABLE TblDiccionari (Password VARCHAR(128), IdIdioma VARCHAR(2), MD5 VARCHAR(32), SHA VARCHAR(64), AES VARCHAR(64), PRIMARY KEY (Password), PRIMARY KEY (IdIdioma))
TblPatrons	CREATE TABLE TblPatrons (Pattern VARCHAR(128), IdIdioma VARCHAR(2), PRIMARY KEY (Pattern), FOREIGN KEY (IdIdioma) REFERENCES TblIdiomes(IdIdioma))
	CREATE TABLE TblTextosGUI (IdIdioma VARCHAR(2), ...)

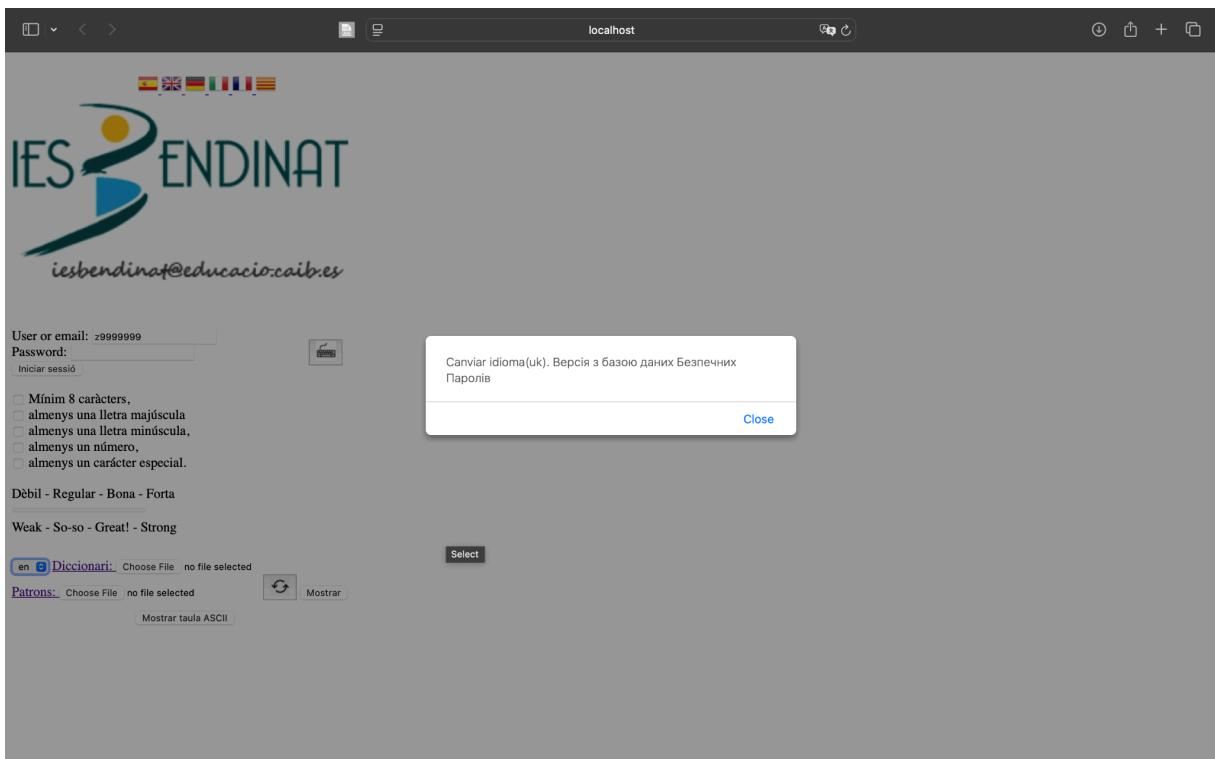
Al presionar el botón “Execute”, los nuevos valores se guardarán. Puede comprobarlo presionando el botón “Tables” y luego la tabla correspondiente “TblTextosGUI”.



Aquí podemos ver que se ha guardado correctamente.

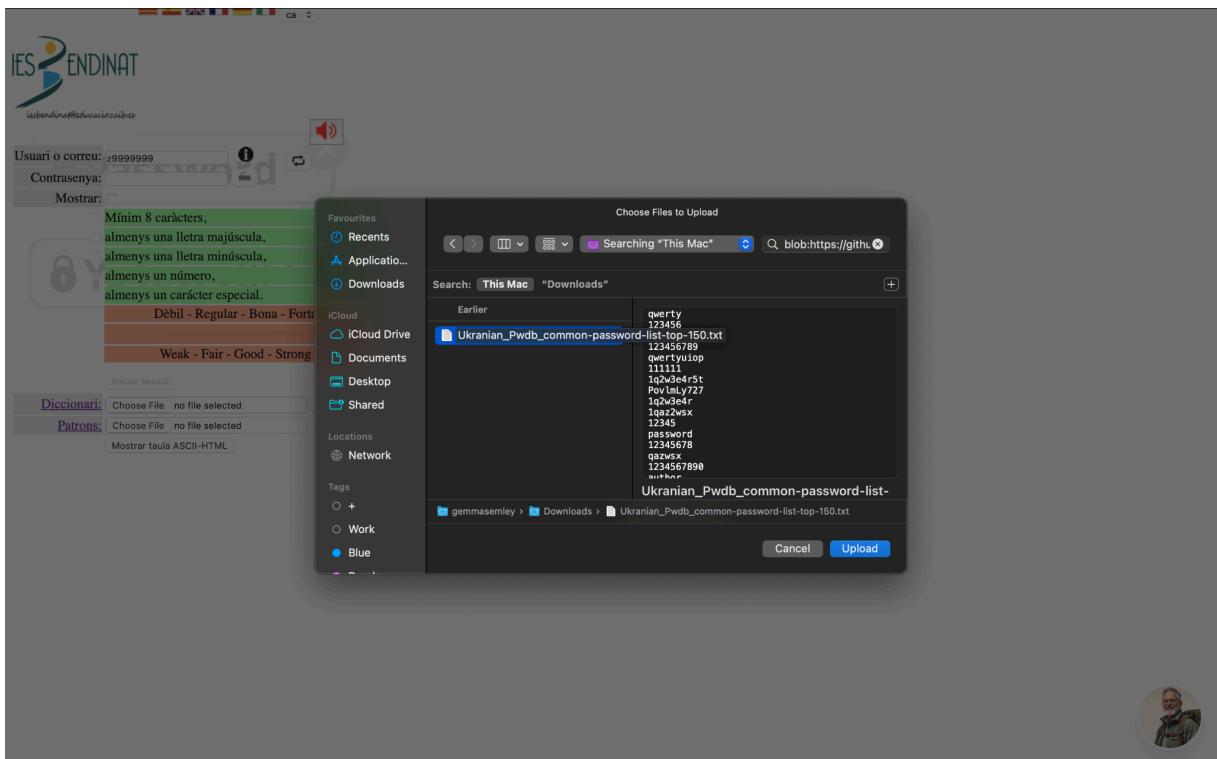


Después de hacer los cambios que quiere, debe guardar la base de datos presionando al botón "Save the db".



Tras unas actualizaciones en el código, se puede ver que ha funcionado.

Por otra parte, se pueden añadir o actualizar contraseñas del idioma deseado en la base de datos. Para ilustrar esto, se recurrirá a una versión del programa posterior.



Nos encontramos en una versión posterior de la aplicación. Primero, con el cargador de ficheros debe subir el fichero de contraseñas con que quiere trabajar en la base de datos. En este caso, he subido una lista de contraseñas comunes en ucraniano, aunque no son específicas de este idioma, lo que significa una redundancia de datos en la base.





Una vez cargado el archivo, presione el botón más para insertar nuevas contraseñas.

[SQL INSERT TblDiccionari for SQLite Studio IdIdioma='ca'](#)

```
DELETE FROM TblDiccionari WHERE IdIdioma='ca';

INSERT INTO TblDiccionari (Password, IdIdioma, MD5, SHA1, AES)
VALUES ('1q2w3e4r5t', 'ca',
'97db1846570837fce6f6f62a408f1c26a',
'b80a9aed8af17118e51d4d0c2d7872ae26e2109e',
'U2FsdGVkX1+A+1/Elrx2nR0xJgh3zrCSi+ClYRchc=');

INSERT INTO TblDiccionari (Password, IdIdioma, MD5, SHA1, AES)
VALUES ('PovlmLy
Oe7afdfsfel20ee30
5bb1f0d70a5490f
U2FsdGVkX19RK
', 'ca',
'Look Up "DELETE FROM TblDiccionari..."',
'Translate "DELETE FROM TblDiccionari..."',
'Search with Google',
'Copy
Copy Link with Highlight
Add to Quick Note
Share...
Speech
>');

INSERT INTO TblDiccionari (Password, IdIdioma, MD5, SHA1, AES)
VALUES ('1q2w3e4r5t', 'ca',
'5416d7cd6ef195a0
'48cf4851e15940a
'U2FsdGVkX197P
', 'ca',
'Look Up "DELETE FROM TblDiccionari..."',
'Translate "DELETE FROM TblDiccionari..."',
'Search with Google',
'Copy
Copy Link with Highlight
Add to Quick Note
Share...
Speech
>');

INSERT INTO TblDiccionari (Password, IdIdioma, MD5, SHA1, AES)
VALUES ('02b92faa38aaefc
', 'ca',
'f64cd8e3/2f5ac755
', 'ca',
'Look Up "DELETE FROM TblDiccionari..."',
'Translate "DELETE FROM TblDiccionari..."',
'Search with Google',
'Copy
Copy Link with Highlight
Add to Quick Note
Share...
Speech
>');

INSERT INTO TblDiccionari (Password, IdIdioma, MD5, SHA1, AES)
VALUES ('q963258741q', 'ca',
'd27c295878cea9d5b8d2711ed9c333b',
'30cal180b9cb9dfc3d216f406414c17757e1365',
'U2FsdGVkX1852IlrijyZvBWNqX3OPSSdXqSw6lY0mOFk=');

INSERT INTO TblDiccionari (Password, IdIdioma, MD5, SHA1, AES)
VALUES ('q1w2e3r4t5', 'ca',
'42d8aa7cd9e78c4757862d84620c335',
'5d70c3d101ef9cc0a69f4ad2ddfd3b21e641f6a',
'U2FsdGVkX19GjhwKu2af0pJTkToQRH8AjhXK6xRbHg=');

INSERT INTO TblDiccionari (Password, IdIdioma, MD5, SHA1, AES)
VALUES ('1q2w3e4r5t', 'ca',
'3de6bb0541387e4ebdadf7c2f31123',
'9ac20922b054316be23842a5bca7d69f29f69d77',
'U2FsdGVkX1+9ejmp4HoL7k02DiuqVSODIEF7wexjpu8=');

INSERT INTO TblDiccionari (Password, IdIdioma, MD5, SHA1, AES)
VALUES ('159753', 'ca',
'558341343164b56500def9a533c7c70',
'3fcfc1f7f34e78a937e81171ba51dc39538db993');
```

Este botón más nos lleva a otra página donde podemos copiar el código SQL

correspondiente al INSERT.

```

0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50
ca uk Replace Replace All Done
VALUES ('1q2w3e4r5t', ca,  

'97db1846570837cc6ff62a408f1c26a',  

'b80a9acd8af17118e51d4d0c2d7872ac26c2109e',  

'U2FsdGVkX1+As+1/pElkk2nR0xLgh2zgCSi+CLvRch=');  

INSERT INTO TbDiccionari (Password, IdIdioma, MD5, SHA1, AES)  

VALUES ('PoxmlLy727', ca,  

'0e7afdf8fe20ee30455874049465e2c',  

'b5b1c0d70a5490f13b6417078b748cf64f564248',  

'U2FsdGVkX18RkpwhUKevF19y0+cHmddyxdc3CUqU0A=');  

INSERT INTO TbDiccionari (Password, IdIdioma, MD5, SHA1, AES)  

VALUES ('1q2w3e4r', ca,  

's416d7cd0ef195a0f7622a9c56b55e84',  

'48efc4851e15940af5d477d3c0ce99211a70a3be',  

'U2FsdGVkX1977976fVkrB3a2IDsyyuMAR+LGyT8=');  

INSERT INTO TbDiccionari (Password, IdIdioma, MD5, SHA1, AES)  

VALUES ('author', ca,  

'02bd92faa38aaa6cc0ea75e59937a1e',  

'f64cd8e32f5ac7553c150bd0d5df72252bb73f68d',  

'U2FsdGVkX1L2mu0wRzClnArvgW6itPtJa772MntVIJQ=');  

INSERT INTO TbDiccionari (Password, IdIdioma, MD5, SHA1, AES)  

VALUES ('q963258741q', ca,  

'027c295878ceaf945b8427111ed99c33b',  

'30cal80b9c69df3d216406414c17757e1365',  

'U2FsdGVkX1852JlnyZvBWNgX3OPSSqXqSw6lY0mOFk=');  

INSERT INTO TbDiccionari (Password, IdIdioma, MD5, SHA1, AES)  

VALUES ('q1w2e3r4t5', ca,  

'42d8aa7cd9e9c78c4757862d84620c335',  

'5d70c3d1011ef9c0a69f4d2df3b21e641f6a',  

'U2FsdGVkX19GjhwKu2aJ0pJTkToQRH8AjhKK6xRhHg=');  

INSERT INTO TbDiccionari (Password, IdIdioma, MD5, SHA1, AES)  

VALUES ('1q2w3e', ca,  

'3fde6bb0541387e4ebdadf7c2f31123',  

'9ac20922b054316be23842a5ka/d69f29f69d77',  

'U2FsdGVkX1+96jmp4HoL7k02DtaVSODiEF7wexjpu8=');  

INSERT INTO TbDiccionari (Password, IdIdioma, MD5, SHA1, AES)  

VALUES ('159753', ca,  

'5583413443164b56500de9a533c7e70',  

'
```

Luego, en un editor de texto plano, debe hacer unas modificaciones al código. Estas incluyen cambiar el idioma “ca” (catalán) al idioma correspondiente, en este caso “uk” (ucraniano).



```

0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50
[Q] Replace
Delete FROM TblDiccionari WHERE IdIdioma='uk';
Replace all occurrences of the find text
Click and hold to see more options
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('1q2w3e4r', 'uk', 97db1a46570837fce6ff62a408fc1c26a', b80a9ed8af17118e51d4d0c2d7872ac26c2109c, U2FsdGVkX1+A++1/pElxk2mR0v1gh3zCs+CLyRhc=);
Replace All | Done
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('PxlmLy727', 'uk', 0e7af8fe20ea30455873049465cc2c, 5bb1c0d70a590f13bf417078b748cf64f564248, U2FsdGVkX18RKpwnUkvf19y0+chmddyxdc3CuqJ0u=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('1q2w3e4r', 'uk', 5416d7cd6ef195a0f7622a9c56b55e84, 48efc4851e15940af5d477d3c0ce99211a70a3be, U2FsdGVkX197P976FVkrctB3a2IDqyyuMArR+LGYt8=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('author', 'uk', 02bd92faa38aaa6cc0ea75e59937a1ef, f64cd8e32f5ac7553c150bd05d6f2252bb73f68d, U2FsdGVkX12nu0wRzClnArqW6itPtJa772MntYUQ=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('q963258741q', 'uk', d27c295878cea9458d82711e9c333b, 300k180bf9cb9dfce3d216f406414c1757e1365, U2FsdGVkX1852lIrrvZBVNqK3OP9dXqSw6LY0mOfK=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('q1w2e3r4t5', 'uk', 42d8aa7cde9c78c475786d2d84620c35, 5d70e3d101ef9cc0a69f4df2ddf3b21e641f6a, U2FsdGVkX19GjhwkXu2a0JTKtOQRH8AjlXK6xRbh=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('1q2w3e', 'uk', 3fd6hb0b541387e4ebdad7fc2f31123, 9ac20922b054316be23842a5huk7d6929f69d77, U2FsdGVkX1+96imp4HoL7k2DltQvSODJF7wexjnuR=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('159753', 'uk', 5583413443164b56500def9a533c7c70, 3fcfc1f7f34e78a937e8117ba51dc39538db993, U2FsdGVkX18zuKOYX144BYgbzvX3f0liOvDebDQhA=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('121212', 'uk', 93279e3308bdbbced9466c965017f67a, 48058e0c99bf7d689ce71c360699a14ce2f99774, U2FsdGVkX1/1P90gpZIX+QAKoASm+2f6mpDA6q/F7vS=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('xnum1348', 'uk', 9557574e569676731a0b8fb6aa8b, 15e98aa5095e29fd61273b212e755f853eafc5aa, U2FsdGVkX1/uhTwMakCCBtZvGxMlPlsQyng+C0=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('q1w2e3c', 'uk', 7ccb3252ba6b7e9c422facs5334d22054, 42d1f9243114643c3b0d2cd3e5e86a94122d2306, U2FsdGVkX1/Jf/XJ+xiSLAKtr8yQuEjgJzWakcU=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('112233', 'uk', d0970714757783e6cf17b26b8e2298f, 3acd0be86de7dccdbf91b20f94a68cea535922d, U2FsdGVkX1+d-RHrAtC4aLAzK3e6cQ7esNeFkjXjMg=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('nikita', 'uk', b00a50c448238a71ed47981fa49066, 7afaa0a74c41394c7122fe61723ddc365f322a5, U2FsdGVkX19hevXyAQXO84Emb/twcOCig1zr5auVhA=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('q1w2e3r4', 'uk', c62d929e7b7e7b6165923a5df60c56, 1fc854110e5532480000542834f453de31936c2f, U2FsdGVkX1/mChy/YBp4D7stuyqiX756AYnw/198a=g=);
INSERT INTO TblDiccionari (Password, IdIdioma, MDS, SHA1, AES) VALUES ('marina', 'uk', cc5225d01c93b2567bs229501d9e610d, 79b333c96cc99512a3b72653b23c7ed8a52dc42, U2FsdGVkX1/);

```

También, debe eliminar los caracteres invisibles que causarán un error de sintaxis.

The screenshot shows the SQLite Studio interface with the 'manual_usuario' database open. The main window displays a table with many rows of data, mostly consisting of 'AES' values. At the bottom of the window, there are several buttons: 'Execute', 'Save the db', 'Load an SQLite database file...', 'Tables', 'Indexes', and 'Relationships'. Below the interface, a note reads: 'Original work by kripken (sql.js). C to Javascript compiler by kripken (emscripten). Project now maintained by lovayosa'.

Una vez realizadas estas modificaciones, debe copiar el código en el SQLite Studio y



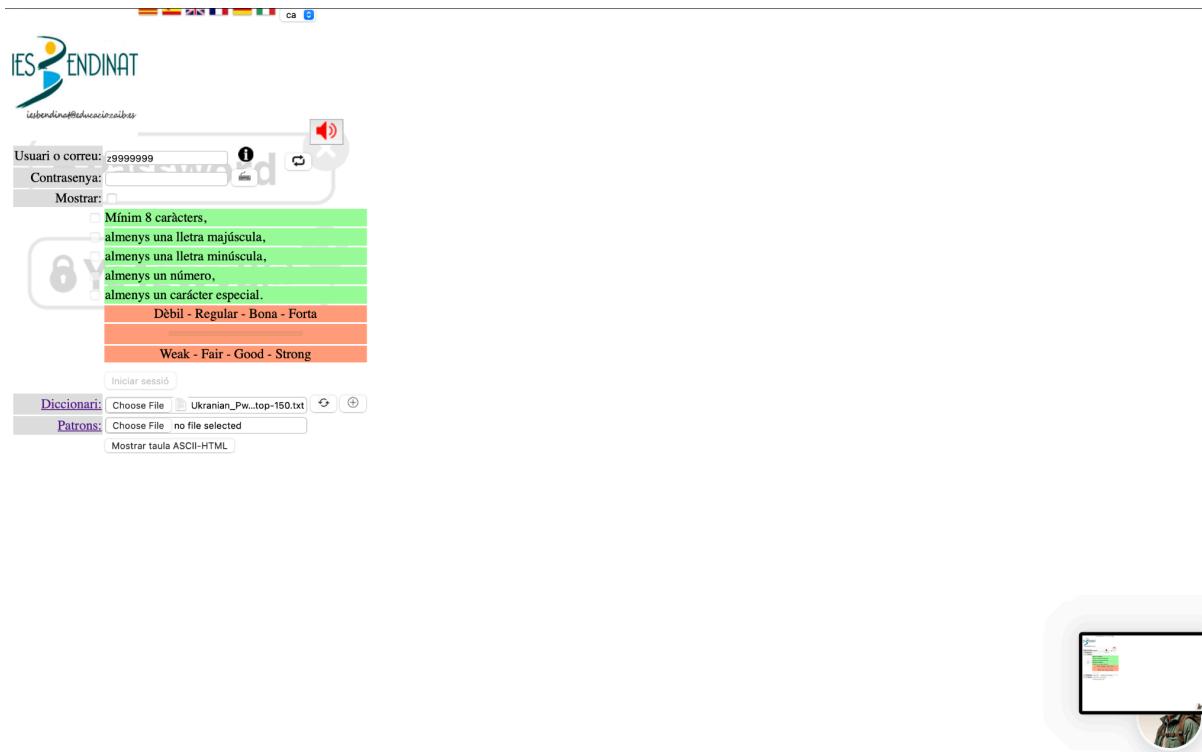
ContraSegur
Manual de Usuario

IES Bendinat

ejecutarlo. Tenga en cuenta que primero deberá cargar la base de datos y, posteriormente, seguir los pasos indicados en la explicación sobre cómo añadir textos a la GUI.

SQL Query Results	
1q2w3e4r5t	uk
Pov1mby727	uk
lg2w3e4r	uk
author	uk
q963258741q	uk
qlw2e3rt4t5	uk
lgw2q3	uk
159753	uk
121212	xrum1348
9327983308dbbde	uk
965575474e569f66731ac08bf6aa8ba15e98a59059e29d1	uk
qlw2e3	uk
112223	d097704717577836eef1726fb282298f3
nikita	uk
qlw2e3r4	uk
marina	uk
andrey	uk
lgw3e4r5t6y	uk
sergey	uk
ghbdtm	uk
12qwaszx	uk
12qvw23we	uk
ruslan	uk
159357	36e1a50728359066ed7175f5d3fa
samsung	uk
qwaszx	uk
1ck75f1guk	uk
131313	e047553875b65986231e4
4780july5604	uk
oksana	uk
133Hjsdfu	uk
elena	uk
stalker	uk
SaIn	uk
natasha	uk
svetlana	uk
ls2a3s4h5a	uk
r899xuQdul	uk
4xfwwx89Xh	uk
galina	uk
25011990	uk
nasty	uk
kirill	uk
1029384756	uk
147258369	uk

Aquí puede ver en la tabla que se ha ejecutado correctamente.



Para actualizar las contraseñas debe seguir los mismos pasos, esta vez presionando el botón de regenerar.

SQL UPDATE TblDiccionari for SQLite Studio IdIdioma='ca'

```
UPDATE TblDiccionari SET
    MD5 = '5f4dcc3b5aa765d61d8327deb882cf99',
    SHA1 = '5baa61e4c9b93f30682250b6cf8331b7ee68fd8',
    AES = 'U2FsdGVKX18wghegeoDxBzmuw8wnmlQ+PKAS/I67mMM='
WHERE TblDiccionari.Password = 'pa'

UPDATE TblDiccionari SET
    MD5 = '8621ffbc5698829397d977',
    SHA1 = 'a8978b1797b72acfff9595',
    AES = 'U2FsdGVKX1+ccJTvzyO+'
WHERE TblDiccionari.Password = 'dr'

UPDATE TblDiccionari SET
    MD5 = '2768db0b86cd47a7680551',
    SHA1 = 'a2c901c8c0de98958c219',
    AES = 'U2FsdGVKX1++O4nPv2C'
WHERE TblDiccionari.Password = 'bd'

UPDATE TblDiccionari SET
    MD5 = '37b4e2d82900d5e94b8da52',
    SHA1 = '2d27b62c597ec858f6e7b54',
    AES = 'U2FsdGVKX1+UUVP-PzgTTIXrvBKZogzw5LwBe8zqVk='
WHERE TblDiccionari.Password = 'football';

UPDATE TblDiccionari SET
    MD5 = 'd0763ca9d9bd2a9516280c9044d885',
    SHA1 = 'a87d724bdc7452e55738de5b5f868ef1f16dea5ace',
    AES = 'U2FsdGVKX1+eKwVgEFRMkFPPhZChnTjVqOe5V1E5LySQ='
WHERE TblDiccionari.Password = 'monkey';

UPDATE TblDiccionari SET
    MD5 = '0d107d09f5bbe40cade3de5c71e9e9b7',
    SHA1 = 'b7a875fc1ea228b9061041b7ecc4bd3c52ab3ce3',
    AES = 'U2FsdGVKX1+eKwVgEFRMkFPPhZChnTjVqOe5V1E5LySQ='
WHERE TblDiccionari.Password = 'letmein';

UPDATE TblDiccionari SET
    MD5 = '3bf1114a986ba87ed28fc1b5884fc2f8',
    SHA1 = 'e99d3d832a99035363a9fd53cd3b8e7f1501c',
    AES = 'U2FsdGVKX1+eKwVgEFRMkFPPhZChnTjVqOe5V1E5LySQ='
WHERE TblDiccionari.Password = 'shadow';

UPDATE TblDiccionari SET
    MD5 = 'eb0a191797624dd3a48fa681d3061212',
    SHA1 = '4'f26aeaf1b2367620a393c973eddb8f8b846ebd,
    AES = 'U2FsdGVKX18Dz+nH5uddf62MpsLWH9F165TfkfeBdkc='
WHERE TblDiccionari.Password = 'master';
```

Este botón de regenerar nos lleva a otra página donde podemos copiar el código SQL correspondiente al UPDATE y luego seguir los pasos anteriores (del INSERT).

3.2.2 Mensajes de error

A continuación se explicarán los mensajes de error más comunes en SQLite que quizás encontrará mientras actualiza la base de datos.

- Error de sintaxis: La sentencia SQL tiene un error (como una coma que falta, una palabra clave incorrecta o un formato incorrecto), por lo que SQLite no puede interpretarla.
- Error en crear la tabla: Intenta crear una tabla que ya existe en la base de datos. Use IF NOT EXISTS o elimine primero la tabla anterior.
- Error en insertar valores: El número de valores que intenta insertar no coincide con el número de columnas esperado (demasiados o muy pocos). Revise la lista de columnas y los valores.

3.2.3 Ayudas contextuales

Si mientras actualiza la base de datos necesita ayuda con el sintaxis, puede consultar los enlaces en la parte superior para obtener ayuda en SQL.

[SQL \(SELECT, UPDATE, DELETE, INSERT INTO, WHERE, ORDER BY, GROUP BY, HAVING, MIN\(\), COUNT\(\), INNER JOIN, CREATE TABLE \)](#)

4 FAQ

4.1 ¿Qué significa que este trabajo está licenciado bajo Creative Commons Reconocimiento 4.0 Internacional?

Significa que puedes compartir y adaptar la obra para cualquier propósito, incluso comercial, siempre que atribuyas adecuadamente al autor, brindes un enlace a la licencia e indiques si realizaste cambios. No puedes aplicar restricciones legales o tecnológicas adicionales que limiten el uso permitido por la licencia. Además, es importante tener en cuenta que otros derechos, como los de privacidad o publicidad, pueden limitar el uso de la obra. (DEED, n.d.)

4.2 ¿Cuál es el propósito de este proyecto?

El proyecto ContraSegur tiene como objetivo educar sobre ciberseguridad mediante una herramienta interactiva que permite crear, evaluar y gestionar contraseñas seguras. Analiza en tiempo real la robustez de las contraseñas e identifica vulnerabilidades usando el algoritmo zxcvbn, ayudando a prevenir ataques como los de fuerza bruta.

El proyecto está diseñado para ser accesible en varios idiomas y ofrece funciones prácticas como un generador de contraseñas, validación dinámica, integración de diccionarios y almacenamiento seguro local. Busca así promover hábitos digitales responsables y hacer accesible la seguridad digital a todos los usuarios.

4.3 ¿Qué hace que una contraseña sea fuerte?

Una contraseña es fuerte cuando es larga (al menos ocho caracteres), combina letras mayúsculas y minúsculas, números y caracteres especiales, y no contiene datos personales ni palabras predecibles. Debe evitar repeticiones, secuencias comunes como "1234" o "QWERTY" y actualizarse periódicamente sin reutilizar combinaciones. No debe compartirse ni guardarse en dispositivos, y se recomienda usar una diferente para cada sitio. Esto dificulta ataques de fuerza bruta, que prueban combinaciones hasta hallar la correcta. (Rosselló, 2023; Fortinet, n.d.)

4.4 ¿Puedo usar esta herramienta para administrar mis contraseñas reales?

No, esto es solo para fines educativos: las contraseñas guardadas no están cifradas, ya que se almacenan en texto plano en cookies o almacenamiento local. Además, la herramienta no cuenta con autenticación multifactor ni con opciones de compartición segura. Para un uso práctico y seguro, se recomienda utilizar servicios como Bitwarden o KeePass.

4.5 ¿Es confiable el generador de contraseñas?

El generador de contraseñas es adecuado para la mayoría de los usos básicos, ya que crea contraseñas al azar utilizando una combinación de letras mayúsculas y minúsculas, números y caracteres especiales del alfabeto latino. Este enfoque asegura que la contraseña cumpla

con los requisitos básicos de seguridad, como la variabilidad de caracteres y la inclusión de tipos diversos de símbolos. Además, garantiza que cada contraseña contenga al menos un carácter de cada tipo (minúscula, mayúscula, número y símbolo), lo que la hace más fuerte frente a ataques simples.

Sin embargo, hay algunas limitaciones. El generador depende exclusivamente del alfabeto latino y no incluye caracteres de otros alfabetos o símbolos Unicode, lo que puede hacer que las contraseñas sean predecibles para ciertos ataques.

4.6 ¿Cuál es la diferencia entre "score" y la puntuación "zxcvbn"?

La "Puntuación" interna comprueba si una contraseña cumple con las reglas técnicas básicas, como la longitud y la variedad de caracteres, y estima cuánto tiempo tardaría en descifrarse mediante fuerza bruta. Sin embargo, no detecta patrones predecibles.

Por otro lado, zxcvbn utiliza un algoritmo más inteligente para detectar patrones (como nombres, fechas o secuencias de teclado), evaluar la aleatoriedad real (entropía) y ofrecer una calificación de seguridad más realista. Si bien ambos utilizan una escala de 0 a 4, zxcvbn proporciona una visión más profunda y ayuda a detectar vulnerabilidades ocultas. (Wheeler, n.d.)

Contraseña	Score Interno	zxcvbn Score	Razón
Slay@1351	4 (cumple requisitos)	2 (patrón: nombre + símbolos)	El Score interno no detecta que "Slay" es un nombre común.
F9#kLp!2Wn	4	4	Ambas coinciden: alta entropía y sin patrones.
Diciembre24	3 (falta símbolo)	1 (patrón: mes + año)	zxcvbn penaliza la predictibilidad.

4.7 ¿Cómo debe ser el formato del fichero?

En esta parte, me centraré en el formato que deben tener los archivos de contraseñas y patrones comunes.

En primer lugar, explicaré las reglas del archivo de contraseñas común. Este archivo contiene contraseñas reales que se piratean con frecuencia (por ejemplo: contraseña, 123456, admin).

- NO debe empezar por / (el sistema lo comprueba para saber que se trata de una lista de contraseñas).
- Una contraseña por línea, texto sin formato (sin símbolos adicionales).
- Sin comillas, comas ni barras.

Por otro lado, explicaré las reglas del archivo de patrones. Este archivo define patrones o secuencias de teclado simples que facilitan la adivinación de contraseñas (p. ej., 123, qwerty, asdf).

- Debe comenzar con el carácter / (esto indica al sistema que es un archivo de patrones).
- Cada patrón debe ir en una nueva línea, entre barras diagonales (/).
- Sin espacios, comas ni símbolos adicionales; solo el patrón dentro de / /.

Acepta tanto \r\n (Windows) como \n (Linux/MacOS).

El código normaliza los saltos de línea reemplazando \r\n y \n por comas, por lo que ambos formatos funcionan.

Además, el código lee el contenido del archivo, no la extensión, por lo que .txt, .list o ninguna extensión funcionarán.

Sin embargo, para mayor claridad, recomendamos .txt (p. ej., passwords.txt, patterns.txt). Evite .csv, .docx, etc., ya que pueden añadir formato oculto.

4.8 ¿Qué ocurre si el formato del fichero es incorrecto?

Si el formato del fichero es incorrecto, el sistema puede interpretarlo erróneamente, lo que provoca fallos en el procesamiento. Por ejemplo, si un archivo de contraseñas comienza con una barra diagonal (/), será tratado como un archivo de patrones y fallará al leerlo. Del mismo modo, si un archivo de patrones no empieza por /, el sistema lo interpretará como una lista de contraseñas, causando errores. Además, el uso de símbolos adicionales como comas, comillas o espacios puede interrumpir la importación, impidiendo que el sistema lea correctamente los datos.

4.9 ¿Cómo maneja el sistema los caracteres no latinos (como cirílico o emojis) en las contraseñas?

El sistema admite completamente caracteres Unicode, por lo que acepta sin problemas contraseñas con alfabetos no latinos como el cirílico, chino o incluso emojis, considerándolos entradas válidas. Esto tiene implicaciones positivas en seguridad, ya que amplía considerablemente el conjunto de caracteres, lo que dificulta los ataques por fuerza bruta. Por ejemplo, una contraseña como Пароль123! ofrece mayor entropía que Password123!, debido a la diversidad del Unicode. Sin embargo, existen limitaciones: zxcvbn podría no detectar palabras comunes o patrones en otros idiomas (como "привет" en ruso), y aunque la barra de progreso valida criterios básicos como longitud y variedad, no siempre refleja la complejidad del guión usado. Se recomienda combinar scripts para aumentar la solidez (ej.: Gërm@ñЯ) y utilizar la herramienta para verificar el nivel estimado de entropía en contraseñas con caracteres no latinos.

Para detectar contraseñas comunes o patrones no latinos, se pueden subir listas personalizadas mediante el lector de archivos, añadiendo contraseñas comunes, como una lista .txt con palabras frecuentes en ruso, o patrones específicos, como expresiones regulares (ej., "/привет/" para secuencias en cirílico). Además, es posible modificar la base de datos utilizando SQLite Studio para actualizar manualmente las tablas correspondientes:

“TblDiccionari”, que almacena diccionarios de contraseñas específicos de cada idioma, y “TblPatrons”, que guarda los patrones de expresiones regulares no latinas.

4.10 ¿Qué se incluirá en versiones posteriores de este proyecto?

En futuras versiones de este proyecto, planeamos integrar un chatbot de IA diseñado para ayudar a los usuarios con cualquier pregunta o problema relacionado con la aplicación web. Asimismo, se incorporará un botón de información que llevará a nuestra página web. Además, implementaremos botones que enlazan a páginas dedicadas para copiar los comandos SQL como UPDATE e INSERT, lo que facilita la interacción directa con la base de datos. Esta funcionalidad reflejará la estructura mostrada en la guía de SQLite Studio, específicamente la gestión de contraseñas. También, pretendemos perfeccionar el diseño visual mejorando el estilo CSS para optimizar la experiencia del usuario, y abordaremos y resolveremos los problemas actuales que afectan a la barra de progreso para garantizar un funcionamiento más fluido y preciso.

5 ANEXOS

5.1 Fichero contraseñas comunes

Aquí está el GitHub donde puedes encontrar archivos con las listas de contraseñas más comunes de diferentes longitudes:

<https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials>

5.2 Fichero patrones comunes

Aquí está el GitHub donde puedes encontrar el archivo con los patrones de contraseñas más comunes: <https://github.com/z125674/Contrasegur/blob/main/patrons2.txt>

5.3 Cálculos internos y externos de la robustez

A continuación, describiré los cálculos realizados para estimar el esfuerzo computacional necesario para descifrar por fuerza bruta contraseñas de diversa complejidad y longitud.

En primer lugar, calculé el número total de combinaciones posibles para contraseñas de distintas longitudes, utilizando diferentes conjuntos de caracteres. Para comenzar, tomé el número de caracteres del conjunto (por ejemplo, dígitos = 10, letras = 26) y la longitud de la contraseña (por ejemplo, 4, 5, 6 caracteres), con valores que indican el número total de combinaciones para esa longitud y conjunto de caracteres. Es decir, si se utilizan solo dígitos (10 caracteres), una contraseña de 4 caracteres tiene 10.000 (=10⁴) combinaciones. Cabe destacar que hice diferentes cálculos dependiendo del idioma ya que el alfabeto varía.

Luego, calculé el tiempo necesario para descifrar contraseñas: utilicé una potencia computacional medida en MIPS (millones de instrucciones por segundo). Y calculé el tiempo necesario para un ataque de fuerza bruta a 1 MIP, en el que descifrar una contraseña puede llevar segundos o años, según la complejidad. Estudié la cantidad de caracteres, elementos en cada categoría y ejemplos específicos de caracteres en estas categorías.

Por último, analicé una tabla de caracteres y sus atributos, utilizando el estándar ASCII. Analicé el código ASCII del carácter, el nombre del carácter, la representación visual del carácter, una descripción textual de lo que hace el carácter, las categorías en las que se pueden clasificar los caracteres (como "no imprimible") y un recuento de caracteres en esta categoría.

Al combinar el tamaño del conjunto de caracteres, la longitud de la contraseña y la velocidad computacional, se demuestra el crecimiento exponencial de la dificultad a medida que las contraseñas se hacen más largas e incluyen más tipos de caracteres.

Para evaluar la solidez de una contraseña de forma más simple, calculé la cantidad de intentos necesarios para que un atacante la descifre. Las contraseñas "demasiado fáciles" se rompen en menos de 1000 intentos, mientras que las "muy fáciles" son vulnerables a ataques en línea (menos de un millón de intentos). Las contraseñas "algo fáciles" protegen moderadamente con hasta 100 millones de intentos, y las "seguramente imposibles" resisten ataques fuera de línea (menos de 10 mil millones). Las contraseñas "muy imposibles" son las más fuertes, requiriendo más de 10 mil millones de intentos.

Zxcvbn

Por otro lado, hemos externalizado los cálculos con "zxcvbn", que es un estimador de la solidez de las contraseñas que evalúa una contraseña mediante un proceso de tres etapas:

coincidencia, puntuación y búsqueda. (Wheeler, n.d.)

En la primera etapa, la coincidencia, "zxcvbn" identifica patrones dentro de la contraseña. Busca una variedad de patrones, como palabras de diccionarios (como palabras en inglés, nombres y contraseñas comunes), patrones de teclado espacial (como QWERTY o Dvorak), caracteres repetidos (como "aaaa"), secuencias (como "12345" o "gfedcba"), fechas y años (por ejemplo, "3-13-1997" o "1997") y sustituciones I33t (leet) comunes (como "4" por "A"). (Wheeler, n.d.)

A continuación, en la etapa de puntuación, "zxcvbn" asigna un valor de entropía a cada patrón coincidente. La entropía, una medida de aleatoriedad, se calcula asumiendo que un atacante ya conoce el patrón e intentará adivinarlo. La entropía se calcula utilizando una fórmula que considera las posibles variaciones o sustituciones para cada patrón coincidente. (Wheeler, n.d.)

En la etapa final, la búsqueda, "zxcvbn" utiliza programación dinámica para determinar la secuencia óptima de coincidencias no superpuestas con la entropía más baja posible. El objetivo es encontrar la secuencia de coincidencias más simple que represente la contraseña completa y requiera la menor cantidad de intentos por parte de un atacante. Por ejemplo, una contraseña como "damnation" podría considerarse como una sola palabra en lugar de dos palabras superpuestas ("dam" y "nation"). (Wheeler, n.d.)

"Zxcvbn" calcula luego la entropía total de la contraseña sumando la entropía de todos los patrones detectados, incluidos los espacios entre patrones que se tratan como segmentos de fuerza bruta. Esta entropía total proporciona una estimación general de la fortaleza de la contraseña y un tiempo estimado de descifrado basado en métodos de ataque comunes. (Wheeler, n.d.)

En lo que respecta a las funciones que ofrece el algoritmo, "result.entropy" mide la imprevisibilidad de la contraseña en bits, donde los valores más altos indican contraseñas más seguras. "Result.crack_time" estima cuánto tiempo le llevaría a un atacante descifrar la contraseña, dada la velocidad de descifrado y su entropía, mientras que "result.crack_time_display" presenta este tiempo en un formato más fácil de usar, como "instantáneo" o "siglos". "Result.score" da un valor numérico de 0 a 4 para calificar rápidamente la solidez de la contraseña, donde las puntuaciones más altas indican una mayor solidez. "Result.match_sequence" muestra una lista de patrones detectados dentro de la contraseña, lo que ayuda a explicar cómo se calculó su entropía. Por último, "result.calculation_time" mide cuánto tiempo se tardó en calcular la fortaleza de la contraseña en milisegundos, lo que proporciona información sobre el rendimiento del proceso de estimación. (Wheeler, n.d.)

6 GLOSARIO

Término	Descripción
Aplicación web	Es un software accesible desde un navegador que permite al usuario interactuar con funciones o servicios en línea sin necesidad de instalación local. (Devs, 2024)
Interfaz gráfica (GUI)	Diseño visual de la aplicación (botones, campos de texto, etc.). (IONOS, 2021)
Menú desplegable	Lista de opciones (ej. idiomas) que se despliega al hacer clic. (IONOS, 2021)
Barra de progreso	Indicador visual que muestra la fortaleza de la contraseña en tiempo real. (Torresburriel Estudio, 2023)
Casillas de verificación	Cuadros para marcar requisitos de contraseña (mayúsculas, números, etc.). (Wikipedia, 2024)
Teclado en pantalla	Teclado virtual para introducir contraseñas sin usar el físico. (Melanie, 2022)
Tabla ASCII	Tabla que muestra caracteres especiales y sus códigos numéricos. (Wikipedia, 2024)
Lectores de archivos	Permiten cargar archivos externos (ej. listas de contraseñas comunes). (Lee, 2022)
Mensaje emergente	Notificación que muestra resultados de análisis o confirmaciones. (Geek, n.d.)
Requisitos básicos	Reglas para contraseñas seguras (longitud, caracteres especiales, etc.). (Tuta, 2024)
Fuerza bruta	Ataque que prueba combinaciones hasta descifrar una contraseña. (Fortinet, n.d.)
MIPS	Unidad de potencia computacional (Millones de Instrucciones Por Segundo). (Wikipedia, 2024)
Coste computacional	Estimación de tiempo/recursos para descifrar una contraseña. (Universidad de Zaragoza, 2017)
Cookies	Archivos que guardan credenciales del usuario en el navegador. (Cloudflare, n.d.)
CSS	CSS (Hojas de Estilo en Cascada) es un lenguaje de hojas de estilo que define la presentación de un documento escrito en HTML o XML. Controla el diseño, los colores, las fuentes y otros aspectos visuales de las páginas web. (MDN, 2025)
SQL	Lenguaje de programación para gestionar bases de datos relacionales. Permite consultar, insertar, actualizar y eliminar datos. (AWS, n.d.)
SQLite	Sistema de base de datos ligero y embebido, usado en la aplicación para almacenar idiomas, contraseñas comunes y patrones. No requiere servidor externo. (Administrador, 2024)



SQLite Studio	Herramienta gráfica externa (https://sqlitesudio.netlify.app) para editar la base de datos ContraSegur.db de la aplicación.
Consulta SQL	Instrucción para interactuar con la base de datos (ej. SELECT * FROM TblTextosGUI WHERE IdIdioma = 'es'). (W3Schools, n.d.)
Clave primaria (PK)	Campo único que identifica cada registro en una tabla (ej. IdIdioma en TblIdiomes). (Wikipedia, 2025)
Clave foránea (FK)	Campo que relaciona una tabla con otra (ej. IdIdioma en TblDiccionari referencia TblIdiomes). (Wikipedia, 2025)
Base de datos relacional	Estructura organizada en tablas relacionadas entre sí (ej. TblIdiomes ↔ TblTextosGUI). (Wikipedia, 2025)

7 BIBLIOGRAFÍA Y REFERENCIAS

Referencia	Título
Administrador. (2024). SQL: El lenguaje estándar para la gestión de bases de datos relacionales - Administración de Sistemas. Administración De Sistemas.	https://administraciondesistemas.com/sql-lenguaje-estandar/
Cloudflare. (n.d.). What are cookies? Cloudflare. Retrieved April 23, 2025, from	https://www.cloudflare.com/es-es/learning/privacy/what-are-cookies/
Colaboradores de Wikipedia. (2024). ASCII. Wikipedia.	https://es.m.wikipedia.org/wiki/ASCII
Colaboradores de Wikipedia. (2024). Casilla de verificación. Wikipedia, La Enciclopedia Libre.	https://es.wikipedia.org/wiki/Casilla_de_verificaci%C3%B3n
CSS: Cascading Style Sheets MDN. (2025). MDN Web Docs.	https://developer.mozilla.org/en-US/docs/Web/CSS
DEED - Atribución/Reconocimiento 4.0 Internacional - Creative Commons. (n.d.).	https://creativecommons.org/licenses/by/4.0/deed.es
Equipo editorial de IONOS. (2021). ¿Qué es una interfaz gráfica de usuario (GUI)? IONOS Digital Guide.	https://www.ionos.mx/digitalguide/paginas-web/desarrollo-web/que-es-una-gui/
JavaScript: Mensajes emergentes usando Alert, Confirm y Prompt – Desarrollo Geek. (n.d.).	https://desarrollo-geek.net/tutoriales/javascript/javascript-alert-confirm-prompt/
Melanie. (2022). Teclado en pantalla. TechEdu.	https://techlib.net/techedu/teclado-en-pantalla/



Prosselloe. (2023). Contraseñas seguras – Mossos d'Esquadra. Pere Miquel Rosselló Espases.	https://prosselloe.wordpress.com/2021/09/01/contraseñas-seguras-mossos-desquadra/
Tuta. (2025). 2024 Normas del NIST sobre la longitud mínima de las contraseñas: 16 caracteres o más.	https://tuta.com/es/blog/minimum-password-length
Torresburriel Estudio. (2023). Barras de progreso en UX	https://torresburriel.com/weblog/barras-de-progreso-e-indicadores-de-tiempo/
W3Schools. (n.d.). SQL SELECT Statement. Retrieved April 23, 2025, from	https://www.w3schools.com/sql/sql_select.asp
Wheeler, D. (n. d.). zxcvbn: realistic password strength estimation. Dropbox.	https://dropbox.tech/security/zxcvbn-realistic-password-strength-estimation
Wikipedia. (2025). Base de datos relacional. Recuperado el 23 de abril de 2025, de	https://es.wikipedia.org/wiki/Base_de_datos_relacional
Wikipedia. (2025). Clave foránea. Recuperado el 23 de abril de 2025, de	https://es.wikipedia.org/wiki/Clave_for%C3%A1nea
Wikipedia. (2025). Clave primaria.	https://es.wikipedia.org/wiki/Clave_primaria
What is a Brute Force Attack? Definition, Types & How It Works	https://www.fortinet.com/lat/resources/cyber-glossary/brute-force-attack
¿Qué es SQL? - Explicación de lenguaje de consulta estructurado (SQL) - AWS. (n.d.). Amazon Web Services, Inc.	https://aws.amazon.com/es/what-is/sql/
Devs, Q. (2024). ¿Qué es una web app? Definición y características. Quality Devs.	https://www.qualitydevs.com/2024/08/22/web-app/



ContraSegur
Manual de Usuario

IES Bendinat