

WikiInfoSeguridad

Galder García

Entrega 1 - Versión 1 (2022-10-16)

Índice de contenidos

Introducción	3
Página principal	4
Barra de navegación	6
Pie de página	7
Inicio de sesión / Registro	8
Creador de artículos	10
Visor de artículos	11

Introducción

Esta documentación pertenece al proyecto práctico de la asignatura Sistemas de Gestión de Seguridad de la Información.

El objetivo de esta práctica consiste en crear una página web alojada en un servidor, que se comunique con una base de datos alojada en otro servidor, y ejecutar todo con contenedores docker. Esto nos permite que se pueda ejecutar correctamente en cualquier sistema Linux.

La página web que he decido crear es “WikiInfoSeguridad”, una Wiki en la que tendremos artículos relacionados con la seguridad informática. Cualquier usuario podrá acceder a todos los artículos ya creados. También podrá registrarse y crear sus propios artículos*.

Todo lo referente al proyecto puede encontrarse en el siguiente repositorio público de github:

<https://github.com/galdergcupv/WikiInfoSeguridad>

No he usado plantillas ni copiado código directamente, pero si que he seguido [tutoriales](#), implementando las modificaciones necesarias y ajustándolos a mi caso, para la creación del diseño de la página web.

*De momento no es necesario registrarse para crear artículos.

Página principal

La página principal de la web está compuesta por una **barra de navegación** en la parte superior (ver pág. 6), el **cuerpo**, y un **pie de página** (ver pág. 7). La barra de navegación y el pie de página se tratarán en sus respectivos apartados.

En el cuerpo de la página principal tenemos: A la derecha una imagen, y a la izquierda un texto acompañado con un botón que nos llevará a la pantalla de registro / inicio de sesión.

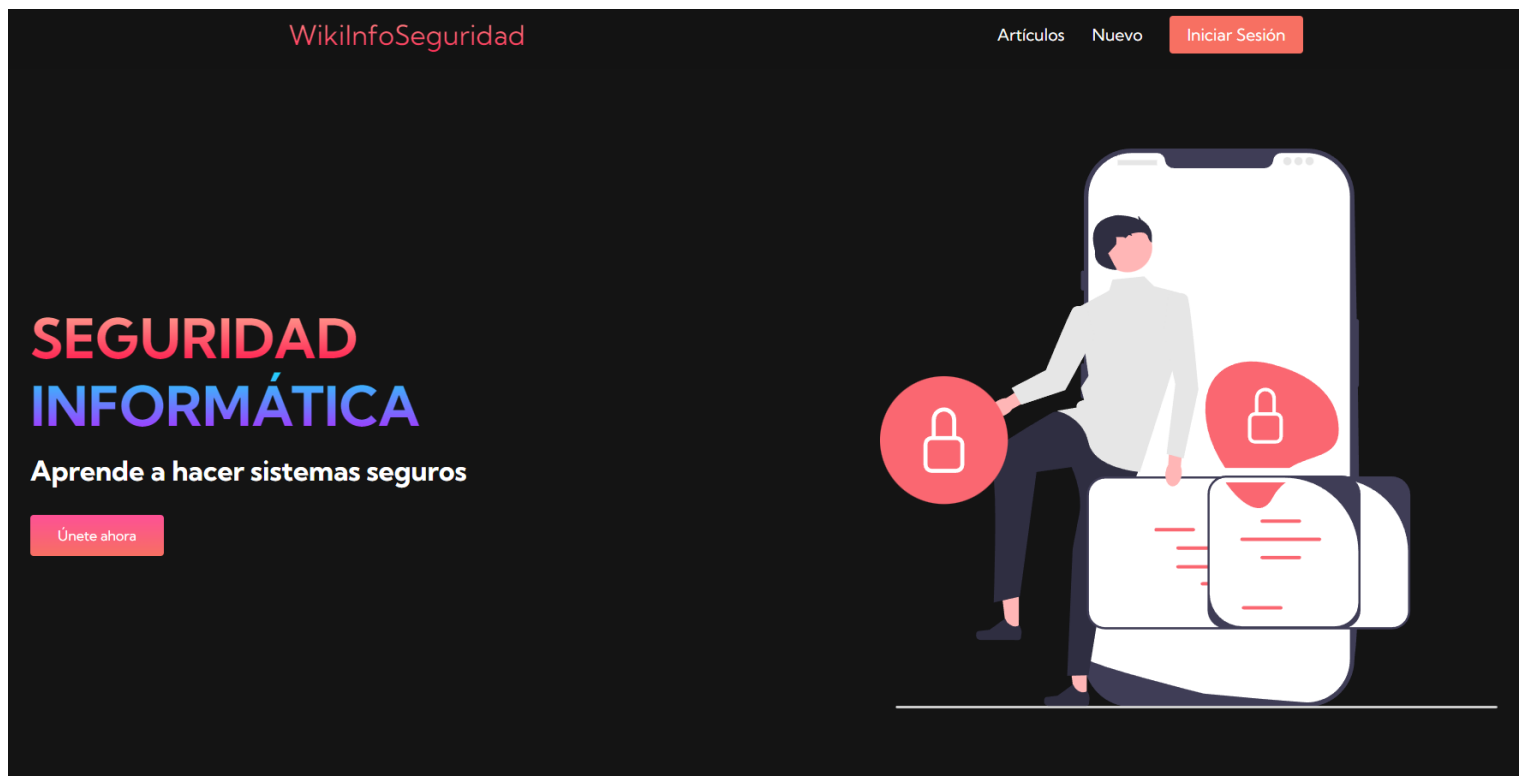


Imagen 1. Página principal (arriba)

Si bajamos en la página principal encontramos dos imágenes interactivas con texto y botones que nos llevan a la página del **visor de artículos** y de **creación de artículos**.



Imagen 2. Página principal (abajo)

Barra de navegación

En la parte superior de todas las páginas se encuentra una barra de navegación que nos permite acceder rápidamente a las pantallas: **Principal** (haciendo click en el nombre de la web a la izquierda), **visor de artículos**, **creador de artículos** e **inicio de sesión / registro**.

WikiInfoSeguridad

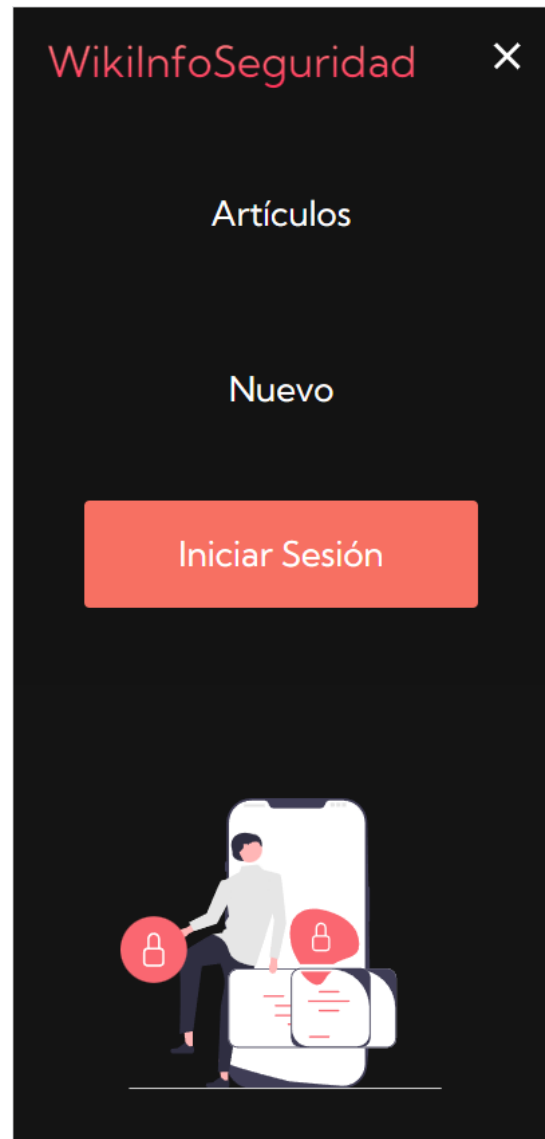
Artículos

Nuevo

Iniciar Sesión

Imagen 3. Barra de navegación (modo normal)

La barra de navegación se ajusta si la ventana es muy estrecha (por ejemplo en un dispositivo móvil), mostrando un boton que al pulsarlo desplegará un menú vertical.



Imágenes 4 y 5. Barra de navegación móvil sin menú (izq.) y con menú (der.)

Pie de página

En la parte inferior de todas las páginas se encuentra un pie de página donde podemos encontrar información adicional. De momento esta sección no es operativa, todos los enlaces redirigen a la página principal.

También encontramos el nombre de la web (al pinchar en él nos redirige a la página principal) y un aviso con el copyright de la web.

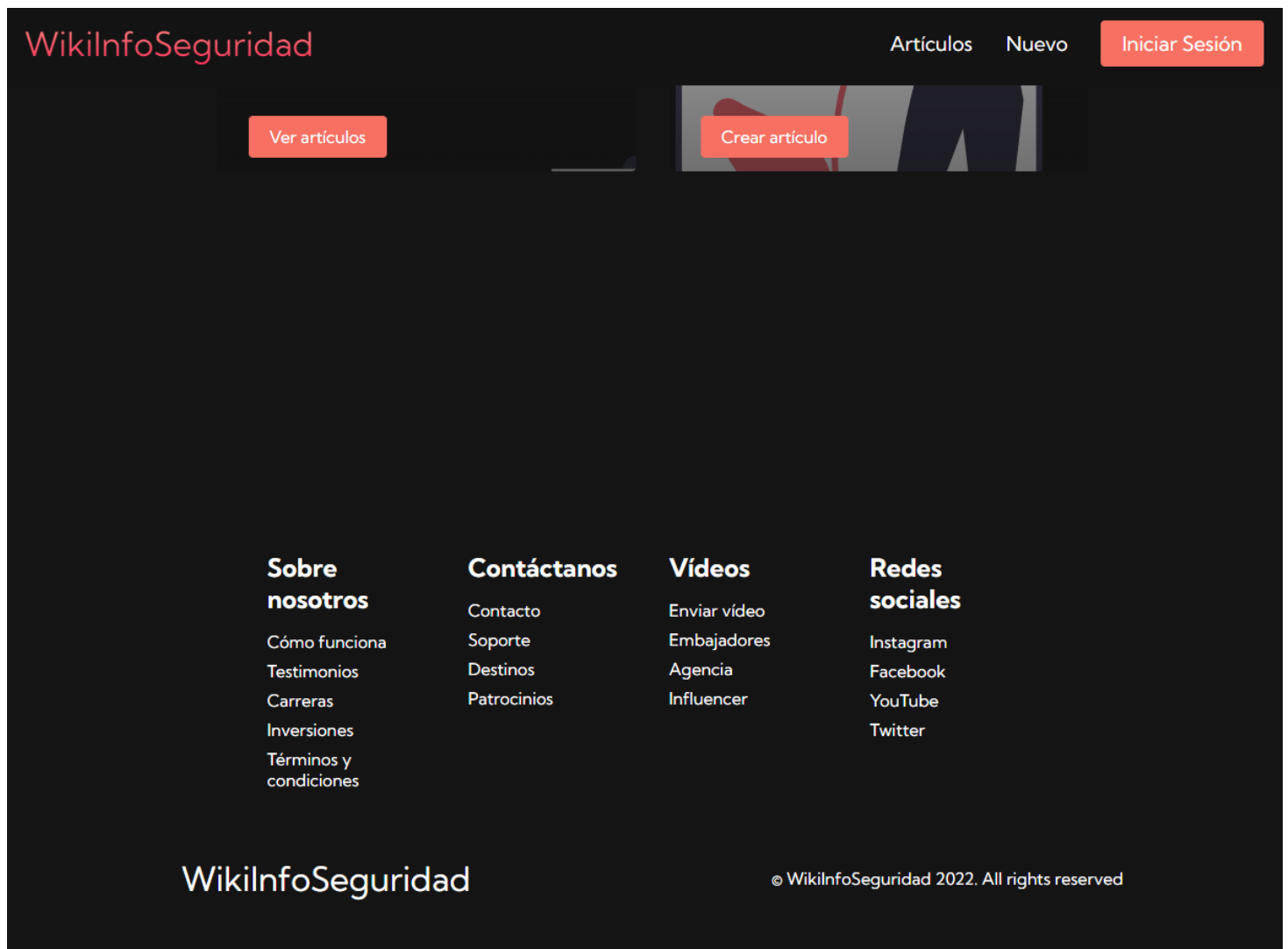
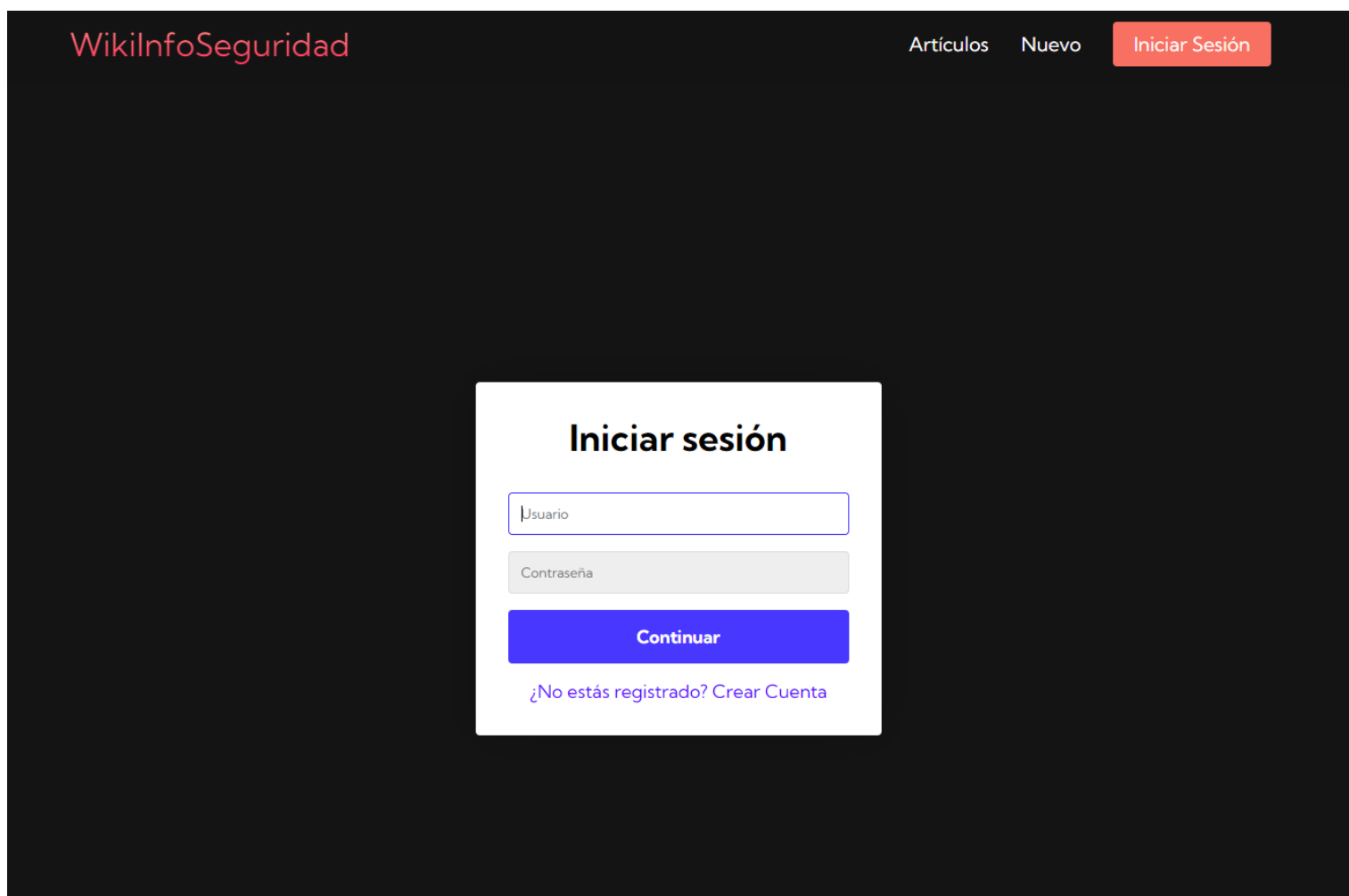


Imagen 6. Pie de página

Inicio de sesión / Registro

En la página de inicio de sesión tenemos un formulario para introducir el usuario y contraseña (**Imagen 7**). También hay un enlace para que si no estamos registrados accedamos al formulario de registro (**Imagen 8**). En el formulario de registro introduciremos nuestros datos y se comprobará si son correctos (El nombre y los apellidos son texto, la fecha es válida, el DNI tiene la letra correspondiente, etc...), si no son correctos aparecerá un texto indicando qué debemos modificar hasta que lo corrijamos.

Una vez registrado podremos iniciar sesión, al hacerlo nos llevará a una página en la que veremos nuestros datos personales (**Imagen 9**).



WikInfoSeguridad

Artículos Nuevo Iniciar Sesión

Iniciar sesión

Usuario

Contraseña

Continuar

[¿No estás registrado? Crear Cuenta](#)

Imagen 7. Inicio de sesión

WikiInfoSeguridad

ArtículosNuevoIniciar Sesión

Crear Cuenta

Nombre

Apellidos

DNI (12345678-A)

Teléfono (9 dígitos)

Fecha de nacimiento (aaaa-mm-dd)

Email (ejemplo@servidor.extensión)

Usuario

Contraseña

Continuar

¿Ya tienes una cuenta? [Iniciar Sesión](#)

Imagen 8. Registro

WikiInfoSeguridad

ArtículosNuevoIniciar Sesión

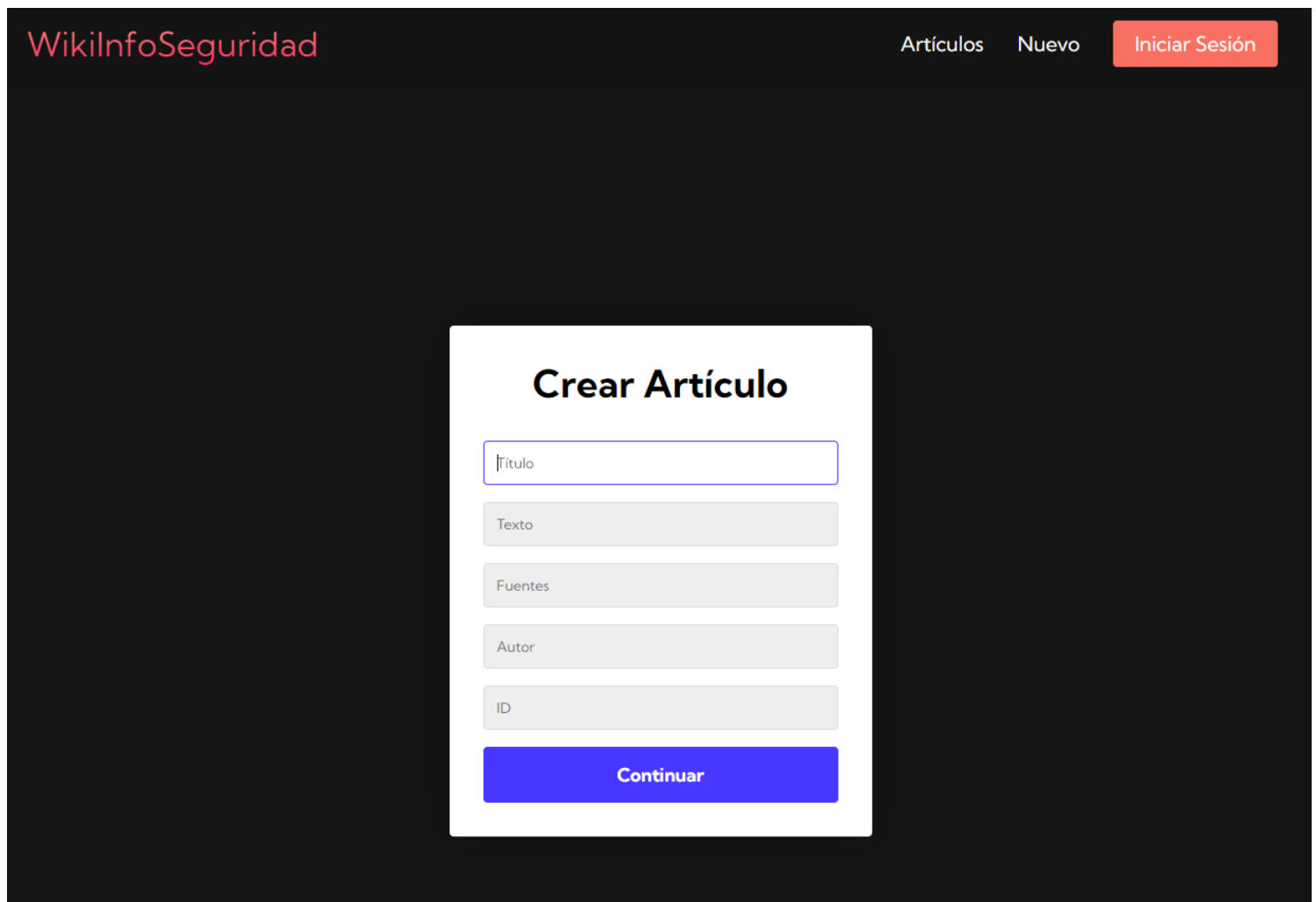
Sesión iniciada correctamente...

Nombre	Apellidos	DNI	Fecha de nacimiento	Telefono	Email	Usuario
Galder	Garcia	79138114-J	2001-01-11	634430400	galdergcupv@gmail.com	Galder

Imagen 9. Datos usuario

Creador de artículos

En la página de creación de artículos tenemos un formulario en el que podemos introducir la información que tendrá el nuevo artículo, al pulsar continuar se creará el artículo en la base de datos y nos redirigirá al **visor de artículos**.



The screenshot shows a web application interface with a dark background. In the top left corner, the text 'WikiInfoSeguridad' is displayed in a light pink font. In the top right corner, there are two links: 'Artículos' and 'Nuevo', followed by a red button labeled 'Iniciar Sesión'. Centered on the screen is a white rectangular form titled 'Crear Artículo' in bold black text. The form contains five input fields: 'Título' (with a cursor), 'Texto', 'Fuentes', 'Autor', and 'ID'. At the bottom of the form is a blue button labeled 'Continuar'.

Imagen 10. Creador de artículos

Visor de artículos

En la página del visor de artículos podemos ver todos los artículos que tenemos en nuestro sistema, leerlos y conocer sus fuentes y autor.

WikiInfoSeguridad			Artículos	Nuevo	Iniciar Sesión
ID	Título	Texto	Fuentes	Autor	
1	Algoritmos resumen	Generan un criptograma que representa el contenido original. De tamaño constante, independientemente del contenido original. Representa todo el contenido original. Si el contenido cambia lo más mínimo cambia completamente. Para el mismo contenido, siempre genera el mismo.	https://github.com/mikel-egana-aranguren/EHU-SGSSI-01/tree/main/Cifrado_resumen	Galder	
2	Cifrado simétrico	En el cifrado simétrico se utilizan sistemas de clave privada. Los objetivos son: Convertir el mensaje en ininteligible. Recuperar la información cifrada. Implementación lo más sencilla posible; Se basan en técnicas de criptografía clásica: Transposición (los caracteres originales simplemente cambian de posición). Sustitución (los caracteres originales se sustituyen por otros).	https://github.com/mikel-egana-aranguren/EHU-SGSSI-01/tree/main/Cifrado_simetrico	Galder	
3	Cifrado asimétrico	En el cifrado asimétrico se utilizan sistemas de clave pública. Hay dos claves por usuario: La clave pública que conoce todo el mundo. La clave privada que sólo conoce el usuario; Están relacionadas matemáticamente, lo que una clave cifra sólo lo puede descifrar la otra.	https://github.com/mikel-egana-aranguren/EHU-SGSSI-01/tree/main/Cifrado_asimetrico	Galder	
4	Firma digital	Podemos firmar un documento cifrándolo con nuestra clave privada. Como solo se puede descifrar con nuestra clave pública garantizamos que lo hemos firmado nosotros. Con esto se consigue: Sólo el usuario legítimo puede firmar su documento. Nadie podrá falsificar una firma. Cualquiera puede verificar una firma digital. No se puede reutilizar una firma. No se puede modificar una firma. No se puede negar haber firmado un documento. No se puede alterar un documento después de haberlo firmado; Logramos: Autenticidad, Integridad y No repudio.	https://github.com/mikel-egana-aranguren/EHU-SGSSI-01/tree/main/Cifrado_firma	Galder	
5	Certificados digitales	Una entidad (Autoridad de Certificación) certifica que el usuario/entidad (su clave pública) es quien dice ser (Depende de la confianza en la AC que lo certifica) y almacena las claves públicas por nosotros. La AC emite un certificado digital. En el certificado digital el CA firma mediante su clave privada la clave pública de un usuario/entidad. Esto se encadena y se crea una jerarquía de ACs. Una AC raíz certifica otras de ACs que certifican usuarios/entidades.	https://github.com/mikel-egana-aranguren/EHU-SGSSI-01/tree/main/Cifrado_certificados	Galder	
6	Comunicaciones seguras	Se usa Transport Layer Security (TLS). Comienzo TLS: El cliente le pide al servidor usar TLS. HTTP: cambiar de puerto 80 a 443. Email: comando STARTTLS; TLS hand-shake: El cliente presenta al servidor una lista de algoritmos de cifrado soportados (simétricos, asimétricos, resumen). El servidor elige de esa lista los que soporta. El servidor presenta un certificado al cliente; el cliente valida el certificado (con un CA). El cliente genera una clave de sesión (Cifrado simétrico): El cliente genera un número aleatorio, lo cifra con la clave pública del servidor y se lo envía. En el cliente y el servidor generan una clave compartida a partir de ese número. Usando el algoritmo Diffie-Hellman, se genera una clave secreta compartida; Si el hand-shake ha sido exitoso se establece la conexión propiamente dicha: Los datos transmitidos se cifran con la clave de sesión y su integridad se verifica con los algoritmos resumen consensuados. Es un conexión que mantiene el estado (stateful).	https://github.com/mikel-egana-aranguren/EHU-SGSSI-01/tree/main/Cifrado_comunicaciones	Galder	
7	Bitcoin	Bitcoin es un sistema de dinero digital basado en una red a la que cualquiera puede unirse a través de un nodo, y no gobernada por bancos ni gobiernos. Protocolo: Bitcoin (con B) Moneda: bitcoin (con b). Símbolo: BTC o XTC. Satoshi: 0.00000001 BTC. Bitcoin asegura: No repudio: no se puede* deshacer una transacción. Integridad: no se puede* modificar la historia del blockchain. Autenticidad. Pseudo-anonimato. *Es computacionalmente y socialmente muy caro e improbable	https://github.com/mikel-egana-aranguren/EHU-SGSSI-01/tree/main/Cifrado_bitcoin	Galder	
Sobre nosotros		Contáctanos	Videos	Redes sociales	
Cómo funciona		Contacto	Enviar video	Instagram	
Testimonios		Soporte	Embajadores	Facebook	
Carreras		Destinos	Agencia	YouTube	
Inversiones		Patrocinios	Influencer	Twitter	
Términos y condiciones					
WikiInfoSeguridad			© WikiInfoSeguridad 2022. All rights reserved		

Imagen 11. Visor de artículos