**SISTEMA DE ENCRIPTACIÓN HASH**

**INFORMACIÓN DEL PROYECTO**

|  |  |
| --- | --- |
| FECHA | 12/10/2022 |
| VERSIÓN | 1.0 |
| EMPRESA | UNIMINUTO |
| PROYECTO | SISTEMA DE ENCRIPTACIÓN HASH |

**HISTORIA DE REVISIONES**

|  |  |  |
| --- | --- | --- |
| Fecha | Versión | Descripción |
| 12/10/2022 | 1.0 | Documento del proyecto |
|  |  |  |
|  |  |  |
|  |  |  |

**CONTENIDO**

[**1.** **DEFINICIÓN GENERAL DEL SISTEMA** 2](#_Toc116499364)

[**1.1.** **OBJETIVO DEL SISTEMA** 3](#_Toc116499365)

[**1.2.** **ALCANCE DEL SISTEMA** 3](#_Toc116499366)

[**1.3.** **CARACTERISTICAS DE LOS USUARIOS** 3](#_Toc116499367)

[**2.** **REQUERIMIENTOS DEL SISTEMA** 3](#_Toc116499368)

[**2.1.** **REQUERIMIENTOS FUNCIONALES** 4](#_Toc116499369)

[**2.2.** **REQUERIMIENTOS NO FUNCIONALES** 9](#_Toc116499370)

[**2.3.** **REQUISITOS DEL SISTEMA** 10](#_Toc116499371)

[**2.3.1.** **INTERFAZ DE USUARIO** 10](#_Toc116499372)

[**2.3.2.** **HARDWARE REQUERIDO** 10](#_Toc116499373)

[**2.3.3.** **SOFTWARE REQUERIDO** 11](#_Toc116499374)

[**3.** **DOCUMENTACIÓN TECNICA DEL SISTEMA** 11](#_Toc116499375)

# **DEFINICIÓN GENERAL DEL SISTEMA**

El sistema nace de la necesidad de continuar mejorando la seguridad de los mensajes o archivos que van a ser trasmitidos en distintas plataformas. Este sistema permitirá cifrar esta información a través de los diversos algoritmos de encriptación existentes.

Para la realización de este sistema se hará uso de los algoritmos MD5, SHA1 y SHA-256.

Adicionalmente con este sistema se pretende llevar a cabo la generación y comparación de los HASH correspondientes a los archivos y mensajes añadidos.

## **OBJETIVO DEL SISTEMA**

Generar y comparar el código Hash de los archivos y mensajes añadidos, haciendo uso de los algoritmos MD5, SHA1 y SHA – 256.

## **ALCANCE DEL SISTEMA**

Este tiene como finalidad proporcionar un sistema de encriptación que permita generar y comparar el código Hash de cualquier tipo de mensaje o archivo añadido, utilizando los algoritmos MD5, SHA1 y SHA-256.

El sistema permitirá adjuntar archivos de cualquier tipo de formato de documentos (pdf, xls, doc, xlsx, docx, odf, etc) o imagen (jpg, png, jpeg etc).

El sistema permitirá escribir un mensaje sin limite de caracteres, para ser encriptado.

El sistema contara con dos pestañas o tabs, que permitan navegar entre si para adjuntar o escribir el mensaje. **Ver Anexo1**

El sistema mostrará el código Hash en la vista una vez sea generado.

El sistema informara si el código no pudo ser generado exitosamente.

El botón de generar funcionara solo si tiene un mensaje escrito o un archivo adjunto.

El sistema será usado por cualquier usuario que tenga acceso y que desee encriptar sus mensajes o archivos.

## **CARACTERISTICAS DE LOS USUARIOS**

|  |  |
| --- | --- |
| TIPO DE USUARIOS | Usuario final |
| FORMACIÓN | Básica o técnica |
| HABILIDADES | Manejo de herramientas ofimáticas, manejo de equipos de cómputo, manejo de internet. |

# **REQUERIMIENTOS DEL SISTEMA**

Este sistema contara con una vista diseñada para el usuario final.

## **REQUERIMIENTOS FUNCIONALES**

A continuación, se visualizarán los requerimientos funcionales del SISTEMA DE ENCRIPTACIÒN HASH:

|  |  |
| --- | --- |
| Identificación del requerimiento | RF 001 |
| Nombre del requerimiento: | Encriptar archivos |
| Características: | Los usuarios deberán adjuntar archivos de documentos o imágenes |
| Descripción del requerimiento: | Todos los usuarios deben poder adjuntar archivos de documentos o imágenes con los siguientes formatos (pdf, xls, doc, xlsx, docx, odf, etc) o (jpg, png, jpeg etc). |
| Entrada: | Archivo |
| Requerimiento NO funcional: | * RNF 001 * RNF 002 * RNF 003 |
| Prioridad del requerimiento: | Alta |
| Salida: | Archivo encriptado y código hash generado |

|  |  |
| --- | --- |
| Identificación del requerimiento | RF 002 |
| Nombre del requerimiento: | Encriptar texto |
| Características: | Los usuarios podrán ingresar un texto que deseen encriptar |
| Descripción del requerimiento: | El usuario podrá escribir un mensaje que desee encriptar en el sistema. El campo no deberá contar con límite de caracteres y será alfanumérico. |
| Entrada: | Texto |
| Requerimiento NO funcional: | * RNF 001 * RNF 002 * RNF 003 |
| Prioridad del requerimiento: | Alta |
| Salida: | Texto encriptado y código hash encriptado |

|  |  |
| --- | --- |
| Identificación del requerimiento | RF 003 |
| Nombre del requerimiento: | Selección de algoritmos |
| Características: | El usuario debe seleccionar el algoritmos que desea usar. |
| Descripción del requerimiento: | El sistema debe permitir al usuario seleccionar el algoritmos que desea usar para la encriptación |
| Entrada: | Texto o archivo seleccionado |
| Requerimiento NO funcional: | * RNF 001 * RNF 002 * RNF 003 |
| Prioridad del requerimiento: | Alta |
| Salida: | Mensaje de confirmación |

## **REQUERIMIENTOS NO FUNCIONALES**

A continuación, se visualizarán los requerimientos no funcionales del SISTEMA DE ENCRIPTACIÓN HASH:

|  |  |
| --- | --- |
| Identificación del requerimiento | RNF 001 |
| Nombre del requerimiento: | Interfaz del sistema |
| Características: | El sistema debe tener una interfaz de uso intuitiva y sencilla |
| Descripción del requerimiento: | El sistema debe tener una interfaz de usuario sencilla para que sea de fácil manejo para los usuarios |
| Prioridad del requerimiento: | Alta |

|  |  |
| --- | --- |
| Identificación del requerimiento | RNF 002 |
| Nombre del requerimiento: | Tiempo de respuesta |
| Características: | El sistema debe tener un tiempo de respuesta pequeño en sus transacciones |
| Descripción del requerimiento: | El sistema debe tener un tiempo de respuesta no mayor a 5 segundos en todas sus transacciones |
| Prioridad del requerimiento: | Alta |

|  |  |
| --- | --- |
| Identificación del requerimiento | RNF 003 |
| Nombre del requerimiento: | Confiabilidad del sistema |
| Características: | El sistema garantizara el correcto funcionamiento, ya que es una página que estará disponible 24 horas. |
| Descripción del requerimiento: | La disponibilidad del sistema será continua es decir 24 horas. |
| Prioridad del requerimiento: | Alta |

## **REQUISITOS DEL SISTEMA**

### **INTERFAZ DE USUARIO**

La interfaz del usuario hace referencia al conjunto de ventanas, botones y campos en general que será visualizada desde el navegador de internet.

### **HARDWARE REQUERIDO**

Sera necesario disponer de equipos de cómputo con las siguientes características:

* Adaptadores de red
* Procesador de 1.66GHz o superior
* Memoria mínima de 256MB
* Mouse
* Teclado

### **SOFTWARE REQUERIDO**

* Sistema operativo: Windows 10 o superior
* Navegador: Mozilla, Chrome o Edge

# **DOCUMENTACIÓN TECNICA DEL SISTEMA**

* **Tecnologías usadas en el Back end**
  + **Implementación de algoritmos**
* **Tecnologías usadas en el Front end**
* **Proceso General Sistema de Encriptación**