**DOCUMENTO DE ESPECIFICACIÓN DE REQUISITOS DE SOFTWARE (SRS)**

**Stiven Daniel Robles Marqués**

**MÓDULO DE SEGURIDAD**

**Centro de Comercio y Servicios**

**Soledad, Atlántico. 2025**

**Tabla de contenido**

[**1.** **REVISION HISTÓRICA** 3](#_Toc189564033)

[**2.** **TABLA DE FIGURAS** 3](#_Toc189564034)

[**2.1.** **Diagrama de Flujo de autenticación de credenciales.** 4](#_Toc189564035)

[**2.2.** **Diagrama de secuencia de Encriptación y Validación de datos.** 4](#_Toc189564036)

[**3.** **MÓDULO DEL SISTEMA** 4](#_Toc189564037)

[**3.1.** **Funciones del Módulo.** 4](#_Toc189564038)

[**3.2.** **Definiciones, Acrónimos y Abreviaciones.** 4](#_Toc189564039)

[**4.** **REQUISITOS** 4](#_Toc189564040)

[**4.1.** **Requisitos Funcionales.** 4](#_Toc189564041)

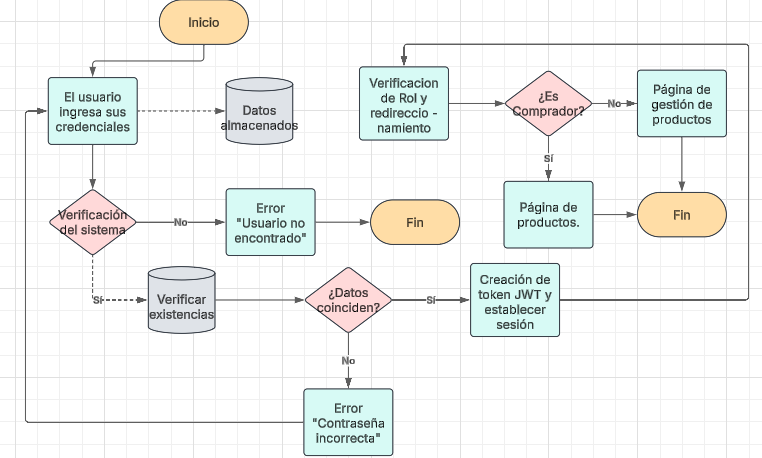
[**4.2.** **Requisitos no Funcionales.** 4](#_Toc189564042)

# **REVISION HISTÓRICA**

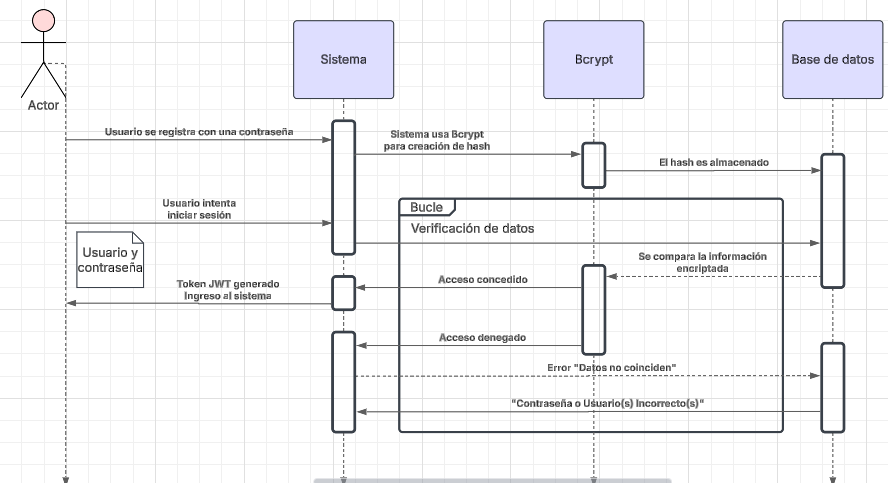
|  |  |  |  |
| --- | --- | --- | --- |
| Fecha | Descripción | Autor | Versión |
| 04/02/2025 | Creación del documento. | Stiven Robles | 1.0 |
| 08/02/2025 | Fase de creación y elaboración de diagramas para representar el flujo. | Stiven robles | 1.1 |
| 12/02/2025 | Elicitación de funcionalidades del módulo. | Stiven robles | 1.3 |
| 13/02/2025 | Análisis y recopilación de información sobre los requisitos del módulo. | Stiven Robles | 1.4 |
| 15/02/2025 | Especificación de requerimientos y finalización del módulo. | Stiven Robles | 1.6 |

# **TABLA DE FIGURAS**

## **Diagrama de Flujo de autenticación de credenciales.**

****

## **Diagrama de secuencia de Encriptación y Validación de datos.**



# **MÓDULO DEL SISTEMA**

En este módulo se llevarán a cabo todas las funcionalidades relacionadas con la gestión, administración y control de toda la información confidencial y credenciales que nos proporcionen los usuarios del sistema. Aquí, se toman ciertas medidas y se ejecutan procesos asociados a la encriptación de datos para su mayor seguridad, respaldos y análisis de la información para tenerla vigilada y fuera de cualquier peligro cibernético posible.

## **Funciones del Módulo.**

**Autenticación: Verificar la identidad de usuarios mediante credenciales**: Esta funcionalidad nos permite cerciorarnos de que realmente sea el usuario creador de la cuenta quien este intentando ingresar nuevamente al sistema. Este sistema de credenciales es almacenado y encriptado como hash en la base de datos para luego ser recuperados al momento de querer iniciar sesión. Los datos de inicio se sesión varían por cada persona, en el caso del usuario requerido en el inicio de sesión, ya que se exige un único usuario al crear la cuenta por vez primera.

**Autorización: Controlar el acceso a funcionalidades según el rol del usuario**: Esta funcionalidad permite el filtrado de información y accesos de información y procesos, además de funcionalidades especificas a cada tipo de rol que puede llegar a presentar un usuario en concreto. Esta función sirve para separar la dinámica de la pagina de manera practica para solo mostrar y permitir acciones especificas para cada tipo de rol. Tiene como objetivo separar las dependencias de los usuarios de rol Vendedor y Comprador para una mayor experiencia de usuario.

**Encriptación: Proteger datos sensibles como contraseñas y Tokens de acceso:** Tanto las contraseñas como los tokens JWT son un tipo de dato muy delicado que debe ser manejado con cautela y protección. La principal característica de esta funcionalidad y su objetivo en general es la de encriptar los datos requeridos para su mayor resguardo en la base de datos y prevenir robo de información en caso de hurtos o ataques cibernéticos hacia el sistema.   
**Monitoreo: Detectar accesos no concebidos y generar alertas:** En el caso de que se filtre información (hipotéticamente hablando) esta funcionalidad se encargará de gestionar un sistema de alertas cuando el software crea que se está vulnerando una información, accediendo de manera sospechosa a una cuenta o ingresando de manera incorrecta cierta cantidad de veces. Esta funcionalidad tiene la responsabilidad de notificar al dueño autentico de la cuenta por medio de alertas cuando esta se vea en peligro de hurto de información, hacking, u otro tipo de delito cibernético.

## **Definiciones, Acrónimos y Abreviaciones.**

|  |  |
| --- | --- |
| Término | Definición |
| Hash | Hash es un proceso de seguridad de consiste en la conversión de una cadena de caracteres a un formato irreconocible e irreversible. |
| JWT | Json Web Token, Es un estándar para la autenticación y autorización. |
| ACL | Lista de Control de Acceso, define que permisos específicos debe tener cierto usuario dependiendo de su rol. |
| Firewall | Sistema de seguridad de filtra la información entrante y saliente según reglas específicas. |
| TLS | Seguridad de Capa de Transporte, es un protocolo que se usa normalmente para cifrar las comunicaciones. |
| Db | Data Base, abreviación de Data Base, o Base de Datos, es un sistema que se encarga de almacenar información de un sistema. |
| Software. | Conjunto de funcionalidades o sistemas que cumplen un propósito, generalmente monitoreados por un grupo de especialistas. |
| Encriptado | Proceso por el cual pasa una serie de datos modificando su estructura y volviendo irreconocible e indescifrable. |

# **REQUISITOS**

## **Requisitos Funcionales.**

* + 1. **Requisito Funcional RF01.**

Esta opción permite administrarle el acceso a los usuarios que realmente recuerden sus credenciales, dado el caso, y si no, siendo ellos mismos el dueño de la cuenta darles la posibilidad de recuperar su cuenta por medio de una actualización de credenciales que solo el propietario sabrá.

|  |  |
| --- | --- |
| Requisito | Autenticación de usuarios (RF01). |
| Dependencias | Node.js, Bcrypt, JWT |
| Actores: | Todos los usuarios. |
| Precondición: | El usuario debe haberse registrado con anterioridad. |
| Prioridad: | Alta |

|  |  |
| --- | --- |
| Curso normal | Observaciones |
| * El usuario ingresa con su usuario y contraseña. * El sistema valida las credenciales suministradas por el usuario. * Si son correctas, se genera un token JWT y se permite el acceso al sistema. Mensaje “Bienvenido de nuevo [Usuario]”. * Si son incorrectas el sistema no permitirá el ingreso “Credenciales incorrectas”. Resaltará la opción de “Recuperar contraseña”. |  |
| Alternativas | Observaciones |
| Una alternativa para el registro del usuario es la siguiente:   * Recuperación de contraseña. * El sistema te enviará a una vista de formulario para preguntarte sobre tu fecha de cumpleaños y tu número de cédula antes de continuar. Si no los has proporcionados se te permitirá recuperar tu cuenta con tu correo ingresado. * El sistema tras validar la información con la db y posteriormente rectificado y autenticando, se te redirigirá a un formulario donde deberás proporcionar tu nueva credencial y te pedirá ingresar los datos anteriormente no registrados (Fecha de cumpleaños, cédula). * Al hacer click en “Confirmar” te saldrá un recuadro con el mensaje “¿Estás seguro?”. Al confirmar, el sistema te llevará a la pagina de inicio de sesión para seguir con el proceso. | Las opciones de agregar “Cedula de ciudadanía” y “Fecha de nacimiento” estarán disponibles para la segunda tanda de versiones del sistema, es decir, en las versiones beta posteriores a la actual (v4.0). |
| Excepciones | Observaciones |
| Conjunto de errores y excepciones si el usuario:   * Proporciona credenciales incorrectas. * Si actica el protocolo de seguridad de las cuentas al intentar acceder repetidas veces sin éxito. Error “Demasiados intentos, inténtelo más tarde”. * Si existen fallas en el tráfico de información o conexión con la db. |  |

* + 1. **Requisito Funcional RF02.**

Esta opción les permite a los usuarios visualizar, ejecutar, procesar y trabajar con la información, funcionalidades o procesos que le conciernan dependiendo del rol único que manejen en el momento al ingresar sesión. Esto permite que los usuarios no se confundan a la hora de administrar su rol y tener la información que necesitan a la mano.

|  |  |
| --- | --- |
| Requisito | Control de Acceso (RF02). |
| Dependencias | Node.js, ACL. |
| Actores: | Administrador del sistema. |
| Precondición: | El usuario debe haber sido autenticado. |
| Prioridad: | Alta |

|  |  |
| --- | --- |
| Curso normal | Observaciones |
| * Validar accesos según corresponda de acuerdo al rol ingresado en el momento por el usuario. * Validar permisos según corresponda de acuerdo al rol del usuario. * Denegar funcionalidades o permisos debido al rol del usuario en el momento. |  |
| Alternativas | Observaciones |
| * Gestionar la administración de registros de los usuarios * Gestionar la configuración manual de permisos otorgados a cada usuario del sistema. |  |
| Excepciones | Observaciones |
| Error si no hay un rol único cambiante establecido en el usuario. La información no se filtra y habría fallo general del sistema. Mensaje “Error general, por favor inicia sesión nuevamente”. |  |

* + 1. **Requisito funcional RF03**.

Esta opción es una de las más importantes puesto que es la que rige la seguridad de los datos y su protección. A partir de aquí se origina la confianza que el usuario puede otorgarnos al entregarnos sus datos personales y sus credenciales. Es la responsable de la encriptación de información confidencial y protegerla de hurtos, hacking o demás delitos cibernéticos.

|  |  |
| --- | --- |
| Requisito | Encriptación de Datos (RF03). |
| Dependencias | Node.js, bcrypt |
| Actores: | Sistema |
| Precondición: | El sistema debe estar Activo y funcional. |
| Prioridad: | Alta |

|  |  |
| --- | --- |
| Curso normal | Observaciones |
| * El usuario proporciona por vez primera su contraseña o credenciales al sistema al registrar. * El sistema genera un hash de esa contraseña y la almacena en la base de datos. * El usuario intenta ingresar sesión * El sistema comprara los datos en la db con los proporcionados. Error “El usuario no se encuentra registrado”. En caso de usuario incorrecto. * El sistema valida la información de la db con la proporcionada. * El usuario ingresa su contraseña que es comparada con el hash almacenado en la db del sistema. * El sistema compara la información. “Contraseña incorrecta”, en caso de error. |  |
| Alternativas | Observaciones |
| Una alternativa para el registro del usuario es la siguiente:   * Ninguna. |  |
| Excepciones | Observaciones |
| Conjunto de errores y excepciones si el usuario:   * Error si el algoritmo de encriptado falla “Ha ocurrido un error en el sistema”. * Error con el registro. “Persona ya existente. * Error con la contraseña. “Contraseña muy extensa”, “Contraseña muy corta”. * Error con el sistema. “El sistema no responde”. |  |

## **Requisitos no Funcionales.**

**RNF01: Seguridad:** Todas las contraseñas deben ser almacenadas con por lo menos bcrypt de al menos 10 salt rounds.

**RNF02: Seguridad:** El sistema debe generar como máximo tokens validos por 24 horas cada vez.

**RNF03: Rendimiento:** El tiempo de respuesta del sistema tras las validaciones de seguridad no debe extenderse más de los 500ms.

**RNF04: Seguridad:** Todos los datos enviados y proporcionados deben transferirse por HTTPS para garantizar la seguridad de las comunicaciones.

**RNF05: Escalabilidad:** El sistema de alertas y recuadros de mensajes debe ser compatible con todos los dispositivos y sistemas operativos (Android, IOS, Windows, Linux).