Universidade de Santiago de Compostela

Escola Politécnica Superior de Enxeñaría

Máster Universitario en Dirección de Proyectos

Especificación de Requisitos de Software (ERS)

ERS Gestionar Usuario

Sistema de Gestión de Candidatos TICs (SIGECA)

Asignatura: Gestión de Calidad

Profesor: Manuel Marey Pérez

Equipo No. 1

Integrantes: Maylin Vega Angulo

Erio Gutierrez Llorens

Curso: 2024/2025, Lugo, Galicia, España

Información de control del documento

Descripción	Valor
Título del Documento:	ERS Gestionar Usuario
Autor del documento:	Ing. Erio Gutierrez Llorens
Propietario del Proyecto:	CEO Empresa de Soluciones Informáticas SIVSA
Director del Proyecto:	Ing. Maylin Vega Angulo
Versión del Documento:	1.0.1
Confidencialidad:	Limitada
Fecha:	10/03/2025

Aprobación y revisión del documento:

NOTA: Se requieren todas las aprobaciones. Se deben mantener registros de cada aprobación. Todos los revisores de la lista se consideran necesarios a menos que se indique explícitamente como Opcionales.

Nombre	Rol	Acción	Fecha
Ing. Maylin Vega Angulo	Director de Proyecto	Aprobar	11/03/2025

Historial del documento:

El Autor del Documento está autorizado a hacer los siguientes tipos de cambios al documento sin requerir que el documento sea aprobado nuevamente:

- *Edición, formato y ortografía.*
- *Aclaraciones.*

Para solicitar un cambio en este documento, póngase en contacto con el Autor del documento o el Propietario del proyecto.

Las modificaciones de este documento se resumen en la siguiente tabla en orden cronológico inverso (primero la última versión).

Revisión	Fecha	Creada por	Breve descripción de los cambios
1.0	10/03/2025	Ing. Erio Gutierrez Llorens	Formato del documento y ajustes en la descripción del flujo de trabajo.

Gestión de la configuración: Localización del documento

La última versión de este documento está guardada en:

https://github.com/sivsa/proyectos_en_curso/2024/sigeca/Requisitos

TABLA DE CONTENIDOS

1. DESCRIPCIÓN GENERAL

El proceso Gestionar Usuario abarca todas las funcionalidades relacionadas con la administración de cuentas dentro del sistema. Su objetivo es garantizar que los usuarios puedan acceder, modificar y controlar su información de manera segura y eficiente.

Este requisito incluye procesos de autenticación, gestión de credenciales, actualización de información y control de accesos, asegurando que todas las acciones cumplan con los estándares de seguridad y usabilidad definidos para el sistema.

2. REQUISITOS FUNCIONALES

2.1. Registrar Usuario

ID	**ERF-001**
Nombre	Registrar Usuario
Categoría	Requisitos Funcionales
Tipo	Modelo de Proceso de Negocios / Flujo de trabajo
Descripción y Detalles	El sistema debe permitir a un usuario registrarse proporcionando los datos necesarios, validando la información ingresada y almacenando la cuenta de manera segura.
Criterios de Aceptación	**Ingreso de Correo Electrónico** • El usuario debe ingresar un correo electrónico válido según una expresión regular. • El sistema debe impedir el ingreso de contraseñas vacías o con espacios en blanco adicionales. • La contraseña ingresada debe cumplir con los requisitos de seguridad definidos (mínimo 8 caracteres, uso de letras mayúscula, minúsculas, números y al menos uno de los caracteres especiales: (!@#$%^&*)). • Si el usuario no completa el reCAPTCHA, el sistema no debe permitir el envío del formulario.
	Verificación de Correo Electrónico • Si el correo electrónico ya está registrado, el sistema debe mostrar un mensaje indicando que ya existe. • El usuario debe poder ingresar un nuevo correo si el actual está registrado. • Si el usuario decide no cambiar el correo electrónico, se le debe redirigir a la interfaz de autenticación.

	Generación y Envío de Token de Verificación • Si el correo electrónico no está registrado, se debe generar un token único de verificación asociado al correo electrónico. • Si el correo electrónico pertenece a una lista bloqueada, el sistema debe impedir el registro y mostrar un mensaje de bloqueo por 24 horas. • El sistema debe enviar un correo electrónico con el token de verificación al usuario. • Si el envío del correo electrónico falla, se debe mostrar un mensaje de error y recomendar intentarlo más tarde (10 minutos).
	Verificación del Token • El usuario debe acceder al token recibido en su correo electrónico (link de verificación). • Si el usuario no ingresa al link de verificación en el tiempo establecido (24 horas), el sistema debe marcar el correo electrónico como no verificado y eliminar el registro (y archivarlo en los logs). • Si el token es incorrecto, se debe mostrar un mensaje de error y permitir su reenvío. • Si el usuario excede los intentos de verificación, el sistema debe bloquear temporalmente el registro.
	Registro del Usuario • Si el token es válido, el sistema debe mostrar un mensaje de verificación exitosa y el sistema debe asociarlo al usuario y marcar su correo electrónico como verificado. • El sistema debe registrar al usuario en la base de datos con la información relevante y activar la cuenta del usuario. • El usuario debe ser redirigido al proceso de creación de contraseña.
	Seguridad y Mecanismos de Protección • El sistema debe limitar el número de intentos de envíos del token antes de bloquear el registro. • El token de verificación debe expirar en 24 horas. • Si se detectan intentos masivos desde una misma IP, el sistema debe bloquear temporalmente los registros desde esa dirección. • El token de verificación debe almacenarse de manera segura con un algoritmo de cifrado.
Estado	Especificado
Solicitado por	Director de Proyecto
Fecha de Identificación	05/10/2024
Referencias	DFT Registrar Usuario

2.2. Autenticar Usuario

ID	**ERF-002**

Nombre	Autenticar Usuario
Categoría	Requisitos Funcionales
Tipo	Modelo de Proceso de Negocios / Flujo de trabajo
Descripción y Detalles	El sistema debe permitir que un usuario autenticado acceda a la plataforma mediante su correo electrónico y contraseña, garantizando la seguridad de los datos.
Criterios de Aceptación	**Ingreso de Credenciales** • El usuario debe ingresar un correo electrónico válido según una expresión regular. • Si el correo electrónico no cumple con estos criterios, el sistema debe mostrar un mensaje de error indicando el problema específico. • El sistema debe impedir el ingreso de contraseñas vacías o con espacios en blanco adicionales. • El sistema debe verificar que la contraseña ingresada no esté vacía. • El sistema debe rechazar contraseñas que contengan espacios en blanco adicionales. • El sistema debe comprobar que la contraseña cumple con los requisitos mínimos de seguridad, como longitud mínima, uso de caracteres especiales y mayúsculas. • Si la contraseña no cumple con estos requisitos, el sistema debe mostrar un mensaje de error indicando el motivo. • El sistema debe validar el reCAPTCHA antes de permitir el envío del formulario de inicio de sesión. • Si la validación del reCAPTCHA falla, el sistema debe impedir el acceso y solicitar al usuario que complete la verificación correctamente.
	Verificación de Existencia del Usuario • El sistema debe comprobar si el correo electrónico ingresado está registrado en la base de datos. • Si el correo no está registrado, el sistema debe mostrar el mensaje: "*Usuario no registrado*" y no permitir continuar con la autenticación. • Si el usuario ha realizado múltiples intentos de inicio de sesión con diferentes correos electrónicos en un corto período de tiempo, el sistema debe activar una verificación adicional para prevenir intentos de fuerza bruta.

	Verificación de Contraseña • El sistema debe comparar la contraseña ingresada con la almacenada en la base de datos utilizando un mecanismo de hash seguro. • Si la contraseña es incorrecta, el sistema debe incrementar el contador de intentos fallidos para ese usuario. • Si el número de intentos fallidos alcanza el límite predefinido (5 intentos), el sistema debe bloquear temporalmente la cuenta y mostrar el mensaje: *"Cuenta bloqueada temporalmente. Intente nuevamente en 30 minutos."* • Si el intento de inicio de sesión proviene de una ubicación o dispositivo no reconocido, el sistema debe solicitar un código de verificación adicional enviado al correo del usuario. • Si la contraseña es incorrecta, el sistema debe mostrar el mensaje: *"Contraseña incorrecta."*
	Verificación del Estado de la Cuenta • El sistema debe comprobar si la cuenta del usuario está activa. • Si la cuenta está desactivada, el sistema debe mostrar el mensaje: *"Cuenta desactivada. Contacte con soporte."* • Si la cuenta está bloqueada debido a intentos fallidos, el sistema debe mostrar el mensaje: *"Cuenta bloqueada temporalmente. Intente nuevamente en 30 minutos."* • Si la cuenta está pendiente de verificación de correo, el sistema debe mostrar el mensaje: *"Debe verificar su correo electrónico antes de iniciar sesión."* • Si la cuenta ha estado inactiva durante un período prolongado, el sistema debe solicitar un paso adicional de autenticación antes de permitir el acceso. • Si la cuenta está activa y sin restricciones, el sistema debe permitir la autenticación exitosa.
	Inicio de Sesión Exitoso • El sistema debe generar un token de sesión seguro (JWT con expiración o cookie segura con protección contra ataques XSS y CSRF). • El sistema debe registrar el evento de autenticación en los logs del sistema, incluyendo la fecha, hora y dirección IP del intento de acceso. • El sistema debe almacenar información del dispositivo y la ubicación de acceso del usuario para detectar posibles accesos no autorizados. • Si el inicio de sesión se realiza desde un dispositivo nuevo, el sistema debe enviar una notificación de alerta al correo del usuario. • Si todas las validaciones se cumplen, el sistema debe redirigir al usuario a la interfaz principal de la aplicación.

	Seguridad y Protección de Datos • El sistema debe almacenar las contraseñas utilizando un algoritmo de hash seguro. • El sistema debe implementar reCAPTCHA en el formulario de inicio de sesión para prevenir ataques automatizados. • El sistema debe bloquear temporalmente la cuenta tras múltiples intentos fallidos y notificar al usuario sobre la medida de seguridad aplicada. • El sistema debe enviar notificaciones al usuario en caso de intentos sospechosos de inicio de sesión desde ubicaciones desconocidas. • El sistema debe asegurar que los tokens de sesión tengan una expiración definida y puedan ser revocados en caso de cierre de sesión.
Estado	Especificado
Solicitado por	Director de Proyecto
Fecha de Identificación	05/10/2024
Referencias	DFT Autenticar Usuario

2.3. Recuperar Contraseña

ID	**ERF-003**
Nombre	Recuperar Contraseña
Categoría	Requisitos Funcionales
Tipo	Modelo de Proceso de Negocios / Flujo de trabajo
Descripción y Detalles	El sistema debe permitir a los usuarios recuperar su contraseña en caso de olvido mediante un proceso de validación con su correo electrónico registrado.
Criterios de Aceptación	**Solicitud de Recuperación** • El sistema debe proporcionar la opción *"¿Olvidaste tu contraseña?"* en la interfaz de inicio de sesión. • Si el usuario selecciona esta opción, el sistema debe solicitar el ingreso de un correo electrónico. • El sistema debe validar que el formato del correo electrónico sea correcto. • Si el correo ingresado tiene un formato inválido, el sistema debe mostrar el mensaje: *"Ingrese un correo electrónico válido."*

	Validación del Correo • El sistema debe verificar si el correo ingresado está registrado en la base de datos. • Si el correo no está registrado, el sistema debe mostrar un mensaje genérico: *"Si el correo existe en nuestro sistema, recibirá un mensaje con las instrucciones para restablecer la contraseña."* (Para evitar exponer si un correo pertenece o no a una cuenta). • Si el correo está registrado, el sistema debe generar un token de recuperación con una validez de 30 minutos. • El sistema debe enviar un correo con un enlace único de recuperación al usuario. • Si el envío del correo falla, el sistema debe registrar el error y mostrar un mensaje genérico al usuario.
	Verificación del Token • El sistema debe validar el token cuando el usuario acceda al enlace de recuperación. • Si el token es válido y no ha expirado, el sistema debe mostrar la interfaz de restablecimiento de contraseña. • Si el token ha expirado, el sistema debe mostrar el mensaje: *"El enlace ha expirado. Solicite una nueva recuperación de contraseña."* y ofrecer la opción de reenviar el correo de recuperación. • Si el token es inválido, el sistema debe mostrar un mensaje de error sin revelar detalles de seguridad.

	Restablecimiento de Contraseña
	• El sistema debe solicitar al usuario que ingrese una nueva contraseña y la confirme.
	• El sistema debe validar que la contraseña cumple con las reglas de seguridad:
	  ○ Longitud mínima de 8 caracteres.
	  ○ Al menos una mayúscula y una minúscula.
	  ○ Al menos un número.
	  ○ Al menos un carácter especial (!@#$%^&*).
	• Si la contraseña no cumple con los criterios, el sistema debe mostrar el mensaje: *"La contraseña no cumple con los requisitos de seguridad. Intente nuevamente."*
	• El sistema debe almacenar la nueva contraseña de forma cifrada utilizando un algoritmo seguro.

	Confirmación y Cierre de Sesión en Otros Dispositivos • El sistema debe informar al usuario que la contraseña ha sido cambiada correctamente. • El sistema debe cerrar la sesión del usuario en todos los dispositivos para evitar accesos no autorizados. • El sistema debe redirigir al usuario a la pantalla de inicio de sesión después del cambio de contraseña.

	Excepciones y Seguridad • Si se detectan múltiples intentos de recuperación de contraseña desde la misma IP en un corto período de tiempo, el sistema debe aplicar medidas de seguridad como bloqueo temporal o reCAPTCHA. • El sistema no debe revelar si un correo está registrado en la base de datos. • El sistema debe registrar todos los intentos de recuperación de contraseña en los logs de auditoría. • Los tokens de recuperación deben ser de uso único y eliminarse una vez utilizados. • El sistema debe prevenir ataques de fuerza bruta limitando la cantidad de intentos de restablecimiento en un período determinado.
Estado	Especificado
Solicitado por	Director de Proyecto
Fecha de Identificación	05/10/2024
Referencias	DFT Recuperar Contraseña

2.4. Cambiar Contraseña

ID	**ERF-004**
Nombre	Cambiar Contraseña
Categoría	Requisito Funcional
Tipo	Modelo de Proceso de Negocio / Flujo de trabajo
Descripción y Detalles del Requisito	Permite a los usuarios autenticados cambiar su contraseña dentro del sistema, asegurando que cumpla con los criterios de seguridad establecidos.
Criterios de Aceptación	**Acceso a la Opción de Cambio de Contraseña** • Si el usuario está autenticado, debe poder acceder a la sección de configuración para cambiar su contraseña. • Si el usuario no está autenticado, el sistema debe redirigirlo a la interfaz de inicio de sesión. • Si la sesión ha expirado, el sistema debe solicitar una nueva autenticación antes de continuar con el proceso.
	Verificación de la Contraseña Actual

	• El usuario debe ingresar su contraseña actual antes de poder establecer una nueva. • Si la contraseña es incorrecta, el sistema debe mostrar un mensaje de error sin revelar si la cuenta existe o no. • El sistema debe limitar la cantidad de intentos fallidos antes de bloquear temporalmente la opción de cambio de contraseña (máximo 5 intentos). • Si se excede el número máximo de intentos fallidos, la funcionalidad debe bloquearse durante un período de tiempo (30 minutos). • Si la contraseña es correcta, el usuario debe poder continuar con el proceso.
	Ingreso de Nueva Contraseña • El usuario debe ingresar la nueva contraseña y confirmarla correctamente. • La nueva contraseña debe cumplir con los requisitos de seguridad establecidos (longitud mínima, combinación de caracteres, etc.). • Si la nueva contraseña no cumple con los requisitos, el sistema debe mostrar un mensaje detallado con las reglas establecidas. • La nueva contraseña no debe ser igual a la contraseña actual. • Si la nueva contraseña está en una base de datos de contraseñas comprometidas, el sistema debe rechazarla y solicitar otra. • Si la confirmación de la nueva contraseña no coincide con la ingresada inicialmente, el sistema debe solicitar que ambas coincidan antes de continuar. • Si la nueva contraseña es correcta, el usuario debe poder continuar con el proceso.
	Almacenamiento Seguro de Contraseña • El sistema debe utilizar un algoritmo de hashing seguro para almacenar la nueva contraseña. • Si la contraseña se almacena correctamente, el sistema debe notificar al usuario y cerrar la sesión en todos los dispositivos activos. • Si ocurre un error en el almacenamiento de la contraseña, el sistema debe mostrar un mensaje de error y solicitar que el usuario intente nuevamente más tarde (10 minutos).
	Notificación al Usuario • Tras cambiar la contraseña, el sistema debe enviar una notificación al correo electrónico registrado del usuario. • Si el usuario no reconoce el cambio, el correo debe proporcionar un enlace o instrucciones para restablecer la contraseña inmediatamente.
	Seguridad y Protección

	• La opción de cambio de contraseña solo debe estar disponible para usuarios autenticados. • El sistema debe bloquear la funcionalidad de cambio de contraseña temporalmente tras múltiples intentos fallidos (máximo 5 intentos). • El sistema debe cerrar automáticamente todas las sesiones activas del usuario después del cambio de contraseña. • El sistema debe registrar intentos de cambio de contraseña fallidos y notificar al usuario en caso de actividad sospechosa. • Todas las comunicaciones relacionadas con el cambio de contraseña deben utilizar HTTPS y TLS para garantizar la seguridad.
Estado	Especificado
Solicitado por	Director de Proyecto
Fecha de Identificación	05/10/2024
Referencias	DFT Cambiar Contraseña

2.5. Eliminar Cuenta

ID	**ERF-005**
Nombre	Eliminar Cuenta
Categoría	Requisito Funcional
Tipo	Modelo de Proceso de Negocio / Flujo de trabajo
Descripción y Detalles del Requisito	Permite a los usuarios autenticados eliminar su cuenta del sistema de forma definitiva, asegurando la validación del usuario antes de la eliminación y confirmación del proceso.
Criterios de Aceptación	**Acceso a la Opción de Eliminación de Cuenta** • El sistema debe solicitar al usuario que ingrese su contraseña actual para verificar su identidad. • Si la contraseña ingresada es incorrecta, el sistema debe mostrar el mensaje: *"La contraseña actual es incorrecta. Intente nuevamente."* • El sistema debe limitar el número de intentos fallidos antes de bloquear temporalmente la acción (máximo 5 intentos). • Si la contraseña ingresada es correcta, el sistema debe permitir continuar con el proceso de eliminación. • Si el usuario no ingresa un código válido dentro del tiempo límite, el sistema debe cancelar la operación y mostrar un mensaje de error.

	Confirmación de Eliminación • El sistema debe mostrar un mensaje de advertencia sobre la eliminación permanente de la cuenta y la pérdida irreversible de datos. • El usuario debe confirmar la eliminación de la cuenta. • Si el usuario no confirma la eliminación, el sistema debe cancelar la operación y mostrar el mensaje: "La eliminación de la cuenta ha sido cancelada." • Si el usuario confirma la eliminación, el proceso debe continuar con la eliminación de los datos.

	Eliminación de la Cuenta
	• El sistema debe eliminar o anonimizar los datos personales del usuario conforme a la normativa de protección de datos.
	• Si la eliminación de la cuenta se completa correctamente, el sistema debe:
	  ○ Mostrar un mensaje de confirmación de la eliminación.
	  ○ Cerrar la sesión en todos los dispositivos del usuario.
	• Si ocurre un error en la eliminación de la cuenta, el sistema debe mostrar el mensaje: *"Ha ocurrido un error al eliminar su cuenta. Inténtelo nuevamente más tarde."*

	Notificación al Usuario • El sistema debe enviar un correo electrónico de confirmación al usuario notificando la eliminación de su cuenta. • Si el usuario no reconoce la acción, el correo debe proporcionar un contacto de soporte y un plazo para intentar revertir la eliminación. • Si el usuario reconoce la acción, el proceso debe concluir sin posibilidad de recuperación.
	Excepciones y Seguridad • Si el usuario no está autenticado, el sistema debe redirigirlo a la interfaz de inicio de sesión antes de iniciar el proceso de eliminación. • Si el token de sesión ha expirado antes de completar el proceso, el sistema debe mostrar el mensaje: *"Su sesión ha expirado. Inicie sesión nuevamente para continuar con la eliminación de su cuenta."* • El sistema debe registrar todos los intentos de eliminación de cuenta en los logs de auditoría. • El sistema debe bloquear intentos repetitivos de eliminación desde la misma IP en un corto período de tiempo. • La eliminación de la cuenta debe cumplir con las normativas de protección de datos aplicables (GDPR).
Estado	Especificado
Solicitado por	Director de Proyecto
Fecha de Identificación	05/10/2024
Referencias	DFT Eliminar Cuenta