Logotipo

Descripción generada automáticamente

**Universidade de Santiago de Compostela**

**Escola Politécnica Superior de Enxeñaría**

**Máster Universitario en Dirección de Proyectos**

Descripción del Flujo de Trabajo (DFT)

DFT Recuperar Contraseña de 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:** | DFT Recuperar Contraseña de Usuario |
| **Autor del documento:** | Ing. Erio Gutierrez Llorens |
| **Propietario del Proyecto:** | CEO Empresa de Soluciones Informáticas SIVSA |
| **Director del Proyecto:** | Ing. Maylin Vega Angulo, Ing. Erio Gutierrez Llorens |
| **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** |
| Dr. Rolando Salazar | CEO SIVSA | Aprobación | 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 | 11/03/2025 | Ing. Maylin Vega Angulo | 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/2 Planificación

**TABLA DE CONTENIDOS**

1. Descripción General 4

2. Diagrama de Flujo de Trabajo 4

3. Descripción del Proceso 4

3.1. Solicitud de Recuperación 4

3.2. Validación del Correo 5

3.3. Verificación del Token 5

3.4. Restablecimiento de Contraseña 5

3.5. Confirmación y Cierre de Sesión en Otros Dispositivos 5

4. Excepciones y Mensajes de Error 5

5. Seguridad y Mecanismos de Protección 5

# Descripción General

El proceso de recuperación de contraseña permite a los usuarios restablecer sus credenciales de acceso de manera segura en caso de olvido o compromiso de la cuenta. Este flujo incorpora múltiples validaciones para evitar accesos no autorizados y garantizar la seguridad de los datos del usuario.

# Diagrama Descripción generada automáticamenteDiagrama de Flujo de Trabajo

Figura No. 1 DFT Recuperar Contraseña de Usuario

# Descripción del Proceso

## Solicitud de Recuperación

* El usuario accede a la opción "¿Olvidaste tu contraseña?" en la interfaz de inicio de sesión.
* Se solicita el correo electrónico asociado a la cuenta.
* Se valida que el formato del correo sea correcto.

## Validación del Correo

* Se verifica si el correo está registrado en el sistema.
* Si el correo no existe, se muestra un mensaje de error indicando que el correo electrónico no se encuentra registrado.
* Si el correo es válido, se genera un token de recuperación con tiempo de expiración y se envía un correo con un enlace único.

## Verificación del Token

* El usuario accede al enlace de recuperación dentro del correo.
* Se valida el token:
* Si es válido y no ha expirado (30 minutos), se muestra la interfaz de restablecimiento.
* Si es inválido o expirado, se muestra un mensaje de error indicando que el token ha expirado.

## Restablecimiento de Contraseña

* Se solicita al usuario una nueva contraseña y su confirmación.
* Se validan las reglas de seguridad de la contraseña.
* Se guarda la nueva contraseña cifrada en el sistema.

## Confirmación y Cierre de Sesión en Otros Dispositivos

* Se informa al usuario que la contraseña ha sido cambiada correctamente.
* Se cierra la sesión en todos los dispositivos para evitar accesos no autorizados.
* Se redirige al usuario a la pantalla de inicio de sesión.

# Excepciones y Mensajes de Error

* Correo electrónico inválido o formato incorrecto: Se solicita corregir correo electrónico.
* Correo electrónico no registrado: Se evita exponer información sobre cuentas existentes.
* Token expirado o inválido: Se ofrece opción de reenviar el correo electrónico de recuperación.
* Contraseña no segura: Se exige una combinación de caracteres adecuados.
* Intentos sospechosos: Se pueden bloquear solicitudes repetitivas desde la misma IP.

# Seguridad y Mecanismos de Protección

* Cifrado de contraseñas con algoritmos seguros.
* Token de recuperación con expiración (30 minutos).
* Límites de intentos y bloqueo temporal para evitar ataques de fuerza bruta.
* Cierre de sesiones en otros dispositivos tras el restablecimiento de la contraseña.