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 Cambiar 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 Cambiar 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 |
| **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 | 11/03/2025 | 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/2 Planificación/Flujo Trabajo

**TABLA DE CONTENIDOS**

1. Descripción General 4

2. Diagrama de Flujo de Trabajo 4

3. Descripción del Proceso 4

3.1. Acceso a la Opción de Cambio de Contraseña 4

3.2. Verificación de la Contraseña Actual 4

3.3. Introducción de la Nueva Contraseña 5

3.4. Almacenamiento Seguro de la Nueva Contraseña 5

3.5. Notificación al Usuario 5

4. Excepciones y Mensajes de Error 5

5. Seguridad y Mecanismos de Protección 6

# Descripción General

El proceso de modificación de contraseña permite a los usuarios autenticados actualizar su contraseña dentro del sistema de manera segura. Este flujo incluye múltiples validaciones para garantizar que la contraseña cumple con los estándares de seguridad y prevenir intentos de comprometer la cuenta.

# Diagrama Descripción generada automáticamenteDiagrama de Flujo de Trabajo

Figura No. 1 DFT Cambiar Contraseña de Usuario

# Descripción del Proceso

## Acceso a la Opción de Cambio de Contraseña

* El usuario autenticado accede a la sección de configuración o seguridad de su cuenta.
* Si el usuario no está autenticado, se redirige a la pantalla de inicio de sesión.
* Si la sesión ha expirado, se solicita una nueva autenticación.

## Verificación de la Contraseña Actual

* El usuario introduce su contraseña actual para verificar su identidad.
* Si la contraseña ingresada es incorrecta, se muestra un mensaje de error y se limita la cantidad de intentos.
* Si se excede el número de intentos permitidos, se bloquea temporalmente la opción de cambio de contraseña.
* Si la contraseña es correcta, el proceso continúa.

## Introducción de la Nueva Contraseña

* El usuario introduce la nueva contraseña y la confirma.
* Si la nueva contraseña no cumple con los requisitos de seguridad (longitud mínima, uso de caracteres especiales, números, combinación de mayúsculas y minúsculas), se muestra un mensaje indicando los cambios necesarios.
* Si la nueva contraseña coincide con la anterior, se solicita ingresar una diferente.
* Si la nueva contraseña está en una lista de contraseñas comprometidas, se solicita elegir una diferente.
* Si repetir nueva contraseña no coincide con la anterior, se solicita verificar que las contraseñas coincidan.
* Si la contraseña cumple con los requisitos, el proceso continúa.

## Almacenamiento Seguro de la Nueva Contraseña

* La nueva contraseña se almacena de manera segura en el sistema utilizando algoritmos de hashing.
* Si la contraseña se almacena correctamente, se informa al usuario y se cierra la sesión en todos los dispositivos activos.
* Si ocurre un error en el almacenamiento, se solicita intentarlo de nuevo.

## Notificación al Usuario

* Se envía un correo electrónico notificando el cambio de contraseña.
* Si el usuario no reconoce el cambio, se le proporciona un enlace para restablecer su contraseña de inmediato.

# Excepciones y Mensajes de Error

* Si el usuario no está autenticado, se muestra un mensaje de error y se redirige a la interfaz de inicio de sesión.
* Si la contraseña actual ingresada es incorrecta, se muestra un mensaje: "La contraseña actual es incorrecta. Intente nuevamente." Se limita la cantidad de intentos antes de bloquear la función temporalmente.
* Si el usuario introduce una nueva contraseña que no cumple con los requisitos de seguridad, se muestra un mensaje con las reglas establecidas: "La contraseña debe contener al menos 8 caracteres, una mayúscula, un número y un carácter especial."
* Si la nueva contraseña coincide con la anterior, se muestra un mensaje: "La nueva contraseña no puede ser igual a la actual."
* Si la contraseña está en una lista de contraseñas comprometidas, se muestra un mensaje: "La contraseña ingresada ha sido detectada en filtraciones de datos. Use una contraseña diferente."
* Si ocurre un error en el almacenamiento de la contraseña, se muestra un mensaje de error interno: "Ha ocurrido un error al actualizar su contraseña. Inténtelo nuevamente más tarde."
* Si el token de sesión ha expirado antes de completar el proceso, se muestra un mensaje: "Su sesión ha expirado. Inicie sesión nuevamente para cambiar su contraseña."

# Seguridad y Mecanismos de Protección

* Uso de autenticación obligatoria para acceder a la función de cambio de contraseña.
* Limitación de intentos de ingreso de la contraseña actual para prevenir ataques de fuerza bruta.
* Aplicación de reglas estrictas de validación de contraseña para fortalecer la seguridad.
* Uso de hashing seguro para el almacenamiento de contraseñas.
* Expiración automática de la sesión tras un tiempo de inactividad prolongado para prevenir accesos no autorizados.
* Cierre de sesión en todos los dispositivos activos tras el cambio de contraseña.
* Envío de notificación por correo electrónico para alertar al usuario sobre el cambio de contraseña y permitir la recuperación inmediata en caso de actividad sospechosa.
* Monitoreo de intentos fallidos y bloqueo temporal tras múltiples intentos incorrectos para evitar ataques automatizados.
* Protección contra ataques de reutilización de contraseñas al verificar que la nueva contraseña no coincida con las últimas usadas.
* Uso de conexiones seguras (HTTPS y TLS) para el cifrado de la información transmitida entre el cliente y el servidor.