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 Autenticar Usuarios

**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 Autenticar Usuarios |
| **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 5

3.1. Ingreso de Credenciales 5

3.2. Verificación de Existencia del Usuario 5

3.3. Verificación de Contraseña 5

3.4. Verificación del Estado de la Cuenta 5

3.5. Inicio de Sesión Exitoso 6

4. Excepciones y Mensajes de Error 6

5. Seguridad y Mecanismos de Protección 6

# Descripción General

El proceso de autenticación de usuario permite validar la identidad del usuario que intenta acceder al sistema, garantizando la seguridad mediante controles de validación de credenciales y verificaciones adicionales para prevenir accesos no autorizados.

# Diagrama Descripción generada automáticamenteDiagrama de Flujo de Trabajo

Figura No. 1 DFT Autenticar Usuarios

# Descripción del Proceso

## Ingreso de Credenciales

* El usuario introduce su correo electrónico y contraseña en el formulario de inicio de sesión.
* Se validan los siguientes aspectos del correo electrónico:
* Formato correcto (estructura válida con "@" y dominio).
* No contiene caracteres especiales no permitidos.
* No pertenece a dominios desechables (correo temporal).
* Se validan los siguientes aspectos de la contraseña:
* No está vacía.
* No contiene espacios en blanco adicionales.
* Cumple con el formato de contraseña válida.
* Se valida el reCAPTCHA.
* Si alguna de estas validaciones falla, se muestra un mensaje de error y se solicita una corrección.

## Verificación de Existencia del Usuario

* Se comprueba si el correo electrónico ingresado está registrado en la base de datos.
* Si el correo no existe, se muestra un mensaje: "Usuario no registrado".
* Si el usuario existe, se pasa a la verificación de la contraseña.
* Si el usuario ha intentado múltiples registros con diferentes correos en un corto período de tiempo, se activa una verificación adicional para prevenir intentos de fuerza bruta.

## Verificación de Contraseña

* Se compara la contraseña ingresada con la almacenada en la base de datos (hash).
* Si la contraseña es incorrecta:
* Se incrementa un contador de intentos fallidos.
* Si el usuario supera el límite predefinido (5 intentos fallidos), la cuenta se bloquea temporalmente.
* Se verifica si el intento proviene de una ubicación o dispositivo sospechoso.
* Si el intento proviene de un dispositivo nuevo, se solicita un código de verificación adicional enviado al correo.
* Se muestra un mensaje de error: "Contraseña incorrecta.".
* Si la contraseña es correcta, se verifica el estado de la cuenta.

## Verificación del Estado de la Cuenta

* Se verifica si la cuenta está activa:
* Si la cuenta está desactivada, se muestra un mensaje: "Cuenta desactivada. Contacte con soporte.".
* Si la cuenta está bloqueada por intentos fallidos, se muestra un mensaje: "Cuenta bloqueada temporalmente. Intente nuevamente en 30 minutos.".
* Si la cuenta está en espera de verificación de correo, se muestra un mensaje: "Debe verificar su correo electrónico antes de iniciar sesión.".
* Si la cuenta ha estado inactiva durante un tiempo prolongado, se solicita un paso adicional de autenticación para mayor seguridad.
* Si la cuenta está activa y en estado normal, se procede a la autenticación exitosa.

## Inicio de Sesión Exitoso

* Se genera un token de sesión o se establece una cookie segura.
* Se registra el evento de autenticación en los logs del sistema.
* Se almacena la información del dispositivo y la ubicación de acceso para detección de anomalías.
* Se redirige al usuario a la interfaz principal de la aplicación.
* Si es el primer inicio de sesión desde un nuevo dispositivo, se envía una notificación al correo del usuario.

# Excepciones y Mensajes de Error

* Correo no registrado: Se solicita al usuario registrarse.
* Formato de correo inválido: Se muestra un mensaje de error específico.
* Contraseña incorrecta: Se limita el número de intentos.
* Cuenta bloqueada por intentos fallidos: Se informa al usuario y se sugiere restablecer contraseña.
* Cuenta desactivada: Se notifica y se recomienda contactar con soporte.
* Intento de acceso sospechoso: Se registra y se puede enviar una alerta de seguridad al usuario.

# Seguridad y Mecanismos de Protección

* Uso de hashes seguros para almacenar contraseñas.
* Implementación de reCAPTCHA para prevenir ataques automatizados.
* Bloqueo temporal de cuenta tras múltiples intentos fallidos.
* Notificaciones al usuario ante intentos sospechosos de inicio de sesión.
* Tokens de sesión seguros (JWT con expiración y revocación de tokens activos en caso de cierre de sesión).