	<b>MANUAL DE CALIDAD</b>		<b>MC413-IT-4</b>
	<b>Política de Contraseñas Seguras</b>		REVISIÓN: 0 FECHA: 25/08/25
Emisión: G. MONTALBETTI Fecha: Firma:	Aprobación: D. PEDROSA Fecha: Firma:		<b>PAG.: 1 / 5</b>

## 1. OBJETIVO

Establecer los requisitos para la creación, gestión y protección de contraseñas en todos los sistemas de información de **Prodismo SRL**. Esta política tiene como objetivo proteger el acceso no autorizado a los activos de información, garantizar la confidencialidad, integridad y disponibilidad de los datos, y cumplir con los requisitos de los controles A.5.17 (Autenticación), A.8.2 (Gestión de derechos de acceso) y A.8.3 (Responsabilidad del usuario por el acceso) del Anexo A de la norma **ISO/IEC 27001:2022**, así como con los requisitos de protección de información del marco **TISAX**.


## 2. ALCANCE

Esta política aplica a:

- **Todos los usuarios:** Empleados, contratistas, proveedores y terceros que tengan acceso a los sistemas de información de la organización.
- **Todos los sistemas:** Servidores, estaciones de trabajo, aplicaciones, bases de datos, servicios en la nube, dispositivos de red y cualquier otro sistema que requiera autenticación por contraseña.
- **Todos los dispositivos:** Equipos corporativos y personales (BYOD) utilizados para acceder a recursos de la empresa.

## 3. REFERENCIAS NORMATIVAS

- ISO/IEC 27001:2022 - Anexo A.5.17 (Autenticación), A.8.2 (Gestión de derechos de acceso)
- ISO/IEC 27002:2022 - Guía para los controles de seguridad
- Marco de evaluación TISAX

	<b>MANUAL DE CALIDAD</b>	<b>MC413-IT-4</b>
	<b>Política de Contraseñas Seguras</b>	REVISIÓN: 0 FECHA: 25/08/25
		<b>PAG.: 2 / 5</b>


- Política de Control de Acceso **MC412-IT-1** **Política de Autenticación y Control de Accesos**
- Política de Uso Aceptable de los Recursos de TI ISMS-POL-00X

#### 4. DEFINICIONES

- **Contraseña Fuerte:** Contraseña que cumple con los requisitos de complejidad establecidos en esta política.
- **MFA (Autenticación Multifactor):** Método de autenticación que requiere dos o más pruebas de identidad.
- **Hash:** Función criptográfica utilizada para almacenar contraseñas de forma segura.
- **Gestor de Contraseñas:** Herramienta autorizada para almacenar y gestionar contraseñas de forma segura.


#### 5. RESPONSABLES

- **Alta Dirección:** Aprobar la política y asegurar los recursos para su implementación.
- **Responsable de Seguridad de la Información (RSI):** Mantener, supervisar y auditar el cumplimiento de esta política.
- **Departamento de TI:** Implementar controles técnicos para aplicar los requisitos de contraseñas (longitud, complejidad, caducidad) en todos los sistemas. Gestionar el acceso de usuarios y proporcionar gestores de contraseñas corporativos.
- **Responsables de Área:** Asegurar que el personal bajo su supervisión conoce y cumple esta política.
- **Todos los Usuarios:** Crear y proteger contraseñas fuertes, cumplir con los requisitos establecidos y reportar cualquier contraseña comprometida.

	<b>MANUAL DE CALIDAD</b>	<b>MC413-IT-4</b>
	<b>Política de Contraseñas Seguras</b>	REVISIÓN: 0 FECHA: 25/08/25
		<b>PAG.: 3 / 5</b>

## 6. REQUISITOS MÍNIMOS PARA CONTRASEÑAS

- Longitud Mínima:** 12 caracteres para usuarios standard. 16 caracteres para cuentas administrativas y de servicio.
- Complejidad:** Debe incluir caracteres de al menos tres de las siguientes cuatro categorías:
  - Letras mayúsculas (A-Z)
  - Letras minúsculas (a-z)
  - Números (0-9)
  - Caracteres especiales (ej: !, @, #, \$, %, &, \*)
- Caducidad (Rotación):**
  - Contraseñas de usuario:** 90 días. No se permite el reuso de las últimas 5 contraseñas.
  - Contraseñas de administrador:** 60 días.
  - Contraseñas de servicio/sistema:** Rotar anualmente o ante cualquier cambio en el personal responsable.
- Bloqueo de Cuenta:** Tras 5 intentos fallidos de inicio de sesión, la cuenta se bloqueará durante un período de 15 minutos.
- Almacenamiento:** Las contraseñas deben almacenarse en forma de **hash** con sal (salt) utilizando algoritmos fuertes (ej: bcrypt, Argon2). **Queda prohibido almacenar contraseñas en texto plano.**
- Autenticación Multifactor (MFA):** Es **obligatorio** el uso de MFA para:
  - Acceso remoto (VPN, escritorio remoto).
  - Acceso a sistemas críticos (ERP SIP 4.0, servidor de diseños 3D).
  - Todas las cuentas con privilegios administrativos.
  - Acceso a servicios en la nube (Microsoft 365, Azure, AWS).

	<b>MANUAL DE CALIDAD</b>	<b>MC413-IT-4</b>
	<b>Política de Contraseñas Seguras</b>	REVISIÓN: 0 FECHA: 25/08/25
		<b>PAG.: 4 / 5</b>


## 7. PROHIBICIONES

Queda **estrictamente prohibido**:

- **Compartir contraseñas:** Cada usuario es responsable de su contraseña. Bajo ninguna circunstancia se deben compartir las credenciales.
- **Reutilizar contraseñas:** No utilizar la misma contraseña para diferentes sistemas (corporativos y personales).
- **Almacenar contraseñas en claro:** No escribirlas en post-its, agendas, archivos de texto sin cifrar o emails.
- **Utilizar contraseñas débiles o comunes:** Ej: "Password123", "Welcome1", "123456", nombres de familiares o mascotas, fechas de cumpleaños.
- **Enviar contraseñas por canales no cifrados:** Como mensajes de texto SMS, WhatsApp no corporativo o correo electrónico sin cifrar.

## 8. GESTIÓN DE CONTRASEÑAS

- **Asignación Inicial:** Las contraseñas iniciales deben ser generadas de forma aleatoria y segura, y se deben cambiar en el primer inicio de sesión.
- **Recuperación:** El proceso de recuperación de contraseñas debe verificar la identidad del usuario a través de métodos alternativos seguros (preguntas de seguridad robustas, email alternativo, MFA). No se deben restablecer contraseñas por teléfono sin una verificación rigurosa.
- **Herramientas:** Se proporcionará y recomendará el uso de un **gestor de contraseñas corporativo** (ej: Bitwarden, Keeper) para almacenar y generar contraseñas fuertes.

	<b>MANUAL DE CALIDAD</b>	<b>MC413-IT-4</b>
	<b>Política de Contraseñas Seguras</b>	REVISIÓN: 0 FECHA: 25/08/25
		<b>PAG.: 5 / 5</b>

## 9. SANCIONES

El incumplimiento de esta política se considerará una violación de las normas de seguridad de la información y dará lugar a acciones disciplinarias, que podrán incluir, dependiendo de la gravedad de la infracción:

- **Amonestación verbal o escrita.**
- **Capacitación obligatoria** en seguridad de la información.
- **Suspensión** de los privilegios de acceso a los sistemas.
- **Desvinculación laboral** en casos graves o reincidentes que pongan en riesgo significativo la seguridad de la información.

## 10. REVISIÓN Y AUDITORÍA DEL DOCUMENTO

- Esta política será revisada **anualmente** por el RSI, o ante cambios en el panorama de amenazas o tecnologías.
- El cumplimiento de esta política se auditará mediante:
  - **Revisiones técnicas** de la configuración de los sistemas para verificar el cumplimiento de los requisitos de longitud, complejidad y caducidad.
  - **Simulaciones de phishing** para evaluar la concienciación de los usuarios.
  - **Auditorías internas** del SGSI y **evaluaciones TISAX**.
- Los resultados de las auditorías se presentarán a la Dirección.

Rev. N°	Fecha	Descripción
0	25/8/2025	Primera Emisión del documento