	MANUAL DE CALIDAD		MC421-IT-2
	Política de Mínimos Privilegios		REVISIÓN: 0 FECHA: 25/08/25
Emisión: G. MONTALBETTI Fecha: Firma:	Aprobación: D. PEDROSA Fecha: Firma:		PAG.: 1 / 9

1. OBJETIVO

Establecer los principios y requisitos para la implementación y mantenimiento del principio de mínimo privilegio en los sistemas de información de **PRODISMO SRL**, garantizando que los usuarios, sistemas y procesos dispongan únicamente de los accesos estrictamente necesarios para el desempeño de sus funciones, en cumplimiento de los controles A.5.3 (Segregación de funciones), A.5.7 (Gestión de derechos de acceso) y A.8.2 (Privilegios de acceso) del Anexo A de **ISO/IEC 27001:2022** y los requisitos de control de acceso del marco **TISAX**.


2. ALCANCE

Esta política aplica a:

- **Todos los usuarios:** empleados, contratistas, proveedores y terceros con acceso a sistemas de información
- **Todos los sistemas** bajo el alcance del SGSI (ERP SIP 4.0, servidores, aplicaciones internas)
- **Todos los procesos** de gestión de identidades y accesos
- **Cuentas de servicio** y aplicaciones con acceso automatizado

3. REFERENCIAS NORMATIVAS

- ISO/IEC 27001:2022 - Anexo A.5.3, A.5.7, A.8.2
- ISO/IEC 27002:2022 - Guía para los controles de seguridad
- Marco de evaluación TISAX
- Procedimiento de Gestión de Accesos **P413-IT-1 Gestión de Accesos a Servicios de Red, Sistemas IT y App**
- Política de Control de Acceso **MC412-IT-1 Política de Autenticación y Control de Accesos**

	MANUAL DE CALIDAD	MC421-IT-2
	Política de Mínimos Privilegios	REVISIÓN: 0 FECHA: 25/08/25
		PAG.: 2 / 9

4. DEFINICIONES

- **Principio de Mínimo Privilegio:** Concesión de los permisos mínimos necesarios para realizar una función específica
- **RBAC (Role-Based Access Control):** Control de acceso basado en roles predefinidos
- **Privilegio:** Derecho o permiso para realizar una acción específica en un sistema
- **Segregación de Funciones (SoD):** Separación de Tareas para prevenir fraudes o errores

5. RESPONSABLES

5.1. Alta Dirección

- Aprobar la política y asignar los recursos necesarios
- Establecer la cultura organizacional de mínimo privilegio
- Autorizar excepciones de alto riesgo

5.2. Responsable de Seguridad de la Información (RSI)


- Supervisar la implementación y cumplimiento de la política
- Aprobar la matriz de roles y permisos
- Revisar y autorizar excepciones

5.3. IT Manager/Departamento de TI

- Implementar los controles técnicos para aplicar el principio
- Gestionar las solicitudes de acceso según roles predefinidos
- Realizar revisiones periódicas de privilegios

5.4. Responsables de Área

- Solicitar accesos necesarios para su personal

	MANUAL DE CALIDAD	MC421-IT-2
	Política de Mínimos Privilegios	REVISIÓN: 0 FECHA: 25/08/25
		PAG.: 3 / 9

- Validar la adecuación de los permisos asignados
- Notificar cambios de funciones que afecten los accesos

5.5. Usuarios Finales

- Utilizar los privilegios únicamente para fines autorizados
- Reportar privilegios excesivos o innecesarios
- Proteger sus credenciales de acceso


6. PRINCIPIOS FUNDAMENTALES

6.1. Principio de Mínimo Privilegio

- Los usuarios dispondrán únicamente de los accesos necesarios para sus funciones actuales
- Denegar por defecto, permitir por excepción explícitamente justificada
- Revisar periódicamente la necesidad de los privilegios concedidos

6.2. Segregación de Funciones (SoD)

Función Conflictiva	Control de Segregación	Revisión
Desarrollador - Despliegue Producción	Entornos separados, aprobación independiente	Mensual
Solicitante - Aprobador Compras	Flujos de trabajo con múltiples aprobadores	Trimestral
Usuario - Administrador Sistema	Roles separados, sin privilegios compartidos	Continuo

	MANUAL DE CALIDAD	MC421-IT-2
	Política de Mínimos Privilegios	REVISIÓN: 0 FECHA: 25/08/25
		PAG.: 4 / 9


6.3. Control Basado en Roles (RBAC)

- Definición de roles estándar según funciones organizacionales
- Asignación de permisos a roles, no a usuarios individuales
- Revisión y actualización periódica de la matriz de roles

7. ROLES Y PERMISOS PREDEFINIDOS

7.1. Matriz de Roles Corporativos

Rol	Sistemas Accesibles	Permisos	Restricciones
Usuario Estándar	Office 365, Intranet	Lectura/escritura en recursos asignados	Sin derechos de administración local
Administrador Sistema	Servidores, Active Directory	Administración completa sistemas asignados	Acceso vía MFA, logging completo
Desarrollador	Entornos desarrollo, GitHub	Escritura código, testing	Sin acceso a producción
Analista Financiero	SIP 4.0 (módulos finanzas)	Consulta, reportes, entrada datos limitada	Sin aprobación pagos, sin modificación maestros
Auditor Interno	Todos los sistemas (solo lectura)	Acceso lectura para auditoría	Ventana temporal, supervisado

	MANUAL DE CALIDAD	MC421-IT-2
	Política de Mínimos Privilegios	REVISIÓN: 0 FECHA: 25/08/25
		PAG.: 5 / 9

7.2. Permisos para Sistemas Críticos

7.2.1. ERP SIP 4.0

Rol ERP	Módulos Accesibles	Transacciones Permitidas	Límites
Consulta Finanzas	Administración, Ventas	Solo consulta reportes	Sin modificación datos
Operador Cuentas a Pagar	Administración, Ventas	Entrada facturas, pagos menores	Límite aprobación: USD5.000
Supervisor Finanzas	Todos módulos financieros	Aprobación pagos, cierres	Límite aprobación: USD100.000


7.2.2. Servidores de Diseño 3D

- **Ingeniero Diseño:** Lectura/escritura en proyectos asignados
- **Líder Proyecto:** Acceso completo a proyectos bajo su responsabilidad
- **Archivista:** Solo lectura para documentación liberada

8. GESTIÓN DEL CICLO DE VIDA DE ACCESOS

8.1. Provisión de Accesos

1. **Solicitud formal** mediante F421-IT-1
2. **Aprobación** del responsable de área y RSI
3. **Asignación** según rol predefinido más restrictivo
4. **Comunicación** segura de credenciales

	MANUAL DE CALIDAD	MC421-IT-2
	Política de Mínimos Privilegios	REVISIÓN: 0 FECHA: 25/08/25
		PAG.: 6 / 9

8.2. Revisiones Periódicas

Tipo de Acceso	Frecuencia Revisión	Responsable
Privilegios administrativos	Trimestral	RSI
Accesos a sistemas críticos	Semestral	IT Manager
Accesos estándar usuarios	Anual	Responsables de área
Cuentas de servicio	Anual	Departamento TI


8.3. Revocación de Accesos

- **Baja laboral:** Revocación inmediata (automática cuando sea posible)
- **Cambio de puesto:** Reasignación según nuevo rol dentro de 24 horas
- **Finalización de proyecto:** Revocación específica a los 7 días

9. EXCEPCIONES

9.1. Solicitud de Excepción

- **Justificación técnica/operativa** detallada
- **Evaluación de riesgo** por el RSI
- **Plan de mitigación** con controles compensatorios
- **Fecha de revisión** definida (máximo 6 meses)

	MANUAL DE CALIDAD	MC421-IT-2
	Política de Mínimos Privilegios	REVISIÓN: 0 FECHA: 25/08/25
		PAG.: 7 / 9

9.2. Aprobación de Excepciones

Nivel de Excepción	Aprobador	Documentación Requerida
Bajo Riesgo (acceso temporal <30 días)	IT Manager	Formulario de excepción
Medio Riesgo (acceso extendido)	RSI	Evaluación de riesgo + mitigación
Alto Riesgo (privilegios elevados permanentes)	Comité de Seguridad	Justificación business + controles

10. REGISTROS Y EVIDENCIAS

10.1. Registros Obligatorios

- **F421-IT-1:** Formulario de Solicitud de Acceso
- **F421-IT-9:** Matriz de Roles y Permisos Predefinidos
- **Registro de excepciones** aprobadas
- **Evidencias de revisiones** periódicas


10.2. Retención de Registros

- **Solicitudes de acceso:** 3 años después de la revocación
- **Matrices de roles:** Versiones históricas por 5 años
- **Excepciones aprobadas:** 3 años después del cierre
- **Logs de acceso privilegiado:** 12 meses

11. MONITOREO Y CUMPLIMIENTO

11.1. Monitorización de Privilegios

- **Alertas por uso de privilegios** administrativos

	MANUAL DE CALIDAD	MC421-IT-2
	Política de Mínimos Privilegios	REVISIÓN: 0 FECHA: 25/08/25
		PAG.: 8 / 9

- **Revisión de logs** de acceso a datos sensibles
- **Reportes de cumplimiento** trimestrales

11.2. Auditorías de Cumplimiento

- **Auditorías internas** semestrales del principio de mínimo privilegio
- **Verificación de SoD** en sistemas críticos trimestralmente
- **Inclusión en evaluaciones TISAX** y auditorías **ISO 27001**

12. SANCIONES POR INCUMPLIMIENTO

El incumplimiento de esta política dará lugar a acciones disciplinarias proporcionales a la gravedad de la infracción:

- **Uso indebido de privilegios:** Amonestación y capacitación obligatoria
- **Compartir credenciales privilegiadas:** Suspensión de accesos
- **Elusión de controles deliberada:** Acciones disciplinarias graves hasta desvinculación


13. REVISIÓN Y ACTUALIZACIÓN

13.1. Revisiones Periódicas

- **Revisión anual** de la política y matriz de roles
- **Actualización trimestral** basada en cambios organizativos
- **Revisión post-incidente** cuando se identifiquen fallos en controles

13.2. Indicadores de Desempeño

- **Porcentaje de usuarios con privilegios mínimos adecuados:** Objetivo >95%
- **Tiempo promedio de revocación de accesos:** Objetivo <24 horas
- **Número de excepciones activas:** Objetivo <5% de usuarios totales

	MANUAL DE CALIDAD	MC421-IT-2
	Política de Mínimos Privilegios	REVISIÓN: 0 FECHA: 25/08/25
		PAG.: 9 / 9

ANEXOS

Anexo A: Matriz Completa de Roles y Permisos (F421-IT-9)

[Definición detallada de todos los roles organizacionales y permisos asociados]

Anexo B: Procedimiento de Solicitud y Aprobación de Accesos

[Flujo detallado del proceso de gestión de accesos]

Anexo C: Checklist de Revisión de Privilegios

[Herramienta para revisiones periódicas de cumplimiento]

14. REVISIONES DEL CAPÍTULO

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