					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P11S					Título del documento: **Política de gestión de cuentas de usuario y privilegios**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineada con las normas y reglamentos aplicables

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 5.3, 8	Funciones, responsabilidades y planificación/control operativo para la gestión de accesos de usuarios
ISO/IEC 27002:2022	Control 8	Controles para la asignación, revisión y retirada de privilegios elevados
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Creación de cuentas, supervisión, mínimo privilegio y segregación de funciones
Directiva NIS2 de la UE	Artículo 21(2)(d)	Gestión de accesos de usuarios para entidades esenciales e importantes
Reglamento DORA de la UE	Artículo 9(2)(b)	Control de accesos privilegiados en entidades financieras
COBIT 2019	DSS05.03, DSS05.04	Aprovisionamiento, desaprovisionamiento de accesos y revisión periódica del acceso de usuarios
RGPD de la UE	Artículo 32	Controles de acceso adecuados para la protección de datos personales

1. Propósito

1.1 Esta política establece las reglas para gestionar las cuentas de usuario y los derechos de acceso de forma segura, coherente y trazable. Garantiza que solo los usuarios autorizados tengan acceso a los sistemas y datos, y que dicho acceso sea adecuado a sus funciones y responsabilidades.

1.2 Una gestión eficaz de cuentas y privilegios es esencial para prevenir accesos no autorizados, minimizar las amenazas internas y garantizar el cumplimiento de ISO/IEC 27001, del RGPD de la UE y de otros requisitos normativos.

1.3 Esta política permite a la organización asignar la titularidad y la responsabilidad sobre el uso de las cuentas, supervisar y auditar las elevaciones de privilegios, y deshabilitar o revocar accesos de forma segura cuando ya no sean necesarios.

1.4 Asimismo, protege las operaciones de la organización frente a errores operativos o usos indebidos causados por accesos excesivos o no supervisados, y ayuda a reducir el riesgo de brechas de datos accidentales, uso indebido de privilegios o incumplimiento normativo.

2. Alcance

2.1 Esta política aplica a:

2.1.1 Todos los empleados, becarios, contratistas y terceros con acceso a los sistemas de TI de la organización.

2.1.2 Todos los sistemas, dispositivos, servicios y plataformas gestionados por la organización o en su nombre, incluidas las plataformas en la nube, la infraestructura local y las herramientas de terceros.

2.2 Abarca todos los tipos de cuentas de usuario, incluidas:

2.2.1 Cuentas de usuario nominales (p. ej., cuentas de correo electrónico, inicios de sesión en sistemas).

2.2.2 Cuentas de administrador y cuentas de sistema.

2.2.3 Credenciales de acceso temporal, de invitado o de terceros.

2.2.4 Cuentas de servicio utilizadas por aplicaciones o sistemas de automatización.

2.3 La política aplica durante todo el ciclo de vida de la cuenta, desde su creación y aprobación hasta su modificación, supervisión y desactivación. Esto incluye el aprovisionamiento inicial durante el alta, las revisiones de acceso durante los cambios de función y la revocación durante la baja.

3. Objetivos

3.1 Asignar identidades de usuario únicas y trazables a todos los usuarios de los sistemas, garantizando la trazabilidad individual y eliminando la dependencia de credenciales compartidas.

3.2 Aplicar el principio de mínimo privilegio, garantizando que a los usuarios solo se les conceda el nivel mínimo de acceso necesario para desempeñar sus funciones.

3.3 Prevenir accesos no autorizados a sistemas o datos sensibles mediante procesos de aprobación y revisión claramente documentados.

3.4 Garantizar la desactivación oportuna de las cuentas de usuario cuando ya no sean necesarias, por ejemplo, al producirse una baja, la finalización de un contrato o un cambio de función.

3.5 Mantener un entorno seguro y preparado para auditorías mediante la documentación de todos los cambios en las cuentas, aprobaciones y revisiones periódicas.

3.6 Garantizar que la elevación de privilegios esté estrictamente controlada, aprobada de manera independiente y registrada, y que el acceso elevado se revoque con prontitud cuando deje de ser necesario.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Es el responsable último de hacer cumplir esta política.

4.1.2 Garantiza que las prácticas de gestión de cuentas estén alineadas con los requisitos de certificación de ISO/IEC 27001 y las obligaciones legales aplicables (p. ej., RGPD de la UE).

4.1.3 Debe ser informado de inmediato de cualquier acceso no autorizado, incidente de seguridad o incumplimiento de la política relacionado con cuentas de usuario.

4.1.4 Supervisa las revisiones de la política, las auditorías y las medidas disciplinarias o correctivas que correspondan.

4.2 Responsable de TI o proveedor externo de TI

4.2.1 Es responsable de implantar técnicamente los controles de cuentas y privilegios en los sistemas utilizados por la organización.

4.2.2 Debe aprovisionar, modificar y desactivar cuentas de usuario basándose únicamente en aprobaciones documentadas.

4.2.3 Debe aplicar requisitos de complejidad de contraseñas, bloqueo automático de pantalla, autenticación multifactor (cuando esté disponible) y registro de eventos del sistema.

4.2.4 Debe mantener registros seguros de todas las aprobaciones de acceso, la titularidad de las cuentas, las elevaciones de privilegios y las revocaciones.

4.2.5 Debe supervisar la existencia de cuentas no autorizadas o cuentas huérfanas e informar de cualquier discrepancia al Director General.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Esta política debe ser revisada al menos una vez al año por el Director General y el Responsable de TI para garantizar el cumplimiento de:

9.1.1 Los controles y directrices vigentes de ISO/IEC 27001:2022.

9.1.2 Las actualizaciones normativas (p. ej., RGPD de la UE, DORA de la UE, Directiva NIS2 de la UE).

9.1.3 Los cambios en los sistemas, servicios o estructura de la organización.

9.2 También deben realizarse revisiones después de:

9.2.1 Incidentes de seguridad significativos o hallazgos de auditoría.

9.2.2 Cambios importantes en los sistemas de TI o en la arquitectura de cuentas.

9.2.3 La introducción de nuevas plataformas que requieran integración con el control de acceso.

9.3 Todos los cambios deben ser aprobados por el Director General y comunicados con claridad al personal afectado.

10. Políticas relacionadas y vínculos

10.1 P2S – Política de funciones y responsabilidades de gobernanza: establece la responsabilidad y la autoridad para la toma de decisiones relativas a las aprobaciones de acceso y la supervisión.

10.2 P4S – Política de control de acceso: regula la aplicación del control de acceso en todo el entorno y los métodos de autenticación.

10.3 P7S – Política de incorporación y cese: garantiza que la creación y retirada de cuentas se integren en los cambios de personal gestionados por Recursos Humanos.

10.4 P8S – Política de concienciación y formación en seguridad de la información: forma a los usuarios sobre prácticas seguras de uso de cuentas y expectativas de uso.

10.5 P30S – Política de respuesta a incidentes: define las acciones que deben adoptarse si el uso indebido de una cuenta provoca una brecha de seguridad o una divulgación no autorizada.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 La cláusula 5.3 exige que las funciones y responsabilidades en seguridad de la información estén claramente asignadas y se apliquen.

11.1.2 La cláusula 8.1 exige que la planificación y el control operativos incluyan la gestión de accesos de usuarios.

11.2 ISO/IEC 27002

11.2.1 El control 8.2 detalla los controles técnicos y procedimentales para asignar, revisar y retirar privilegios elevados.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2 exige la creación, supervisión y revocación de cuentas en función de roles y procesos definidos.

11.3.2 AC-5 aborda la segregación de funciones para prevenir conflictos o abusos de privilegios.

11.3.3 AC-6 exige la aplicación del principio de mínimo privilegio a todos los derechos de acceso.

11.4 RGPD de la UE

11.4.1 El artículo 32 exige controles de acceso adecuados para proteger los datos personales frente a accesos no autorizados o alteraciones.

11.5 Directiva NIS2 de la UE

11.5.1 El artículo 21(2)(d) exige la gestión de accesos de usuarios como parte de los controles básicos de seguridad para entidades esenciales e importantes.

11.6 DORA de la UE

11.6.1 El artículo 9(2)(b) exige que las entidades financieras implanten controles de acceso que restrinjan y supervisen los privilegios de acceso.

11.7 COBIT 2019

11.7.1 DSS05.03 especifica el aprovisionamiento y desaprovisionamiento de accesos de usuarios como parte del gobierno de TI.

11.7.2 DSS05.04 exige la revisión continua y la alineación del acceso de los usuarios con las funciones de la organización.