					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P11					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**

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 6.1.3, Cláusula 8	-
ISO/IEC 27002:2022	Controles 5.15-5.18	-
NIST SP 800-53 Rev. 5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
RGPD de la UE	Artículos 5(1)(f), 32; Considerando 39	-
Directiva NIS2 de la UE	Artículos 21(2)(a, d), 21(3)	-
DORA de la UE	Artículos 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Propósito

1 Esta política establece controles obligatorios para la gestión de cuentas de usuario y privilegios en todos los sistemas y servicios de información. Garantiza que el acceso a los recursos de la organización se conceda sobre la base de una identidad validada, la necesidad derivada del rol y los principios de mínimo privilegio y segregación de funciones.

1.1 Respalda el compromiso de la organización con la seguridad de la información mediante la implantación de procesos estructurados y auditables para el aprovisionamiento de accesos, la asignación de privilegios, la supervisión del uso y la revocación de cuentas.

1.2 Esta política es fundamental para reducir el riesgo de acceso no autorizado, uso indebido de privilegios, amenazas internas e incumplimiento de los marcos regulatorios aplicables.

2. Alcance

2.1 Esta política aplica a todos los empleados, contratistas, proveedores de servicios externos, consultores y demás personas a las que se conceda acceso a los recursos de TI, aplicaciones o datos de la organización.

2.2 Regula todos los sistemas y entornos en los que se apliquen mecanismos de autenticación de usuarios y control de acceso, incluidos, entre otros:

2.2.1 Aplicaciones corporativas y bases de datos

2.2.2 Plataformas en la nube y entornos SaaS

2.2.3 Sistemas operativos y consolas administrativas

2.2.4 Herramientas de acceso remoto y VPN

2.2.5 Sistemas de gestión de identidades y accesos (IAM)

2.3 La política abarca tanto las cuentas de usuario estándar como las privilegiadas, e incluye controles sobre:

2.3.1 Creación, modificación y desactivación de cuentas

2.3.2 Elevación y delegación de privilegios

2.3.3 Control y supervisión de sesiones

2.3.4 Métodos de autenticación y gestión de credenciales

3. Objetivos

3.1 Garantizar que todas las cuentas de usuario sean identificables de forma única, estén debidamente autorizadas y solo se asignen tras una validación formal de la necesidad.

3.2 Aplicar los principios de mínimo privilegio y evitar accesos innecesarios o excesivos mediante la aplicación de controles estrictos sobre la concesión y el uso de cuentas privilegiadas.

3.3 Exigir actualizaciones oportunas del estado de las cuentas en función de cambios laborales o de rol, incluida la desactivación inmediata tras la baja.

3.4 Permitir la detección y remediación proactivas de cuentas inactivas, utilizadas de forma indebida o no autorizadas mediante registro de eventos, revisiones y automatización.

3.5 Mantener la alineación con ISO/IEC 27001:2022 y las normas asociadas, y dar cumplimiento a las obligaciones de marcos legales y regulatorios pertinentes, como el RGPD de la UE, la Directiva NIS2 de la UE, DORA de la UE y COBIT 2019.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es responsable de esta política y garantiza su aplicación en toda la organización.

4.1.2 Revisa y aprueba cualquier excepción formal o caso de acceso de emergencia.

4.1.3 Informa sobre los hallazgos de auditoría relacionados con cuentas y escala los riesgos a la Dirección Ejecutiva.

4.2 Responsable de control de acceso / Administrador de TI

4.2.1 Mantiene y opera los controles técnicos para la gestión del ciclo de vida de las cuentas de usuario.

4.2.2 Ejecuta las acciones de aprovisionamiento, desaprovisionamiento y gestión de privilegios previa solicitud aprobada.

4.2.3 Mantiene un registro fehaciente de todas las cuentas de usuario, su estado y su nivel de privilegio.

4.2.4 Da soporte a auditorías y revisiones de cumplimiento mediante registros e informes de actividad.

[... 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 deberá revisarse al menos una vez al año o cuando se produzcan cambios significativos en:

9.1.1 La estructura organizativa o los procesos de negocio

9.1.2 Los sistemas de TI, las plataformas de identidad o los métodos de acceso

9.1.3 Los requisitos regulatorios o contractuales relacionados con la gestión de identidades y accesos

9.2 El Director de Seguridad de la Información (CISO), conjuntamente con el Responsable de control de acceso, será responsable de iniciar el proceso de revisión y coordinar la retroalimentación de las partes interesadas.

9.3 Podrán activarse revisiones intermedias por:

9.3.1 Incidentes de seguridad relacionados con el uso indebido de cuentas

9.3.2 Hallazgos de auditoría que pongan de manifiesto deficiencias en la gestión del ciclo de vida de las cuentas

9.3.3 Despliegue de nuevas herramientas de gestión de identidades o de gestión de accesos privilegiados (PAM)

9.4 Las actualizaciones de esta política deben:

9.4.1 Estar sujetas a control de versiones y registradas en la biblioteca documental del SGSI

9.4.2 Comunicarse a todas las partes interesadas pertinentes, incluidos responsables de departamento, operaciones de TI y Recursos Humanos

9.4.3 Estar respaldadas por materiales de formación y guías procedimentales actualizados

9.5 Todos los cambios deben ser aprobados por la Dirección Ejecutiva o el Comité Directivo de Seguridad de la Información y registrarse a efectos de auditoría.

10. Políticas relacionadas y vinculaciones

10.1 Esta política está vinculada operativamente con las siguientes políticas relacionadas del conjunto del SGSI y se sustenta en ellas:

10.1.1 P4 Política de Control de Acceso: Establece los principios y mecanismos generales de control de acceso, incluidos los controles basados en reglas y los controles de acceso basados en roles.

10.1.2 P7 Política de alta y baja: Proporciona los pasos procedimentales para iniciar y finalizar el acceso de usuarios, alineados con las acciones de Recursos Humanos.

10.1.3 P8 Política de Concienciación y Formación en Seguridad de la Información: Refuerza las responsabilidades del usuario respecto de la seguridad de las cuentas y la protección de credenciales.

10.1.4 P13 Política de clasificación y etiquetado de datos: Orienta los niveles de acceso en función de la clasificación de los datos, garantizando que los límites de privilegios se ajusten a los niveles de sensibilidad.

10.1.5 P22 Política de registro de eventos y supervisión: Garantiza que se recopilen trazas de auditoría para todas las actividades relacionadas con cuentas y que se revisen para detectar anomalías o usos no autorizados.

10.1.6 P30 Política de Respuesta a Incidentes: Regula el escalado, la contención y las acciones posteriores al incidente en casos de uso indebido de privilegios o actividad no autorizada de cuentas.

10.2 Cada una de estas políticas actúa de forma conjunta para aplicar un marco coherente de gestión de identidades y accesos basado en riesgos en toda la organización.

11. Normas y marcos de referencia

11.1 Esta política está alineada con normas de ciberseguridad y marcos regulatorios reconocidos globalmente que exigen una gestión segura de identidades, accesos y privilegios como componente esencial de la seguridad de la información de la organización.

11.2 ISO/IEC 27001:

11.2.1 La cláusula 6.1.3 exige que las organizaciones determinen, evalúen y traten los riesgos de seguridad de la información, lo que convierte la gestión de accesos y privilegios en un control formal basado en riesgos e integrado en el proceso de planificación del SGSI.

11.2.2 La cláusula 8.1, Planificación y control operacional, refuerza la implantación de salvaguardas técnicas y procedimentales que rigen el acceso de usuarios y el acceso privilegiado.

11.3 ISO/IEC 27002:2022 - controles 5.15 a 5.18:

11.3.1 El control 5.15, gestión de accesos de usuarios, respalda procesos formales para el aprovisionamiento de accesos, la autorización de acceso y la revisión periódica de los derechos de acceso.

11.3.2 El control 5.16, gestión de identidades, establece la unicidad de la identidad, los controles del ciclo de vida y la aplicación de una autenticación segura.

11.3.3 El control 5.17 garantiza que la asignación y el uso de derechos de acceso privilegiado estén estrictamente controlados, sean trazables y estén alineados con el principio de mínimo privilegio durante todo el ciclo de vida de la cuenta de usuario.

11.3.4 El control 5.18, derechos de acceso, se aborda íntegramente mediante la asignación de privilegios basada en roles, la auditoría y los requisitos de aprobación de accesos elevados.

11.4 Estos controles orientan una implantación estructurada del alta y la baja de cuentas, la separación de privilegios y el uso de la información de autenticación. La política aplica la gobernanza del ciclo de vida de la identidad, el acceso justo a tiempo y la supervisión de sesiones elevadas para impedir el uso no autorizado de los sistemas.

11.5 NIST SP 800-53 Rev. 5:

11.5.1 AC-1 (Política de control de acceso) y AC-2 (Gestión de cuentas): Se corresponden con los mandatos de la política sobre aprobaciones de acceso, asignación de roles y auditoría de cuentas de usuario.

11.5.2 AC-5 (Segregación de funciones) y AC-6 (Mínimo privilegio): Se cumplen mediante la restricción de privilegios, la alineación con las funciones del puesto y la doble aprobación para tareas de alto riesgo.

11.5.3 IA-2 a IA-5 (Identificación y autenticación): Se aplican mediante mecanismos robustos de autenticación, reglas del ciclo de vida de credenciales y requisitos de MFA.

11.5.4 AU-2, AU-12 (Registro de auditoría y análisis): Se abordan mediante grabación de sesiones y supervisión de actividad privilegiada en entornos sensibles.

11.6 RGPD de la UE (2016/679):

11.6.1 El artículo 32, Seguridad del tratamiento, exige controles de acceso y mecanismos de verificación de identidad para proteger los datos personales. Se cumple al exigir aprobaciones de cuentas, revisiones de privilegios y salvaguardas robustas de autenticación.

11.6.2 El artículo 5(1)(f), Integridad y confidencialidad, garantiza que solo los usuarios autorizados con funciones legítimas accedan a los datos personales, reforzado mediante la aplicación de la gestión de cuentas.

11.6.3 El considerando 39 exige limitaciones claras de acceso y responsabilidad proactiva; esta política respalda la trazabilidad completa de las identidades de usuario y de las asignaciones de privilegios.

11.7 Directiva NIS2 de la UE (2022/2555):

11.7.1 El artículo 21(2)(a, d) exige que las entidades apliquen políticas de gestión de accesos y manejo seguro de credenciales y sesiones privilegiadas, respaldado por los controles de aprovisionamiento, supervisión y excepciones de esta política.

11.7.2 El artículo 21(3) promueve la disciplina de acceso y una sólida garantía de identidad en sectores críticos, cumplido mediante el uso de identificadores únicos, control de acceso basado en roles (RBAC) y acceso elevado restringido temporalmente.

11.8 DORA de la UE (2022/2554):

11.8.1 El artículo 5, gobierno y control de las TIC, exige procesos formalizados para la gestión de usuarios TIC, cubiertos mediante el aprovisionamiento, la desactivación y la gestión de excepciones documentados.

11.8.2 El artículo 9, gestión del riesgo de las TIC, orienta a las organizaciones a proteger los sistemas mediante restricciones de acceso y supervisión, abordado a través de MFA, registro de accesos privilegiados y revisiones centralizadas.

11.9 COBIT 2019:

11.9.1 DSS01 - Operaciones gestionadas: Promueve la aplicación de controles operativos estandarizados, incluida la gestión del ciclo de vida de las cuentas de usuario y la documentación de accesos.

11.9.2 DSS05 - Gestionar los servicios de seguridad: Refleja la administración segura de privilegios de usuarios y sistemas, apoyando la mitigación del riesgo mediante mínimo privilegio y validación de la pista de auditoría.

11.9.3 APO13 - Seguridad gestionada: Exige gobernanza del acceso sobre los activos digitales, cumplida mediante prácticas formalizadas de autorización de cuentas y roles con revisiones periódicas obligatorias.