					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P04					Título del documento: **Política de Control de Acceso**							
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 normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 5.15, 5.17, 5.18	Gestión del acceso lógico y físico
ISO/IEC 27002:2022	Controles 8.2, 8.3	Acceso basado en roles y gestión de identidades
NIST SP 800-53 Rev. 5	AC-1 a AC-20, IA-1 a IA-8	Controles de cuentas y acceso, identidad y autenticación
RGPD de la UE	Artículos 5(1)(f), 32(1)(b); considerando 39	Protección y minimización de datos
Directiva NIS2 de la UE	Artículo 21(2)(c–e)	Control de acceso, autenticación de usuarios y protección de activos
DORA de la UE	Artículos 6, 9(2)	Acceso de usuarios a las TIC y control reforzado de terceros
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Incorporación, operaciones, supervisión y cumplimiento

1. Propósito

1.1 Esta política establece los principios, las responsabilidades y los requisitos de control obligatorios para gestionar el acceso a los sistemas de información, las aplicaciones, las instalaciones físicas y los activos de información en toda la organización.

1.2 Garantiza que el acceso se conceda en función de las necesidades del negocio, las funciones del puesto y la exposición al riesgo, aplicando principios como el mínimo privilegio, la necesidad de conocer y la segregación de funciones.

1.3 La política respalda la implementación de la cláusula 5.15 de ISO/IEC 27001:2022 y de los controles relacionados que regulan el acceso lógico y físico, la autenticación de usuarios y la gestión del ciclo de vida de los accesos.

1.4 Esta política sustenta la protección de los recursos digitales y físicos frente al acceso no autorizado, el uso indebido o la puesta en riesgo de su seguridad.

2. Alcance

2.1 Esta política se aplica a todos los usuarios, sistemas e instalaciones incluidos en el alcance del SGSI, entre ellos:

2.1.1 Empleados, contratistas, proveedores y personal temporal

2.1.2 Infraestructura local, sistemas alojados en la nube y entornos híbridos

2.1.3 Todos los activos corporativos: hardware, software, datos y áreas físicas seguras

2.1.4 Acceso lógico (p. ej., sistemas, redes, aplicaciones, API) y acceso físico (p. ej., edificios, centros de datos)

2.2 Regula el acceso durante todo el ciclo de vida de la identidad y de la interacción con los recursos, desde la incorporación y el aprovisionamiento hasta los cambios de puesto y la baja.

2.3 La política también cubre los contextos de dispositivos personales para uso laboral (BYOD) y acceso remoto, garantizando que los controles sean coherentes en todas las ubicaciones y modelos de propiedad de los dispositivos.

3. Objetivos

3.1 Implementar controles de acceso seguros y basados en roles que respalden la integridad operativa y el cumplimiento normativo.

3.2 Garantizar que los derechos de acceso se aprueben, supervisen y revoquen adecuadamente y de forma oportuna.

3.3 Prevenir el acceso no autorizado, la elevación de privilegios y la persistencia de derechos de acceso obsoletos.

3.4 Respaldar los principios de confianza cero denegando el acceso por defecto, salvo aprobación y justificación expresas.

3.5 Proporcionar garantías a auditores y partes interesadas mediante revisiones automatizadas de acceso basadas en evidencia y la aplicación de políticas.

3.6 Integrar el control de acceso en los procesos de la organización, los eventos del ciclo de vida de RR. HH. y las arquitecturas técnicas.

4. Funciones y responsabilidades

4.1 Dirección Ejecutiva

4.1.1 Aprueba la política de control de acceso y garantiza un presupuesto y una dotación de personal adecuados para su aplicación.

4.1.2 Revisa los riesgos asociados al control de acceso durante las revisiones por la dirección y asigna la responsabilidad a nivel estratégico.

4.2 CISO / Responsable del SGSI

4.2.1 Es responsable del marco de control de acceso y garantiza su alineación con ISO/IEC 27001 y normas relacionadas.

4.2.2 Coordina la aplicación de la política, la verificación de controles y la elaboración de informes sobre métricas de control de acceso.

4.2.3 Supervisa el modelado de accesos basado en riesgos y vigila la existencia de brechas sistémicas de control.

[... 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 Desencadenantes y frecuencia de revisión

9.1.1 Esta política debe revisarse:

9.1.1.1 Anualmente, o

9.1.1.2 Tras un cambio importante en la infraestructura de TI, los requisitos normativos o la exposición al riesgo

9.1.1.3 Después de incidentes que revelen debilidades en los controles de acceso

9.1.1.4 Cuando se produzcan cambios significativos en las tecnologías de autenticación o en las plataformas de identidad

9.2 Autoridad y proceso de revisión

9.2.1 El CISO o el responsable designado del SGSI gestionará el ciclo de revisión, incorporando:

9.2.1.1 Hallazgos de auditoría interna

9.2.1.2 Resultados y métricas de revisiones de acceso

9.2.1.3 Actualizaciones legales y regulatorias

9.2.1.4 Cambios en plataformas tecnológicas

9.2.2 Todas las revisiones deben ser aprobadas por la Dirección Ejecutiva y comunicadas a todas las partes interesadas.

9.2.3 Podrá exigirse a los usuarios afectados que vuelvan a acusar recibo de la política tras actualizaciones sustanciales.

9.3 Control de versiones y documentación

9.3.1 La versión maestra se almacenará en el Repositorio Documental del SGSI con los siguientes metadatos:

9.3.1.1 Número de versión y registro de cambios

9.3.1.2 Fecha de entrada en vigor y próxima fecha de revisión

9.3.1.3 Propietario y autoridad de aprobación

9.3.1.4 Registros de distribución y acuse de recibo

9.3.2 Las versiones sustituidas deben archivarse y permanecer accesibles durante un mínimo de 3 años.

10. Políticas relacionadas y vínculos

10.1 Esta política depende funcionalmente de las siguientes y debe interpretarse junto con ellas:

10.1.1 P01 – Política de Seguridad de la Información: Define el compromiso de seguridad de la organización y las expectativas de alto nivel sobre el control de acceso.

10.1.2 P03 – Política de Uso Aceptable: Establece las condiciones de comportamiento para el acceso y la responsabilidad del usuario en el uso adecuado de los sistemas.

10.1.3 P05 – Política de Gestión de Cambios: Regula cómo deben implementarse y verificarse de forma segura los cambios en configuraciones de acceso, roles o estructuras de grupos.

10.1.4 P07 – Política de Incorporación y Baja: Rige el alta y la revocación de derechos de acceso de acuerdo con los eventos del ciclo de vida del usuario.

10.1.5 P11 – Política de Gestión de Cuentas de Usuario y Privilegios: Operativiza los controles a nivel de cuenta y complementa esta política con directrices técnicas de aplicación del acceso.

10.2 En conjunto, estas políticas proporcionan un marco de gobierno de accesos coherente y exigible en todas las unidades de negocio y tecnologías.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001:2022:

11.1.1 Cláusula 5.15 – Control de acceso: Esta política cumple el requisito de controlar el acceso a la información y a otros activos asociados con base en los requisitos del negocio y de seguridad de la información.

11.1.2 Cláusula 5.17 – Gestión de identidades y cláusula 5.18 – Información de autenticación: Se aplican operativamente mediante el aprovisionamiento de identidades, los mecanismos de autenticación y las asignaciones de privilegios.

11.1.3 Controles del anexo A 8.2 (Política de control de acceso) y 8.3 (Gestión de identidades): Proporcionan la base para los objetivos de control de esta política, incluido el acceso basado en roles, la integración con el ciclo de vida del usuario y la protección del acceso privilegiado.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 Familia AC (AC-1 a AC-20): Esta política respalda los requisitos de control de acceso de NIST para sistemas físicos y lógicos, incluida la definición de políticas (AC-1), la gestión de cuentas (AC-2) y la segregación de funciones (AC-5).

11.2.2 Familia IA (IA-1 a IA-8): Proporciona directrices para la autenticación de identidades, la protección de credenciales y la MFA.

11.2.3 AU-2, AU-12: Los requisitos de registro y auditoría aplicados en virtud de esta política respaldan la rendición de cuentas del usuario y la investigación de incidentes.

11.2.4 PE-2 a PE-6: Abordan las restricciones de acceso físico, que esta política aplica parcialmente mediante controles de credenciales físicas y permisos de acceso a edificios.

11.3 RGPD de la UE (2016/679):

11.3.1 Artículo 5(1)(f): Los datos personales deben protegerse frente al acceso no autorizado. Esta política garantiza la aplicación técnica y procedimental de ese principio.

11.3.2 Artículo 32(1)(b): Exige la implementación de controles de acceso, seudonimización y cifrado para prevenir el tratamiento no autorizado de datos personales.

11.3.3 Considerando 39: Exige la minimización del acceso a los datos personales, aplicada aquí mediante el principio de mínimo privilegio y los requisitos de justificación del acceso.

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

11.4.1 Artículo 21(2)(c–e): Esta política habilita medidas técnicas y organizativas para el control de acceso, la autenticación de usuarios y la protección de activos en entidades esenciales e importantes.

11.5 DORA de la UE (2022/2554):

11.5.1 Artículo 6: Exige políticas de gestión de riesgos de las TIC que incluyan expresamente la gestión del acceso de usuarios y los controles del ciclo de vida de la identidad. Esta política cumple dicho requisito para los sectores financiero y de servicios TIC.

11.5.2 Artículo 9(2): Esta política respalda la aplicación de controles de acceso robustos como parte de la gestión de servicios TIC de terceros y dentro del grupo.

11.6 COBIT 2019:

11.6.1 APO07 – Gestión de Recursos Humanos: Aplica controles de incorporación y baja para respaldar el gobierno de accesos.

11.6.2 BAI03 – Gestión de la Identificación y Construcción de Soluciones: Integra requisitos de control de acceso en el diseño de sistemas y en los procesos de cambio.

11.6.3 DSS01 – Gestión de Operaciones y DSS05 – Gestión de Servicios de Seguridad: Regulan la aplicación de restricciones de acceso lógico y la supervisión de incumplimientos.

11.6.4 MEA03 – Supervisar, Evaluar y Valorar el Cumplimiento: Respalda los mecanismos de auditoría y aseguramiento para validar la eficacia del control de acceso.