					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P04S					Título del documento: **Política de Control de Acceso P04S**							
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 5	
ISO/IEC 27002:2022	Controles: 5.15, 5.16, 5	
NIST SP 800-53 Rev. 5	AC-1 a AC-5	
RGPD de la UE	Artículo 32	
Directiva NIS2 de la UE	Artículo 21(2)(b)	
DORA de la UE	Artículo 9	
COBIT 2019	APO07, DSS	

1. Propósito

1.1. Esta política define cómo la organización gestiona el acceso a sistemas, datos e instalaciones para garantizar que únicamente las personas autorizadas puedan acceder a la información en función de una necesidad de negocio.

1.2. Establece reglas claras para el alta, la modificación, la supervisión y la baja de usuarios, con el fin de minimizar el riesgo de acceso no autorizado y respaldar el cumplimiento de la legislación y las normas aplicables.

1.3. La política aplica el principio de mínimo privilegio y exige que el acceso se limite al mínimo necesario para desempeñar las funciones del puesto.

2. Alcance

2.1. Esta política se aplica a todas las personas que utilizan o gestionan el acceso a los sistemas de información, redes, datos o instalaciones de la organización, entre ellas:

2.1.1. Empleados

2.1.2. Contratistas

2.1.3. Personal temporal

2.1.4. Proveedores externos de servicios de TI

2.2. Abarca el acceso a:

2.2.1. Aplicaciones corporativas, recursos compartidos de archivos y bases de datos

2.2.2. Correo electrónico, VPN y sistemas de acceso remoto

2.2.3. Servicios en la nube utilizados para fines de negocio

2.2.4. Acceso físico a instalaciones seguras, como oficinas o salas de servidores

2.3. Esta política es de obligado cumplimiento en todos los dispositivos, ya sean proporcionados por la empresa o BYOD autorizado, plataformas y ubicaciones.

3. Objetivos

3.1. Garantizar que los derechos de acceso se concedan únicamente tras una aprobación formal basada en la función y en una justificación de negocio.

3.2. Prevenir el acceso no autorizado o excesivo a datos sensibles, sistemas o infraestructura.

3.3. Definir procedimientos claros para el alta, la modificación y la baja de accesos de usuarios.

3.4. Exigir revisiones periódicas de acceso y el registro automatizado o manual para dar soporte a las auditorías.

3.5. Respaldar la aplicación técnica de las restricciones de acceso mediante configuración y supervisión.

4. Funciones y responsabilidades

4.1. Director General

4.1.1. Aprueba esta política y garantiza la disponibilidad de recursos para implantar controles de acceso eficaces.

4.1.2. Aprueba las excepciones y revisa las auditorías anuales de acceso.

4.2. Responsable de TI / Proveedor externo de TI

4.2.1. Gestiona el alta, la modificación y la baja de cuentas de usuario.

4.2.2. Mantiene un Registro de Control de Acceso con toda la actividad de altas, cambios y bajas.

4.2.3. Implanta controles de acceso basados en roles (RBAC) y aplica autenticación robusta, por ejemplo, MFA.

4.2.4. Revisa los registros de acceso para detectar actividad sospechosa e informa de las incidencias 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. Revisión anual de la política

9.1.1. El Responsable de TI debe revisar esta política anualmente. Cualquier cambio en el contexto legal, técnico u organizativo debe dar lugar a una actualización inmediata.

9.2. Desencadenantes de revisión

9.2.1. La política también debe revisarse si se produce cualquiera de las siguientes circunstancias:

9.2.2. Cambios significativos en los sistemas o migraciones a la nube

9.2.3. Cambios en funciones o en la estructura organizativa

9.2.4. Un incidente de seguridad que implique acceso no autorizado

9.2.5. Cambios regulatorios, por ejemplo actualizaciones del RGPD de la UE, la Directiva NIS2 de la UE o DORA de la UE

9.3. Documentación y comunicación de cambios

9.3.1. Las revisiones deben registrarse con historial de versiones, aprobación del Director General y comunicación a todo el personal afectado.

9.4. Accesibilidad y formación

9.4.1. Esta política debe ponerse a disposición de todo el personal, y debe impartirse la formación pertinente como parte del proceso de incorporación y, posteriormente, con periodicidad anual.

10. Políticas relacionadas y vinculaciones

10.1. Esta política debe aplicarse de forma coordinada con las siguientes políticas para pymes, a fin de garantizar la aplicación integral de prácticas seguras de acceso:

10.1.1. P3S – Política de Uso Aceptable: garantiza que los usuarios comprendan el comportamiento aceptable en relación con los accesos concedidos.

10.1.2. P5S – Política de Gestión de Cambios: garantiza que los derechos de acceso estén alineados con los cambios de sistema aprobados.

10.1.3. P7S – Política de Incorporación y Baja: define los puntos de activación para el alta y la retirada del acceso de los usuarios.

10.1.4. P17S – Política de Protección de Datos y Privacidad: garantiza que los controles de acceso estén alineados con las salvaguardas de los datos personales.

10.1.5. P30S – Política de Respuesta a Incidentes: define cómo se gestionan e investigan los incidentes relacionados con el acceso, por ejemplo uso indebido o brechas.

11. Normas y marcos de referencia

11.1. ISO/IEC 27001

11.1.1. Cláusula 5.15: exige políticas y procesos de control de acceso formalizados.

11.2. ISO/IEC 27002

11.2.1. Controles 5.15–5.17: especifican orientaciones detalladas sobre acceso basado en roles, gestión del ciclo de vida del usuario y gestión de accesos privilegiados.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 a AC-5: exigen políticas estructuradas para la gestión de accesos, incluida la autorización de cuentas, la revisión y la supervisión.

11.4. RGPD de la UE

11.4.1. Artículo 32: exige controles técnicos y organizativos, como la gestión de accesos, para garantizar la seguridad y confidencialidad de los datos.

11.5. Directiva NIS2 de la UE

11.5.1. Artículo 21(2)(b): exige control de acceso operativo y sistemas de gestión de identidades para prevenir el acceso no autorizado a los sistemas.

11.6. DORA de la UE

11.6.1. Artículo 9: hace hincapié en la gestión segura de los riesgos de las TIC, incluido un control de acceso robusto para las entidades financieras.

11.7. COBIT 2019

11.7.1. APO07: Seguridad gestionada: exige responsabilidades de acceso definidas y aplicadas.

11.7.2. DSS01: Gestionar las operaciones: incluye procedimientos para gestionar el acceso lógico y mantener entornos operativos seguros.