					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P03S					Título del documento: **Política de Uso Aceptable**							
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	Relevante para el alcance general y la implementación de la política
ISO/IEC 27002:2022	5.10, 5.11, 5	Proporciona orientación sobre requisitos y controles de uso aceptable
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Abarca el uso de sistemas y dispositivos, la supervisión y la formación de usuarios
RGPD de la UE	Artículos 5(1)(f), 32	Integridad y confidencialidad de los datos y medidas de seguridad
Directiva NIS2 de la UE	Artículo 21(2)(b)	Exige políticas adecuadas de seguridad y de uso aceptable
DORA de la UE	Artículo 9	Política de gestión de riesgos de las TIC, controles y aplicación
COBIT 2019	DSS05, BAI	Servicios de seguridad y gestión del conocimiento

1. Propósito

1.1. Esta política define el uso aceptable, responsable y seguro de los sistemas, dispositivos, acceso a Internet, correo electrónico, servicios en la nube y cualquier dispositivo de propiedad personal utilizado para fines de la organización.

1.2. Garantiza que las personas comprendan sus obligaciones al utilizar los recursos de TI de la organización, protegiendo la integridad de los datos, la privacidad y la continuidad operativa.

1.3. Esta política respalda el cumplimiento de ISO/IEC 27001:2022 mediante la aplicación de normas claras de comportamiento de los usuarios, alineadas con los requisitos legales, contractuales y regulatorios.

2. Alcance

2.1. Esta política se aplica a todas las personas que accedan a los sistemas o datos de la empresa, los gestionen o interactúen con ellos, incluidos:

2.1.1. Empleados y contratistas

2.1.2. Trabajadores temporales o becarios

2.1.3. Proveedores externos de servicios de TI

2.2. Abarca:

2.2.1. Ordenadores, teléfonos y tabletas propiedad de la empresa

2.2.2. Dispositivos de propiedad personal autorizados para uso profesional (BYOD)

2.2.3. Redes de la empresa, plataformas en la nube y servicios de software

2.2.4. Acceso a Internet, sistemas de correo electrónico, almacenamiento compartido y aplicaciones de negocio

2.3. Esta política se aplica en todos los entornos de trabajo —presencial, remoto e híbrido— y durante toda la jornada laboral.

3. Objetivos

3.1. Definir qué constituye un uso aceptable y un uso no aceptable de los sistemas de TI.

3.1.1. Reducir los riesgos de seguridad derivados del uso indebido, del acceso no autorizado o de la introducción de malware.

3.1.2. Proteger los datos de la organización, la información de clientes y la reputación de la empresa.

3.1.3. Establecer reglas exigibles y garantizar la rendición de cuentas de todos los usuarios.

3.1.4. Respaldar la supervisión y el cumplimiento para detectar incumplimientos de forma temprana y adoptar medidas correctivas.

4. Funciones y responsabilidades

4.1. Director General

4.1.1. Aprueba esta política y es responsable de garantizar que existan los recursos y la autoridad necesarios para su aplicación.

4.1.2. Revisa y autoriza cualquier excepción a esta política.

4.2. Responsable de TI o proveedor externo de TI

4.2.1. Mantiene los inventarios de software y hardware aprobados.

4.2.2. Configura los dispositivos para aplicar las reglas de uso aceptable (p. ej., filtrado de contenidos y registro de accesos).

4.2.3. Supervisa el uso para identificar posibles incumplimientos e investiga los incidentes.

4.2.4. Garantiza que los dispositivos personales (BYOD) estén autorizados y sean seguros cuando se utilicen para fines de la organización.

[... 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

9.1.1. Esta política debe ser revisada anualmente por el Responsable de TI, con aprobación final del Director General, para garantizar que siga alineada con los patrones de uso de la tecnología, los riesgos emergentes y las obligaciones de cumplimiento.

9.2. Desencadenantes de revisión extraordinaria

9.2.1. También deben realizarse revisiones en respuesta a:

9.2.2. Nuevos sistemas o tecnologías (p. ej., un nuevo servicio en la nube o una nueva plataforma de endpoints)

9.2.3. Incumplimientos significativos de la política

9.2.4. Actualizaciones de leyes o de condiciones contractuales que afecten al uso de TI

9.3. Documentación de cambios

9.3.1. Todas las actualizaciones deben registrarse en un control de versiones que incluya:

9.3.1.1. Número de versión

9.3.1.2. Fecha de revisión

9.3.1.3. Resumen de cambios

9.3.1.4. Autoridad aprobadora

9.4. Comunicación de la política

9.4.1. Las versiones revisadas de esta política deben comunicarse a todos los usuarios afectados. Los empleados deben acusar recibo y confirmar su comprensión como parte de sus obligaciones de concienciación en seguridad.

10. Políticas relacionadas y vinculaciones

10.1. Esta política funciona conjuntamente con otras políticas de la pyme para garantizar una cobertura integral de las responsabilidades de seguridad:

10.1.1. P4S – Política de Control de Acceso: Define la aplicación técnica y procedimental del uso permitido y de las restricciones de cuentas.

10.1.2. P8S – Política de Concienciación y Formación en Seguridad de la Información: Proporciona formación a los usuarios sobre los límites del uso aceptable y las obligaciones de notificación.

10.1.3. P9S – Política de Trabajo Remoto: Regula el uso de los sistemas de la empresa en entornos externos o domésticos.

10.1.4. P17S – Política de Protección de Datos y Privacidad: Aplica reglas de tratamiento de datos personales que se relacionan con la supervisión del uso aceptable y BYOD.

10.1.5. P30S – Política de Respuesta a Incidentes: Establece los procedimientos para investigar y responder al uso indebido o a incumplimientos de las condiciones de uso aceptable.

11. Normas y marcos de referencia

11.1. ISO/IEC 27001

11.1.1. Cláusula 5.10 – Exige que las organizaciones definan y apliquen el uso aceptable de los activos de información.

11.2. ISO/IEC 27002

11.2.1. Control 5.10 – Proporciona directrices sobre el uso aceptable de los sistemas, incluidos los comportamientos permitidos y prohibidos.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Aborda el control del uso de los sistemas, incluidos los dispositivos de propiedad personal.

11.3.2. AC-20 – Exige la autorización y la supervisión de sistemas externos.

11.3.3. AT-2 – Destaca la formación de los usuarios sobre prácticas de uso aceptable.

11.4. RGPD de la UE

11.4.1. Artículo 5(1)(f) – Exige la integridad y confidencialidad de los datos personales, que pueden verse comprometidas por el uso indebido por parte de los usuarios.

11.4.2. Artículo 32 – Exige la implementación de medidas técnicas y organizativas para proteger los sistemas y los datos.

11.5. Directiva NIS2 de la UE

11.5.1. Artículo 21(2)(b) – Exige políticas de seguridad adecuadas, incluidas reglas sobre uso aceptable, para mitigar las ciberamenazas.

11.6. DORA de la UE

11.6.1. Artículo 9 – Exige políticas de gestión de riesgos de las TIC, que incluyen controles de uso y mecanismos de aplicación.

11.7. COBIT 2019

11.7.1. DSS05 – Gestionar los servicios de seguridad: destaca el control del comportamiento de los usuarios basado en políticas.

11.7.2. BAI08 – Gestionar el conocimiento: aborda la concienciación sobre las responsabilidades de la política y la formación en uso aceptable.