					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P34S					Título del documento: **Política de dispositivos móviles y BYOD**							
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	Cláusulas 5.1, 5.2, 6.1, 6.2, 8	Requisitos generales del SGSI y controles aplicables a dispositivos móviles y BYOD
ISO/IEC 27002:2022	Controles 5.10–5.13	Controles detallados para dispositivos móviles, BYOD y acceso remoto
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Controles aplicables a dispositivos, soportes y configuración
RGPD de la UE	Artículos 5(1)(f)	Protección de datos personales y de terminales móviles
Directiva NIS2 de la UE	Artículo 21(2)(d)	Protección de dispositivos críticos para las operaciones de la organización, incluido BYOD
DORA de la UE	Artículos 9, 10	Riesgo de las TIC y continuidad para terminales móviles
COBIT 2019	APO13, DSS01, DSS05	Gobierno de TI, operaciones y controles de los servicios de seguridad

1. Propósito

1.1. Esta política establece los requisitos de seguridad obligatorios para el uso de dispositivos móviles, incluidos teléfonos inteligentes, tabletas y portátiles, al acceder a la información, los sistemas o los servicios de la empresa.

1.2. También regula el uso de dispositivos personales para el trabajo (BYOD) con el fin de garantizar la protección de los datos de clientes y de la organización, con independencia de la titularidad del dispositivo.

1.3. La política aplica protecciones coherentes al acceso móvil, contribuye al cumplimiento de los objetivos de certificación ISO/IEC 27001 y previene la pérdida de datos o el compromiso derivados de terminales móviles perdidos, robados o utilizados de forma indebida.

1.4. Garantiza la aplicación de salvaguardas técnicas y procedimentales al uso móvil en pymes sin personal de TI dedicado, incluidos los entornos de trabajo remoto y los servicios en la nube.

2. Alcance

2.1. Esta política se aplica a todos los empleados, contratistas, becarios y proveedores de servicios que:

2.1.1. Utilicen un dispositivo móvil para acceder, tratar o almacenar datos o sistemas de la empresa.

2.1.2. Se conecten a servicios de la empresa, incluidos el correo electrónico, las carpetas compartidas, las aplicaciones en la nube o los sistemas internos a través de VPN.

2.2. Cubre:

2.2.1. Todos los dispositivos móviles: teléfonos inteligentes, tabletas y portátiles, ya sean propiedad de la empresa o dispositivos personales BYOD.

2.2.2. Todos los sistemas operativos (p. ej., iOS, Android, Windows, macOS).

2.2.3. Todas las ubicaciones (oficina, domicilio, remoto, espacios públicos).

2.3. La política se aplica en todos los entornos de trabajo y debe cumplirse con independencia de la titularidad del dispositivo.

3. Objetivos

3.1. Prevenir la pérdida de datos: garantizar que el uso móvil no exponga datos sensibles de la empresa o de clientes a accesos no autorizados, robo o uso indebido.

3.2. Definir reglas claras para BYOD: establecer condiciones exigibles para el uso de dispositivos personales con fines profesionales, garantizando salvaguardas jurídicas y técnicas.

3.3. Respaldar el cumplimiento normativo: cumplir los requisitos de ISO/IEC 27001, del RGPD, de la Directiva NIS2 y otras obligaciones legales mediante prácticas exigibles de seguridad móvil.

3.4. Minimizar el riesgo operativo: reducir la probabilidad de interrupciones operativas causadas por el uso indebido, el compromiso o el fallo de dispositivos móviles.

3.5. Mantener la confianza de los clientes: demostrar a clientes y socios que sus datos siguen protegidos incluso cuando se accede a ellos desde dispositivos móviles o personales.

4. Funciones y responsabilidades

4.1. Director General (DG):

4.1.1. Asume la responsabilidad de esta política.

4.1.2. Aprueba todo uso de acceso móvil y BYOD a los sistemas de la empresa.

4.1.3. Garantiza que los acuerdos de BYOD se firmen, conserven y supervisen.

4.1.4. Verifica que los proveedores externos de servicios de TI apliquen las protecciones móviles exigidas.

4.2. Personal designado o soporte de TI:

4.2.1. Presta apoyo en la configuración, el registro y la parametrización de los dispositivos móviles utilizados para el trabajo.

4.2.2. Aplica controles de acceso relacionados con el uso móvil, restricciones de aplicaciones y políticas de supervisión.

4.2.3. Da soporte a la respuesta ante incidentes relacionados con dispositivos móviles, incluidos los dispositivos perdidos, robados o comprometidos.

[... 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. El Director General (DG) debe revisar esta política al menos una vez cada 12 meses.

9.1.2. La revisión debe verificar la alineación continuada con los requisitos de ISO/IEC 27001, la evolución de las tecnologías móviles y los cambios en las operaciones de la organización.

9.1.3. Las actualizaciones también deben tener en cuenta incidentes recientes, resultados de auditoría o novedades regulatorias (p. ej., RGPD, Directiva NIS2, DORA).

9.2. Eventos desencadenantes para revisión intermedia

9.2.1. Esta política debe actualizarse de inmediato si se produce cualquiera de los siguientes supuestos:

9.2.1.1. Incidente grave de seguridad móvil (p. ej., brecha de seguridad a través de un dispositivo perdido o comprometido).

9.2.1.2. Cambio en las plataformas compatibles o en las herramientas de gestión móvil.

9.2.1.3. Cambio legal o regulatorio que afecte al uso de dispositivos personales o a la protección de datos.

9.2.1.4. Incorporación de nuevas aplicaciones, servicios o herramientas de terceros utilizadas en dispositivos móviles.

9.3. Documentación de cambios

9.3.1. Todas las revisiones y actualizaciones deben documentarse, incluida la fecha de revisión, los cambios realizados y la aprobación del Director General.

9.3.2. Debe conservarse un historial de control de versiones con fines de auditoría.

9.4. Comunicación y acceso

9.4.1. El Director General debe garantizar que todos los usuarios (empleados, contratistas y terceros) sean informados de los cambios.

9.4.2. Las versiones actualizadas deben estar fácilmente accesibles, por ejemplo, en carpetas compartidas o plataformas internas.

10. Políticas relacionadas e interrelaciones

10.1. Esta política forma parte del conjunto general de políticas de seguridad de la información de la pyme y debe implantarse junto con las siguientes:

10.1.1. P4S – Política de control de acceso: define los requisitos para gestionar el acceso seguro a los sistemas, incluidos aquellos a los que se accede mediante dispositivos móviles. Aplica higiene de contraseñas y control de sesiones.

10.1.2. P8S – Política de concienciación y formación en seguridad de la información: garantiza que los usuarios reciban formación sobre el uso seguro de dispositivos móviles, la notificación de incidentes y las condiciones de BYOD.

10.1.3. P17S – Política de protección de datos y privacidad: establece el tratamiento conforme al RGPD de los datos personales y de la empresa en plataformas móviles, especialmente cuando se utilizan dispositivos personales para el trabajo.

10.1.4. P9S – Política de trabajo remoto: se alinea con los requisitos de uso móvil cuando se trabaja fuera de las instalaciones o desde casa, incluido el uso de dispositivos y las salvaguardas de acceso a la red.

10.1.5. P30S – Política de respuesta a incidentes: proporciona el marco de respuesta para incidentes relacionados con dispositivos móviles, incluidos los dispositivos comprometidos o perdidos.

10.2. Estas políticas relacionadas funcionan conjuntamente para constituir un conjunto completo de controles para la seguridad de dispositivos móviles en pymes sin personal de TI dedicado, garantizando aplicabilidad, transparencia y preparación para la certificación.

11. Normas y marcos de referencia

11.1. Esta política respalda la alineación plena con las siguientes normas de seguridad y cumplimiento:

11.2. ISO/IEC 27001:

11.2.1. Cláusula 5.1 – Liderazgo y compromiso: garantiza la supervisión de la dirección y la asunción de responsabilidades sobre el acceso móvil y BYOD.

11.2.2. Cláusula 6.1 – Acciones para abordar riesgos: exige que los riesgos de seguridad móvil sean evaluados y tratados.

11.2.3. Cláusula 8.1 – Planificación y control operacional: exige procedimientos coherentes de acceso móvil para proteger los datos de la organización.

11.3. ISO/IEC 27002:

11.3.1. Controles 5.10 (uso de dispositivos móviles), 5.11 (teletrabajo), 5.12 (acceso remoto) y 5.13 (BYOD): proporcionan directrices de implantación para gestionar los riesgos de los dispositivos en el contexto de una pequeña empresa.

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Control de acceso para dispositivos móviles: exige ajustes de configuración de seguridad para el uso móvil autorizado.

11.4.2. AC-20 – Uso de sistemas externos: regula los riesgos de BYOD y acceso remoto.

11.4.3. CM-6 – Ajustes de configuración: aplica configuraciones seguras por defecto y personalizadas en plataformas móviles.

11.4.4. MP-7 – Uso de soportes: aborda el uso adecuado y las restricciones para el almacenamiento móvil y el acceso a datos.

11.5. RGPD de la UE (2016/679):

11.5.1. Artículo 5(1)(f) – Integridad y confidencialidad: exige la protección de los datos mediante una seguridad adecuada de los datos personales, especialmente en plataformas móviles.

11.5.2. Artículo 32 – Seguridad del tratamiento: obliga al uso de medidas técnicas y organizativas apropiadas para proteger los datos accedidos o almacenados en dispositivos móviles.

11.6. Directiva NIS2 de la UE (2022/2555):

11.6.1. Artículo 21(2)(d) – Medidas de seguridad de los dispositivos: exige controles de seguridad para el hardware y software utilizados para acceder a sistemas críticos para las operaciones de la organización, incluidos los dispositivos personales.

11.7. DORA de la UE (2022/2554):

11.7.1. Artículo 9 – Marco de gestión del riesgo de las TIC: exige la protección de terminales móviles utilizados para comunicaciones críticas de la organización y servicios en la nube.

11.7.2. Artículo 10 – Continuidad del negocio de las TIC: exige mantener un acceso seguro y continuado a los sistemas de la organización incluso durante interrupciones o trabajo remoto.

11.8. COBIT 2019:

11.8.1. APO13 – Gestionar la seguridad: exige que la organización aplique políticas de movilidad y BYOD alineadas con el riesgo empresarial.

11.8.2. DSS01 – Gestionar las operaciones: garantiza la implantación técnica de mecanismos de acceso seguro.

11.8.3. DSS05 – Gestionar los servicios de seguridad: regula la participación de terceros en el mantenimiento de entornos móviles seguros y la coordinación de la respuesta a incidentes.