					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P34					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	5.2, 6.1, 7.5, 8	Aplica controles de seguridad y requisitos de cumplimiento
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Proporciona controles detallados para la gestión de dispositivos móviles
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Control de acceso, acceso remoto, configuración y requisitos de seguridad para entornos móviles
RGPD de la UE	5(1)(f), 25, 32	Requisitos obligatorios de privacidad, cifrado de datos y seguridad del tratamiento
Directiva NIS2 de la UE	21(2)(d)	Medidas técnicas y organizativas de protección para el acceso móvil
DORA de la UE	9, 10	Gestión del riesgo de las TIC y requisitos de seguridad para entornos móviles
COBIT 2019	APO13.02, DSS01.04, BAI09	Planes de seguridad de la información, configuración de activos y controles para entornos móviles

1. Propósito

1.1 Esta política establece los requisitos de seguridad, cumplimiento y operación para el uso de dispositivos móviles y dispositivos personales (Bring Your Own Device, BYOD) al acceder a los sistemas, aplicaciones o datos de la organización.

1.2 Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información de la empresa a la que se accede o que se trata mediante endpoints móviles, incluidos teléfonos inteligentes, tabletas, portátiles y dispositivos híbridos.

1.3 Asimismo, establece la aplicación de los controles técnicos y procedimentales necesarios para mitigar riesgos como la fuga de datos, el acceso no autorizado, la pérdida o robo de dispositivos y el compromiso de aplicaciones móviles.

1.4 Esta política respalda el cumplimiento normativo y contractual, al tiempo que permite una productividad móvil segura para empleados, contratistas y terceros autorizados.

2. Alcance

2.1 Esta política se aplica a todo el personal, incluidos empleados, contratistas, becarios y proveedores de servicios externos, que utilicen dispositivos móviles para acceder a datos, sistemas, aplicaciones o plataformas de comunicación de la empresa.

2.2 Abarca todos los dispositivos de computación móvil, incluidos, entre otros:

2.2.1 Teléfonos inteligentes y tabletas (iOS, Android, etc.)

2.2.2 Portátiles y ultrabooks (Windows, macOS, Linux)

2.2.3 Dispositivos wearables y dispositivos inteligentes híbridos con capacidad de sincronización de datos

2.3 Se aplica con independencia de si el dispositivo es propiedad de la empresa o de propiedad personal en virtud de un acuerdo BYOD.

2.4 La política abarca todos los vectores de acceso, incluidos VPN, escritorios virtuales, aplicaciones en la nube, correo electrónico, plataformas de colaboración (p. ej., SharePoint, Teams) y herramientas de sincronización de archivos (p. ej., OneDrive, Dropbox, si están autorizadas).

2.5 Incluye su uso en trabajo remoto, en las instalaciones, durante viajes o en modalidades de trabajo híbrido.

3. Objetivos

3.1 Reducir el riesgo de compromiso, fuga o pérdida de datos derivado del uso inseguro de dispositivos móviles.

3.2 Aplicar controles de seguridad consistentes y exigibles en todos los endpoints móviles, con independencia del modelo de propiedad (corporativo o BYOD).

3.3 Garantizar que el uso de dispositivos móviles cumpla con ISO/IEC 27001 y otros marcos regulatorios aplicables en materia de privacidad, protección de datos y ciberseguridad.

3.4 Facilitar la integración segura de los dispositivos móviles en los flujos operativos, de comunicación y de colaboración de la organización.

3.5 Establecer responsabilidades y procesos claramente definidos para la gestión de dispositivos móviles (MDM), incluida la inscripción, el borrado remoto, el cifrado, la autenticación y la supervisión.

3.6 Proteger los derechos de privacidad de las personas que utilicen sus propios dispositivos, salvaguardando al mismo tiempo la información sensible de la organización.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO) / Responsable de Seguridad de la Información

4.1.1 Define la política y los estándares técnicos para el uso de dispositivos móviles y BYOD.

4.1.2 Supervisa el cumplimiento, la respuesta a incidentes y la gestión de excepciones relativas a los controles de dispositivos móviles.

4.1.3 Coordina con los equipos jurídicos y de recursos humanos para garantizar una aplicación jurídicamente sólida y alineada con la organización.

4.2 Administrador de Tecnologías de la Información (TI) / Administrador de MDM

4.2.1 Gestiona el aprovisionamiento de accesos, la inscripción y la configuración de dispositivos móviles mediante soluciones MDM.

4.2.2 Aplica controles a nivel de dispositivo (p. ej., cifrado, PIN, controles de aplicaciones).

4.2.3 Ejecuta el borrado remoto, el bloqueo del dispositivo y la revocación de acceso cuando sea necesario.

[... 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 debe revisarse al menos una vez al año por el Director de Seguridad de la Información o el Responsable de Seguridad de la Información designado para asegurar su alineación con:

9.1.1 Cambios en plataformas de sistemas operativos móviles, tecnologías MDM o estándares de autenticación

9.1.2 Cambios regulatorios o contractuales que afecten a la protección de datos móviles (p. ej., RGPD de la UE, DORA de la UE, Directiva NIS2 de la UE)

9.1.3 Revisiones de los conjuntos de controles de ISO/IEC 27001:2022, ISO/IEC 27002:2022 o NIST SP 800-53 Rev.5

9.1.4 Retroalimentación de los usuarios procedente de auditorías, revisiones posteriores a incidentes o notificaciones de empleados

9.2 Podrán activarse revisiones intermedias por:

9.2.1 Incidentes de seguridad que involucren dispositivos móviles o plataformas BYOD

9.2.2 Notificación del proveedor sobre vulnerabilidades de alto riesgo en plataformas soportadas

9.2.3 Introducción de nuevas aplicaciones móviles o plataformas de colaboración utilizadas para las operaciones de la organización

9.3 Las actualizaciones de la política deben:

9.3.1 Documentarse en el historial de versiones de la política

9.3.2 Comunicarse a todo el personal y a los contratistas afectados

9.3.3 Confirmarse nuevamente mediante un acuse de recibo actualizado para todos los usuarios de BYOD

9.4 Todas las revisiones y modificaciones deben ser aprobadas formalmente por la alta dirección y registradas en el Registro de Cambios de Políticas.

10. Políticas relacionadas e interdependencias

10.1 Esta política es interdependiente con varias políticas clave del marco del SGSI de la organización. Entre las principales interrelaciones se incluyen:

10.1.1 P1 – Política de Seguridad de la Información: establece los principios generales de gobernanza para todos los controles de seguridad de la información, incluidos los que rigen el uso de dispositivos móviles.

10.1.2 P3 – Política de Uso Aceptable: define los comportamientos permitidos y las restricciones relativas al uso de la tecnología, que se aplican directamente al acceso móvil y BYOD.

10.1.3 P9 – Política de Trabajo Remoto: aborda obligaciones de seguridad adicionales para entornos de trabajo móvil y complementa los controles específicos de movilidad definidos en esta política.

10.1.4 P13 – Política de Clasificación y Etiquetado de Datos: regula cómo deben manejarse los datos en dispositivos móviles según su nivel de clasificación, afectando al almacenamiento, la transferencia y la aplicación del cifrado.

10.1.5 P22 – Política de Registro y Supervisión: respalda la recopilación y revisión de registros de acceso móvil para detectar anomalías o incumplimientos.

10.1.6 P30 – Política de Respuesta a Incidentes: regula cómo se gestionan y escalan los incidentes relacionados con dispositivos móviles (p. ej., pérdida de dispositivos, acceso no autorizado).

10.1.7 P33 – Política de Supervisión de Auditoría y Cumplimiento: proporciona la base para comprobaciones periódicas del cumplimiento de la seguridad móvil, incluida la adhesión a la política de BYOD.

11. Normas y marcos de referencia

11.1 Esta política está alineada con marcos de ciberseguridad reconocidos internacionalmente y con obligaciones legales para garantizar el uso seguro de dispositivos móviles y dispositivos personales (BYOD) en entornos empresariales.

11.2 ISO/IEC 27001:

11.2.1 Cláusula 5.10 – Uso aceptable de la información y de los activos: exige controles para el uso responsable de los activos corporativos, incluidos los dispositivos móviles.

11.2.2 Cláusula 5.11 – Trabajo remoto: regula las prácticas seguras al acceder a sistemas desde fuera de las instalaciones de la empresa.

11.2.3 Cláusula 5.12 – Uso de dispositivos móviles: exige controles basados en riesgos para endpoints móviles y configuraciones BYOD.

11.2.4 Cláusula 5.13 – Transferencia de información: establece la protección de la información transferida a través de canales móviles.

11.3 ISO/IEC 27002:2022 – controles 5.10 a 5.13:

11.3.1 Los controles del Anexo A 5.10 a 5.13 especifican cómo debe aplicarse el acceso móvil, el cifrado, la supervisión y la mitigación de pérdidas dentro de un Sistema de Gestión de la Seguridad de la Información (SGSI). Estos controles proporcionan una guía de implantación detallada para proteger endpoints móviles, aplicar la contenerización, supervisar la integridad de los dispositivos y garantizar configuraciones compatibles con la privacidad para el uso de BYOD.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Control de acceso para dispositivos móviles: define protecciones de referencia, incluido el cifrado, la autenticación y la aplicación de MDM.

11.4.2 AC-17 – Acceso remoto: exige autenticación segura y protecciones de sesión para usuarios móviles remotos.

11.4.3 CM-7 – Funcionalidad mínima: respalda la eliminación de aplicaciones y funcionalidades innecesarias de los endpoints móviles para reducir el riesgo.

11.4.4 MP-5 – Protección del transporte de soportes: regula la transmisión segura de datos desde sistemas móviles a destinos externos o en la nube.

11.4.5 SC-12 – Establecimiento de claves criptográficas: exige el uso de protocolos criptográficos seguros para la comunicación y el almacenamiento en movilidad.

11.5 RGPD de la UE (2016/679):

11.5.1 Artículo 5(1)(f) – Integridad y confidencialidad: exige a las organizaciones proteger los datos personales en dispositivos móviles frente a accesos no autorizados o ilícitos.

11.5.2 Artículo 25 – Protección de datos desde el diseño y por defecto: exige que la privacidad esté integrada en los procesos de BYOD y MDM.

11.5.3 Artículo 32 – Seguridad del tratamiento: exige controles basados en riesgos (p. ej., cifrado, autenticación, control de acceso) para datos personales en plataformas móviles.

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

11.6.1 Artículo 21(2)(d): exige que el acceso móvil a sistemas e información críticos esté protegido mediante medidas técnicas y organizativas apropiadas, como control del endpoint, cifrado y supervisión.

11.7 DORA de la UE (2022/2554):

11.7.1 Artículo 9 – Marco de gestión del riesgo de las TIC: exige que las entidades del sector financiero mitiguen los riesgos del acceso móvil y remoto como parte de la resiliencia operativa.

11.7.2 Artículo 10 – Requisitos de seguridad de los sistemas TIC: exige una arquitectura móvil segura, supervisión y mecanismos de respuesta frente a ciberamenazas originadas en dispositivos móviles.

11.8 COBIT 2019:

11.8.1 APO13.02 – Establecer y mantener un plan de seguridad de la información: exige que el uso de dispositivos móviles, incluido el BYOD, se integre en las estrategias de seguridad de la organización.

11.8.2 DSS01.04 – Gestionar la configuración e integridad de los activos: se aplica al control de la configuración y al despliegue seguro de dispositivos móviles.

11.8.3 BAI09.01 – Establecer y mantener controles: respalda la implantación de salvaguardas técnicas y procedimentales para operaciones móviles y remotas seguras.