POLÍTICA DE USO DE DISPOSITIVOS DIGITALES Y DESCONEXIÓN DIGITAL

Modelo práctico para empresas · Compliance laboral · Prueba lícita · Derechos digitales

Versión que es necesario adaptar a cada empresa

OBJETIVO DEL DOCUMENTO

Regular el uso de medios digitales corporativos y la desconexión digital.
Prevenir sanciones, prueba ilícita, nulidad de actuaciones y daño reputacional.
Aportar trazabilidad y seguridad jurídica a RRHH, Legal, DPO y Compliance.

Preparado por Estaire Abogados / Jesús J Martínez
Madrid · 2026

Nota de uso profesional

Este documento es un modelo base. Debe adaptarse a la actividad real de la empresa, al convenio colectivo aplicable, al sistema de trabajo, a las herramientas tecnológicas utilizadas, a la existencia de representación legal de las personas trabajadoras y a la política de protección de datos.

No debe utilizarse como plantilla cerrada. En compliance laboral, el valor jurídico no está solo en el documento, sino en su implantación, comunicación, formación, trazabilidad y revisión periódica.

CRITERIO PRÁCTICO

La empresa no solo debe poder probar los hechos.
Debe poder probarlos de forma lícita, proporcionada y respetuosa con los derechos fundamentales.

1. Marco normativo de referencia

Esta política se apoya principalmente en las siguientes normas y criterios prácticos:

Norma	Artículos	Fuente	URL
Estatuto de los Trabajadores	Arts. 18, 20.3 y 20 bis	BOE-A-2015-11430	enlace oficial
LO 3/2018	Arts. 87, 88, 89 y 90	BOE-A-2018-16673	enlace oficial
LRJS	Art. 90.2	BOE-A-2011-15936	enlace oficial
Guía AEPD	Protección de datos y relaciones laborales	AEPD	enlace oficial

La jurisprudencia constitucional y europea exige un **análisis previo de idoneidad, necesidad y proporcionalidad cuando una medida empresarial pueda afectar a intimidad, protección de datos o secreto de comunicaciones**.

2. Índice operativo del modelo

1. Ficha de implantación
2. Política interna
3. Reglas de uso de medios digitales
4. Procedimiento de acceso a correo o dispositivos
5. Desconexión digital
6. Régimen disciplinario
7. Protección de datos
8. Anexos: acuse, acta, checklist y cláusulas

3. Ficha de implantación

Cumplimentar antes de aprobar la política. Esta ficha permite demostrar que la empresa ha identificado sus herramientas, riesgos y responsables.

Empresa	[●]
CIF	[●]
Centros afectados	[●]
Convenio colectivo	[●]
RLT	[Sí / No]
DPO	[Sí / No / Externo]
Responsable RRHH	[●]
Responsable Legal/Compliance	[●]
Fecha aprobación	[●]
Fecha comunicación plantilla	[●]
Fecha formación mandos	[●]
Versión	v1.0

4. Política interna

4.1. Objeto

La presente política regula el uso de dispositivos digitales, herramientas tecnológicas y sistemas corporativos puestos a disposición de las personas trabajadoras por [NOMBRE EMPRESA].

Su finalidad es garantizar un uso profesional, seguro, proporcionado y respetuoso con los derechos fundamentales, así como establecer reglas claras sobre desconexión digital y eventuales controles empresariales.

4.2. Ámbito subjetivo

Esta política se aplica a toda persona que utilice medios digitales corporativos: plantilla, dirección, personal temporal, becarios, colaboradores, personal externo y usuarios autorizados.

Cuando exista personal externo, la empresa deberá incorporar obligaciones equivalentes en contratos mercantiles, encargos de tratamiento o normas de acceso.

4.3. Medios incluidos

Quedan incluidos ordenadores, portátiles, móviles, tablets, correo corporativo, internet, VPN, nube corporativa, CRM, ERP, aplicaciones de gestión, herramientas colaborativas, mensajería profesional, impresoras, escáneres, sistemas de acceso remoto y cualquier otro medio digital corporativo.

4.4. Principios de actuación

Toda medida de control deberá responder a una finalidad legítima y superar el triple juicio de idoneidad, necesidad y proporcionalidad.

La empresa evitará accesos masivos, indiscriminados o preventivos que no estén conectados con una necesidad real.

Las actuaciones relevantes deberán documentarse mediante acta, informe o registro interno.

4.5. Uso profesional

Los medios digitales se entregan para el desempeño de funciones laborales y deberán usarse conforme a buena fe, diligencia, confidencialidad y seguridad.

Cada persona trabajadora deberá custodiar los equipos, proteger sus credenciales y comunicar cualquier incidencia de seguridad.

4.6. Uso personal

- [Opción A] Los medios digitales tienen uso exclusivamente profesional, salvo supuestos urgentes, excepcionales y razonables.

- [Opción B] Se permite un uso personal residual, razonable y no abusivo, siempre que no afecte al trabajo, la seguridad, la reputación o la confidencialidad de la empresa.

La empresa deberá elegir una de las dos opciones y comunicarla de forma clara.

4.7. Usos prohibidos

Queda prohibido utilizar medios corporativos para actividades ilícitas, discriminatorias, ofensivas, de acoso, extracción no autorizada de información, descarga de software no autorizado, cesión de contraseñas, envío de documentación empresarial a cuentas personales o uso de herramientas no aprobadas.

También queda prohibido cualquier uso que comprometa datos personales, secretos empresariales, seguridad informática o reputación corporativa.

4.8. Correo electrónico corporativo

El correo corporativo es una herramienta profesional. Debe emplearse con lenguaje adecuado, finalidad laboral y respeto a confidencialidad y protección de datos.

La empresa podrá acceder al correo corporativo cuando exista finalidad legítima: continuidad del servicio, ausencia prolongada, incidente de seguridad, investigación interna, cumplimiento normativo o indicios de incumplimiento laboral.

El acceso deberá ser limitado, trazable y proporcionado.

4.9. Internet y navegación

La navegación desde redes o dispositivos corporativos deberá ser compatible con las funciones laborales.

La empresa podrá aplicar medidas de seguridad, filtrado, registro técnico de accesos y bloqueo de páginas cuando resulte necesario para proteger sistemas, datos o productividad, siempre de forma proporcionada.

4.10. Mensajería profesional

Las herramientas de mensajería profesional deberán utilizarse para comunicaciones laborales, evitando grupos informales que sustituyan canales oficiales.

No deberán usarse WhatsApp personal u otras aplicaciones privadas para instrucciones ordinarias, salvo que la empresa haya aprobado una política específica.

4.11. Dispositivos personales

Como regla general, la empresa no exigirá el uso de dispositivos personales para fines profesionales.

Si se permite BYOD, deberá existir autorización expresa, separación entre entorno personal y profesional, medidas de seguridad y reglas claras sobre acceso, conservación y borrado de información corporativa.

4.12. Teletrabajo y trabajo híbrido

En teletrabajo o trabajo híbrido se aplicarán las mismas reglas de seguridad, uso profesional, confidencialidad y desconexión digital.

El control empresarial no podrá invadir el domicilio ni la esfera privada de la persona trabajadora.

4.13. Geolocalización

La geolocalización solo se utilizará cuando sea necesaria para la prestación de servicios, seguridad, rutas, vehículos o protección de bienes.

La plantilla será informada previamente de la finalidad, datos tratados, horario de activación, destinatarios, conservación y derechos.

4.14. Videovigilancia y grabación de sonido

La videovigilancia deberá respetar información previa, finalidad legítima, proporcionalidad y zonas excluidas por intimidad.

La grabación de sonido será excepcional y exigirá justificación reforzada.

Las cámaras ocultas solo podrán valorarse en supuestos excepcionales con indicios graves, alcance limitado y ausencia de alternativa menos invasiva.

4.15. Desconexión digital

La empresa reconoce el derecho de las personas trabajadoras a no atender comunicaciones profesionales fuera de su jornada, vacaciones, permisos, descansos o situaciones de incapacidad temporal.

Los mandos deberán evitar correos, llamadas, mensajes o reuniones fuera de jornada, salvo urgencia real y justificada.

Se recomienda usar envío diferido de correos y fijar franjas ordinarias de comunicación.

4.16. Urgencias

Se entenderá por urgencia una situación excepcional que pueda generar daño grave a personas, sistemas, clientes, seguridad, continuidad del servicio o cumplimiento legal inmediato.

La urgencia no puede convertirse en una práctica ordinaria de gestión.

4.17. Formación

La empresa comunicará esta política a toda la plantilla y formará especialmente a mandos, RRHH, IT, Legal, DPO y Compliance.

La formación deberá incluir prueba lícita, desconexión, protección de datos, ciberseguridad y límites de control empresarial.

4.18. Régimen disciplinario

El incumplimiento de esta política podrá dar lugar a medidas disciplinarias conforme al Estatuto de los Trabajadores, convenio colectivo y normativa interna.

Antes de sancionar, la empresa valorará gravedad, intencionalidad, reiteración, daño, proporcionalidad, tolerancia previa, prescripción y prueba disponible.

4.19. Protección de datos

Los tratamientos derivados de esta política se realizarán conforme al RGPD y la LO 3/2018.

La empresa informará sobre responsable, finalidad, base jurídica, datos tratados, destinatarios, conservación, derechos y posibilidad de reclamar ante la AEPD.

4.20. Revisión

Esta política será revisada cuando cambie la normativa, se incorporen nuevas herramientas, existan incidentes relevantes o lo recomienden RRHH, Legal, DPO, Compliance o RLT.

5. Procedimiento de acceso a correo o dispositivo corporativo

Este **procedimiento debe activarse antes de acceder a correos, dispositivos, nubes corporativas o herramientas digitales de una persona trabajadora**.

REGLA DE ORO

No acceder primero y justificar después.
Primero se documenta la finalidad, la necesidad, el alcance y la medida menos invasiva.

Se debe recoger por escrito al menos la siguiente información:

- Identificar la finalidad concreta del acceso.
- Verificar la existencia de política comunicada.
- Delimitar hechos o indicios.
- Valorar medida menos invasiva.
- Definir periodo temporal.
- Definir palabras clave o carpetas.
- Autorizar por persona competente.
- Intervenir con RRHH, Legal, DPO, Compliance o IT.
- Levantar acta.
- Custodiar evidencia con acceso restringido.

6. Checklist de licitud de la prueba

Control previo	Sí/No	Evidencia
Finalidad legítima	[ ]	[●]
Información previa	[ ]	[●]
Idoneidad	[ ]	[●]
Necesidad	[ ]	[●]
Menor invasión	[ ]	[●]
Proporcionalidad	[ ]	[●]
Trazabilidad	[ ]	[●]
Custodia segura	[ ]	[●]
Acceso restringido	[ ]	[●]
Sin conflicto de interés	[ ]	[●]

Si alguna respuesta es negativa, debe revisarse la actuación antes de ejecutar el control o antes de utilizar la prueba en un procedimiento disciplinario.

ANEXO I. Acuse de recibo

D./Dña. [●], con DNI/NIE [●], declara haber recibido la Política de uso de dispositivos digitales y desconexión digital de [NOMBRE EMPRESA].

Declara conocer que los medios digitales corporativos tienen finalidad profesional, que el uso personal permitido es limitado o inexistente según la política aplicable, que la empresa puede realizar controles proporcionados y que tiene derecho a la desconexión digital.

La firma acredita recepción y conocimiento. No implica renuncia a derechos fundamentales.

Fecha: [●]

Firma persona trabajadora: _____

Firma empresa: _____

ANEXO II. Acta de acceso a correo o dispositivo

Fecha y hora	[●]
Persona afectada	[●]
Sistema revisado	[Correo / portátil / móvil / nube / CRM]
Motivo	[●]
Finalidad	[●]
Indicios	[●]
Periodo revisado	[●]
Palabras clave	[●]
Intervinientes	[RRHH / Legal / DPO / Compliance / IT]
Resultado	[●]
Evidencias conservadas	[●]
Custodia	[●]

ANEXO III. Cláusula para contrato o manual de bienvenida

La persona trabajadora declara conocer que los medios digitales facilitados por la empresa tienen finalidad profesional y se rigen por la Política de uso de dispositivos digitales y desconexión digital vigente.

La empresa podrá realizar controles proporcionados sobre dichos medios para verificar el cumplimiento de obligaciones laborales, garantizar la seguridad de los sistemas y proteger la información corporativa, siempre conforme a normativa laboral, protección de datos y derechos fundamentales.

La persona trabajadora tiene derecho a la desconexión digital en los términos previstos en la política interna, convenio colectivo y normativa aplicable.

ANEXO IV. Matriz de riesgos

Riesgo	Medida	Responsable	Evidencia
Prueba ilícita	Triple test	Legal	Acta
Sanción AEPD	Información	DPO	Cláusula
Daño reputacional	Protocolo	Compliance	Informe
Hiperconexión	Desconexión	RRHH	Política
Ciberincidente	Seguridad	IT	Registro
Despido nulo	Garantías	Legal	Expediente

Cierre práctico para la empresa

Una política digital no debe ser un documento de archivo. Debe ser una herramienta operativa para prevenir conflictos y sostener decisiones empresariales.

Para que funcione, la empresa debe comunicarla, formar a mandos, conservar acuses, actualizarla y aplicarla de forma coherente.

MENSAJE CLAVE

Tener una política no basta.
La política debe estar implantada, comunicada, documentada y aplicada con proporcionalidad.