Ribas
Artículos
Publicaciones
01/12/2025

Permitir un uso razonable del e-mail de la empresa para fines personales es la peor estrategia que se puede aplicar.

Razones para prohibir el uso personal del e-mail corporativo

Inconvenientes de permitir un uso personal razonable

Uso razonable

Permitir un uso razonable del correo electrónico de la empresa para fines personales es la peor estrategia que se puede aplicar.

En este documento se describen las razones y los argumentos jurídicos por los que es recomendable una prohibición total del uso personal de los recursos TIC corporativos, especialmente teniendo en cuenta que todos los trabajadores disponen de dispositivos móviles personales que les permiten satisfacer todas sus necesidades de comunicación y entretenimiento.

Lectura previa

Antes de ver los argumentos se recomienda leer este artículo publicado en Expansión en marzo de 2017:

https://www.expansion.com/blogs/ribas/2017/03/04/sobre-la-necesidad-de-prohibir-el-uso.html

ribas

Expectativa de intimidad

Si la empresa autoriza al trabajador a utilizar el correo electrónico corporativo o los restantes recursos TIC, el trabajador puede generar una expectativa de intimidad en dicho uso.

Sin perjuicio de las facultades de control del cumplimiento y de la integridad del dispositivo, tanto el artículo 87 de la LOPDGDD, como el artículo 20 bis del Estatuto de los Trabajadores, reconocen el derecho de los trabajadores a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador,

Mensajes personales

La autorización para un uso personal y la consiguiente expectativa de intimidad tiene como posible consecuencia jurídica la creación de un espacio personal protegido en el correo electrónico corporativo, formado por los mensajes personales enviados y los mensajes personales recibidos.

El artículo 87.2 de la LOPDGDD permite el acceso a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos. Pero, en la práctica, muchas empresas no disponen de normas claras para el uso de los dispositivos corporativos ni de protocolos de acceso adecuados.

Estado del mensaje

El Tribunal Supremo español ha interpretado que los mensajes no abiertos tienen una doble protección.

Mensajes en tránsito	Secreto de las comunicaciones
	Derecho a la intimidad
Mensajes enviados	Derecho a la intimidad
Mensajes recibidos no abiertos	Secreto de las comunicaciones
	Derecho a la intimidad
Mensajes abiertos	Derecho a la intimidad

Espacio personal protegido

La existencia autorización general para un uso personal de los recursos TIC genera la apariencia de que existe un espacio personal protegido en los sistemas corporativos si no se han establecido claramente los dispositivos o servicios en los que está prohibido dicho uso personal.

El trabajador puede entender que este espacio está fuera del control de la empresa, ya que, con la autorización del uso personal, la propia empresa puede haber quedado excluida de ese control, dando un mensaje de que el usuario tiene libertad para aplicar los recursos TIC corporativos para finalidades extralaborales.

Fórmula peligrosa

El hecho de indicar en las políticas de uso del correo electrónico que, a pesar de la autorización para un uso personal, seguirá existiendo control sobre el mismo, y que podrán realizarse inspecciones, puede resultar arriesgado, ya que implica una extensión del control laboral sobre la esfera personal del trabajador.

Además, es una técnica exigente, ya que obliga a aplicar de forma casi perfecta protocolos complejos que se ajusten al test Barbulescu y al artículo 87 de la LOPDGDD.

Cambios en los protocolos

La existencia de un espacio personal protegido, y fuera del control de la empresa, dentro de los sistemas corporativos plantea la necesidad de modificar el protocolo de actuación en muchos de estos casos:

1. Investigaciones internas.
2. Mantenimiento informático.
3. Auditorías de seguridad.
4. Gestión de incidentes de seguridad.
5. Inspecciones.
6. Obtención de evidencias de delitos.
7. Registros de los sistemas (logs).
8. Trazabilidad y control.
9. Estadísticas.
10. Data Loss Prevention (DLP).

En relación a este punto debe tenerse en cuenta el test Barbulescu y el artículo 87 de la LOPDGDD.

Mezcla de mensajes personales y corporativos

En el caso de que se deba realizar una inspección del correo electrónico a causa de una sospecha razonable de incumplimiento, deberá aplicarse una técnica que permita acceder únicamente a los mensajes corporativos, con el consiguiente riesgo de error.

El uso personal impide distinguir qué actividad se relaciona con la empresa y cuál no, entorpeciendo la trazabilidad de los datos, auditorías internas o investigaciones por compliance, seguridad y protección de datos.

Defensa procesal

La empresa puede ver perjudicada su defensa procesal, en sede penal, laboral o civil a causa de la mezcla de evidencias de origen corporativo y personal.

La parte contraria puede impugnar las pruebas por por haberse contaminado entre ellas o incluso, por haber sido ilegítimamente obtenidas, poniendo en duda también la cadena de custodia, como es habitual en estos casos.

ribas

Riesgo de querella

En el caso de realizarse una inspección del correo electrónico existe el riesgo de que el titular de la cuenta que contiene mensajes personales presente una querella por violación del secreto de las comunicaciones y del derecho a la intimidad. (Artículo 197 del Código Penal español).

ribas

Malas prácticas

El uso personal transmite un mensaje de laxitud sobre el control de activos críticos.

Esto puede derivar en otras conductas no autorizadas como compartir contraseñas, instalar software no corporativo o utilizar servicios no verificados (Shadow IT).

De acuerdo con la *teoría de las ventanas rotas*, la falta de control sobre los pequeños incumplimientos, derivada de la imposibilidad de controlar los mensajes personales, puede llevar a una percepción de ausencia de control e impunidad, que lleve al usuario a cometer infracciones más graves.

Riesgos de ciberseguridad

El uso personal incrementa el riesgo de filtraciones de información confidencial, metadatos y de datos personales, así como de malware, phishing o ransomware, ya que el trabajador puede recibir archivos maliciosos por correo electrónico al haber utilizado la dirección corporativa para registrarse en servicios no verificados.

Una gran parte de los ciberataques recibidos por las empresas tienen como vector inicial el error humano y el uso personal de los recursos TIC corporativos.

Mayor riesgo de errores humanos

El uso del mismo sistema para envío de mensajes personales y corporativos por parte de un usuario incrementa el riesgo de cometer errores, como el envío de información confidencial a personas ajenas a la empresa.

Riesgo de fuga de datos

A pesar del uso de sistemas DLP, la exigible falta de control sobre las cuentas personales puede impedir que se detecte la exfiltración de datos personales por parte de trabajadores desleales, especialmente en los periodos previos su salida de la empresa.

ribas

Responsabilidad civil y penal

Las infracciones cometidas por los trabajadores utilizando el correo electrónico de la empresa pueden generar responsabilidad civil e incluso penal para la persona jurídica, ya que el trabajador comete la infracción utilizando un nombre de dominio y una dirección IP corporativos.

ribas

Infracción del RGPD y la LOPDGDD

La existencia de mensajes personales en un tratamiento corporativo, con una finalidad corporativa, puede generar los siguientes riesgos en materia de protección de datos:

1. Incumplimiento del principio de limitación de la finalidad, ya que el tratamiento está orientado exclusivamente a mensajes corporativos.
2. Incumplimiento de las obligaciones de confidencialidad y seguridad, al permitir el envío de mensajes con contenido que escapa al control del responsable del tratamiento, a personas no relacionadas con la empresa y desde una plataforma corporativa con medidas que deberían impedirlo.
3. Incumplimiento del principio de minimización, al tratar datos que no son necesarios para cumplir la finalidad del tratamiento.
4. Incumplimiento de las obligaciones relativas a la gestión de brechas de seguridad en el caso de que su causa se haya originado en un mensaje personal sobre el que se bloqueado la trazabilidad y el acceso.
5. Incumplimiento de las obligaciones en materia de ejercicio de derechos de los remitentes o destinatarios de los mensajes personales sobre los que la empresa no tiene control.

Artículo 87.3 de la LOPDGDD

El segundo apartado del artículo 87.3 de la LOPDGDD establece que: “El acceso por el empleador al contenido de dispositivos digitales **respecto de los que haya admitido su uso con fines privados** requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores”.

De este texto se desprende el siguiente régimen:

Dispositivos digitales en los que se ha autorizado el uso personal.	Especificación de los usos autorizados.
	Garantías para preservar la intimidad de los trabajadores.
Dispositivos digitales en los que se ha prohibido el uso personal.	Las obligaciones de las dos filas anteriores no son aplicables.

Confusión de esferas y derecho a la desconexión

Permitir el uso personal del correo electrónico corporativo provoca una confusión entre la esfera laboral y la esfera personal, poniendo en peligro el derecho a la desconexión.

Por ejemplo, si un trabajador espera respuesta a un mensaje personal, consultará el correo electrónico fuera del horario laboral, y verá mensajes corporativos que podrá sentirse obligado a contestar.

Acceso a documentos personales por trabajadores despedidos

Los trabajadores despedidos, a los que se ha bloqueado el uso del ordenador y del correo electrónico pueden ejercer su derecho de acceso a sus datos, mensajes y documentos personales.

Ello exige dedicar recursos y disponer de un protocolo para atender estas peticiones, con el fin de asegurar que el acceso se limite a la información estrictamente personal y no se incumpla ninguna medida de seguridad.

ribas

Alternativa actual

Pasar una jornada laboral sin utilizar el mail corporativo para temas personales ha dejado de ser una conducta heroica, como alegaba el Tribunal Supremo en 2007, ya que el usuario dispone de su smartphone para poder enviar y recibir mensajes personales.

ribas

Conclusión

Permitir el uso personal del correo electrónico corporativo genera riesgos en materia de:

1. Responsabilidad penal.
2. Responsabilidad civil.
3. Responsabilidad administrativa.
4. Datos personales.
5. Confidencialidad.
6. Ciberseguridad.
7. Trazabilidad.
8. Cumplimiento normativo.

Una política clara de prohibición, acompañada de formación y concienciación, es la forma más eficaz de preservar los intereses legítimos de la empresa sin comprometer los derechos de los trabajadores.

Formación corporativa

Además de las normas de uso de los recursos TIC corporativos, la empresa debe ofrecer una formación adecuada a sus usuarios.

Esta formación debe contemplar cuestiones relacionadas con el cumplimiento normativo, entre las que destacan las siguientes:

- Formación básica en materia de ciberseguridad.
- Formación básica en materia de phishing.
- Formación básica en materia de protección de datos.
- Formación básica en materia de compliance.
- Formación básica en materia de ESG.
- Formación básica sobre el uso del canal de denuncias.
- Formación obligatoria para usuarios de sistemas de IA.
- Formación obligatoria para usuarios con funciones supervisión de los resultados ofrecidos por un sistema de IA.

Si deseas tener más información sobre los cursos corporativos que impartimos en Campus Ribas puedes solicitar información a xavier.ribas@ribastic.com. Te enviaremos el Plan de formación corporativa 2025-2026.

ribas

Formación individual

La gestión y prevención de los riesgos jurídicos asociados al uso de las nuevas tecnologías exige disponer de la formación adecuada.

También ofrece oportunidades laborales de especialización en funciones internas que las empresas necesitan, y nuevos perfiles profesionales, como los siguientes:

1. Curso de asesor jurídico experto en IA.
2. Curso de auditor de riesgos jurídicos de modelos y sistemas de IA.
3. Curso de Compliance Officer (impartido desde 2010 y actualizado en 2025).
4. Curso de DPO - Delegado de Protección de Datos
5. Curso de Experto en Investigaciones Internas.
6. Curso de Experto en Due Diligence de la Cadena de Suministro.
7. Curso de Experto en ESG.
8. Curso sobre la Data Act.

Si deseas tener más información sobre los cursos especializados que impartimos en Campus Ribas puedes solicitar información a xavier.ribas@ribastic.com. Te enviaremos el Plan de formación individual 2025-2026.

ribas

Datos de contacto

Nombre del despacho	Ribas
Domicilio	Diagonal 640 1C - 08017 Barcelona
Persona de contacto	Xavier Ribas
Correo electrónico	xavier.ribas@ribastic.com
Teléfono fijo	934940748
Teléfono móvil	639108413
LinkedIn	https://www.linkedin.com/in/javierribas/
Web	http://ribas.legal
Blog	http://xribas.com