

**Aspecto Legales de la Fuga de  
Información:**

**CRITERIOS JURISPRUDENCIALES DE  
EQUILIBRIO EN LA RELACIÓN  
EMPLEADOR-EMPLEADO**

Ecija... ¿Quiénes somos?

Ecija se dedica a:

- Legal
- Servicios Profesionales
- Compliance

### Reconocimientos



**Ranking Expansión 2007** -  
Top 20 en la clasificación de  
despachos españoles



**Ranking La Gaceta 2006** -  
Top 25 en la clasificación de  
los despachos españoles



**Chambers Europe 2007** -  
Hugo Écija nombrado mejor  
abogado en Derecho  
Audiovisual y de los Medios



**Chambers Global 2007**  
- Líderes del mercado  
español en TMT



**The Legal 500 2007** -  
Top Tier en IT &  
Telecommunications



**Chambers Global 2007** -  
Líderes del mercado español  
en Propiedad Intelectual



**The Legal 500 2007** - Top  
Tier en Propiedad Intelectual  
Firma recomendada en  
Inmobiliario



**European Legal Experts  
2007** - Líderes en Corporate  
& Commercial en IT &  
Telecom



**Iberian Lawyer Top 40  
under 40 Awards 2007** -  
Hugo y Álvaro Écija  
nominados entre los 40  
mejores abogados de España  
menores de 40 años

### Servicios Profesionales

Ecija es innovadora en la prestación de servicios profesionales entorno a la seguridad de la información

- Protección de Datos: Auditoría y Consultoría a empresas en su adecuación a la LOPD
- Seguridad de la Información: Consultoría integral a empresas de su gestión de Seguridad de la Información y adecuación a la ISO 27001
- Seguridad gestionada: Asesoría e implantación de sistemas para la detección de vulnerabilidades y fraude
- Firma electrónica: Prestación de servicios de consultoría a entidades de certificación, voto electrónico, factura electrónica.
- Proyectos Externos: Prestación a grandes empresas de personal informático cualificado para el desarrollo de determinados proyectos
- Compliance: Asesoría integral para el cumplimiento de normativas y de políticas: Buen Gobierno Corporativo, SOX, Basilea, Solvencia II, MiFID, ISO 27001, etc.

### Índice

- Problemática más habitual desde el punto de vista empresarial. Aspectos a considerar.
- Fundamento jurídico. Jurisprudencia más relevante.
- Soluciones. Políticas de uso de recursos informáticos.

Problemática más habitual

**RIESGOS FRENTE A LOS QUE  
HAY QUE...**

**PREVENIR CONFLICTOS**

entre el empresario y el trabajador  
derivados del uso de la tecnología  
para fines ajenos  
al desempeño del puesto de trabajo

**EVITAR INFRACCIONES  
DE LA LEGALIDAD VIGENTE**

los riesgos legales para la empresa  
del uso indebido  
de las herramientas tecnológicas

### Problemática más habitual



**El ABUSO de Mail nos produce pérdida de rendimiento y problemas en la red**

**¿Podemos tener problemas por acceder al disco duro del personal que causa baja temporal o definitiva?**



**Sabemos que hay personal que se ha instalado el Emule, y estamos preocupados**



**Queremos separar el uso profesional y el uso personal del E-mail sin crear un conflicto con los empleados**



**Buscamos monitorizar y controlar la actividad de los empleados, pero no estamos seguros de qué tecnología es adecuada a la normativa aplicable**



**Tenemos sospechas de que un empleado está cometiendo una actividad ilícita y queremos poder probar en juicio que lo está haciendo**



# ECIJA

## Aspectos Legales de la Fuga de Información

### Problemática más habitual

**No queremos permitir el uso de pendrives o teléfonos con memoria si no podemos cubrirnos frente a la pérdida de información que pueden suponer**



**Queremos que el personal esté realmente vinculado por las políticas de seguridad de la Entidad**



**¿Cuál es la responsabilidad de la empresa en caso de fuga de información cometidos por empleados?**



**Creemos que algunos de nuestros empleados están montando una empresa paralela y no estamos dispuestos a permitirlo**



### Aspectos a considerar

#### INTERNET

- Qué es utilización con fines profesionales.
- Posibilidad y límites (cuantitativos y cualitativos) del uso personal. **USO ABUSIVO**
- Monitorización y filtrado (listas blancas / listas negras).
- Servicios específicos (webmail, descargas, banca electrónica, etc.).

#### CORREO ELECTRÓNICO

- Qué es utilización con fines profesionales.
- Diferenciación email enviados – emails recibidos.
- Email filtering / screening.
- Duplicidad de cuentas: personal / profesional.
- Acceso a cuentas (**MOVILIDAD**, vacaciones, permisos, etc.).
- Acceso a cuentas tras el cese de la relación laboral.

#### MENSAJERÍA INSTANTANEA

- Diferenciación con los servicios de voz.
- Particularidades en el control de utilización.

### Aspectos a considerar

#### DISCO DURO LOCAL

- **¿Se puede guardar información "personal"?**
- **La utilización con fines personales, debilitamiento de la seguridad.**
- **Control de uso del disco duro.**
- **Procesos de cambio de equipos: formateo de disco duros locales.**

#### ORDENADORES PORTÁTILES

- **Refuerzo de la seguridad.**
- **Volcado de información hacia / desde ubicaciones seguras**
- **Inventario y control de ubicación / usuario en cada momento**

#### DISPOSITIVOS REMOVIBLES (USB, MEMORY CARDS, ETC.)

- **Determinación de usuarios autorizados**
- **Gestión de la instalación / desinstalación: control de puertos**
- **Refuerzo de la seguridad**
- **Datos personales: nuevo reglamento LOPD**

### Aspectos a considerar

#### PROPIEDAD INTELECTUAL

- **Uso de software pirata.**
- **Almacenamiento de archivos (música, películas, libros, etc.) vulnerando la Ley de Propiedad Intelectual.**
- **Intercambio de archivos en redes P2P (música, películas, libros, etc.) vulnerando la Ley de Propiedad Intelectual.**
- **Inclusive, VULNERACIÓN DE LA NORMATIVA SOBRE PROPIEDAD INDUSTRIAL**

#### TELEFONÍA FIJA Y MÓVIL

- **Control de llamadas: número de origen / destino, duración**
- **Control para facturación**
- **Servicios con grabación de llamadas: call center de contratación, contact center de atención a clientes**
- **¿Qué supone la histórica "tolerancia" en el uso de la telefonía fija?**

### Aspectos a considerar

#### **INTRANET / EXTRANET**

- **Utilización de la información corporativa (societaria, comercial, de clientes, proveedores, etc.). ¿Y LOS BLOGS?**
- **Utilización de la información sobre empleados.**
- **Publicación de información.**
- **Refuerzo de la seguridad en la utilización de Extranets.**

#### **ACCESO REMOTO**

- **Refuerzo de la seguridad.**
- **Responsabilidad por la conexión realizadas desde un entornos no seguros.**
- **Descarga de información en equipos no corporativos (p.e PC particular en el domicilio).**

#### **ACTIVIDAD SINDICAL**

- **Incidencia de comunicaciones sindicales en los sistemas de información.**
- **Puesta a disposición de medios informáticos, lógicos (cuenta de correo electrónico, tableros virtuales, carpetas de red, etc.) y físicos (hardware).**

### Fundamento jurídico

#### CONSTITUCIÓN ESPAÑOLA

- Vulneración de la intimidad del trabajador.
- Violación del secreto de las comunicaciones.
- Protección de datos personales.

#### ESTATUTO DE LOS TRABAJADORES

- Poder de dirección del empresario y control de los medios de producción.
- Dignidad e intimidad del trabajador.
- Instrumentos de vinculación a políticas internas.

#### PROTECCIÓN DE DATOS

- Cesiones o comunicaciones ilícitas de datos.
- Incumplimiento deber de secreto y confidencialidad.
- Incumplimiento medidas de seguridad.

### Jurisprudencia más relevante

- **STSJ Andalucía Febrero 2000.**- *El art. 18 ET autoriza el registro en el terminal de ordenador (el ordenador se asimila a la taquilla. El ordenador es un instrumento de trabajo propiedad de la empresa.*
- **STSJ Cataluña Julio 2000.**- *El empleador puede ejercer un control sobre la forma de utilizar los medios de la empresa, que son de su propiedad, así como sobre la propia actividad laboral del trabajador.*
- **STSJ Cataluña Julio 2002.**- *La empresa puede investigar la procedencia de emails recibidos y las direcciones remitentes, pero es una vulneración del derecho a la intimidad que las personas contratadas por la empresa averiguaran la dirección personal particular y privada del demandante.*
- **STSJ Madrid Julio 2002.**- *No cabe deducir actuación dolosa por parte del trabajador, pues la empresa toleraba un uso moderado para fines privados de los medios informáticos, concretamente del acceso a Internet. Si la empresa considera excesivo el uso privado de Internet, debió advertir al trabajador, instaurar normas de uso...*
- **ST Juzgado de lo Social nº 33 de Madrid Octubre 2002.**- *Se debe llegar a la conclusión de que la empresa cercenó el derecho fundamental a la libertad informática desde el momento en que no se informó al trabajador de la existencia de una base de datos controlando el acceso a págs. web desde su puesto de trabajo.*
- **STSJ Cataluña, Sala de lo Social Marzo 2004.**- *Despido procedente por uso de chat en el trabajo, previa información de que el uso de Internet para fines personales estaba prohibido.*
- **STC 5/11/2005.**- *El Tribunal Constitucional avala el uso del email con fines sindicales (caso CC.OO vs. BBVA) con limitaciones (no perturbar la normal actividad de la empresa; no perjudicar el uso empresarial del email; no puede implicar gravamen para la empresa – asunción de mayores costes).*

### Jurisprudencia más relevante

#### Sentencia de 28/06/2006, de la Sala de lo Social del Tribunal Supremo

La **ausencia de prohibición expresa** y específica sobre el **uso privado** de medios informáticos **debe entenderse** en el sentido de estar **autorizado**.

Considera que el **uso privado de Internet** por un plazo superior a **1,30 hrs/día** implica infringir la buena fe contractual.

**Necesidad** de configurar y **desarrollar normas de uso** de los recursos Informáticos en los que **prohibir** o, en su caso, **delimitar** el uso privado de los medios informáticos.

### Jurisprudencia más relevante

#### Sentencia de 26/09/2007, de la Sala de lo Social del Tribunal Supremo – UNIFICACIÓN DE DOCTRINA (I)

*El control del uso del ordenador facilitado al trabajador por el empresario no se regula por el artículo 18 del Estatuto de los Trabajadores, sino por el artículo **20.3 del Estatuto de los Trabajadores** (...). La primera se refiere a los límites de ese control y en esta materia el propio precepto citado remite a un **ejercicio de las facultades de vigilancia y control** que guarde "en su adopción y aplicación la **consideración debida**" a la **dignidad del trabajador**, (...).*

- Art. 20 ET = poder de control de empresario.
- Límites al art. 20 ET: finalidad de control y respeto a la dignidad de trabajadores.
- Ya no se equipara, el control del email, con el control de taquillas. No son exigibles las cautelas del art. 18 ET.

### Jurisprudencia más relevante

#### Sentencia de 26/09/2007, de la Sala de lo Social del Tribunal Supremo – UNIFICACIÓN DE DOCTRINA (II)

*En este punto es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos **usos personales moderados** de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque **tampoco convertirse en un impedimento permanente del control empresarial, porque aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio.***

- Se presume una tolerancia en el uso personal de los recursos informáticos, dentro de los límites de la buena fe contractual.
- La presunción no aplica cuando se trate de un medio empresarial y se hayan dado instrucciones sobre su uso.

### Jurisprudencia más relevante

#### Sentencia de 26/09/2007, de la Sala de lo Social del Tribunal Supremo – UNIFICACIÓN DE DOCTRINA (III)

*Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las **REGLAS DE USO DE ESOS MEDIOS** - con aplicación de prohibiciones absolutas o parciales - e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.*

- Cuando se adopten reglas de uso de los recursos informáticos, éstas prevalecerán sobre la presunción anterior.
- Cabe tanto una restricción en el uso personal de dichos medios como una prohibición absoluta.

### INFORME AEPD 391/2007: CRIBADO DEL EMAIL

SE DEBE LLEVAR A CABO UNA EVALUACIÓN CASO POR CASO, en atención a los principios de:

- **NECESIDAD:** Las medidas deben estar justificadas por el empresario en su establecimiento.
- **FINALIDAD:** Las finalidades deben ser claras, adecuadas y preestablecidas.
- **TRANSPARENCIA:** El empleado debe estar informado de la existencia de los controles y sobre qué información se guarda.
- **LEGITIMIDAD:** El control debe encuadrarse en el ámbito de la relación laboral.
- **PROPORCIONALIDAD:** Los medios que se utilicen deben ser proporcionales al riesgo que corre el empresario.
- **EXACTITUD Y CONSERVACIÓN DE LOS DATOS:** Los datos deben ser correctos, actualizados y conservarse de modo que el interesado pueda acceder con periodicidad razonable.
- **SEGURIDAD:** Cumplimiento de las medidas de seguridad aplicables en función del tipo de datos.

### Cómo solucionarlo

- **Es necesaria la elaboración y redacción de una Política Interna de Uso de las herramientas y recursos informáticos, y consecuencias legales derivadas de su incumplimiento.**
- **Establecimiento de sistemas de control en la empresa, p.e. monitorización y prevención de fugas de información (ILP).**
- **Redacción clara y transparente. Puesta en conocimiento de los trabajadores y aceptación previa de éstos.**
- **Debe evitarse su imposición de forma unilateral, debiendo ser consensuada con los trabajadores o sus representantes.**
- **Se trata de implantar un sistema regulador y preventivo de conflictos.**

### Cómo solucionarlo

- **Son normas que pueden estar vinculadas a otros procedimientos:**
  - **Clasificación de activos.**
  - **Documento de Seguridad.**
  - **SGSI.**
- **Introducción en la relación laboral:**
  - **Redacción de documento o cláusula.**
  - **Publicación en Intranet o anexo al contrato.**
  - **Mediante negociación colectiva.**
  - **Mediante negociación individual.**

Cómo solucionarlo



### Cómo solucionarlo

#### La importancia de obtener EVIDENCIAS (ELECTRÓNICAS):

- El objetivo es poder **DEFENDER LOS INTERESES** de la empresa en sede judicial (saber qué ha pasado y poder probarlo)
- Las **REGLAS PROCESALES NO CAMBIAN** porque la prueba sea electrónica
- El proceso de **GENERACIÓN** de la evidencia electrónica debe **GARANTIZAR**:
  - Integridad
  - Imposibilidad de manipulación
  - Conservación con las mismas condiciones

### CONCLUSIONES

- Tratar y prevenir los riesgos legales en los que incurre la empresa por posibles infracciones realizadas por los empleados
- Definir y establecer los mecanismos de control de la actividad laboral de los empleados cumpliendo con la legalidad
- Definir y determinar unas Políticas Internas de Uso de Herramientas y Recursos tecnológicos, contribuyendo a un ahorro de costes y un mejor clima laboral.
- Implantar la Política Interna de Uso con éxito y con el consentimiento de los Representantes de los empleados
- Formar a los responsables de la puesta en marcha.

**Gracias por su atención**

**ECIJA**  
**Plaza del Marqués de Salamanca, 3-4, planta 4**  
**28006 Madrid**  
**Tfno: 91 781 61 60**  
**Fax: 91 578 38 79**