

Actos desleales de trabajadores usando sistemas informáticos e internet*





Actos desleales de
trabajadores usando
sistemas informáticos
e internet



Sumario

1. Introducción	5
2. Objeto del estudio	6
3. Metodología	6
4. Infracciones más habituales.....	7
5. Tratamiento de las infracciones en el sistema jurídico español	8
6. Estrategia seguida por las empresas	10
7. Análisis por nivel de frecuencia	13
8. Análisis por sectores.....	15
9. Análisis por cargos.....	16
10. Análisis por motivaciones.....	17
11. Análisis por cuantía de los perjuicios.....	18
12. Evolución cronológica.....	19
13. Conclusiones.....	20
14. Medidas preventivas.....	21
15. "Checklist" de autodiagnóstico	23

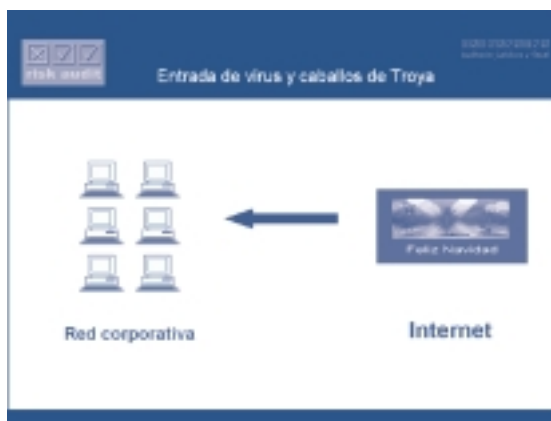
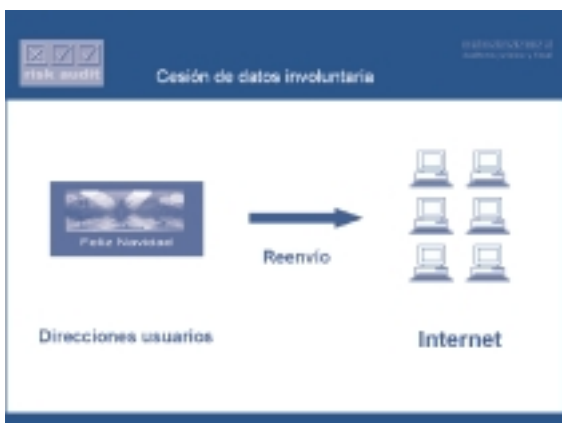
1. INTRODUCCIÓN

El uso de las nuevas tecnologías en las empresas aporta ventajas evidentes que facilitan el trabajo y la conexión permanente entre los departamentos de la empresa, así como la comunicación con clientes y proveedores.

Estos nuevos canales de acceso al exterior abren puertas a través de las cuáles la información circula velozmente, pero que también pueden ser utilizadas para enviar información confidencial fuera de la empresa.

Esta doble faceta de ventaja y riesgo que toda tecnología aporta, obliga a aplicar una serie de cautelas que permitan explotar al máximo sus beneficios y minimizar las amenazas. Como todas las tecnologías, el uso correcto o incorrecto y sus consecuencias dependen de la buena o mala fe de las personas que las utilizan.

En este estudio, se analizan los casos en los que los sistemas informáticos y la infraestructura de comunicaciones de la empresa han sido utilizados por sus trabajadores para cometer actos desleales o delitos.



El envío de una simple felicitación de Navidad por correo electrónico puede provocar la cesión a terceros de datos de otros usuarios de la empresa o la entrada de virus y caballos de Troya.

2. OBJETO DEL ESTUDIO

El objeto de este estudio es analizar los casos más habituales en los que los trabajadores utilizan los sistemas informáticos y la infraestructura de comunicaciones de la empresa en la que trabajan con el fin de cometer actos que pueden generar perjuicios económicos para la misma.

La finalidad principal es obtener conclusiones sobre:

- los tipos de infracciones que se cometen con más frecuencia,
- la estrategia seguida por las empresas,
- el porcentaje de casos a los que se llega a un acuerdo,
- los sectores más afectados,
- las motivaciones que hacen que los trabajadores actúen de esta manera,
- la cuantía de los daños y
- la evolución cronológica de las infracciones.



El uso de redes inalámbricas y de soportes informáticos miniaturizados aumenta el riesgo de extracción no autorizada de información confidencial de la empresa.

3. METODOLOGÍA

Este estudio se ha basado en el análisis de 393 casos reales que han tenido lugar en empresas españolas y que han sido protagonizados por trabajadores contratados en plantilla de la empresa afectada.

Los datos han sido recopilados mediante el análisis de sentencias, autos y procedimientos judiciales, y han sido completados mediante entrevistas a los responsables de las empresas afectadas y a través de la lectura de los dictámenes jurídicos, actas de reuniones, acuerdos transaccionales y noticias aparecidas en la prensa.

Los interlocutores de las empresas consultadas han sido los siguientes:

- Director General
- Director de Recursos Humanos.
- Director de Sistemas.
- Asesor Jurídico.

Los datos estadísticos se basan en los siguientes parámetros:

1. Muestra: 393 casos
2. Universo: Se desconoce el nivel de incidencia en el conjunto total de las empresas españolas, ya que, como podemos ver en el punto 6 de este estudio, una gran parte de las empresas afectadas por este tipo de acciones prefieren llegar a un acuerdo amistoso y no divulgar los hechos.
3. Periodo analizado: Del 1 de enero de 2001 al 31 de diciembre de 2003

4. INFRACCIONES MÁS HABITUALES

4.1. *Creación de empresa paralela, utilizando activos inmateriales de la empresa*

Consiste en la explotación en una empresa de nueva creación, de la propiedad intelectual, la propiedad industrial o el know how de la empresa en la que el trabajador trabaja. Generalmente, el trabajador constituye la nueva compañía antes de solicitar la baja voluntaria y realiza un proceso de trasvase de información mediante soportes informáticos o a través de Internet. Es posible que el trabajador actúe aliado con otros compañeros de la empresa.

4.2. *Daños informáticos y uso abusivo de recursos informáticos*

Los daños informáticos se producen generalmente como respuesta a un conflicto laboral o a un despido que el trabajador considera injusto. Consisten en la destrucción, alteración o inutilización de los datos, programas o cualquier otro activo inmaterial albergado en redes, soportes o sistemas informáticos de la empresa. Los casos más habituales son los virus informáticos, el sabotaje y las bombas lógicas, programadas para que tengan efecto unos meses después de la baja del trabajador. También es habitual el uso abusivo de recursos informáticos, especialmente el acceso a Internet.

4.3. *Información confidencial y datos personales*

Consiste en el acceso no autorizado y en la posterior revelación a terceros, generalmente competidores o clientes, de información confidencial de la empresa. En algunas ocasiones, la revelación la realizan trabajadores que tienen un acceso legítimo, pero con obligación de reserva, a la información posteriormente divulgada. En este capítulo también se contempla la cesión no autorizada a terceros de datos personales de trabajadores y clientes.

4.4. *Amenazas, injurias y calumnias*

El medio utilizado habitualmente es el correo electrónico corporativo, aunque también se han utilizado cuentas anónimas, e incluso se ha suplantado la identidad de otro trabajador de la misma empresa. En el caso de las amenazas, se busca un beneficio material o inmaterial para el trabajador. Si el beneficio no se produce, el trabajador llevará a cabo la conducta anunciada en el mensaje amenazador. En el caso de las injurias y las calumnias, se busca desacreditar a la empresa, o a alguno de sus directivos. También se han producido insultos a clientes habituales o a clientes potenciales de la empresa con el que el trabajador tenía algún conflicto.

4.5. Infracción propiedad intelectual e introducción de obras de la empresa en redes P2P

Consiste en la copia de activos inmateriales de la empresa, especialmente obras protegidas por la propiedad intelectual, con el fin de cederlas posteriormente a terceros. En los últimos dos años se han dado casos de difusión a través de Internet, mediante el uso de redes de intercambio de ficheros (peer to peer). De esta manera, una multitud de usuarios acceden de forma gratuita a programas de ordenador desprotegidos, información o contenidos multimedia.

4.6. Intercambio de obras de terceros a través de redes P2P

Este es el caso más habitual y se detecta generalmente en el curso de una auditoría de seguridad informática, mediante el análisis del caudal de datos transferido por los trabajadores a través de la red corporativa. En algunas ocasiones, se ha detectado directamente la instalación del programa P2P o el uso de puertos típicos para el acceso a redes P2P. Este caso es especialmente grave, ya que la empresa se convierte en proveedora directa de copias no autorizadas de música, películas y programas de ordenador.

4.7. Infracción de derechos de propiedad industrial

El caso más habitual ha sido la infracción de marcas de la empresa mediante el registro del nombre de dominio por parte del trabajador. En algunos casos, se ha creado una página web con contenidos ofensivos para conseguir un mayor efecto nocivo para la empresa o para obtener una suma de dinero por la transferencia.

5. TRATAMIENTO DE LAS INFRACCIONES EN EL ORDENAMIENTO JURÍDICO ESPAÑOL

5.1. Creación de empresa paralela, utilizando activos inmateriales de la empresa

Puede constituir un acto desleal previsto en el artículo 11 de la Ley de Competencia Desleal. La imitación de prestaciones e iniciativas empresariales ajenas es libre, salvo que estén amparadas por un derecho de exclusiva reconocido por la Ley. No obstante, la imitación de prestaciones se reputará desleal cuando resulte idónea para generar la asociación por parte de los consumidores respecto a la prestación o comporte un aprovechamiento indebido de la reputación o el esfuerzo ajeno.

Puede concurrir con un supuesto de inducción a la infracción contractual, previsto en el artículo 14 de la misma ley. Se considera desleal la inducción a trabajadores, proveedores, clientes y demás obligados, a infringir los deberes contractuales básicos contraídos con la empresa en la que el trabajador prestaba sus servicios. La inducción a la terminación regular de un contrato o el aprovechamiento en beneficio propio o de un tercero de una infracción contractual ajena sólo se reputará desleal cuando, siendo conocida, tenga por objeto la difusión o explotación de un secreto industrial o empresarial o vaya acompañada de circunstancias tales como el engaño, la intención de eliminar a un competidor del mercado u otras análogas.

La reproducción, plagio, distribución o comunicación pública no autorizada de obras protegidas por la propiedad intelectual puede constituir un delito previsto en el artículo 270 del Código Penal.

La revelación de secretos empresariales por parte de trabajadores está tipificada como delito en el artículo 199 del Código Penal.

5.2. Daños informáticos

La destrucción, alteración, inutilización de datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos constituye un delito de daños previsto en el artículo 264 del Código Penal.

5.3. Información confidencial y datos personales

La revelación de secretos empresariales por parte de trabajadores está tipificada como delito en los artículos 199, 278 y 279 del Código Penal. La revelación de datos personales de carácter reservado está prevista en el artículo 197 del Código Penal.

5.4. Amenazas, injurias y calumnias

Las amenazas están tipificadas como delito en el artículo 169 y siguientes del Código Penal. Las injurias están tipificadas como delito en el artículo 205 y siguientes del Código Penal. Las calumnias están tipificadas como delito en el artículo 208 y siguientes del Código Penal.

5.5. Introducción obras de la empresa en redes P2P

La reproducción, distribución o comunicación pública no autorizada, a través de redes P2P, de obras protegidas por la propiedad intelectual puede constituir un delito previsto en el artículo 270 del Código Penal.

5.6. Intercambio de obras de terceros a través de redes P2P

El intercambio, a través de redes P2P, de obras protegidas por la propiedad intelectual puede constituir un delito previsto en el artículo 270 del Código Penal.

5.7. Infracción de derechos de propiedad industrial

La infracción de derechos de propiedad industrial está tipificada como delito en el artículo 274 del Código Penal.

6. ESTRATEGIA SEGUIDA POR LAS EMPRESAS

6.1. Tipo de investigación

La mayoría de las empresas prefieren encomendar la investigación de los posibles actos desleales de un trabajador a un equipo interno, generalmente formado por miembros del departamento de RRHH y del departamento de sistemas. Sólo un 22% de las empresas que sospechan de un empleado deciden externalizar la investigación. El tipo de investigación depende de la intención de la empresa de llegar a un acuerdo o plantear una reclamación judicial. Cuando se ha tomado la decisión de llevar la infracción a los tribunales, la obtención de las evidencias electrónicas se encarga a un tercero, con el fin de conseguir mayor objetividad y valor probatorio. El procedimiento de recopilación de las evidencias debe respetar los derechos del trabajador para que sea válido judicialmente. Una investigación se inicia a partir de las sospechas e indicios generados por la propia conducta del trabajador, por un consumo de recursos poco usual o por el descubrimiento de los efectos de la infracción.



Gráfico 6.1

Estrategia de investigación	Casos	Porcentaje
Investigación interna	305	78%
Investigación externa	88	22%
	393	100%

6.2. Actuación de la empresa

Sólo el 26% de las infracciones detectadas acaban en los tribunales. El resto de las infracciones son objeto de un acuerdo privado o de una sesión finalizada con aveniencia en un organismo de mediación y conciliación laboral. Este punto está en clara correspondencia con el anterior. Cada empresa tiene una forma distinta de responder a un acto desleal de un trabajador, que puede variar si la gravedad de los perjuicios causados o la mala fe demostrada es superior a lo normal. En general, las empresas prefieren solucionar sus conflictos de forma privada y ello incide en la forma de investigar y tratar las posibles infracciones de sus trabajadores. Si los daños producidos están previstos en la cobertura de un seguro, es muy probable que la empresa deba plantear una reclamación judicial para poder solicitar la correspondiente compensación económica.

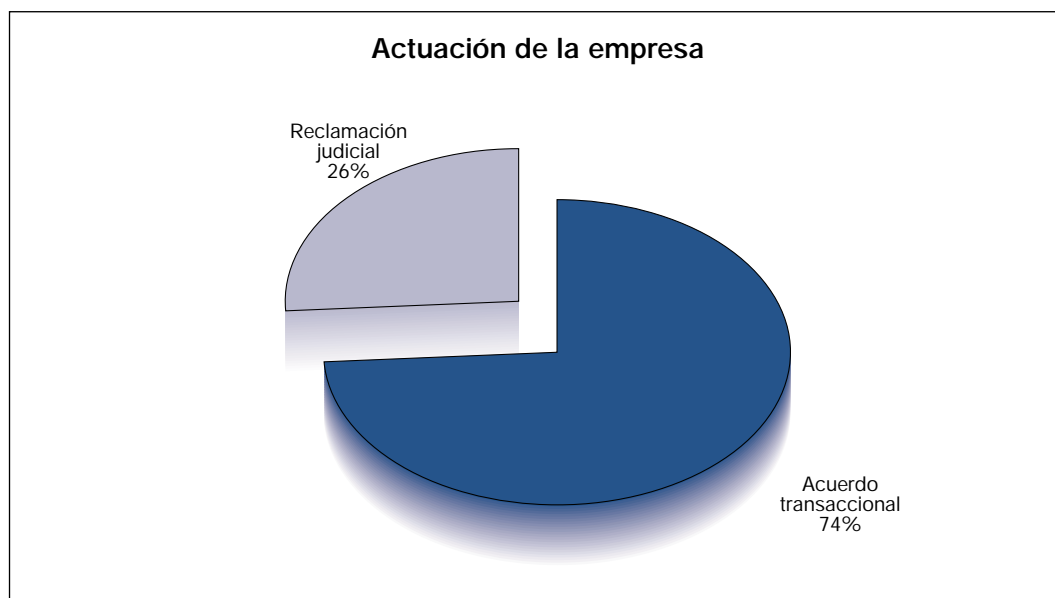


Gráfico 6.2

Actuación de la empresa	Casos	Porcentaje
Acuerdo transaccional	290	74%
Reclamación judicial	103	26%
	393	100%

6.3. Divulgación de la infracción

En el gráfico 6.3 puede comprobarse que sólo el 13% de las empresas deciden divulgar la existencia de la infracción detectada, mientras que el resto de las empresas prefieren mantener el conflicto en privado. Esta decisión puede depender del ánimo de la empresa de preservar su reputación, ya que la revelación de problemas de seguridad informática o de conflictos con los trabajadores puede generar desconfianza en el mercado. Este efecto negativo de la divulgación de una vulnerabilidad informática puede tener mayor trascendencia si la empresa cotiza en bolsa. También son especialmente sensibles las empresas que prestan servicios financieros o que disponen de información confidencial de sus clientes.

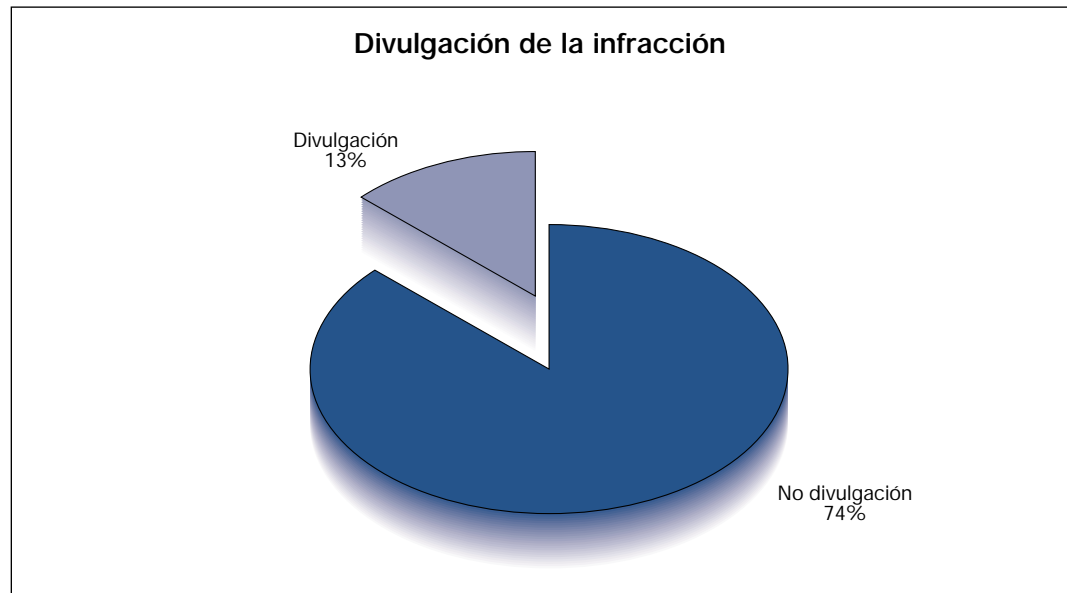


Gráfico 6.3

Divulgación de la infracción	Casos	Porcentaje
No divulgación	342	87%
Divulgación	51	13%
	393	100%

Las empresas que han decidido divulgar que han detectado una infracción y han actuado rápidamente para evitar sus consecuencias perjudiciales tenían como objetivo conseguir un efecto disuasorio sobre los demás trabajadores, usuarios del sistema o hackers externos. El mensaje ejemplarizante es una prioridad en las empresas sometidas a numerosos ataques y cuya actividad no depende de la confianza del mercado en su seguridad interna. En este segmento estarían las empresas de software que descubren que uno de sus programas ha sido copiado o desprotegido.

7. ANÁLISIS POR NIVEL DE FRECUENCIA

En el gráfico 7.1 puede apreciarse la distribución de las infracciones más habituales en función de su nivel de frecuencia. La infracción más habitual es el uso de la red corporativa para intercambiar música, películas o software a través de las *redes peer to peer (P2P)* accesibles a través de Internet.

Durante los dos últimos años analizados el número de usuarios de estas redes de intercambio ha aumentado de tal manera que es difícil encontrar una empresa que no tenga instalado un programa de este tipo. Una adecuada configuración del firewall puede impedir el uso de programas P2P como Kazaa, eDonkey o eMule, pero las nuevas versiones permiten acceder a la red a través de puertos de comunicación no bloqueados por la empresa.

La segunda infracción más habitual es la explotación de la propiedad intelectual de la empresa en otra empresa de nueva creación. Este se ha convertido en un problema habitual en las empresas que concentran las actividades de investigación y desarrollo en equipos muy reducidos o unipersonales. Cuando la tecnología está controlada por pocas personas, existe el riesgo de que minusvaloren el papel de la empresa en la creación del producto y decidan explotarlo por su cuenta, o con la ayuda de un inversor externo. Este riesgo puede minimizarse con una adecuada segregación de las tareas de un proyecto, con sistemas de motivación del personal de desarrollo y con cláusulas penales que cumplan un papel disuasorio.

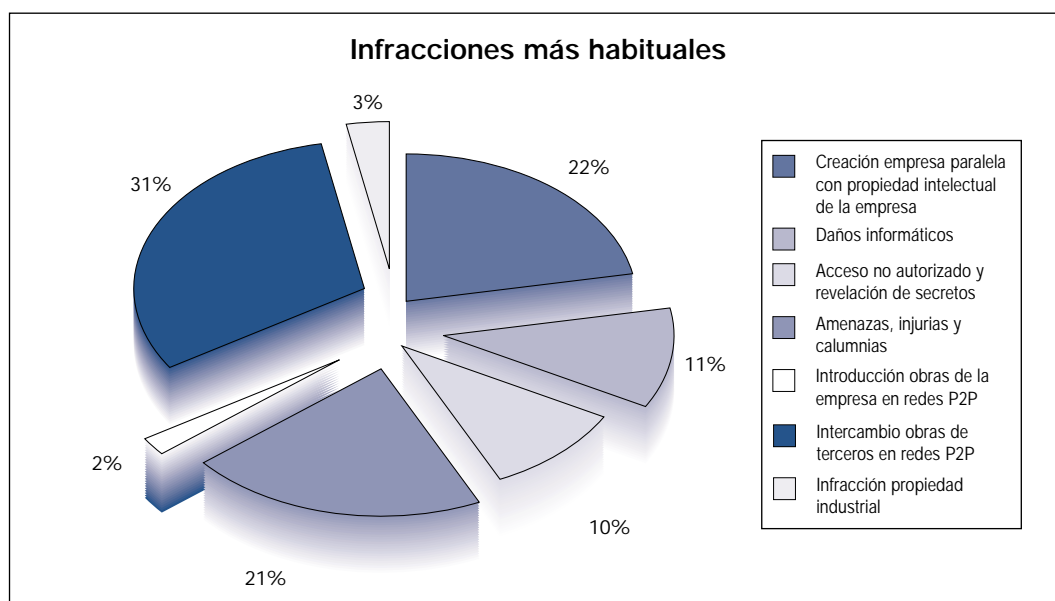


Gráfico 7.1

Infracción	Casos	Porcentaje
Creación empresa paralela con propiedad intelectual de la empresa	87	22%
Daños informáticos	42	11%
Acceso no autorizado, revelación de secretos y datos personales	38	10%
Amenazas, injurias y calumnias	83	21%
Introducción de obras de la empresa en redes P2P	7	2%
Intercambio de obras de terceros en redes P2P	124	31%
Infracción propiedad industrial	12	3%
	393	100%

Otra infracción habitual es la utilización del correo electrónico corporativo para enviar mensajes amenazantes, injuriosos o calumniosos. Es raro el caso en el que dichos mensajes van dirigidos a directivos o trabajadores de la misma empresa. Generalmente se dirigen a terceros. Cuando el e-mail se utiliza para fines particulares, es posible que el trabajador no tenga en cuenta que sus afirmaciones pueden comprometer a la empresa en la que trabaja. Pero el canal más habitual para este tipo de mensajes está constituido por los foros de debate y los chats. En ellos, el trabajador tiene una sensación de anonimato que le permite participar en discusiones de forma acalorada. En algunos casos, la intención inicial es la de defender la imagen de la compañía o de sus productos frente a las críticas de otros participantes. En otros casos, son debates sobre temas ajenos a la actividad de la empresa. En cualquier caso, es importante sensibilizar a los trabajadores sobre el carácter vinculante de las afirmaciones que hagan en la red utilizando el dominio de la empresa o su dirección IP.

La revelación de información confidencial de forma no intencionada está aumentando su frecuencia de forma significativa a causa de la proliferación de unos programas que bajo el nombre genérico de *spyware* se instalan en el ordenador del usuario cuando navega por Internet y permiten capturar datos albergados en el sistema.

8. ANÁLISIS POR SECTORES

El gráfico 8.1 muestra que el sector más afectado es el de desarrollo de software. Es posible que ello se deba a los conocimientos técnicos de los trabajadores, que les permiten aprovechar mejor la tecnología para su beneficio personal o para perjudicar a la empresa. También es el sector en el que se produce con mayor la frecuencia la usurpación de código fuente por parte de los programadores para crear programas parecidos.

El sector que le sigue es el de los servicios a empresas, con un alto nivel de informatización. Los trabajadores de este tipo de compañías desarrollan un trabajo predominantemente intelectual que explota de forma continuada los recursos informáticos y telemáticos corporativos, aumentando el riesgo de infracciones.

La incidencia en los demás sectores es menos significativa. Resalta el sector financiero por la escasez de incidentes (sólo tres casos en tres años).

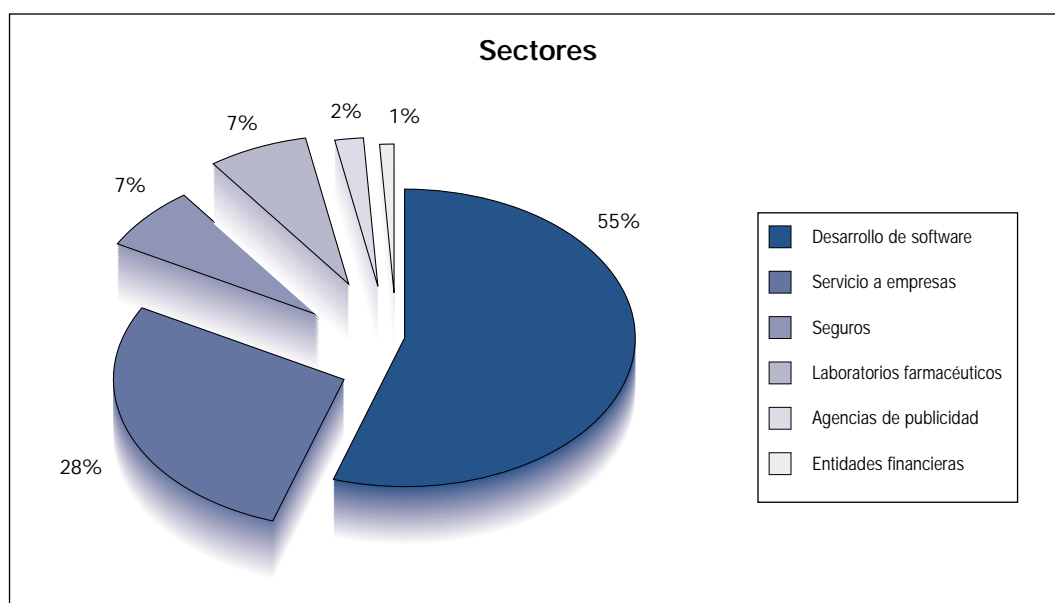


Gráfico 8.1

Sectores	Casos	Porcentaje
Desarrollo de software	216	55%
Servicios a empresas	112	28%
Seguros	29	7%
Laboratorios farmacéuticos	27	7%
Agencias de publicidad	6	2%
Entidades financieras	3	1%
	393	100%

9. ANÁLISIS POR CARGOS

En el análisis por cargos se comprueba que el usuario genérico de la red corporativa representa el puesto de trabajo en el que mayor número de infracciones se producen. La causa de ello radica en que el tipo de infracción más frecuente es el intercambio de copias no autorizadas a través de las redes P2P en Internet. Dicha infracción afecta a todos los usuarios por igual, y no se concentra en un puesto de trabajo concreto.

La siguiente categoría es la de analista o programador. Se trata de profesionales con un gran conocimiento de la tecnología, que pueden acceder a privilegios vedados para otros usuarios y realizar funciones que, de forma intencionada o no, pueden comprometer la seguridad del sistema. Las empresas deben segregar las funciones de estos profesionales para evitar que tengan acceso a los ordenadores de explotación y puedan realizar actos no autorizados.

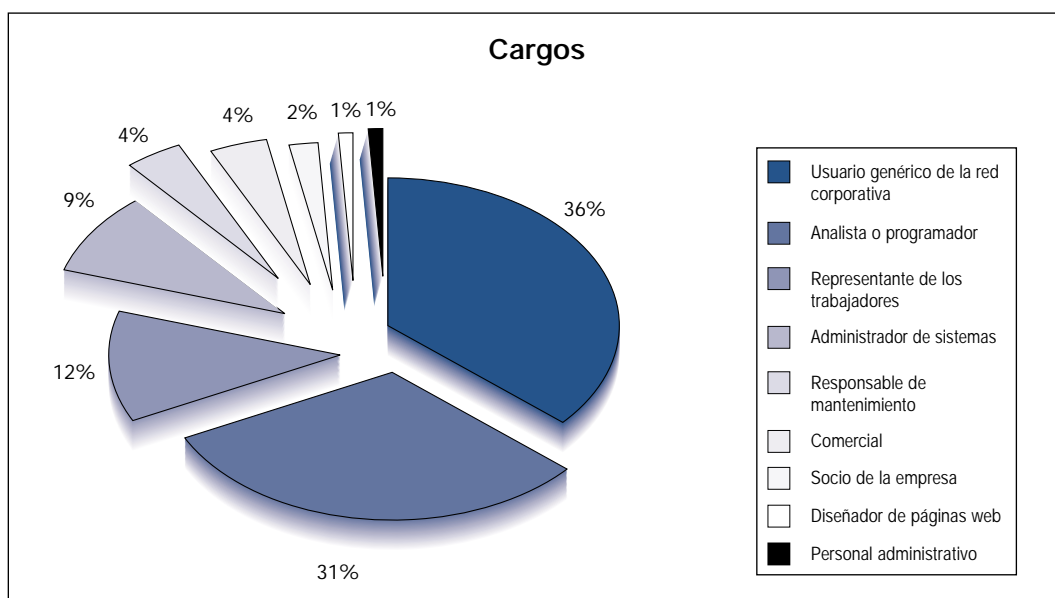


Gráfico 9.1

Cargos	Casos	Porcentaje
Usuario genérico de la red corporativa	142	36%
Analista o programador	122	31%
Representante de los trabajadores	48	12%
Administrador de sistemas	36	9%
Responsable de mantenimiento	16	4%
Comercial	14	4%
Socio de la empresa	7	2%
Diseñador de páginas web	5	1%
Personal administrativo	3	1%
	393	100%

10. ANÁLISIS POR MOTIVACIONES

El ánimo de lucro es la principal motivación de los trabajadores que cometen alguna infracción. La jurisprudencia del Tribunal Supremo entiende por ánimo de lucro cualquier ventaja patrimonial, incluido el ahorro de un gasto que debería corresponder al trabajador. Esta ventaja económica puede consistir en el uso de un recurso empresarial para fines personales y puede llegar a la apropiación de un bien o a la explotación económica de un activo en una nueva empresa.

Le sigue el ánimo de responder a una decisión de la empresa que le perjudica, especialmente si se trata de un despido. Esta es la principal motivación de los daños informáticos consistentes en sabotajes o en la introducción intencionada de virus.

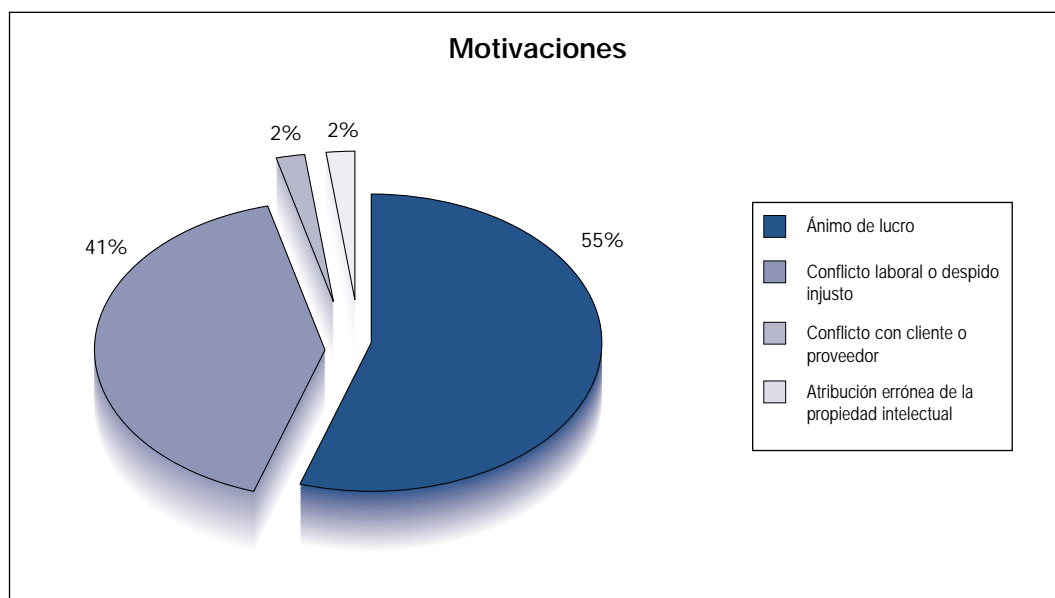


Gráfico 10.1

Motivaciones	Casos	Porcentaje
Ánimo de lucro	216	55%
Conflicto laboral o despido injusto	160	41%
Conflicto con cliente o proveedor	9	2%
Atribución errónea de la propiedad intelectual	8	2%
	393	100%

11. ANÁLISIS POR CUANTÍA DE LOS PERJUICIOS

La mayor parte de las infracciones cometidas por los trabajadores produce a las empresas afectadas perjuicios de menos de 60.000 euros. Sin embargo, la escasa trascendencia de un acto aislado no debe hacer olvidar la gravedad del efecto acumulativo de pequeñas defraudaciones cometidas de forma continuada por muchos trabajadores.

Sólo el 3% de las infracciones analizadas generan perjuicios superiores a los 300.000 euros. Estos perjuicios más elevados corresponden a casos graves de apropiación indebida de código fuente de aplicaciones informáticas y a la explotación de activos inmateriales a través de terceros o de empresas constituidas por los trabajadores.

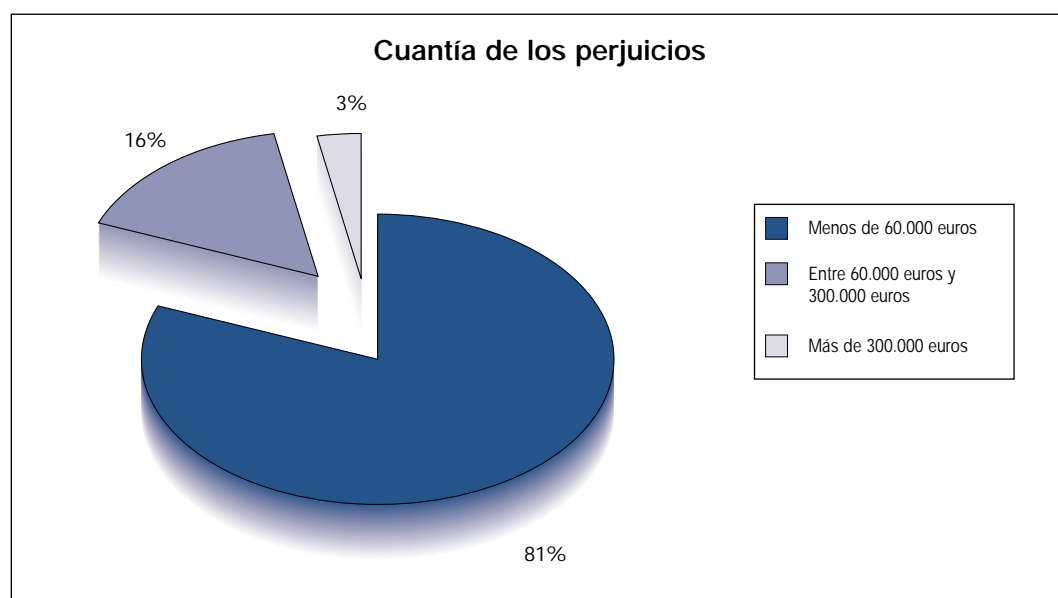


Gráfico 11.1

Cuantía daños	Casos	Porcentaje
Menos de 60.000 euros	317	81%
Entre 60.000 euros y 300.000 euros	64	16%
Más de 300.000 euros	12	3%
	393	100%

12. EVOLUCIÓN CRONOLÓGICA

En este gráfico se aprecia la evolución ascendente del número de casos detectados cada año. Aunque la progresión no es alarmante, está clara la tendencia al alza del número de infracciones cometidas por los trabajadores y descubiertas por las empresas.

Un factor que contribuye a este crecimiento es el mayor grado de implantación de la informática y las comunicaciones en las organizaciones. También influye el mayor conocimiento de los sistemas de información por parte de los trabajadores, y la aparición de nuevas herramientas como los programas P2P que facilitan la comisión de nuevos delitos.

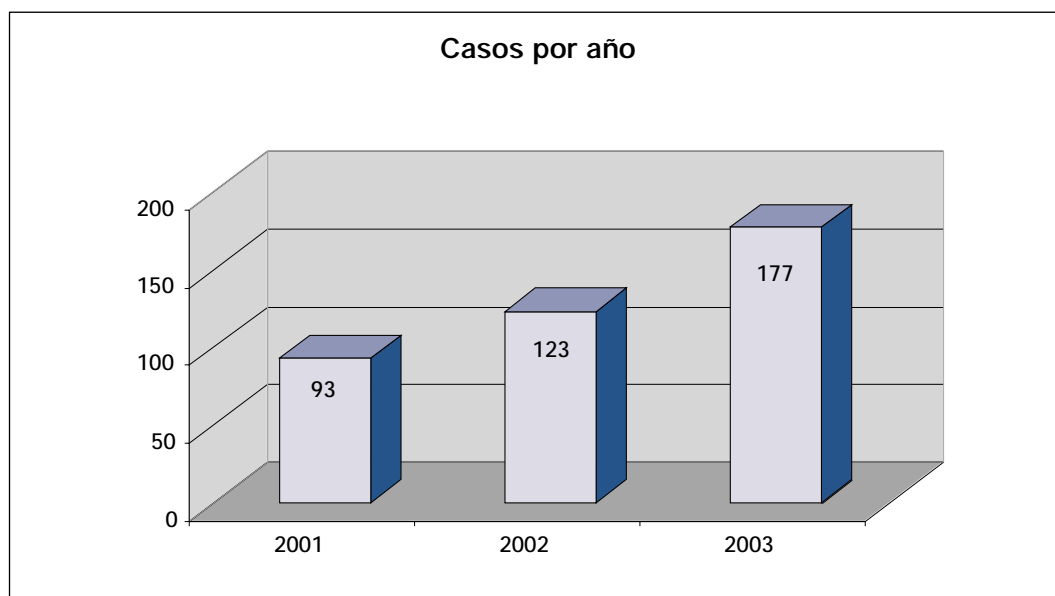


Gráfico 12.1

Año	Casos	Incremento
2001	93	24%
2002	123	31%
2003	177	45%
	393	

13. CONCLUSIONES

- Las empresas prefieren encomendar la investigación de eventuales infracciones de sus empleados a un equipo interno.
- Sólo una cuarta parte de las infracciones detectadas acaban en los tribunales. El resto son objeto de un acuerdo transaccional.
- Las empresas son reacias a divulgar la existencia de la infracción detectada. Sólo se deciden a publicarla cuando consideran que podrán explotar su efecto disuasorio.
- Las infracciones más habituales son el intercambio de copias no autorizadas a través de Internet y la explotación de activos inmateriales de la empresa en otras compañías.
- Los sectores más afectados por este tipo de infracciones son el de desarrollo de software y el de servicios a empresas.
- Los trabajadores que más han participado en este tipo de infracciones son los usuarios genéricos de la red corporativa y los programadores.
- La principal motivación del trabajador al cometer una infracción utilizando los recursos informáticos de la empresa, es el ánimo de lucro.
- La mayor parte de las infracciones analizadas producen individualmente perjuicios de menos de 60.000 euros.

14. MEDIDAS PREVENTIVAS

14.1. Políticas y normas de seguridad

Es conveniente reflejar en un documento cuál es la política de la empresa en materia de seguridad y los objetivos a largo plazo en el uso estratégico de los sistemas informáticos para evitar que se produzcan incidentes que puedan perjudicar la reputación de la empresa y sus activos inmateriales.

La redacción de unas normas internas que regulen el uso de los sistemas informáticos corporativos, el correo electrónico y el acceso a Internet es una obligación establecida en el Real Decreto 994/1999. En dichas normas se establecerán las obligaciones de los trabajadores en materia de seguridad informática y confidencialidad de la información. La empresa debe generar evidencias de la comunicación de estas normas a los trabajadores.

14.2. Objetivos en materia de prevención

Es importante establecer los objetivos de la empresa respecto a los niveles de cumplimiento que espera conseguir de las medidas preventivas y las normas de seguridad internas. Estos objetivos se definirán a corto, medio y largo plazo y serán objeto de seguimiento periódico.

14.3. Panel de control

Para efectuar un seguimiento y reportar a la Dirección de la empresa el nivel de cumplimiento de los objetivos establecidos en materia de seguridad, es conveniente utilizar un panel de control o cuadro de mando en el que se pueda tener una visión global de la empresa en esta materia.

En el siguiente gráfico se puede apreciar un ejemplo de panel de control en el que los códigos de color verde, amarillo y rojo indican la situación de la empresa respecto a los objetivos, indicadores y riesgos considerados críticos.



14.5. Formación y sensibilización

La formación y sensibilización del personal es un paso obligado para poder acreditar la diligencia de la empresa en el caso de un incidente de seguridad que genere perjuicios a los clientes de la empresa o a terceros. También permite generar pruebas de la divulgación de las normas de seguridad y aumenta su fuerza disuasoria. Para que la formación sea efectiva, debe impartirse de forma periódica.

14.6. Medidas de seguridad

La aplicación de medidas de seguridad informática es una obligación establecida en el Real Decreto 994/1999 y ayuda a minimizar el riesgo de fugas de información confidencial fuera de la empresa. La extensión de estas normas a todo el sistema informático corporativo permite aumentar la protección de los activos inmateriales de la empresa.

14.7. Auditorías y controles periódicos

Para que los objetivos establecidos en materia de seguridad tengan un nivel de cumplimiento aceptable, deben realizarse auditorías y controles de forma periódica. Al hablar de tecnologías de la información, cualquier medida de seguridad queda rápidamente obsoleta si no es objeto de una constante actualización. Además, la realización de auditorías y controles periódicos también es una obligación establecida en el Real Decreto 994/1999.

15. "CHECKLIST" DE AUTODIAGNÓSTICO

Código	Punto de comprobación	SI
0001	Correo electrónico	
0101	¿Utiliza la empresa el correo electrónico para el envío de documentos a destinatarios internos de la empresa?	
0102	¿Utiliza la empresa el correo electrónico para el envío de documentos a destinatarios externos?	
0103	¿Dispone la empresa de normas de uso del correo electrónico?	
0104	¿Se establece en ellas la prohibición del uso del correo electrónico para fines particulares?	
0105	¿Se advierte en ellas sobre la posibilidad de que la empresa establezca medidas de control sobre el correo electrónico?	
0106	¿Dispone la empresa de pruebas de la aceptación de dichas normas por parte de los trabajadores?	
0107	¿Existe alguna medida técnica que impida el arrastre de direcciones de otros usuarios en el caso de reenvío de mensajes anteriores?	
0108	¿Existe alguna medida técnica que impida el envío de un mismo mensaje a un gran número de usuarios?	
0109	¿Está prohibido en la empresa el envío de mensajes publicitarios no solicitados a través de correo electrónico?	
0110	¿Existe alguna medida técnica que impida el envío involuntarios de mensajes a listas abiertas de destinatarios que desvelen la identidad de los mismos?	
0111	¿Existen recomendaciones para prevenir la confusión entre dominios .es y .com y otras modalidades de error humano relacionadas con el correo electrónico?	
0112	¿Existen recomendaciones para prevenir el engaño por correo electrónico a los trabajadores de la empresa para que divulguen datos confidenciales?	
0113	¿Existen medidas técnicas para impedir la entrada de virus informáticos en la red local y los ordenadores de la empresa?	
0114	¿Existen medidas técnicas para impedir la entrada de caballos de Troya a través del correo electrónico, con el fin de facilitar el acceso de terceros al sistema?	
0115	¿Existen medidas técnicas para detectar una eventual salida por correo electrónico de información confidencial camuflada en imágenes?	
0116	¿Han realizado estadísticas para comprobar la posible disminución del rendimiento de los trabajadores por culpa de un uso personal del correo electrónico?	
0002	Navegación por Internet	
0201	¿Disponen los empleados de su empresa de acceso a Internet?	
0202	¿Dispone la empresa de normas de uso de Internet?	
0203	¿Permiten el uso de Internet para fines particulares?	
0204	¿Han realizado estadísticas para comprobar la posible disminución del rendimiento de los trabajadores por culpa de un uso personal de Internet?	
0205	¿Existen medidas técnicas para impedir la instalación no consentida de dialers a teléfonos tipo 906, 80, 803, etc.?	

0206	¿Existen medidas técnicas para impedir la instalación no consentida de spyware, mediante el que la actividad del usuario puede ser monitorizada por terceros?	
0207	¿Existen medidas técnicas para impedir la instalación no consentida de addware, mediante el que el usuario verá constantemente anuncios en su ordenador?	
0208	¿Existen medidas técnicas para impedir la entrada de caballos de Troya a través de la visita de páginas web?	
0209	¿Han actualizado los navegadores de los usuarios para eliminar agujeros de seguridad descubiertos en los últimos meses?	
0003	Redes inalámbricas	
0301	¿Dispone la empresa de alguna red inalámbrica?	
0302	¿Dispone la empresa de ordenadores con capacidad para conectarse a redes inalámbricas?	
0303	¿Ha comprobado si existen redes inalámbricas en la zona donde radica la empresa?	
0304	¿Existe en la empresa alguna prohibición de instalar puntos de acceso inalámbricos no autorizados?	
0305	¿Dispone la empresa de equipos o teléfonos móviles con tecnología bluetooth?	
0004	Programas P2P	
0401	¿Existen medidas técnicas para impedir el uso de programas de intercambio de ficheros a través de redes P2P?	
0402	¿Existen medidas técnicas para detectar el uso de programas de intercambio de ficheros a través de redes P2P?	
0005	Mensajería instantánea	
0501	¿Existen medidas técnicas para impedir el uso de programas de mensajería instantánea tipo Messenger?	
0502	¿Existen medidas técnicas para detectar el uso de programas de mensajería instantánea?	
0006	Soportes informáticos miniaturizados	
0601	¿Existe algún tipo de control para impedir la salida de información confidencial a través de soportes informáticos miniaturizados tipo USB o tarjetas de memoria?	
0602	¿Están inventariados y codificados todos los soportes informáticos de la empresa?	
0603	¿Existe un registro de entrada y salida de soportes informáticos?	
0007	Información oculta	
0701	¿Utilizan los trabajadores de la empresa el paquete OFFICE?	
0702	¿Han configurado las aplicaciones de OFFICE para evitar que guarden información oculta en las propiedades del documento?	
0703	¿Existen recomendaciones para impedir que un tercero pueda acceder al historial de revisiones del documento?	
0008	Error humano	
0801	¿Existen medidas preventivas para limitar los errores derivados de la impericia en el uso de las nuevas tecnologías?	
0802	¿Existen medidas preventivas para limitar los errores derivados de métodos de trabajo incorrectos?	

0803	¿Existen medidas preventivas para limitar los errores derivados de actos repetitivos?	
0804	¿Existen medidas preventivas para limitar los errores derivados de comunicaciones defectuosas o incompletas?	
0009	Portátiles y PDA	
0901	¿Los comerciales, repartidores, instaladores o televentas de la empresa disponen de portátiles, PDA o dispositivos similares?	
0902	¿La empresa utiliza sistemas de localización vía GPS o GSM?	
0903	¿Existen normas de seguridad específicas para equipos portátiles y PDA?	
0010	Acceso remoto	
1001	¿Es accesible desde el exterior la red o la intranet de la empresa?	
1002	¿Tiene la empresa empleados que trabajan de forma fija o temporal en su casa?	
1003	¿Existen normas de seguridad específicas para los trabajadores que realizan accesos remotos a la red corporativa?	
0011	Colaboradores externos y proveedores	
1101	¿La empresa contrata servicios externos que exigen el acceso temporal o continuado a datos de trabajadores o clientes? (Imprenta, nóminas, limpieza, etc.)	
1102	¿Exige en estos casos el cumplimiento de las normas de seguridad de la empresa?	
0012	Datos personales	
1201	¿Registra la empresa los datos de las personas que visitan sus instalaciones?	
1202	En caso afirmativo, ¿ha comunicado el fichero a la APD?	
1203	¿Dispone la empresa de una aplicación CRM que le permita establecer perfiles de consumo de sus clientes?	
1204	¿Retiene la empresa la cuota sindical a sus trabajadores?	
1205	¿Hay algún trabajador minusválido en plantilla? ¿Algún trabajador tiene un familiar minusválido?	
1206	¿Gestiona la empresa de datos de absentismo de sus trabajadores?	
1207	¿Tiene la empresa servicio médico o accede a datos de salud de sus trabajadores? (Tramitación seguro de vida)	
1208	¿Realiza la empresa valoraciones del desempeño y la personalidad de sus trabajadores?	
1209	¿Accede la empresa al historial de llamadas del móvil del trabajador o al consumo de su tarjeta de crédito o Teletac?	
1210	¿Contiene el contrato laboral una cláusula relativa a los datos personales del trabajador?	
0013	Activos inmateriales	
1301	¿Dispone la empresa de pruebas de la titularidad de sus activos inmateriales? (Know-how, propiedad intelectual e industrial)	
1302	¿El contrato laboral contiene una cláusula de confidencialidad?	
1303	¿El contrato laboral contiene una cláusula de propiedad intelectual?	
1304	¿Se pactan plazos de permanencia en la empresa cuando el trabajador recibe formación especializada?	

0014	Seguridad informática	
1401	¿Dispone la empresa de un documento en que se describen todas la medidas de seguridad de la empresa?	
1402	¿Cumple este documento los requisitos del Reglamento de Seguridad aprobado mediante RD 994/1999?	
1403	¿Se han adecuado las normas de seguridad a la ISO 17799?	
1404	¿Se están aplicando las medidas de seguridad al papel?	
1405	¿Existen evidencias documentales de la aplicación de las medidas de seguridad por la empresa?	
1406	¿Existe un plan continuado y certificado por terceros de formación y sensibilización del personal en materia de seguridad?	

Contactos Landwell - PricewaterhouseCoopers

Javier Ribas

Socio

Responsable del Departamento de Derecho de las Tecnologías de la Información

javier.ribas@es.landwellglobal.com

Tel.: 639 108 413

Carlos Pérez Sanz

Asociado Senior

Miembro del Departamento de Derecho de las Tecnologías de la Información

carlos.perez.sanz@es.landwellglobal.com

Tel.: 932 532 506

Assumpta Zorraquino

Asociado Senior

Miembro del Departamento de Derecho de las Tecnologías de la Información

assumpta.zorraquino@es.landwellglobal.com

Tel.: 932 532 507

Carlos Rodríguez Sau

Asociado Senior

Miembro del Departamento de Derecho de las Tecnologías de la Información

carlos.rodriguez.sau@es.landwellglobal.com

Tel.: 915 684 325

Raúl Rubio

Asociado Senior

Miembro del Departamento de Derecho de las Tecnologías de la Información

raul.rubio.velazquez@es.landwellglobal.com

Tel.: 915 685 565

Judit Barnola

Asociado Senior

Miembro del Departamento de Derecho de las Tecnologías de la Información

judit.barnola@es.landwellglobal.com

Tel.: 932 532 509

Si desea obtener más ejemplares, solicitarlos en la siguiente dirección de e-mail:

pwc.comunicacion@es.pwc.com

Dirección del estudio: Javier Ribas

www.landwellglobal.com/es

LANDWELL
Abogados y Asesores Fiscales

Law firm associated with

PRICEWATERHOUSECOOPERS 

PricewaterhouseCoopers (www.pwc.com) ofrece a las empresas y a la Administración servicios de auditoría, asesoramiento legal y fiscal (Landwell-PwC), consultoría de negocio, corporate finance y consultoría de recursos humanos especializados en cada sector. Más de 120.000 personas en 139 países aúnan sus conocimientos, experiencia y soluciones para dar confianza e incrementar el valor de sus clientes y stakeholders.

© PricewaterhouseCoopers Jurídico y Fiscal, S.L. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a la red de firmas miembros de PricewaterhouseCoopers International Limited; cada una de las cuales es una entidad legal separada e independiente. *connectedthinking es una marca registrada de PricewaterhouseCoopers.