



A Websense® White Paper

Riesgos asociados al uso de sistemas de información corporativos

Contenido:

Informe Jurídico relativo a las infracciones y las subsiguientes responsabilidades derivadas de determinados usos de los sistemas informáticos corporativos.

Table of Contents:

1. Introducción	4
2. Resumen ejecutivo	4
• 2.1. Amenazas	4
• 2.2. Riesgos	4
• 2.3. Conclusiones.....	5
3. Análisis de los escenarios propuestos por Websense	5
• 3.1. Escenario 1	5
a) Descripción del escenario	5
b) Normativa afectada	5
c) Infracciones y Responsabilidades derivadas de las mismas.....	5
d) Recomendaciones.....	6
• 3.2. Escenario 2	7
a) Descripción del escenario	7
b) Normativa afectada	7
c) Infracciones y Responsabilidades derivadas de las mismas.....	7
d) Recomendaciones.....	8
• 3.3. Escenario 3	8
a) Descripción del escenario	8
b) Normativa afectada	8
c) Infracciones y Responsabilidades derivadas de las mismas.....	8
d) Recomendaciones.....	10
• 3.4. Escenario 4	10
a) Descripción del escenario	10
b) Normativa afectada	10
c) Infracciones y Responsabilidades derivadas de las mismas.....	10
d) Recomendaciones.....	11
• 3.5. Escenario 5	12
a) Descripción del escenario	12
b) Normativa afectada	12
c) Infracciones y Responsabilidades derivadas de las mismas.....	12
d) Recomendaciones.....	12
• 3.6. Escenario 6	13
a) Descripción del escenario	13
b) Normativa afectada	13
c) Infracciones y Responsabilidades derivadas de las mismas.....	13
d) Recomendaciones.....	15
• 3.7. Escenario 7	15
a) Descripción del escenario	15
b) Normativa afectada	15
c) Infracciones y Responsabilidades derivadas de las mismas.....	15
d) Recomendaciones.....	16
• 3.8. Escenario 8	16
a) Descripción del escenario	16
b) Normativa afectada	16
c) Infracciones y Responsabilidades derivadas de las mismas.....	16
d) Recomendaciones.....	18

- 3.9. Escenario 9 18
 - a) Descripción del escenario 18
 - b) Normativa afectada 18
 - c) Infracciones y Responsabilidades derivadas de las mismas..... 18
 - d) Recomendaciones..... 19
- 3.10. Escenario 10 20
 - a) Descripción del escenario 20
 - b) Normativa afectada 20
 - c) Infracciones y Responsabilidades derivadas de las mismas..... 20
 - d) Recomendaciones..... 21

1. Introducción

El objeto del presente informe es la descripción, a través del análisis de 10 escenarios propuestos por Websense, de las responsabilidades derivadas de determinados usos del sistema informático corporativo por parte de los trabajadores.

Las responsabilidades estudiadas serán las que puedan derivarse para la compañía, para los trabajadores, así como para los Responsables del Departamento de IT, cuyo rol en la estructura empresarial implica el mantenimiento y la seguridad de los sistemas corporativos.

A través de dicho análisis, Landwell identificará los riesgos que pueden venir asociados a una gestión ineficiente / descuidada por parte de la compañía de los procedimientos de seguridad, control y gestión de la protección de la compañía frente al uso no autorizado del sistema informático corporativo por parte de sus trabajadores o de terceros a los efectos de Websense pueda utilizar los mismos como argumento comercial para promocionar la venta de sus productos.

2. Resumen ejecutivo

El uso de los sistemas de información corporativos conlleva un conjunto de riesgos y amenazas, cuya falta de control puede llevar aparejada consecuencias altamente negativas para la organización, sus administradores y para las personas responsables de gestionar dichos recursos de forma correcta.

2.1. Amenazas

Los estudios y estadísticas sobre seguridad en la gestión de sistemas de información confirman que la mayoría de sus malos usos provienen de la propia organización, aunque también están sometidos a amenazas externas.

Las principales amenazas son:

a) Amenazas Internas

- Divulgación de información confidencial por los trabajadores de la empresa
- Envío de mensajes difamatorios bajo direcciones de e mail corporativas
- Uso de los sistemas corporativos para la descarga ilegal de obras o almacenamiento de contenidos ilícitos

b) Amenazas externas

- Accesos no autorizados a los sistemas de información corporativos
- Acceso no autorizado a secretos industriales e información confidencial (intrusión, *spyware*, etc...)
- Inutilización de los sistemas de información por ataques externos (virus, denegaciones de servicio, etc..).
- Defraudaciones (*phishing*, divulgación de claves de acceso, etc...).
- Uso de los sistemas corporativos por elementos externos para ataques a sistemas informáticos de terceros

2.2. Riesgos

Una falta de control adecuado de dichas amenazas, puede tener consecuencias enormemente negativas para las empresas y sus órganos directivos:

Riesgos para la empresa

- Perjuicios derivados de los daños o inutilización de los sistemas de información
- Pérdida de reputación y efectos negativos para la imagen de la empresa
- Riesgo de insolvencia

Riesgos para los administradores

Responsabilidad civil frente a la empresa, sus accionistas o frente a terceros en caso de falta de diligencia en la protección de los sistemas informáticos como activo de la empresa
Posible responsabilidad penal directa en algunos casos

Riesgo para el Director de Sistemas de Información

Posible despido en caso de falta de ejercicio diligente de sus funciones
Posibles responsabilidades civiles y penales en algunos casos

2.3. Conclusiones

Constituyendo los sistemas de información un elemento clave para el éxito empresarial, se hace necesario disponer de sistemas de protección adecuados frente a sus amenazas internas y externas, con el fin de asegurar su adecuado uso, así como para reducir y evitar posibles responsabilidades laborales, civiles y penales.

3. Análisis de los escenarios propuestos por Websense

3.1. Escenario 1

a) Descripción del escenario

El empleado utiliza los sistemas informáticos de la compañía y el acceso corporativo a Internet para enviar mensajes con contenido difamatorio durante el ejercicio de su actividad laboral.

b) Normativa afectada

Código Penal: Artículos 27 a 30.

Código Penal: Artículos de 205 a 219.

Por contenido difamatorio se entienden comprendidas las lesiones del derecho al honor que se corresponden con los tipos penales que el Código Penal identifica como calumnia e injuria.

Código Penal: Artículos 116 a 122, de las personas civilmente responsables.

Código Penal: Artículo 30, que establece el régimen de responsabilidad penal para los delitos y faltas.

c) Infracciones y Responsabilidades derivadas de las mismas

El Código Penal define en su Artículo 205 la calumnia como la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad. Se castiga con las penas de prisión de seis meses a dos años o multa de doce a 24 meses, si se propagaran con publicidad y, en otro caso, con multa de seis a 12 meses.

Por su parte, el delito de injurias se define en el Artículo 208 del Código Penal como la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación. Las injurias graves hechas con publicidad se castigarán con la pena de multa de seis a catorce meses y, en otro caso, con la de tres a siete meses.

El Artículo 211 del Código Penal especifica que la calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Una vez definido el tipo penal, en lo que se refiere a la determinación de la persona responsable, el ordenamiento español (Artículo 27 Código Penal) establece que incurren en responsabilidad criminal únicamente el autor del delito, es decir la persona emisora del mensaje calificado como calumnia o injuria y sus cómplices.

El Código Penal establece en su Artículo 30 un régimen específico en materia de responsabilidad penal para los delitos y faltas cometidos "utilizando medios o soportes de difusión mecánicos" (esto es, a través de los medios de comunicación social) independiente del régimen general de responsabilidad por autoría y participación criminal de los Artículos 27 a 29 del Código.

Los autores a los que se refiere el artículo 28 responderán de forma escalonada, excluyente y subsidiaria de acuerdo con el siguiente orden: 1º. Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo. 2º. Los directores de la publicación o programa en que se difunda. 3º. Los directores de la empresa editora, emisora o difusora. 4º. Los directores de la empresa grabadora, reproductora o impresora.

De acuerdo con este sistema de responsabilidad escalonada, la empresa responderá penalmente de forma subsidiaria al autor.

La determinación de la identidad del autor del delito resulta necesaria para que la compañía evite verse imputada.

Por su parte el ordenamiento español, en cuanto a la responsabilidad civil ex delicto considera responsables civiles las personas naturales o jurídicas que se dediquen a la industria o el comercio, por los delitos o faltas que hayan cometido sus empleados o dependientes, representantes o gestores en el desempeño de sus obligaciones o la prestación de sus servicios.

El hecho de que el envío del mensaje constitutivo de delito se lleve a cabo o no en el desempeño de la prestación de los servicios del empleado a la compañía determinará la consideración de la empresa como responsable civil.

En lo que respecta al régimen disciplinario, evidentemente la comisión de un delito por un empleado valiéndose de las herramientas proporcionadas por la empresa para el desempeño de las labores inherentes a su puesto de trabajo constituye una causa de despido disciplinario procedente por la trasgresión de la buena fe contractual Art. 54.1 ET.

El Responsable de IT de la compañía deberá en todo caso disponer de los mecanismos técnicos en sus sistemas que permitan la monitorización de los mensajes emitidos desde la compañía y la identificación de la autoría de los mismos, o como mínimo, hacer llegar a dirección de la compañía necesidad de adoptar estos mecanismos advirtiéndolo de los riesgos a los que está expuesta la compañía.

La ausencia de diligencia del Responsable de IT en esta materia supone una dejación de las funciones inherentes a su puesto de trabajo y, por consiguiente, puede dar lugar a una causa de despido procedente y una trasgresión de la buena fe contractual por comportamiento negligente.

d) Recomendaciones

- Incorporación en la normativa interna de utilización de los sistemas de información de la compañía de una mención relativa a la prohibición de emitir, en nombre o por cuenta de la compañía, determinados mensajes que puedan resultar difamatorios.
- Establecer en la normativa interna referencia expresa a la responsabilidad del empleado por el contenido de los mensajes que emita al exterior.
- Implementación de las medidas técnicas que permitan la monitorización y registro de la actividad de los empleados así como la elaboración de un procedimiento interno a los efectos de generar pruebas de forma legítima en relación con el acceso a Internet y la utilización del correo electrónico.

3.2. Escenario 2

a) Descripción del escenario

Almacenamiento, por parte del empleado, de material protegido por derechos de autor (obras musicales, películas, etc.) en su carpeta de servidor o de forma local en su ordenador.

b) Normativa afectada

Ley de Propiedad Intelectual 1/1996, de 12 de abril, que, en su Artículo 17, establece los derechos de explotación de los que el autor será titular, entre ellos el de reproducción de la obra.

Código Penal, artículos 270 y siguientes, en los que se tipifican los delitos relativos a la propiedad intelectual.

Normativa interna de la compañía.

Régimen disciplinario interno de la compañía y sectorial.

c) Infracciones y Responsabilidades derivadas de las mismas

La instalación, por parte del trabajador, de material protegido sin la correspondiente autorización del titular (obras musicales, películas, etc.) por derechos de propiedad intelectual en la red corporativa de la compañía o de forma local en su ordenador constituye una infracción de derechos de propiedad intelectual de la que será responsable la compañía debido a que la misma se realiza en sus equipos, siempre que no se hayan adoptado medidas preventivas.

Asimismo, en el supuesto de que el trabajador utilice dispositivos P2P de intercambio de ficheros a través de Internet, podría considerarse que el mismo distribuye materiales de forma no autorizada y con ánimo de lucro, debido a beneficio implícito de conseguir obras gratuitamente, constituyendo en un delito contra la propiedad intelectual imputable al trabajador conforme a lo dispuesto en el Artículo 270 del Código Penal.

En el supuesto de que la instalación no vulnere derechos de propiedad intelectual, ésta podría derivar en acciones de tipo disciplinario por parte de la compañía por uso no autorizado de las herramientas tecnológicas para fines privados. Asimismo, cabe destacar que dicho uso habitualmente lleva asociada la disminución del rendimiento del trabajador.

La realización de las acciones descritas en el supuesto de hecho analizado en el presente apartado por parte de un trabajador constituiría el quebrantamiento de la buena fe contractual predicada en el Artículo 20.2 y 5.1.a) del Estatuto de los Trabajadores como regente en la relación contractual entre trabajador y empresario. Cabe destacar, que el Artículo 54.1d) del Estatuto de los Trabajadores, en su definición de los incumplimientos contractuales por parte del trabajador que pueden provocar el despido disciplinario del mismo, incorpora la trasgresión de la buena fe contractual así como la disminución continuada y voluntaria del rendimiento del trabajador. Ambas circunstancias concurren en el supuesto de que el trabajador que lleve a cabo las acciones analizadas en el presente escenario, existan o no normas internas/corporativas explícitas prohibiendo las mismas y con independencia que la instalación se realice de forma abusiva o no abusiva¹.

Por lo que se refiere a la responsabilidad del Responsable de IT, cabe destacar que el mismo tiene la obligación de garantizar la seguridad de los sistemas informáticos corporativos, que puede verse amenazada por la instalación de materiales no autorizados procedentes de Internet, así como de controlar las características del tráfico de información procedentes de Internet y el volumen de las mismas. Por ello, el Responsable de IT deberá procurar la instalación de las herramientas técnicas necesarias en los sistemas de la compañía para identificar

¹ Existe jurisprudencia en sede social que considera el uso de herramientas corporativas para fines particulares como una trasgresión por parte del trabajador sea o no al misma abusiva o incluso si la misma no implica un retraso en el trabajo del trabajador: STSJ Murcia de 15 de junio 1999, STSJ Castilla y León/Valladolid de 29 de enero de 2001.

los intentos de almacenamiento de obras no autorizadas por la compañía o ilegales, y, en su caso, el bloqueo de los mismos.

Asimismo, el Responsable de IT será responsable de la distribución y conocimiento, por parte de los trabajadores, de la normativa corporativa en relación con el uso de Internet. Dichas normas son relevantes en el supuesto que nos ocupa debido a que las obras almacenadas por los trabajadores podrán ser descargadas de Internet.

En el supuesto que el Responsable de IT no realice de forma diligente sus funciones, podría considerarse que el mismo ha incurrido en el incumplimiento de las instrucciones de la empresa por la falta de realización de las tareas asignadas al mismo ya sea por negligencia o de forma dolosa, lo cual facultará al empresario a emprender acciones disciplinarias contra el mismo conforme a lo establecido en la normativa sectorial.

d) Recomendaciones

- Incorporación de la prohibición de la instalación de material protegido por derechos de autor (obras musicales, películas, etc.) en las normas corporativas.
- Notificación de las normas corporativas a los trabajadores de modo que se asegure el conocimiento de las mismas por parte de los trabajadores.
- Incorporación en los sistemas informáticos de la compañía de programas dirigidos al control de consumo de banda ancha, monitorización del consumo de Internet y de los sitios Web consultadas.
- Instalación de programas de control del rendimiento de los trabajadores a los efectos de detectar aquéllos casos en los que se produzca la pérdida de tiempo y rendimiento debido a la utilización de recursos de la empresa para albergar música, juegos, etc. y la posible práctica de los mismos en el ordenador de la compañía.
- Elaboración, por parte de la compañía, de un procedimiento interno a los efectos de generar pruebas de forma legítima en relación con el acceso a Internet de determinados trabajadores.

3.3. Escenario 3

a) Descripción del escenario

Se detecta la presencia de material de pornografía infantil en el ordenador de un empleado o en el espacio asignado determinado empleado en el servidor corporativo.

b) Normativa afectada

Código Penal: Artículo 27 a 30.

Código Penal: Artículos 187 a 190, delitos relativos a la prostitución y la corrupción de menores.

Código Penal: Artículos 116 a 122, de las personas civilmente responsables.

Régimen disciplinario interno.

c) Infracciones y Responsabilidades derivadas de las mismas

El tipo penal ante el que nos encontramos en el presente escenario es al que el Código Penal se refiere como "delitos relativos a la prostitución y la corrupción de menores".

El Artículo 189.2 se refiere a las circunstancias que concurren en el presente escenario, estableciendo que quien para su propio uso posea material pornográfico en cuya elaboración se hubieran utilizado menores de edad o incapaces, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.

El propio Artículo 189 establece una pena de uno a cuatro años para quien produjere, vendiere, distribuyere,

exhibiere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

El Artículo 189.7 hace extensiva la definición de pornografía infantil a material pornográfico en el que, no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada. Se establece una pena de prisión de tres meses a un año o multa de seis meses a dos años el que produjere, vendiere, distribuyere, exhibiere o facilitare por cualquier medio material este material.

Resulta relevante para la identificación de la conducta delictiva, la determinación de si el contenido pornográfico encontrado se limita al consumo privado o por el contrario puede considerarse que se constituye una actividad de distribución de estos contenidos.

Dado el carácter personal de las conductas delictivas en el ordenamiento español, únicamente resulta responsable penalmente el empleado que lleve a cabo la conducta delictiva.

No obstante, el Artículo 189.8 establece expresamente que se podrán imponer las medidas previstas en el artículo 129 del Código Penal cuando el culpable perteneciere a una sociedad, organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades. Estas medidas que podrá imponer el juez son las siguientes:

Clausura de la empresa, sus locales o establecimientos, con carácter temporal o definitivo. La clausura temporal no podrá exceder de cinco años.

Disolución de la sociedad, asociación o fundación.

Suspensión de las actividades de la sociedad, empresa, fundación o asociación por un plazo que no podrá exceder de cinco años.

Prohibición de realizar en el futuro actividades, operaciones mercantiles o negocios de la clase de aquellos en cuyo ejercicio se haya cometido, favorecido o encubierto el delito. Esta prohibición podrá tener carácter temporal o definitivo. Si tuviere carácter temporal, el plazo de prohibición no podrá exceder de cinco años.

La intervención de la empresa para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo necesario y sin que exceda de un plazo máximo de cinco años.

En el escenario en el que nos encontramos resulta altamente improbable que pueda considerarse que la compañía se dedique a la realización de tal actividad, dado que se trata de una actividad individual de un determinado empleado.

No obstante, será de aplicación el régimen a que se refiere el artículo 28 que regula la responsabilidad escalonada, y así, responderán de forma escalonada, excluyente y subsidiaria de acuerdo con el siguiente orden: 1.º Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo. 2º. Los directores de la publicación o programa en que se difunda. 3º. Los directores de la empresa editora, emisora o difusora. 4º. Los directores de la empresa grabadora, reproductora o impresora.

De acuerdo con este sistema de responsabilidad escalonada, la empresa responderá penalmente de forma subsidiaria al autor.

El ordenamiento español, en cuanto a la responsabilidad civil ex delicto (Artículo 116 Código Penal) considera responsables civiles las personas naturales o jurídicas que se dediquen a la industria o el comercio, por los delitos o faltas que hayan cometido sus empleados o dependientes, representantes o gestores en el desempeño de sus obligaciones o la prestación de sus servicios.

De ahí se desprende por tanto la necesidad de que la compañía disponga de las medidas y procedimientos de identificación y autenticación necesarias para probar que el material encontrado pertenece a determinado

empleado y que el empleado ha actuado al margen del desempeño de la prestación de sus servicios.

En este sentido, el Tribunal Constitucional en STC 82/2001, de 26 de marzo de 2001 establece que “La responsabilidad civil subsidiaria hay que proyectarla sobre la naturaleza del hecho delictivo que la genera y así, cuando un funcionario actúa fuera de servicio o cuando un empleado colabora con una actuación al margen de su tarea específica, libera a su principal de las consecuencias civiles de los delitos o faltas que cometiere”.

En lo que respecta al régimen disciplinario, evidentemente la comisión de un delito por un empleado valiéndose de las herramientas proporcionadas por la empresa para el desempeño de las labores inherentes a su puesto de trabajo constituye una causa de despido disciplinario procedente por la trasgresión de la buena fe contractual Art. 54.1 ET.

El Responsable de IT de la compañía, en el cumplimiento de sus funciones, deberá adoptar las medidas técnicas necesarias para evitar en lo posible este tipo de actividades. La dejación de estas funciones inherentes al cargo podría considerarse una trasgresión de la buena fe contractual por comportamiento negligente y ser causa de despido disciplinario.

d) Recomendaciones

- Con carácter preventivo resulta recomendable que la compañía adopte las medidas técnicas oportunas para evitar, controlar y registrar el acceso de los empleados a determinados contenidos, especialmente del correo y de la Web. Restringir el uso del navegador y el bloqueo de direcciones evita en gran medida las posibilidades de que tenga lugar el presente escenario así pone de relieve una actitud diligente de la compañía en aras de evitar estas actividades delictivas.
- Reiteramos la importancia de que la compañía disponga las medidas técnicas y procedimientos de identificación y autenticación que resulten necesarias para probar la autoría de todas las actividades que los usuarios de los sistemas lleven a cabo en todo momento.

3.4. Escenario 4

a) Descripción del escenario

El empleado instala en su ordenador de la empresa software no autorizado por la empresa o software pirata.

b) Normativa afectada

Ley de Propiedad Intelectual 1/1996, de 12 de abril, que, en su Artículo 99 describe el derecho exclusivo de los titulares de derechos de autor sobre programas de ordenador a realizar o autorizar su reproducción.

Código Penal, artículos 270 y siguientes, en los que se tipifican los delitos relativos a la propiedad intelectual.

Normativa interna de la compañía.

Régimen disciplinario interno de la compañía y sectorial.

c) Infracciones y Responsabilidades derivadas de las mismas

La instalación, por parte del trabajador, de software no autorizado en la red corporativa de la compañía o de forma local en su ordenador constituye una infracción de derechos de propiedad intelectual de la que será responsable la compañía debido a que la misma se realiza en sus equipos siempre que no haya adoptado las medidas preventivas correspondientes.

Asimismo, en el supuesto de que el trabajador utilice dispositivos P2P de intercambio de ficheros a través de Internet, podría considerarse que el mismo distribuye materiales de forma no autorizada y con ánimo de lucro,

debido a beneficio implícito de conseguir obras gratuitamente, constituyendo en un delito contra la propiedad intelectual imputable al trabajador conforme a lo dispuesto en el Artículo 270 del Código Penal.

En el supuesto de que el software instalado sea legal pero no autorizado por la compañía, instalar el mismo podría derivar en acciones de tipo disciplinario por parte de la compañía por uso no autorizado de las herramientas tecnológicas para fines privados. Asimismo, cabe destacar que dicho uso habitualmente lleva asociada la disminución del rendimiento del trabajador.

Con independencia de la existencia de normas internas de la compañía que explícitamente prohíban las acciones descritas en el supuesto de hecho analizado en el presente apartado, la instalación de software ilegal o no autorizado por la compañía constituiría el quebrantamiento de la buena fe contractual predicada en el Artículo 20.2 y 5.1.a) del Estatuto de los Trabajadores como regente en la relación contractual entre trabajador y empresario. Cabe destacar, que el Artículo 54.1d) del Estatuto de los trabajadores, en su definición de los incumplimientos contractuales por parte del trabajador que pueden provocar el despido disciplinario del mismo incorpora la trasgresión de la buena fe contractual así como la disminución continuada y voluntaria del rendimiento del trabajador. Ambas circunstancias concurren en el supuesto de que el trabajador que lleve a cabo las acciones analizadas en el presente escenario, existan o no normas internas/corporativas explícitas prohibiendo las mismas y con independencia que la instalación se realice de forma abusiva o no abusiva².

Por lo que se refiere a la responsabilidad del Responsable de IT, cabe destacar que el mismo tiene la obligación de garantizar la seguridad de los sistemas informáticos corporativos, que puede verse amenazada por la instalación de materiales no autorizados procedentes de Internet, así como de controlar las características del tráfico de información procedentes de Internet y el volumen de las mismas. Por ello, el Responsable de IT deberá procurar la instalación de las herramientas técnicas necesarias en los sistemas de la compañía para identificar los intentos de almacenamiento de obras no autorizadas por la compañía o ilegales, y, en su caso, el bloqueo de los mismos.

Asimismo, el Responsable de IT será responsable de la distribución y conocimiento, por parte de los trabajadores, de la normativa corporativa en relación con el uso de Internet. Dichas normas son relevantes en el supuesto que nos ocupa debido a que las obras almacenadas por los trabajadores podrán ser descargadas de Internet.

En el supuesto que el Responsable de IT no realice de forma diligente sus funciones, podría considerarse que el mismo ha incurrido en el incumplimiento de las instrucciones de la empresa por la falta de realización de las tareas asignadas al mismo ya sea por negligencia o de forma dolosa, lo cual facultará al empresario a emprender acciones disciplinarias contra el mismo conforme a lo establecido en la normativa sectorial.

d) Recomendaciones

- Incorporación de la prohibición de la instalación de software pirata o no autorizado por la compañía en las normas corporativas.
- Notificación de las normas corporativas a los trabajadores de modo que se asegure el conocimiento de las mismas por parte de los trabajadores.
- Incorporación en los sistemas informáticos de la compañía de programas dirigidos al control de consumo de banda ancha, monitorización del consumo de Internet y de los sitios Web consultados.
- Instalación de programas de control del rendimiento de los trabajadores a los efectos de detectar aquéllos casos en los que se produzca la pérdida de tiempo y rendimiento debido a la utilización de recursos de la empresa para albergar música, juegos, etc. y la posible práctica de los mismos en el ordenador de la compañía.

² Existe jurisprudencia en sede social que considera el uso de herramientas corporativas para fines particulares como una trasgresión por parte del trabajador sea o no al mismo abusiva o incluso si la misma no implica un retraso en el trabajo del trabajador: STSJ Murcia de 15 de junio 1999, STSJ Castilla y León/Valladolid de 29 de enero de 2001.

- Elaboración, por parte de la compañía, de un procedimiento interno a los efectos de generar pruebas de forma legítima en relación con el acceso a Internet de determinados trabajadores.

3.5. Escenario 5

a) Descripción del escenario

Una empresa contamina a otra empresa a causa de un virus o de spyware en su propio sitio Web.

b) Normativa afectada

Código Penal: Artículo 27 a 30 de las personas criminalmente responsables de los delitos y faltas.

Código Penal: Artículo 264.2, relativo a daños a datos, programas o documentos electrónicos ajenos.

Código Civil: Artículo 1902. Responsabilidad extracontractual.

c) Infracciones y Responsabilidades derivadas de las mismas

El artículo 264.2 del Código Penal establece una pena de prisión de uno a tres años y multa de doce a veinticuatro meses para el que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Puede observarse que la conducta típica no atiende a la existencia de voluntad del autor para causar el daño.

Será de aplicación el régimen a que se refiere el artículo 28 que regula la responsabilidad escalonada, y así, responderán de forma escalonada, excluyente y subsidiaria de acuerdo con el siguiente orden: 1.º Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo. 2º. Los directores de la publicación o programa en que se difunda. 3º. Los directores de la empresa editora, emisora o difusora. 4º. Los directores de la empresa grabadora, reproductora o impresora.

Adicionalmente al tipo penal mencionado, es evidentemente de aplicación el régimen de responsabilidad civil extracontractual de acuerdo con el Artículo 1902 del Código Civil que establece expresamente que el que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.

La responsabilidad civil derivada de la infección de determinados sistemas por un virus alojado en un Sitio Web corporativo corresponde al titular del sitio Web.

El Responsable de IT de la compañía, en el cumplimiento de sus funciones, deberá adoptar las medidas técnicas preventivas que eviten la causación de los daños. No tomar estas medidas preventivas conlleva la dejación de las funciones inherentes al cargo y constituir una trasgresión de la buena fe contractual por comportamiento negligente y ser causa de despido disciplinario.

d) Recomendaciones

- Utilización por el Responsable de IT de herramientas para la detección de virus, troyanos y cualesquiera otros elementos que puedan causar daños a terceros con el fin de evitar la causación de estos daños o, en su caso, demostrar la diligencia de la empresa en el control de sus sistemas informáticos.

3.6. Escenario 6

a) Descripción del escenario

El empleado guarda en un dispositivo USB información confidencial de la compañía y la divulga a terceros.

b) Normativa afectada

Normativa laboral: mala fe por parte del trabajador (Art. 5 y 20 ET) y convenios aplicables.

Normativa en materia de protección de datos:

a) Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal:

Artículo 9: obligación del responsable del fichero de aplicar las medidas de seguridad dispuestas en la normativa de desarrollo a los efectos de garantizar la seguridad de los datos de carácter personal;

Artículo 10: deber de secreto del responsable del fichero y de quienes intervengan en el tratamiento de los datos;

Artículo 44.1.e): infracción leve el incumplir el deber de secreto cuando no sea una infracción grave;

Artículo 44.3.h): infracción grave el no aplicar las medidas de seguridad;

Artículo 44.4.b): infracción muy grave la comunicación de datos personales salvo en los supuestos en que esté permitido);

b) Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal: deber del responsable del fichero de comunicar las normas a los empleados (Artículos 1 y 9).

Código Penal, Artículo 278 y 279 apoderamiento de secretos de la empresa y divulgación de los mismos; y 197, relativo al apoderamiento de datos reservados de carácter personal.

Código Penal, Artículo 30 relativo al régimen de responsabilidad de los delitos y faltas cometidos.

Código Civil: Artículo 1902. Responsabilidad extracontractual.

Ley de Sociedades Anónimas, Artículo 133 relativo a la Responsabilidad de los administradores.

Régimen disciplinario interno de la compañía y sectorial.

Normativa interna de la compañía.

c) Infracciones y Responsabilidades derivadas de las mismas

La apropiación y la divulgación de información confidencial de la compañía por parte de un trabajador constituye un ilícito penal tipificado en los Artículos 278 y 279 del Código Penal, la cual implica el quebrantamiento de la buena fe contractual para con el empresario y un comportamiento desleal así como, por otro lado, el abocar a la compañía a una situación de riesgo de infracción de la LOPD, lo cual lleva asociadas sanciones elevadas.

La compañía podrá emprender acciones legales contra trabajador por vía penal por apoderarse de la información y por su divulgación que podrían derivar en condena de hasta cinco años de prisión y multa de 12 a 24 meses, conforme a lo establecido por el Artículo 278 y 179.

Asimismo, el artículo 197.2 del Código Penal establece una pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses para aquel que se apodere, en perjuicio de tercero, de datos reservados de carácter personal. Dicha pena aumentará de dos a cinco años si los datos se revelan o difunden, tal y como sucede en el supuesto de hecho analizado en el presente apartado.

El Código Penal establece en su Artículo 30 un régimen específico en materia de responsabilidad penal para los

delitos y faltas cometidos a "utilizando medios o soportes de difusión mecánicos". De acuerdo con este sistema de responsabilidad escalonada, la empresa responderá penalmente de forma subsidiaria al autor por la divulgación de información confidencial así como de datos de carácter personal conforme a lo establecido por el Artículo 30 del Código Penal, en el que se establece: 1.º Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo. 2.º Los directores de la publicación o programa en que se difunda. 3.º Los directores de la empresa editora, emisora o difusora. 4.º Los directores de la empresa grabadora, reproductora o impresora.

De ello se desprende que conviene a la compañía el incorporar los medios necesarios para evitar que dichas situaciones se produzcan a los efectos de estar en condiciones de demostrar que la custodia de documentación confidencias y datos de carácter personal ha sido realizada con la con la máxima diligencia posible.

Adicionalmente a los tipos penales mencionados, es evidentemente de aplicación el régimen de responsabilidad civil extracontractual de acuerdo con el Artículo 1902 del Código Civil que establece expresamente que el que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.

Conforme a lo establecido por el Artículo 133 de la Ley de Sociedades Anónimas, los administradores responderán frente a la sociedad, frente a los accionistas y los acreedores sociales del daño causado por actos u omisiones o por los actos realizados incumpliendo los deberes inherentes al desempeño de su cargo. En el escenario que nos ocupa, los administradores de la compañía podrían responder por una omisión de la protección del deber de proteger la información confidencial de la compañía y sus activos inmateriales así como de realizar acciones dirigidas al control de los trabajadores.

Por lo que se refiere a los datos de carácter personal, la compañía es responsable de custodiar aquéllos albergados en sus sistemas y garantizar su seguridad y recae sobre la misma el deber de secreto. En el supuesto de producirse el robo de datos de carácter personal y su divulgación, la compañía podría llegar a ser responsable de una infracción muy grave de la LOPD consistente en la comunicación de datos a terceros de forma no autorizada, con sanciones de hasta 600.000 Euros.

Cabe destacar que el Responsable de IT, en el presente escenario, sería responsable la instalación de medios tecnológicos que permitan, conforme al estado de la técnica, el control y registro de la salida de información a través de los puertos USB. En el supuesto que no existan medios en el mercado suficientes para proteger los activos de la compañía frente a este tipo de ataques, el Responsable de IT tendrá la obligación de advertir a la compañía del riesgo así como proponer a la compañía medidas de protección alternativas a los efectos de conseguir el mayor grado de protección.

El Responsable de IT será también responsable de la distribución y conocimiento, por parte de los trabajadores, de la normativa corporativa en relación con el uso de las herramientas informáticas y al deber de secreto de los trabajadores.

En materia de medidas de seguridad aplicables a los soportes que incorporen datos de carácter personal, habitualmente el Responsable de IT, sea o no Responsable de Seguridad conforme a lo establecido en el RMS, será el responsable de la creación de procedimientos internos que garanticen el cumplimiento de la normativa en materia de protección de datos a los efectos de custodiar los datos de carácter personal de forma segura y de la divulgación de dichos procedimientos a los trabajadores de la compañía.

En el supuesto que el Responsable de IT no realice de forma diligente sus funciones, podría considerarse que el mismo ha incurrido en el incumplimiento de las instrucciones de la empresa por la falta de realización de las tareas asignadas al mismo ya sea por negligencia o de forma dolosa, lo cual facultará al empresario a emprender acciones disciplinarias contra el mismo conforme a lo establecido en la normativa sectorial. Sin embargo, cabe destacar que el presente escenario implica una acción dolosa por parte del trabajador que podría pasar inadvertida.

d) Recomendaciones

- Incorporar en las normas internas de la compañía el deber de secreto para los trabajadores de toda información de la compañía y la prohibición de su divulgación a terceros.
- Informar a los trabajadores, tal y como establece el Artículo 9 del RMS, de su obligación de velar por el secreto de los datos de carácter personal albergados en los sistemas de la compañía.
- Instalar, en los sistemas informáticos de la compañía, de herramientas técnicas dirigidas a identificar y evitar las posibles fugas de información por los puertos USB o cualquier otra vía.
- Establecer procedimientos internos por los que se limite el acceso de información a los trabajadores a aquella estrictamente necesaria para su puesto de trabajo.

3.7. Escenario 7

a) Descripción del escenario

Un empleado encargado de reportar a bancos sufre un ataque de phishing y comunica involuntariamente a un tercero las claves de acceso a la cuenta bancaria on-line de la compañía.

b) Normativa afectada

Régimen disciplinario interno.

Ley de Sociedades Anónimas, Artículo 133 relativo a la Responsabilidad de los administradores.

c) Infracciones y Responsabilidades derivadas de las mismas

El escenario no presenta la comisión de infracción alguna de carácter penal por parte del empleado. Por el contrario es el empleado, y por extensión la empresa, quienes son víctima de un delito de estafa (Art. 248 Código Penal) valiéndose para ello de la técnica del Phishing.

La jurisprudencia del Tribunal Supremo ha incluido como modalidad de estafa las que se llevan a cabo mediante manipulación informática u otros artificios semejantes (STS 2175/2001).

Para determinar la responsabilidad del empleado en el presente supuesto deberá realizarse un estudio individualizado de las características de la estafa de la que ha sido víctima. Con ello se determinará hasta que punto se trata de un error humano, o por el contrario, el empleado es responsable de no haber tomado las medidas oportunas para la verificación de la autenticidad del portal de la entidad bancaria, habida cuenta de que su puesto de trabajo se circunscribe a la realización de forma habitual de este tipo de actividades, y por ello se le ha de exigir una mayor diligencia.

Conforme a lo establecido por el Artículo 133 de la Ley de Sociedades Anónimas, los administradores responderán frente a la sociedad, frente a los accionistas y los acreedores sociales del daño causado por actos u omisiones o por los actos realizados incumpliendo los deberes inherentes al desempeño de su cargo.

En el escenario que nos ocupa, los administradores de la compañía podrían responder por una omisión del deber de proteger la información confidencial de la compañía y sus activos inmateriales así como de realizar acciones dirigidas al control y formación de los trabajadores.

Por lo que se refiere a la responsabilidad del responsable de IT de la compañía, éste deberá en todo caso advertir a la compañía de la obligación de informar de los riesgos asociados a las actividades de fishing y recomendar la realización de una formación específica para los usuarios que más posibilidades tienen de ser víctimas de fishing.

La ausencia de diligencia del Responsable de IT en esta materia supone una dejación de las funciones inherentes a su puesto de trabajo y, por consiguiente, puede dar lugar a una causa de despido procedente y una trasgresión de la buena fe contractual por comportamiento negligente.

d) Recomendaciones

- En la normativa interna de la compañía conviene establecer una mención a la utilización de Internet por los empleados, en el sentido de exigir a estos una extrema precaución y diligencia especialmente en los puestos de trabajos en los que, como en el presente escenario, se opere con datos bancarios u otros datos sensibles referidos a la compañía, de empleados o de clientes.
- Resultaría necesaria, especialmente en puestos de trabajo de especial riesgo, la formación del personal en sistemas así como en "Ingeniería Social" para demostrar una diligencia mínima en la evitación de este tipo de situaciones.
- En cuanto a medidas técnicas, recomendamos el establecimiento de controles de acceso a determinados contenidos y mecanismos que eviten el envío de información a direcciones IP que sean sospechosas de estar detrás de actividades ilícitas.

3.8. Escenario 8

a) Descripción del escenario

- Se instala spyware en el sistema informático de la compañía, lo cual implica el robo de la base de datos de personal de la misma.
- Se instala spyware en el sistema informático de una compañía dedicada al e-márketing, lo cual implica el robo de la base de datos de un cliente.

b) Normativa afectada

Normativa en materia de protección de datos:

a) Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal:

- Artículo 9: obligación del responsable del fichero de aplicar las medidas de seguridad dispuestas en la normativa de desarrollo a los efectos de garantizar la seguridad de los datos de carácter personal;
- Artículo 10: deber de secreto del responsable del fichero y de quienes intervengan en el tratamiento de los datos;
- Artículo 44.1.e): infracción leve el incumplir el deber de secreto cuando no sea una infracción grave;
- Artículo 44.3.h): infracción grave el no aplicar las medidas de seguridad;
- Artículo 44.4.b): infracción muy grave la comunicación de datos personales salvo en los supuestos en que esté permitido);

b) Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal: deber del responsable del fichero de comunicar las normas a los empleados (Artículos 1 y 9).

Código Penal, Artículo 278 y 279 apoderamiento de secretos de la empresa y divulgación de los mismos; y 197, relativo al apoderamiento de datos reservados de carácter personal.

Código Penal, Artículo 30 relativo al régimen de responsabilidad de los delitos y faltas cometidos.

Ley de Sociedades Anónimas, Artículo 133 relativo a la Responsabilidad de los administradores.

c) Infracciones y Responsabilidades derivadas de las mismas

La compañía es responsable de custodiar los datos de carácter personal albergados en sus sistemas y garantizar su seguridad y recae sobre la misma el deber de secreto.

El Artículo 9 de la LOPD establece que es obligación del responsable del fichero el aplicar las medidas de seguridad dispuestas en la normativa de desarrollo a los efectos de garantizar la seguridad de los datos de carácter personal habida cuenta del estado de la tecnología. De ello se deduce que la compañía deberá protegerse contra la instalación de spyware mediante la instalación de programas informáticos que se comercialicen para ello.

En el supuesto de producirse el robo de datos de carácter personal titularidad de la compañía y su divulgación, la compañía podría llegar a ser responsable de una infracción muy grave de la LOPD, con sanciones de hasta 600.000 Euros.

Cabe destacar que el Artículo 45.5 de la LOPD establece la posibilidad de disminuir la cuantía de una sanción por infracción de la LOPD, siendo aplicable las sanciones de grado inmediatamente menor, en aquéllos casos en los que concurra *“una cualificada disminución de la culpabilidad del imputado o de la antijuricidad del hecho”*. En el caso que nos ocupa, en que la compañía responsable del fichero podría ser sancionada por no haber evitado la divulgación datos de carácter personal de su titularidad como consecuencia de un ataque de spyware, la instalación de un programa que detecte y bloquee la instalación de spyware por parte de la compañía podría implicar la aplicación, por parte de la Agencia Española de Protección de Datos, de la citada reducción de la cuantía de la sanción.

Conforme a lo establecido por el Artículo 133 de la Ley de Sociedades Anónimas, los administradores responderán frente a la sociedad, frente a los accionistas y los acreedores sociales del daño causado por actos u omisiones o por los actos realizados incumpliendo los deberes inherentes al desempeño de su cargo. En el escenario que nos ocupa, los administradores de la compañía podrían responder por una omisión de la protección del deber de proteger la información confidencial de la compañía y sus activos inmateriales así como de realizar acciones dirigidas al control de los trabajadores.

Por lo que se refiere a la posible responsabilidad penal de la compañía, podría ser de aplicación el artículo 197.2 del Código Penal que establece una pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses para aquel que se apodere, en perjuicio de tercero, de datos reservados de carácter personal. Dicha pena aumentará de dos a cinco años si los datos se revelan o difunden, tal y como sucede en el supuesto de hecho analizado en el presente apartado.

El Código Penal establece en su Artículo 30 un régimen específico en materia de responsabilidad penal para los delitos y faltas cometidos a "utilizando medios o soportes de difusión mecánicos". De acuerdo con este sistema de responsabilidad escalonada, la empresa responderá penalmente de forma subsidiaria al autor por la divulgación de información confidencial así como de datos de carácter personal conforme a lo establecido por el Artículo 30 del Código Penal, en el que se establece: 1.º Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo. 2º. Los directores de la publicación o programa en que se difunda. 3º. Los directores de la empresa editora, emisora o difusora. 4º. Los directores de la empresa grabadora, reproductora o impresora.

De ello se desprende que conviene a la compañía el incorporar los medios necesarios para evitar que dichas situaciones se produzcan a los efectos de estar en condiciones de demostrar que la custodia de documentación confidenciales y datos de carácter personal ha sido realizada con la con la máxima diligencia posible.

Por lo que se refiere a la responsabilidad del Responsable de IT en relación con la instalación de spyware en los sistemas de la compañía, éste deberá en todo caso advertir a la compañía de dicha posibilidad y recomendar la instalación de medidas técnicas dirigidas a la detección y bloqueo de spyware.

En el supuesto que el Responsable de IT no realice de forma diligente sus funciones, podría considerarse que el mismo ha incurrido en el incumplimiento de las instrucciones de la empresa por la falta de realización de las tareas asignadas al mismo ya sea por negligencia o de forma dolosa, lo cual facultará al empresario a emprender acciones disciplinarias contra el mismo conforme a lo establecido en la normativa sectorial.

d) Recomendaciones

- Incorporar software destinado a bloquear la instalación de spyware en los sistemas de la compañía a los efectos de intentar minimizar la cuantía de la sanción en aquellos casos de instalación del mismo y robo de datos de carácter personal responsabilidad de la compañía.
- Incorporar, en los sistemas de Websense, un sistema de control de acceso a Webs (control de reenvío de información a direcciones IP).

3.9. Escenario 9

a) Descripción del escenario

Los ordenadores de la compañía forman parte, sin conocimiento de la empresa, de una red Botnet que realiza un ataque del tipo *denial of service* a una tercera empresa.

b) Normativa afectada

Código Penal: Artículo 27 a 30 de las personas criminalmente responsables de los delitos y faltas.

Código Penal: Artículo 264.2, relativo a daños a datos, programas o documentos electrónicos ajenos.

Código Penal, Artículos 27 al 30, relativos al régimen de responsabilidad de los delitos y faltas cometidos.

DECISIÓN MARCO 2005/222/JAI DEL CONSEJO de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

Código Civil: Artículo 1902. Responsabilidad extracontractual.

Ley de Sociedades Anónimas, Artículo 133 relativo a la Responsabilidad de los administradores.

c) Infracciones y Responsabilidades derivadas de las mismas

En lo que se refiere a la determinación de la persona responsable, el Artículo 27 Código Penal establece que incurren en responsabilidad criminal únicamente el autor del delito y sus cómplices.

El Código Penal establece en su Artículo 30 un régimen específico en materia de responsabilidad penal para los delitos y faltas cometidos a "utilizando medios o soportes de difusión mecánicos" (esto es, a través de los medios de comunicación social) independiente del régimen general de responsabilidad por autoría y participación criminal de los Artículos 27 a 29 del Código.

Así, el Artículo 30.2 del Código penal establece que los autores a los que se refiere el artículo 28 responderán de forma escalonada, excluyente y subsidiaria de acuerdo con el siguiente orden: 1º. Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo. 2º. Los directores de la publicación o programa en que se difunda. 3º. Los directores de la empresa editora, emisora o difusora. 4º. Los directores de la empresa grabadora, reproductora o impresora.

De acuerdo con este sistema de responsabilidad escalonada, la empresa responderá penalmente de forma subsidiaria al autor.

La Decisión Marco 2005/222/JAI del Consejo establece una serie de medidas contra el hacking, entendiendo por hacking tanto el acceso ilegal a datos como la causación de daños en datos, programas o sistemas informáticos ajenos.

La Decisión Marco tiene especial relevancia en lo que se refiere a que considera responsable de la realización de estas actividades:

- A la persona jurídica en beneficio de la cual se haya realizado el hacking.
- A la persona jurídica que haya hecho posible que una persona sometida a su autoridad cometa las mencionadas infracciones.

Tanto la responsabilidad escalonada que establece el Código Penal como el contenido de la Decisión Marco antes mencionada daría lugar a la consideración de la empresa como responsable de las actividades de hacking llevadas a cabo desde sus sistemas corporativos por no haber adoptado las medidas necesarias para evitar la realización de la actividad ilícita.

De acuerdo con el ordenamiento español, los empleados que han creado la red son los primeros responsables penales de la comisión del delito en calidad de autores materiales no obstante lo cual es evidente que la compañía desde la cual se realiza el hecho ilícito será declarada responsable subsidiaria y responsable civil derivada de delito, por los daños que haya ocasionado.

Sin perjuicio de la próxima implementación de estas medidas en el ordenamiento interno español, la comisión de un hacking consistente en la causación de un denial of service a un tercero se encuadra en el tipo delictivo establecido en el Art. 264.2 del Código Penal, delito de daños.

Estas formas de ataque atentan contra la red sobrecargándola con mensajes artificiales que dificultan o impiden el acceso legítimo. La causación de daños de este tipo a empresas que ofrecen sus productos de forma on-line es muy importante ya que por un ataque del tipo "denegación de servicio" pueden verse paralizadas.

El artículo 264.2 del Código Penal establece una pena de prisión de uno a tres años y multa de doce a veinticuatro meses para el que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

En el orden interno, en el supuesto de que el Responsable de IT no fuera conocedor de estos hechos y, por consiguiente no fuera autor material del delito, tiene una evidente responsabilidad por cuanto sus funciones principales estriban en el control y vigilancia del uso de los sistemas informáticos de la compañía.

En el plano laboral por tanto, en el presente escenario es evidente la vulneración de la buena fe contractual dolosa de los autores del delito así como la existencia de una causa de despido procedente por vulneración de la buena fe contractual por comportamiento negligente del Responsable de IT.

Conforme a lo establecido por el Artículo 133 de la Ley de Sociedades Anónimas, los administradores responderán frente a la sociedad, frente a los accionistas y los acreedores sociales del daño causado por actos u omisiones o por los actos realizados incumpliendo los deberes inherentes al desempeño de su cargo.

En el escenario que nos ocupa, los administradores de la compañía podrían responder por una omisión de la protección del deber de proteger la información confidencial de la compañía y sus activos inmateriales así como de realizar acciones dirigidas al control de los trabajadores.

d) Recomendaciones

- Incorporación de la prohibición de la realización de dichas actividades en las normas corporativas.
- Utilización por el Responsable de IT de herramientas para la detección de actividades prohibidas por la normativa interna o constitutivas de infracción penal, administrativa o de cualquier otra índole.

3.10. Escenario 10

a) Descripción del escenario

La esposa de un trabajador se conecta de forma remota con el ordenador portátil de la compañía a la red corporativa y causa la propagación de un virus.

b) Normativa afectada

Normativa laboral: quebrantamiento de la buena fe contractual por parte del trabajador (Art. 5 y 20 ET) y convenios aplicables.

Código Penal: Artículo 264.2, relativo a daños a datos, programas o documentos electrónicos ajenos.

Normativa en materia de protección de datos:

a) Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal:

Artículo 9: obligación del responsable del fichero de aplicar las medidas de seguridad dispuestas en la normativa de desarrollo a los efectos de garantizar la seguridad de los datos de carácter personal;

Artículo 10: deber de secreto del responsable del fichero y de quienes intervengan en el tratamiento de los datos;

Artículo 44.1.e): infracción leve el incumplir el deber de secreto cuando no sea una infracción grave;

Artículo 44.3.h): infracción grave el no aplicar las medidas de seguridad;

Artículo 44.4.b): infracción muy grave la comunicación de datos personales salvo en los supuestos en que esté permitido);

b) Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal: deber del responsable del fichero de comunicar las normas a los empleados (Artículos 1 y 9).

Código Civil: Artículo 1902. Responsabilidad extracontractual.

c) Infracciones y Responsabilidades derivadas de las mismas

El presente escenario conlleva el incumplimiento, por parte del trabajador, de la normativa interna de la compañía que habitualmente establece la prohibición al trabajador de facilitar su nombre de usuario y clave a una persona ajena a la compañía y el quebrantamiento de la buena fe contractual que dicho incumplimiento implica, suficientes para que la compañía emprenda acciones disciplinarias contra el trabajador.

Sin perjuicio de lo indicado, la instalación de un virus en el sistema de la compañía coincide con el tipo penal descrito en el artículo 264.2 del Código Penal que establece una pena de prisión de uno a tres años y multa de doce a veinticuatro meses para el que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Puede observarse que la conducta típica no atiende a la existencia de voluntad del autor para causar el daño. En el caso que nos ocupa, la autora sería la esposa del trabajador.

Adicionalmente al tipo penal mencionado, es evidentemente de aplicación el régimen de responsabilidad civil extracontractual de acuerdo con el Artículo 1902 del Código Civil que establece expresamente que el que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.

El responsable de IT debería asegurar la protección de los sistemas informáticos de la compañía mediante la instalación de herramientas que eviten la instalación de virus en dichos sistemas.

En el supuesto que el Responsable de IT no realice de forma diligente sus funciones, podría considerarse que el mismo ha incurrido en el incumplimiento de las instrucciones de la empresa por la falta de realización de las tareas asignadas al mismo ya sea por negligencia o de forma dolosa, lo cual facultará al empresario a emprender acciones disciplinarias contra el mismo conforme a lo establecido en la normativa sectorial.

d) Recomendaciones

- Incorporar en las normas corporativas la prohibición a los trabajadores de comunicar sus claves a cualquier otra persona.
- Utilización por el Responsable de IT de herramientas para la detección de virus y cualesquiera otros elementos que puedan causar daños a terceros con el fin de evitar la causación de los daños o, en su caso, demostrar la diligencia de la empresa en el control de sus sistemas informáticos.

Websense, Inc
World Headquarters
10240 Sorrento Valley Road
San Diego, California 92121
USA

Tel: +1 800 723 1166

www.websense.com
www.websense.com.es

Karen Gaines Cordero
Country Manager, Websense Iberia
Calle Ribera del Loira 46
28042 Madrid
Spain

Tel:+34 699 233 332

kgaines@websense.com
www.websense.com.es

Descargue el software gratuitamente durante un periodo de evaluación de 30 días en www.websense.com/downloads



©2007 Websense, Inc. Todos los derechos reservados. Websense y Websense Enterprise son marcas comerciales registradas de Websense, Inc. en los Estados Unidos y en ciertos mercados internacionales. Websense dispone muchas otras marcas comerciales no registradas en los Estados Unidos y el resto del mundo. El resto de marcas comerciales son propiedad de sus respectivos propietarios. ES_WP_Oct07