

**FUENTE :**



**Nota:**

**La responsabilidad directa de las empresas y sus directivos por las infracciones previstas en esta Decisión que cometan sus empleados es uno de los argumentos jurídicos para la implantación de la ISO 17799 (Sistema de gestión de la seguridad de la información) y la obtención de la certificación de AENOR correspondiente a la norma UNE 71502**

(Actos adoptados en aplicación del título VI del Tratado de la Unión Europea)

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

EL CONSEJO DE LA UNIÓN EUROPEA, Visto el Tratado de la Unión Europea y, en particular, sus artículos 29, 30, apartado 1, letra a), 31, apartado 1, letra e), y 34, apartado 2, letra b),

Vista la propuesta de la Comisión, Visto el dictamen del Parlamento Europeo (1),

Considerando lo siguiente:

(1) El objeto de la presente Decisión marco es reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, incluida la policía y los demás servicios represivos especializados de los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información.

(2) Se ha comprobado la existencia de ataques contra los sistemas de información, en particular como consecuencia de la amenaza de la delincuencia organizada, y crece la inquietud ante la posibilidad de ataques terroristas contra sistemas de información que forman parte de las infraestructuras vitales de los Estados miembros. Esto pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia, y por tanto exige una respuesta por parte de la Unión Europea.

(3) Para responder con eficacia a esas amenazas es necesario un planteamiento global en materia de seguridad de las redes y de la información, como se puso de manifiesto en el plan de acción eEurope, en la Comunicación de la Comisión titulada «Seguridad de las redes y de la información: Propuesta para una perspectiva política europea» y en la Resolución del Consejo de 28 de enero de 2002 relativa a un enfoque común y a acciones específicas en materia de seguridad de las redes y de la información (2).

(4) En la Resolución del Parlamento Europeo de 5 de septiembre 2001 se destaca la necesidad de sensibilizar más al público sobre los problemas relacionados con la seguridad de la información, así como de proporcionar asistencia práctica.

(5) La distancia y las divergencias significativas que existen entre las legislaciones de los Estados miembros en este ámbito pueden dificultar la lucha contra la delincuencia organizada y el terrorismo y pueden complicar la cooperación eficaz de los servicios de policía y las administraciones de justicia en materia de ataques contra los sistemas de información. La naturaleza transnacional y transfronteriza de los modernos sistemas de información significa que los ataques suelen revestir un carácter transfronterizo, lo que plantea la necesidad urgente de proseguir la aproximación de las legislaciones penales en este ámbito.

(6) El plan de acción del Consejo y de la Comisión sobre la mejor manera de aplicar las disposiciones del Tratado de Amsterdam relativas a la creación de un espacio de libertad, seguridad y justicia (3), las

conclusiones del Consejo Europeo de Tampere de los días 15 y 16 de octubre de 1999, las del Consejo Europeo de Santa María da Feira de los días 19 y 20 de junio de 2000, el «Marcador» de la Comisión y la Resolución del Parlamento Europeo de 19 de mayo de 2000 constituyen o reclaman medidas legislativas contra la delincuencia de alta tecnología, lo cual abarca definiciones, tipificaciones y sanciones comunes.

(7) Es necesario dar un complemento a los trabajos realizados por las organizaciones internacionales, más concretamente los del Consejo de Europa sobre la armonización del Derecho penal y los del G-8 sobre la cooperación transnacional en el ámbito de la delincuencia de alta tecnología, ofreciendo un enfoque común de la Unión Europea en este ámbito. Esta invitación se desarrolló más ampliamente en la Comunicación que la Comisión envió al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones, titulada «Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos».

(8) Debe aproximarse la legislación penal en materia de ataques contra los sistemas de información para conseguir la mayor cooperación policial y judicial posible respecto de las infracciones penales vinculadas a ataques contra los sistemas de información y para contribuir a la lucha contra el terrorismo y la delincuencia organizada.

(9) Todos los Estados miembros han ratificado el Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Los datos personales tratados en el contexto de la aplicación de la presente Decisión marco se protegerán de conformidad con los principios de dicho Convenio.

(10) Unas definiciones comunes en este ámbito, más concretamente de los sistemas de información y los datos informáticos, son importantes para garantizar la aplicación coherente de la presente Decisión marco en los Estados miembros.

(11) Es necesario llegar a un enfoque común respecto de los elementos constitutivos de las infracciones penales, estableciendo delitos comunes de acceso ilegal a un sistema de información intromisión ilegal en el sistema e intromisión ilegal en los datos.

(12) Para combatir los delitos cibernéticos, cada Estado miembro debe garantizar una cooperación judicial efectiva respecto de los delitos basados en los tipos de conducta contemplados en los artículos 2, 3, 4 y 5. (13) Es necesario evitar una tipificación penal excesiva, especialmente de los casos de menor gravedad, así como la inculpación de titulares de derechos y personas autorizadas.

(14) Es necesario que los Estados miembros prevean sanciones para reprimir los ataques contra los sistemas de información. Las sanciones previstas deberán ser efectivas, proporcionadas y disuasorias.

(15) Es conveniente establecer sanciones más severas cuando un ataque contra un sistema de información se comete en el marco de una organización delictiva, tal como se define en la Acción Común 98/733/JAI, de 21 de diciembre de 1998, relativa a la tipificación penal de la participación en una organización delictiva en los Estados miembros de la Unión Europea (1). Asimismo es conveniente establecer sanciones más severas cuando dicho ataque haya causado daños graves o afectado a intereses esenciales.

(16) Deben también preverse medidas de cooperación entre los Estados miembros con el fin de combatir eficazmente los ataques contra los sistemas de información. Por consiguiente, los Estados miembros deben hacer uso de la red existente de puntos de contacto operativos para el intercambio de información a los que se hace referencia en la Recomendación del Consejo de 25 de junio de 2001 sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología (2).

(17) Dado que los objetivos de la Decisión marco propuesta, a saber, garantizar que los ataques contra los sistemas de información sean castigados en todos los Estados miembros mediante sanciones penales

efectivas, proporcionadas y disuasorias y mejorar y fomentar la cooperación judicial superando las posibles complicaciones, no pueden ser alcanzados de manera suficiente por los Estados miembros, ya que las normas tienen que ser comunes y compatibles, y, por consiguiente, pueden lograrse mejor a escala de la Unión, ésta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado CE. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Decisión marco no excede de lo necesario para alcanzar dichos objetivos.

(18) La presente Decisión marco respeta los derechos fundamentales y los principios reconocidos en el artículo 6 del Tratado de la Unión Europea y reflejados en la Carta de los Derechos Fundamentales de la Unión Europea, en particular en sus capítulos II y VI.

HA ADOPTADO LA PRESENTE DECISIÓN MARCO:

## Artículo 1

### Definiciones

A los efectos de la presente Decisión marco se entenderá por:

- a) «sistema de información», todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento;
- b) «datos informáticos», toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función;
- c) «persona jurídica», toda entidad a la cual el derecho vigente reconoce este estatuto, salvo los Estados y otros organismos públicos que ejercen prerrogativas estatales y las organizaciones internacionales de derecho público,
- d) «sin autorización», el acceso o la intromisión no autorizados por el propietario o titular de otro tipo de derecho sobre el sistema o parte del mismo o no permitidos por la legislación nacional.

## Artículo 2

### Acceso ilegal a los sistemas de información

1. Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.
2. Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad.

## Artículo 3

### Intromisión ilegal en los sistemas de información

Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de

información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

#### Artículo 4

##### Intromisión ilegal en los datos

Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

#### Artículo 5

##### Inducción, complicidad y tentativa

1. Cada Estado miembro garantizará que la inducción a los delitos contemplados en los artículos 2, 3 y 4 y la complicidad con ellos sean sancionables como infracciones penales.
2. Cada Estado miembro garantizará que la tentativa de cometer los delitos mencionados en los artículos 2, 3 y 4 sea sancionable como infracción penal.
3. Cada Estado miembro podrá decidir que no se aplique el apartado 2 a las infracciones mencionadas en el artículo 2.

#### Artículo 6

##### Sanciones

1. Cada Estado miembro adoptará las medidas necesarias para garantizar que las infracciones mencionadas en los artículos 2, 3, 4 y 5 se castiguen con sanciones penales efectivas, proporcionadas y disuasorias.
2. Cada Estado miembro adoptará las medidas necesarias para garantizar que las infracciones mencionadas en los artículos 3 y 4 se castiguen con sanciones penales de uno a tres años de prisión como mínimo en su grado máximo.

#### Artículo 7

##### Circunstancias agravantes

1. Cada Estado miembro adoptará las medidas necesarias para garantizar que las infracciones mencionadas en los artículos 2, apartado 2, 3 y 4 se castiguen con sanciones penales de dos a cinco años de prisión como mínimo en su grado máximo cuando se cometan en el marco de una organización delictiva tal como la define la Acción Común 98/733/JAI, con independencia del nivel de sanción mencionado en dicha Acción Común.
2. Los Estados miembros podrán adoptar asimismo las medidas contempladas en el apartado 1 cuando la infracción de que se trate haya ocasionado graves daños o afectado a intereses esenciales.

#### Artículo 8

## Responsabilidad de las personas jurídicas

1. Cada Estado miembro adoptará las medidas necesarias para que a las personas jurídicas se les puedan exigir responsabilidades por las infracciones mencionadas en los artículos 2, 3, 4 y 5, cuando dichas infracciones sean cometidas en su beneficio por cualquier persona, actuando a título particular o como parte de un órgano de la persona jurídica, que ostente un cargo directivo en el seno de dicha persona jurídica basado en:

- a) un poder de representación de dicha persona jurídica, o
- b) una autoridad para tomar decisiones en nombre de dicha persona jurídica, o
- c) una autoridad para ejercer un control en el seno de dicha persona jurídica.

2. Sin perjuicio de los casos previstos en el apartado 1, los Estados miembros garantizarán que a las personas jurídicas se les puedan exigir responsabilidades cuando la falta de vigilancia o control por parte de alguna de las personas a que se refiere el apartado 1 haya hecho posible que una persona sometida a su autoridad cometa las infracciones mencionadas en los artículos 2, 3, 4 y 5 en beneficio de esa persona jurídica.

3. La responsabilidad de las personas jurídicas en virtud de los apartados 1 y 2 se entenderá sin perjuicio de la incoación de acciones penales contra las personas físicas que sean autores, incitadores o cómplices en la comisión de las infracciones mencionadas en los artículos 2, 3, 4 y 5.

## Artículo 9

### Sanciones aplicables a las personas jurídicas

1. Cada Estado miembro adoptará las medidas necesarias para que a la persona jurídica considerada responsable en virtud de lo dispuesto en el artículo 8, apartado 1, le sean impuestas sanciones efectivas, proporcionadas y disuasorias, que incluirán multas de carácter penal o administrativo y podrán incluir otras sanciones, tales como:

- a) exclusión del disfrute de ventajas o ayudas públicas;
- b) prohibición temporal o permanente del desempeño de actividades comerciales;
- c) vigilancia judicial, o
- d) medida judicial de liquidación.

2. Cada Estado miembro adoptará las medidas necesarias para que a la persona jurídica considerada responsable en virtud de lo dispuesto en el artículo 8, apartado 2, le sean impuestas sanciones o medidas efectivas, proporcionadas y disuasorias.

## Artículo 10

### Competencia

1. Cada Estado miembro establecerá su competencia respecto de las infracciones mencionadas en los artículos 2, 3, 4 y 5 cuando la infracción se haya cometido:

- a) total o parcialmente en su territorio, o
- b) por uno de sus nacionales, o
- c) en beneficio de una persona jurídica que tenga su domicilio social en el territorio de ese Estado miembro.

2. Al establecer su competencia de acuerdo con el apartado 1, letra a), cada Estado miembro garantizará que

su competencia incluya los casos en que:

- a) el autor de la infracción comete ésta estando físicamente presente en su territorio, independientemente de que la infracción se cometa o no contra un sistema de información situado en su territorio, o
- b) la infracción se comete contra un sistema de información situado en su territorio, independientemente de que el delincuente cometa o no la infracción estando físicamente presente en su territorio.

3. Todo Estado miembro que, con arreglo a su legislación, aún no extradite o entregue a sus nacionales adoptará las medidas necesarias para establecer su competencia y, en su caso, iniciar acciones judiciales respecto de las infracciones mencionadas en los artículos 2, 3, 4 y 5 cuando las haya cometido uno de sus nacionales fuera de su territorio.

4. Cuando una infracción sea competencia de más de un Estado miembro y cualquiera de estos Estados pueda legítimamente iniciar acciones judiciales por los mismos hechos, los Estados miembros de que se trate colaborarán para decidir cuál de ellos iniciará acciones judiciales contra los autores de la infracción, con el objetivo de centralizar, en la medida de lo posible, dichas acciones en un solo Estado miembro. Con este fin, los Estados miembros podrán recurrir a cualquier órgano o mecanismo creado en el marco de la Unión Europea para facilitar la cooperación entre sus autoridades judiciales y la coordinación de sus actuaciones. Se podrán tener en cuenta los siguientes criterios por orden consecutivo:

- el Estado miembro en cuyo territorio se hayan cometido las infracciones de acuerdo con los apartados 1, letra a), y 2,
- el Estado miembro del que sea nacional el autor,
- el Estado miembro en el que se haya encontrado al autor.

5. Un Estado miembro podrá decidir no aplicar, o aplicar sólo en casos o circunstancias específicas, las normas de competencia establecidas en el apartado 1, letras b) y c).

6. Los Estados miembros informarán a la Secretaría General del Consejo y a la Comisión de su decisión de aplicar el apartado 5, indicando, si procede, los casos o circunstancias específicos en los cuales se aplica dicha decisión.

## Artículo 11

### Intercambio de información

1. A efectos del intercambio de información sobre las infracciones mencionadas en los artículos 2, 3, 4 y 5, y de acuerdo con las normas de protección de datos, los Estados miembros procurarán hacer uso de la red existente de puntos de contacto operativos disponibles las 24 horas del día todos los días de la semana.
2. Cada Estado miembro comunicará a la Secretaría General del Consejo y a la Comisión los puntos de contacto designados para el intercambio de información sobre las infracciones relativas a los ataques contra los sistemas de información. La Secretaría General transmitirá esta información a los demás Estados miembros.

## Artículo 12

### Aplicación

1. Los Estados miembros adoptarán las medidas necesarias para dar cumplimiento a la presente Decisión

marco a más tardar el 16 de marzo de 2007.

2. A más tardar el 16 de marzo de 2007, los Estados miembros transmitirán a la Secretaría General del Consejo y a la Comisión el texto de las disposiciones por las que incorporen a su Derecho nacional las obligaciones que la presente Decisión marco les impone. Tomando como base un informe elaborado a partir de estos datos y un informe escrito de la Comisión, el Consejo evaluará, a más tardar el 16 de septiembre de 2007, en qué medida los Estados miembros han dado cumplimiento a las disposiciones de la presente Decisión marco.

### Artículo 13

#### Entrada en vigor

La presente Decisión marco entrará en vigor el día de su publicación en el Diario Oficial de la Unión Europea.

Hecho en Bruselas, el 24 de febrero de 2005.

Por el Consejo  
El Presidente  
N. SCHMIT