DECISIÓN DEL CONSEJO

de 31 de marzo de 1992

relativa a la seguridad de los sistemas de información

(92/242/CEE)

EL CONSEJO DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Económica Europea y, en particular, su artículo 235,

Vista la propuesta de la Comisión (1),

Visto el dictamen del Parlamento Europeo (2),

Visto el dictamen del Comité Económico y Social (3),

Considerando que la Comunidad tiene por misión promover, mediante el establecimiento de un mercado común y la progresiva aproximación de las políticas económicas de los Estados miembros, un desarrollo armonioso de las actividades económicas en el conjunto de la Comunidad, una expansión continua y equilibrada, una estabilidad creciente, una elevación acelerada del nivel de vida y relaciones más estrechas entre los Estados que la integran ;

Considerando que la información almacenada, tratada y transmitida por medios electrónicos desempeña un papel cada vez más importante en las actividades económicas y sociales ;

Considerando que la implantación de unas comunicaciones globales y eficaces y la generalización del tratamiento electrónico de la información acentúan la necesidad de contar con una protección adecuada de los usuarios ;

Considerando que el Parlamento Europeo, en sus deliberaciones y resoluciones, ha subrayado repetidamente la importancia de la seguridad de los sistemas de información ;

Considerando que el Comité Económico y Social ha destacado la necesidad de tomar medidas comunitarias sobre los asuntos relacionados con la seguridad de los sistemas de información, particularmente con vistas a las repercusiones de la realización del mercado interior ;

Considerando que las acciones llevadas a cabo a nivel nacional, internacional y comunitario representan una buena base ;

Considerando que existe una estrecha relación entre las telecomunicaciones, la tecnología de la información, la normalización, el mercado de la información, las políticas de investigación y desarrollo tecnológico y los trabajos ya emprendidos en estos ámbitos por la Comunidad ;

Considerando que conviene concertar los esfuerzos apoyándose en los trabajos nacionales e internacionales ya existentes y fomentando la cooperación de los principales interesados ; que, por tanto, conviene proceder en el marco de un plan de acción coherente ;

Considerando que la complejidad de la seguridad de los sistemas de información requiere el desarrollo de estrategias que permitan la libre circulación de información en el mercado único garantizando al mismo tiempo la seguridad de utilización de los sistemas de información en toda la Comunidad ;

Considerando que es responsabilidad de cada Estado miembro tener en cuenta las limitaciones que imponen la seguridad y el orden público ;

Considerando que la responsabilidad de los Estados miembros en este ámbito supone un enfoque concertado basado en una estrecha colaboración con altos funcionarios de los Estados miembros ;

Considerando que procede establecer una acción que incluya un plan de acción durante un período inicial de 24 meses y crear un Comité de altos funcionarios con un mandato a largo plazo para asesorar a la Comisión sobre las acciones en materia de seguridad de los sistemas de información ;

Considerando que se estima necesario un importe de 12 millones de ecus para ejecutar la acción durante un período inicial de 24 meses ; que los fondos estimados necesarios para 1992 ascienden a 2 millones de ecus, en el marco de la actual perspectiva financiera ;

Considerando que los importes que se deberán comprometer para la financiación del programa para el período siguiente al ejercicio de 1992 tendrán que incluirse en el marco financiero comunitario vigente,

DECIDE :

Artículo 1

Mediante la presente Decisión se adopta una acción, en el ámbito de la seguridad de los sistemas de información. Dicha acción incluye :

— el desarrollo de estrategias globales para la seguridad de los sistemas de información (plan de acción) durante un período inicial de 24 meses, y

— la creación de un grupo de altos funcionarios, en lo sucesivo denominado « Comité », que tendrá la misión a largo plazo de asesorar a la Comisión sobre acciones en materia de seguridad de los sistemas de información.

(1) DO nº C 277 de 5. 11. 1990, p. 18.
(2) DO nº C 94 de 13. 3. 1992.
(3) DO nº C 159 de 17. 6. 1991, p. 38.

Artículo 2

1. La Comisión consultará sistemáticamente al Comité sobre las cuestiones relacionadas con la seguridad de los sistemas de información de las diferentes actividades comunitarias en particular acerca de la definición de estrategias y programas de trabajo.

2. El plan de acción, como se indica en el Anexo, incluirá los trabajos preparatorios relativos a los siguientes temas :

I. Desarrollo de un marco estratégico para la seguridad de los sistemas de información.

II. Definición de las necesidades de los usuarios y de los prestadores de servicios en materia de seguridad de los sistemas de información.

III. Elaboración de soluciones para determinadas necesidades a corto y medio plazo de los usuarios, de los proveedores y prestadores de servicios.

IV. Desarrollo de especificaciones, normalización, evaluación y certificación respecto a la seguridad de los sistemas de información.

V. Innovaciones técnicas y de funcionamiento en materia de seguridad de los sistemas de información.

VI. Puesta en práctica de la seguridad de los sistemas de información.

Artículo 3

1. El importe de los recursos financieros comunitarios considerado necesario para la aplicación de la acción durante un período inicial de 24 meses es de 12 millones de ecus, de los cuales 2 millones de ecus para el período 1991-1992 en el marco de las perspectivas financieras 1988-1992.

Para el período ulterior de aplicación de la acción, el importe deberá insertarse en el marco financiero comunitario vigente.

2. La autoridad presupuestaria determinará los créditos disponibles para cada ejercicio atendiendo a los principios de buena gestión contemplados en el artículo 2 del Reglamento financiero aplicable al presupuesto general de las Comunidades Europeas.

Artículo 4

Un grupo de expertos independientes evaluará para la Comisión los progresos realizados durante los 24 meses iniciales del plan de acción. El informe de grupo, junto con los comentarios de la Comisión se remitirán al Parlamento Europeo y al Consejo.

Artículo 5

1. La Comisión será responsable de la ejecución de la acción. Estará asistida por un Comité consultivo compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

2. El plan de acción se ejecutará de acuerdo con los objetivos establecidos en el artículo 2, que se actualizará cuando sea necesario. El plan establecerá los objetivos pormenorizados y los tipos de medidas que deban tomarse, así como las disposiciones financieras al respecto. La Comisión hará convocatorias de propuestas tomando por base el plan de acción.

3. El plan de acción se llevará a cabo en estrecha colaboración con los sectores interesados y tendrá en cuenta, fomentará y complementará las actividades de normalización europeas e internacionales que se están llevando a cabo en este ámbito.

Artículo 6

1. El procedimiento establecido en el artículo 7 se aplicará a las medidas relativas a la política comunitaria en el ámbito de la seguridad de los sistemas de información.

2. El procedimiento establecido en el artículo 8 se aplicará :

— a la preparación y actualización del plan de acción a que se refiere el artículo 5 ;

— al contenido de las convocatorias de propuesta, a la evaluación de las mismas y al importe estimado de la contribución de la Comunidad a las medidas cuando dicho importe supere 200 000 ecus ;

— a la cooperación en cualquier actividad emprendida en virtud de la presente Decisión por parte de organizaciones no comunitarias ;

— a disposiciones para la difusión, protección y explotación de los resultados de las medidas ;

— a las medidas que se tomen para evaluar la acción.

3. Cuando el importe de la contribución comunitaria a las medidas sea inferior o igual a 200 000 ecus, la Comisión consultará al Comité sobre las medidas que vayan a adoptarse e informará al Comité del resultado de su evaluación.

Artículo 7

El representante de la Comisión presentará al Comité un proyecto de medidas. El Comité emitirá su dictamen sobre el proyecto, dentro de un plazo que el presidente podrá determinar según la urgencia de la cuestión, por votación cuando sea necesario.

El dictamen se incluirá en acta ; además, cada Estado miembro tendrá derecho a que su posición conste en la misma.

La Comisión tendrá en la mayor cuenta posible el dictamen del Comité e informará a éste de la manera en que se haya tenido en cuenta dicho dictamen.

Artículo 8

El representante de la Comisión presentará al Comité un proyecto de medidas. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión. El dictamen se emitirá según la mayoría prevista en el apar-

tado 2 del artículo 148 del Tratado para adoptar aquellas decisiones que el Consejo deba tomar a propuesta de la Comisión. Los votos de los representantes de los Estados miembros en el Comité se ponderarán de la manera definida en el artículo anteriormente citado. El presidente no tomará parte en la votación.

La Comisión adoptará las medidas previstas cuando sean conformes al dictamen del Comité.

Cuando las medidas previstas no sean conformes al dictamen del Comité o a falta de dictamen, la Comisión presentará sin demora al Consejo una propuesta relativa a las medidas que deban tomarse. El Consejo se pronunciará por mayoría cualificada.

Si transcurrido un plazo de tres meses a partir del momento en que la propuesta se haya presentado al Consejo, éste no se hubiere pronunciado, la Comisión adoptará las medidas propuestas, excepto en el caso en que el Consejo se haya pronunciado por mayoría simple contra dichas medidas.

Hecho en Bruselas, el 31 de marzo de 1992.

Por el Consejo

El Presidente

Vitor MARTINS

ANEXO

Resumen de las líneas de actuación

ORIENTACIONES PARA UN PLAN DE ACCIÓN EN MATERIA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

INTRODUCCIÓN

El plan de acción tendrá como finalidad la creación de técnicas globales destinadas a proporcionar a los usuarios y a los productores de información almacenada, procesada o transmitida electrónicamente la protección adecuada de los sistemas de información contra amenazas accidentales o deliberadas.

El plan de acción tendrá en cuenta y complementará las actividades en curso a nivel mundial para la normalización en este ámbito.

El plan incluirá las siguientes líneas de actuación :

— desarrollo de un marco estratégico para la seguridad de los sistemas de información ;

— definición de las necesidades de los usuarios y de los productores de servicios en materia de seguridad de los sistemas de información ;

— elaboración de soluciones para determinadas necesidades a corto y medio plazo de los usuarios, proveedores y prestadores de servicios ;

— desarrollo de especificaciones, normalización, evaluación y certificación respecto a la seguridad de los sistemas de información ;

— innovaciones técnicas y de funcionamiento en materia de seguridad de los sistemas de información ;

— puesta en práctica de la seguridad de los sistemas de información.

El plan de acción será aplicado por la Comisión en estrecha asociación con las acciones afines en los Estados miembros y conjuntamente con las acciones comunitarias de investigación y desarrollo al respecto.

1. Línea de actuación I : creación de un marco estratégico para la seguridad de los sistemas de información

1.1. *Problema*

La seguridad de los sistemas de información constituye un elemento universalmente necesario en la sociedad moderna. Los servicios de información electrónica exigen una infraestructura segura de telecomunicaciones, con equipos y programas informáticos seguros y una utilización y gestión seguras. Es preciso establecer una estrategia global que tenga en cuenta todos los aspectos de la seguridad de los sistemas de información y evite un planteamiento fragmentado. Toda estrategia referida a la seguridad de la información tratada por medios electrónicos debe reflejar el deseo de cualquier sociedad de actuar con eficacia y a un tiempo protegiéndose en un mundo de rápidos cambios.

1.2. *Objetivos*

Debe establecerse un marco orientado estratégicamente que ponga en sintonía los objetivos sociales, económicos y políticos con las opciones técnicas, operativas y jurídicas para la Comunidad en un contexto internacional. Es preciso que los protagonistas del sector, mediante la colaboración en el establecimiento de una percepción común y un marco estratégico convenido, encuentren el delicado equilibrio entre las diferentes preocupaciones, objetivos y restricciones. Este es un requisito previo para conciliar intereses y necesidades tanto en la adopción de medidas como en los desarrollos industriales.

1.3. *Situación y tendencias*

La situación se caracteriza por una creciente conciencia de la necesidad de actuar. No obstante, a falta de una iniciativa de concertación de esfuerzos, cualquier trabajo disperso en diversos sectores crearía probablemente una situación de hecho contradictoria que generaría más problemas jurídicos, sociales y económicos.

1.4. *Requisitos, opciones y prioridades*

El marco de cooperación tendrá que abordar y examinar el análisis y la gestión de los riesgos asociados con la vulnerabilidad de los servicios de información y afines, la armonización de las disposiciones legales y reglamentarias relativas al empleo abusivo e incorrecto de los ordenadores y las telecomunicaciones, las infraestructuras administrativas, incluidas las políticas de seguridad y su efectiva aplicación por diversas industrias y disciplinas, y las preocupaciones sociales y de protección de la intimidad (por ejemplo, la aplicación de los sistemas de identificación, autentificación, no rechazo y, eventualmente, autorización en un entorno democrático).

Es preciso aportar una orientación clara para la creación de estructuras físicas y lógicas para unos servicios distribuidos de información seguros, normas, orientaciones y definiciones para unos productos y servicios de seguridad garantizados, modelos y prototipos que permitan comprobar la viabilidad de diversas organizaciones administrativas, así como arquitecturas y normas relacionadas con las necesidades de sectores concretos.

Debe concienciarse a los usuarios para fomentar en ellos la preocupación por la seguridad en materia de tecnologías de la información (TI).

2. Línea de actuación II : definición de las necesidades de los usuarios y de los prestadores de servicios en materia de seguridad de los sistemas de información

2.1. *Problema*

La seguridad de los sistemas de información es un requisito previo intrínseco para la integridad, la fiabilidad de las aplicaciones para empresas, la propiedad intelectual y la confidencialidad. Este hecho dificulta inevitablemente el equilibrio, y en ocasiones hay que hacer una opción entre el compromiso con el libre comercio y el compromiso con la garantía de la intimidad y la propiedad intelectual. Estas opciones y compromisos tienen que basarse en una apreciación completa de las necesidades y de las repercusiones de las distintas opciones para que la seguridad de los sistemas de información pueda darles respuesta.

Los usuarios necesitan funciones de seguridad en los sistemas de información interdependientes con los aspectos técnicos, de funcionamiento y reglamentarios. En consecuencia, una investigación sistemática de las necesidades en materia de seguridad de los sistemas de información constituye un requisito esencial para la elaboración de medidas apropiadas y eficaces.

2.2. *Objetivos*

Determinar la naturaleza y características de las necesidades de los usuarios y de los prestadores de servicios y su relación con las medidas de seguridad de los sistemas de información.

2.3. *Situación y tendencias*

Hasta el presente, no se ha emprendido ningún trabajo concertado que permita averiguar cuáles son las necesidades, en rápida evolución y cambio, de los principales interesados en el sector de la seguridad de los sistemas de información. Los Estados miembros de la Comunidad han señalado cuáles son las necesidades en cuanto a la armonización de las actividades nacionales (especialmente de los « criterios de evaluación de la seguridad de la TI »). Reviste la mayor importancia contar con criterios y normas de evaluación uniformes para el reconocimiento mutuo de los certificados de evaluación.

2.4. *Requisitos, opciones y prioridades*

Como base para un tratamiento coherente y transparente de las necesidades justificadas de los protagonistas del sector, se considera necesario elaborar una clasificación de las necesidades de los usuarios y de su relación con las medidas de seguridad en los sistemas de información.

Se considera también importante determinar cuáles son las necesidades en cuanto a legislación, reglamentos, y códigos de prácticas a la luz de una valoración de las tendencias de las características y tecnología del servicio, con vistas a encontrar distintas estrategias que permitan cumplir los objetivos mediante disposiciones administrativas, de servicio, operativas y técnicas y a valorar la eficacia, facilidad de uso y costes de las opciones y estrategias alternativas en materia de seguridad de los sistemas de información para los usuarios, los prestadores de servicios y los operadores.

3. Línea de actuación III : soluciones para determinadas necesidades a corto y medio plazo de los usuarios, proveedores y prestadores de servicios

3.1. *Problema*

En la actualidad es posible proteger adecuadamente los ordenadores del acceso no autorizado desde el exterior mediante « aislamiento », es decir, aplicando medidas convencionales de tipo organizativo y físico. Lo mismo cabe decir de las comunicaciones electrónicas dentro de un grupo cerrado de usuarios que trabaje con una red dedicada. La situación es muy distinta si la información la comparten grupos de usuarios o se intercambia a través de una red pública o de acceso general. No se cuenta normalmente con la tecnología, las terminales y los servicios ni con las normas y procedimientos relacionados para ofrecer, en estos casos, una seguridad comparable de los sistemas de información.

3.2. *Objetivos*

El objetivo debe proporcionar, a corto plazo, soluciones que puedan responder a las necesidades más urgentes de los usuarios, prestadores de servicios y fabricantes. Esto incluye el uso de los criterios de evaluación de seguridad de las TI comunes y debería concebirse de manera abierta hacia futuras necesidades y soluciones.

3.3. *Situación y tendencias*

Algunos grupos de usuarios han creado técnicas y procedimientos para su uso específico que responden, en particular, a la necesidad de autentificación, integridad y no rechazo. En general, se utilizan tarjetas magnéticas o tarjetas « inteligentes ». Otros utilizan técnicas criptográficas más o menos perfeccionadas, lo que a menudo implica la creación de « autoridades » específicas del grupo de usuarios. Sin embargo, resulta difícil generalizar estas técnicas y métodos para satisfacer las necesidades de un entorno abierto.

La ISO está trabajando sobre una seguridad de los sistemas de información OSI (ISO DIS 7498-2) y el CCITT en el contexto del X400. También es posible insertar segmentos de seguridad en los mensajes. La autenticación, la integridad y el no rechazo se tratan como parte de los mensajes (EDIFACT) y X400 MHS.

En este momento, el marco jurídico del « Electronic Data Enterchange » (EDI) se halla aún en fase de concepción. La Cámara de comercio internacional ha publicado unas orientaciones uniformes para el intercambio de datos comerciales a través de las redes de telecomunicación.

Varios países (por ejemplo, Alemania, Francia, Reino Unido y Estados Unidos) han elaborado o están elaborando criterios de evaluación de la credibilidad de los productos y sistemas de TI y los correspondientes procedimientos para realizar las evaluaciones. Estos criterios se han coordinado con los fabricantes nacionales y darán lugar a un número creciente de productos y sistemas fiables, partiendo de productos sencillos. El establecimiento de organizaciones nacionales que efectúen las evaluaciones y extiendan certificados vendrá a reforzar esta tendencia.

La mayor parte de los usuarios considera que la legislación sobre confidencialidad es de importancia menos inmediata. En el futuro, sin embargo, es probable que esta situación se modifique a medida que se generalicen los servicios avanzados de comunicación, y en particular los servicios móviles.

3.4. *Requisitos, opciones y prioridades*

Resulta esencial elaborar lo antes posible los procedimientos, normas, productos y herramientas necesarios para garantizar la seguridad tanto en los sistemas de información (ordenadores y periféricos) como en las redes públicas de comunicaciones. Debe concederse una elevada prioridad a la autentificación, integridad y no rechazo. Deben llevarse a cabo proyectos piloto para comprobar la validez de las soluciones propuestas. Las soluciones a las necesidades principales planteadas por el EDI se estudian en el programa TEDIS, dentro del marco más general de este plan.

4. Línea de actuación IV : desarrollo de las especificaciones, normalización, evaluación y certificación de la seguridad de los sistemas de información

4.1. *Problema*

Las necesidades de seguridad de los sistemas de información tienen carácter omnipresente y, en consecuencia, adquieren importancia crucial las especificaciones comunes y las normas. La ausencia de normas y especificaciones generalmente aceptadas para la seguridad del TI puede constituir un importante obstáculo para la difusión de los procesos y servicios basados en la información en toda la economía y la sociedad. Es preciso también tomar medidas que permitan acelerar la elaboración y aplicación de la tecnología y las normas en diversas áreas relacionadas con las redes informáticas y de comunicaciones que son de suma importancia para los usuarios, la industria y las administraciones.

4.2. *Objetivos*

Hay que esforzarse por proporcionar medios para apoyar y ejecutar funciones específicas y de seguridad en las áreas generales de OSI, ONP, RDSI/CBA y gestión de redes. Intrínsecamente relacionados con la normalización y la especificación se encuentran los planteamientos y técnicas necesarios para la verificación, incluida la certificación previa al reconocimiento mutuo. Es preciso fomentar soluciones aceptadas internacionalmente siempre que sea posible. También debería fomentarse el desarrollo y la utilización de sistemas informatizados con funciones de seguridad.

4.3. *Situación y tendencias*

Los Estados Unidos, en particular, han adoptado importantes iniciativas con respecto al tema de la seguridad de los sistemas de información. En Europa se trata en el contexto de la normalización de la TI y de las telecomunicaciones en el marco del ETSI y el CEN/CELENEC, en preparación de los trabajos del CCITT y la ISO.

Al aumentar el interés por el tema, se intensifica rápidamente el ritmo de los trabajos efectuados en este ámbito en los Estados Unidos, tanto por los vendedores como por los prestadores de servicios. En Europa, Francia, Alemania y el Reino Unido han emprendido actividades semejantes de forma individual, pero está aún lejos de alcanzarse un esfuerzo común comparable al de Estados Unidos.

4.4. *Requisitos, opciones y prioridades*

En el ámbito de la seguridad de los sistemas de información, la relación entre los aspectos reglamentarios, operativos, administrativos y técnicos es necesariamente muy estrecha. Es preciso que los reglamentos se vean reflejados en las normas y que las disposiciones sobre seguridad de los sistemas de información se atengan de manera verificable a las normas y reglamentos. En varios aspectos, los reglamentos exigen unas especificaciones que se salen del ámbito convencional de la normalización, es decir, que incluyen códigos de práctica. La necesidad de contar con normas y códigos de prácticas se extiende a todas las áreas de la seguridad de los sistemas de información, y es preciso establecer una distinción entre las necesidades de protección que corresponde a los objetivos de seguridad y algunos de los requisitos técnicos que pueden confiarse a los organismos de normalización europeos competentes (CEN/CENELEC/ETSI).

Las especificaciones y las normas deben abordar los temas de : servicios de seguridad de los sistemas de información (autentificación personal y de empresa, protocolos de no rechazo, pruebas electrónicas jurídicamente aceptables, control de la autorización), sus servicios de comunicación (intimidad de la comunicación de imágenes, intimidad en las comunicaciones móviles de voz y datos, protección de las bases de imágenes y datos, seguridad de los servicios integrados), su gestión de la seguridad y la comunicación (sistema de claves públicas/privadas para funcionamiento de redes abiertas, protección de la gestión de redes, protección de los prestadores de servicios) y su certificación (criterios y niveles de garantía, procedimientos de garantía de la seguridad para los sistemas de información seguros).

5. Línea de actuación V : innovaciones técnicas y de funcionamiento en materia de seguridad de los sistemas de información

5.1. *Problema*

Una investigación y un desarrollo técnico sistemáticos que permitan llegar a soluciones económicamente viables y satisfactorias en la práctica para diversas necesidades de seguridad de la información presentes y futuras constituyen un requisito previo para el desarrollo del mercado de servicios y para la competitividad de la economía europea en conjunto.

Cualquier innovación técnica de la seguridad de los sistemas de información tendrá que incluir tanto los aspectos de seguridad informática como de seguridad de las comunicaciones, ya que la mayor parte de los sistemas actuales son distribuidos y el acceso a tales sistemas se realiza a través de servicios de comunicación.

5.2. *Objetivo*

Efectuar una investigación y desarrollo tecnológico sistemáticos que permitan dar una solución económicamente viable y satisfactoria en la práctica a una amplia gama de necesidades, presentes y futuras, en cuanto a la seguridad de los sistemas de información.

5.3. *Requisitos, opciones y prioridades*

Los trabajos sobre seguridad de los sistemas de información deberán abordar las estrategias de desarrollo y aplicación, las correspondientes tecnologías y su integración y verificación.

El trabajo estratégico de investigación y desarrollo tecnológico deberá incluir modelos conceptuales de sistemas seguros (en cuanto a modificaciones no autorizadas y denegación de servicio), modelos de requisitos funcionales, modelos de riesgo y arquitecturas de seguridad.

La investigación y desarrollo tecnológico de orientación tecnólogica deberá incluir la autentificación de usuarios y mensajes (por ejemplo, mediante análisis de voz y firmas electrónicas), interfaces y protocolos técnicos de cifrado, mecanismos de control de acceso y métodos de implantación de sistemas, seguros y verificables.

La verificación y validación de la seguridad del sistema técnico y su aplicabilidad se investigarán mediante proyectos de integración y verificación.

Además de la consolidación y el desarrollo de la tecnología de la seguridad, se precisan diversas medidas complementarias relacionadas con la creación, mantenimiento y aplicación coherente de las normas y validación y certificación de los productos de TI y telecomunicaciones con respecto a sus propiedades de seguridad, incluida la validación de los métodos de diseño e implantación de sistemas.

Se utilizará el tercer programa marco comunitario de investigación y desarrollo tecnológico para fomentar la realización de proyectos de cooperación a niveles precompetitivo y prenormativo.

6. Línea de actuación VI: puesta en práctica de seguridad para los sistemas de información

6.1. *Problema*

Dependiendo de la naturaleza exacta de las características de seguridad del sistema de información, habrá que incorporar las funciones necesarias en distintas partes de los sistemas de información, desde terminales y ordenadores, servicios, gestión de redes hasta dispositivos de cifrado, tarjetas « inteligentes », claves públicas y privadas, etc. Algunas de ellas podrán ir incorporadas a los soportes lógicos y físicos suministrados por los vendedores, mientras que otras formarán parte de los sistemas distribuidos (por ejemplo, la gestión de la red), estarán en posesión de los usuarios individuales (por ejemplo, las tarjetas inteligentes) o serán suministradas por una organización especializada (por ejemplo, las claves públicas y privadas).

Cabe esperar que la mayor parte de los productos y servicios de seguridad de la información los suministren los vendedores, prestadores de servicios y operadores. Para determinadas funciones, por ejemplo, el suministro de claves públicas y privadas o la autorización de auditorías, puede resultar necesario designar organizaciones apropiadas y efectuar el correspondiente encargo.

Lo mismo cabe decir de la certificación, evaluación y verificación de la calidad del servicio, que son funciones que tendrán que atender organizaciones independientes de los intereses de vendedores, proveedores de servicios y operadores. Estas organizaciones podrían ser privadas o públicas, o contar con la autorización de los gobiernos para actuar por delegación suya.

6.2. *Objetivos*

Para facilitar un desarrollo armonioso de la aplicación de la seguridad de los sistemas de información en la Comunidad, con vistas a proteger los intereses de la población y las empresas, será necesario elaborar un planteamiento coherente de dicha aplicación. Cuando sea necesario formular encargos a organizaciones independientes, sus funciones y condiciones tendrán que ser definidas, aprobadas y, cuando proceda, incluidas en el marco reglamentario. El objetivo será llegar a un reparto de responsabilidades claramente definido y acordado entre los diferentes interesados a nivel comunitario como requisito previo para el reconocimiento mutuo.

6.3. *Situación y tendencias*

En la actualidad, la seguridad de los sistemas de información sólo está bien organizada para determinadas áreas y limitada a la satisfacción de necesidades específicas. La organización a nivel europeo rara vez es formal y el reconocimiento mutuo de la verificación y la certificación o existe aún fuera de ciertos grupos cerrados. Al adquirir mayor importancia la seguridad de los sistemas de información, se acentúa la necesidad de definir un planteamiento coherente de la oferta de seguridad de los sistemas de información en Europa e internacionalmente.

6.4. *Requisitos, opciones y prioridades*

Dado el número de partes interesadas y la estrecha relación con las cuestiones de tipo legal y reglamentario, reviste especial importancia ponerse de acuerdo de antemano sobre los principios que deben regir la oferta de seguridad de los sistemas de información.

En la elaboración de un planteamiento coherente de este tema será necesario abordar aspectos de identificación y especificación de funciones que exigen, por su propia naturaleza, la participación de algún organismo independiente (o la colaboración de más de uno). Entre estas funciones podrían figurar la administración de un sistema de claves públicas/privadas.

Además, es necesario determinar y especificar desde los primeros momentos qué funciones deben confiarse, en aras del interés público, a un organismo independiente (o más de uno en colaboración). Entre ellas podrían figurar, por ejemplo, la auditoría, la garantía de calidad, la verificación, la certificación y funciones análogas.