DECISÃO DO CONSELHO

de 31 de Março de 1992

no domínio da segurança dos sistemas de informação

(92/242/CEE)

O CONSELHO DAS COMUNIDADES EUROPEIAS,

Tendo em conta o Tratado que institui a Comunidade Económica Europeia e, nomeadamente, o seu artigo 235º,

Tendo em conta a proposta da Comissão (1),

Tendo em conta o parecer do Parlamento Europeu (2),

Tendo em conta o parecer do Comité Económico e Social (3),

Considerando que a Comunidade tem como missão, através do estabelecimento de um mercado comum e da aproximação progressiva das políticas económicas dos Estados-membros, promover um desenvolvimento harmonioso das actividades económicas, uma expansão contínua e equilibrada, uma maior estabilidade e um aumento acelerado do nível de vida em toda a Comunidade, bem como relações mais estreitas entre os Estados-membros;

Considerando que a informação armazenada, tratada e transmitida electronicamente desempenha um papel cada vez mais importante nas actividades económicas e sociais;

Considerando que a introdução de comunicações globais eficazes e a utilização em todos os domínios do tratamento electrónico da informação colocou mais em destaque a necessidade de uma protecção adequada;

Considerando que nos seus debates e resoluções, o Parlamento Europeu tem repetidamente sublinhado a importância de que se reveste a segurança dos sistemas de informação;

Considerando que o Comité Económico e Social sublinhou a necessidade de tratar as questões relativas à segurança dos sistemas de informação nas acções da Comunidade, tendo especialmente em vista o impacte da realização do mercado interno;

Considerando que o desenvolvimento de acções a nível nacional, internacional e comunitário proporciona uma boa base;

Considerando que existe uma relação estreita entre as telecomunicações, as tecnologias da informação, a normalização, o mercado da informação e as políticas de investigação e desenvolvimento tecnológico (I&D) e atendendo aos trabalhos já empreendidos nestes domínios pela Comunidade Europeia;

Considerando que é oportuno concertar esforços, desenvolvendo os trabalhos nacionais e internacionais já existentes e promovendo a cooperação entre as principais partes envolvidas; que, consequentemente, é oportuno proceder a esta concertação no quadro de um plano de acção coerente;

Considerando que a complexidade da segurança dos sistemas de informação implica o desenvolvimento de estratégias que permitam a livre circulação da informação no mercado único, garantindo, simultaneamente, a segurança da utilização dos sistemas de informação em toda a Comunidade;

Considerando que compete a cada Estado-membro ter em conta os condicionalismos impostos pela segurança e ordem públicas;

Considerando que as responsabilidades dos Estados-membros neste domínio implicam uma abordagem concertada baseada numa estreita colaboração com os altos funcionários dos Estados-membros;

Considerando a necessidade de prever uma acção que inclua um plano de acção por um período inicial de vinte e quatro meses e a criação de um comité de altos funcionários com um mandato a longo prazo para aconselhar a Comissão sobre as acções no domínio da segurança dos sistemas de informação;

Considerando que, para implementar a acção durante um período inicial de vinte e quatro meses, o montante considerado necessário é de 12 milhões de ecus; que, no âmbito das perspectivas financeiras actuais, o montante considerado necessário para 1992 é de dois milhões de ecus;

Considerando que os montantes a autorizar para o financiamento do programa durante o período subsequente ao exercício de 1992 se devem inscrever no enquadramento financeiro comunitário em vigor,

DECIDE:

Artigo 1º

É adoptada pela presente decisão uma acção no domínio da segurança dos sistemas de informação. Essa acção abrange:

— o desenvolvimento de estratégias globais para a segurança dos sistemas de informação (plano de acção) por um período inicial de vinte e quatro meses, e

— a criação de um grupo de altos funcionários com um mandato a longo prazo, a seguir designado por « comité », incumbido de aconselhar a Comissão sobre as acções a empreender no domínio da segurança dos sistemas de informação.

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

Artigo 2.º

1. A Comissão consultará sistematicamente o comité sobre as questões relacionadas com a segurança dos sistemas de informação das diversas actividades empreendidas pela Comunidade, em especial no que respeita à definição de estratégias e programas de trabalho.

2. Tal como é indicado no anexo, o plano de acção inclui trabalhos preparatórios relativos aos seguintes temas :

I. Desenvolvimento de um quadro estratégico para a segurança dos sistemas de informação ;

II. Apuramento das necessidades dos utilizadores e dos prestadores de serviços no que se refere à segurança dos sistemas de informação ;

III. Soluções para as necessidades a curto e a médio prazo dos utilizadores, dos fornecedores e dos prestadores de serviços ;

IV. Desenvolvimento de especificações, normalização, avaliação e certificação da segurança dos sistemas de informação ;

V. Evolução tecnológica e operacional no domínio da segurança dos sistemas de informação ;

VI. Garantia da segurança dos sistemas de informação.

Artigo 3.º

1. O montante dos recursos financeiros comunitários considerado necessário para a execução da acção durante o período inicial é de 12 milhões de ecus, dos quais dois milhões de ecus para 1992 no âmbito das perspectivas financeiras para 1988/1992.

No período subsequente de aplicação da acção, o montante deve inscrever-se no enquadramento financeiro comunitário em vigor.

2. A autoridade orçamental determinará as dotações disponíveis para cada exercício, tendo em consideração os princípios da boa gestão referidos no artigo 2º do Regulamento Financeiro aplicável ao orçamento geral das Comunidades Europeias.

Artigo 4.º

Os progressos realizados durante o período inicial serão avaliados, por conta da Comissão, por um grupo de peritos independentes. O relatório deste grupo, acompanhado das eventuais observações da Comissão, será apresentado ao Parlamento Europeu e ao Conselho.

Artigo 5.º

1. A Comissão será responsável pela implementação da acção e será assistida por um comité consultivo composto por representantes dos Estados-membros e presidido pelo representante da Comissão.

2. O plano de acção será posto em prática de acordo com os objectivos enunciados no artigo 2º e actualizado sempre que necessário. Este plano estabelecerá objectivos específicos e os tipos de acções a empreender, bem como as disposições financeiras a tomar no que lhes diz respeito. A Comissão lançará convites para apresentação de propostas com base no plano de acção.

3. O plano de acção será posto em prática em estreita colaboração com os intervenientes no sector e tomará em conta, incentivará e complementará as actividades de normalização em curso neste domínio a nível europeu e internacional.

Artigo 6.º

1. O procedimento previsto no artigo 7º aplica-se às medidas relativas à política comunitária no domínio da segurança dos sistemas de informação.

2. O procedimento previsto no artigo 8º aplica-se :

— à preparação e actualização do plano de acção, a que se refere o artigo 5º,

— ao teor dos convites para apresentação de propostas, à avaliação das propostas e ao montante calculado da contribuição comunitária para as medidas, quando esse montante exceder 200 000 ecus,

— à participação de organizações não comunitárias em qualquer actividade ao abrigo da presente decisão,

— às modalidades de divulgação, protecção e exploração dos resultados das medidas,

— às medidas a tomar para avaliar a acção.

3. Se o montante da contribuição comunitária para as medidas for igual ou inferior a 200 000 ecus, a Comissão consultará o comité acerca das medidas a tomar e informá-lo-á do resultado da sua avaliação.

Artigo 7.º

O representante da Comissão submeterá à apreciação do comité um projecto das medidas a tomar. O comité emitirá o seu parecer sobre esse projecto num prazo que o presidente pode fixar em função da urgência da questão em causa, se necessário procedendo a uma votação.

Esse parecer deve ser exarado em acta ; além disso, cada Estado-membro tem o direito de solicitar que a sua posição conste da acta.

A Comissão tomará na melhor conta o parecer emitido pelo comité. O comité será por ela informado do modo como esse parecer foi tomado em consideração.

Artigo 8.º

O representante da Comissão submeterá à apreciação do comité um projecto das medidas a tomar. O comité emitirá o seu parecer sobre esse projecto num prazo que o presidente pode fixar em função da urgência da questão em causa. O parecer será emitido por maioria, nos termos previstos no nº 2 do artigo 148º do Tratado para a adop-

ção das decisões que o Conselho é chamado a tomar sob proposta da Comissão. Nas votações no comité, os votos dos representantes dos Estados-membros estão sujeitos à ponderação definida no artigo atrás referido. O presidente não participa na votação.

A Comissão adoptará as medidas projectadas desde que sejam conformes com o parecer do comité.

Se as medidas projectadas não forem conformes com o parecer do comité ou na ausência de parecer, a Comissão submeterá sem demora ao Conselho uma proposta relativa às medidas a tomar. O Conselho deliberará por maioria qualificada.

Se, no termo de um prazo de três meses a contar da data em que o assunto foi submetido à apreciação do Conselho, este último ainda não tiver deliberado, a Comissão adoptará as medidas propostas, excepto no caso de o Conselho se ter pronunciado por maioria simples contra as referidas medidas.

Feito em Bruxelas, em 31 de Março de 1992.

Pelo Conselho

O Presidente

Vitor MARTINS

ANEXO

Resumo das linhas de acção

ORIENTAÇÕES PARA UM PLANO DE ACÇÃO NO DOMÍNIO DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

INTRODUÇÃO

O plano de acção terá como objectivo o desenvolvimento de estratégias globais destinadas a dispensar aos utilizadores e produtores de informações electronicamente armazenadas, tratadas ou transmitidas, uma protecção adequada dos sistemas de informação contra ameaças acidentais ou deliberadas.

O plano de acção terá em conta e complementará as actividades de normalização em curso a nível mundial neste domínio.

O plano de acção inclui as seguintes linhas de acção :

— desenvolvimento de um quadro estratégico para a segurança dos sistemas de informação,

— apuramento das necessidades dos utilizadores no que se refere à segurança dos sistemas de informação,

— soluções para necessidades a curto e a médio prazo dos utilizadores, fornecedores e prestadores de serviços,

— desenvolvimento de especificações, normalização, avaliação e certificação no que se refere à segurança dos sistemas de informação,

— evolução tecnológica e operacional no domínio da segurança dos sistemas de informação,

— garantia de segurança dos sistemas de informação.

O plano de acção será implementado pela Comissão, em estreita associação com acções afins dos Estados-membros e em articulação com acções comunitárias de investigação e desenvolvimento nesta matéria.

1. Linha de acção I — Desenvolvimento de um quadro estratégico para a segurança dos sistemas de informação

1.1. *Tema*

A segurança dos sistemas de informação é reconhecida como uma qualidade fundamental na sociedade moderna. Os serviços de informação electrónica necessitam de uma infra-estrutura de telecomunicações segura, de equipamentos e suportes lógicos seguros e de condições de utilização e gestão seguras. É necessário estabelecer uma estratégia global que tenha em conta todos os aspectos da segurança dos sistemas de informação, evitando uma abordagem fragmentada. Qualquer estratégia para a segurança da informação tratada sob forma electrónica deve reflectir a vontade de qualquer sociedade de funcionar de forma eficaz e de ao mesmo tempo se proteger a si mesma num mundo em rápida mutação.

1.2. *Objectivo*

Deve ser criado um quadro estratégico que concilie os objectivos sociais, económicos e políticos com as opções técnicas, funcionais e legislativas à disposição da Comunidade num contexto internacional. O delicado equilíbrio entre diferentes preocupações, objectivos e limitações deve ser encontrado pelos intervenientes no sector por meio de um trabalho conjunto de desenvolvimento de uma percepção comum e de um quadro estratégico consensual. Tais são os pré-requisitos para a conciliação de interesses e necessidades, tanto na elaboração de políticas como no desenvolvimento industrial.

1.3. *Situações e tendências*

A situação caracteriza-se por uma consciência crescente da necessidade de actuação. Contudo, na ausência de uma iniciativa de concertação de esforços, é muito provável que a dispersão dos esforços em vários sectores venha a criar uma situação de facto contraditória, dando origem a problemas jurídicos, sociais e económicos cada vez mais graves.

1.4. *Necessidades, opções e prioridades*

Num quadro desta natureza será necessário abordar e tratar a análise e gestão de riscos no que toca às vulnerabilidades dos serviços de informação e serviços associados, o alinhamento de legislações e regulamentações relacionadas com abusos e utilizações indevidas de computadores/telecomunicações, as infra-estruturas administrativas, incluindo as políticas de segurança e o modo como elas podem ser executadas de modo eficiente nas diferentes indústrias/disciplinas e as preocupações sociais e de privacidade (por exemplo, a aplicação de sistemas de identificação, autenticação, não repúdio e, eventualmente, autorização num ambiente democrático).

Deve ser fornecida uma orientação clara para o desenvolvimento de arquitecturas físicas e lógicas destinadas a serviços seguros de distribuição de informações, normas, linhas de orientação e definições para produtos e serviços de segurança garantidos, experiências-piloto e protótipos para o estudo da viabilidade de diferentes estruturas administrativas, arquitecturas e normas relacionadas com as necessidades de sectores específicos.

Deve ser promovida uma tomada de consciência da questão da segurança que influencie a atitude dos utilizadores, para que aumente a preocupação com a segurança nos sistemas de tecnologias de informação (TI).

2. Linha de acção II — Apuramento das necessidades dos utilizadores e dos prestadores de serviços no que se refere à segurança dos sistemas de informação

2.1. *Tema*

A segurança dos sistemas de informação é o pré-requisito para garantir a integridade e a fiabilidade das aplicações comerciais, o respeito da propriedade intelectual, e a confidencialidade. Isto conduz inevitavelmente a um equilíbrio difícil e, por vezes, a escolhas, entre um empenhamento no comércio livre e um empenhamento na garantia da privacidade e da propriedade intelectual. Essas escolhas e compromissos devem basear-se na plena apreciação das necessidades e do impacte das possíveis opções para a segurança dos sistemas de informação destinados a satisfazê-las.

As necessidades dos utilizadores implicam funcionalidades de segurança dos sistemas de informação interdependentes com aspectos tecnológicos, operacionais e regulamentares. Deste modo, um estudo sistemático das necessidades de segurança dos sistemas de informação faz parte integrante do desenvolvimento de medidas adequadas e eficazes.

2.2. *Objectivo*

Estabelecimento da natureza e características das necessidades dos utilizadores e dos prestadores de serviços e sua relação com as medidas de segurança dos sistemas de informação.

2.3. *Situação e tendências*

Até hoje não foram empreendidos esforços concertados para identificar as necessidades em rápida evolução e mutação dos principais intervenientes na segurança dos sistemas de informação. Os Estados-membros da Comunidade identificaram as necessidades de harmonização das actividades nacionais (nomeadamente os « critérios de avaliação da segurança das TI »). Reveste-se de grande importância a existência de critérios e de regras de avaliação uniformes para o reconhecimento mútuo de certificados de avaliação.

2.4. *Necessidades, opções e prioridades*

Como base para um tratamento coerente e transparente das necessidades justificadas dos intervenientes no sector, considera-se ser necessário estabelecer uma classificação concertada das necessidades dos utilizadores e sua relação com a garantia de segurança dos sistemas de informação.

Considera-se também importante identificar necessidades nos domínios da legislação, regulamentações e códigos de conduta, à luz de uma avaliação das tendências das características e tecnologias dos serviços, identificar estratégias alternativas para a consecução dos objectivos por meio de disposições administrativas, de serviço, operacionais e técnicas e avaliar a eficácia, a facilidade de utilização e os custos de opções e estratégias alternativas em matéria de segurança dos sistemas de informação para utilizadores, prestadores de serviços e operadores.

3. Linha de acção III — Soluções para necessidades a curto e a médio prazo dos utilizadores, fornecedores e prestadores de serviços

3.1. *Tema*

Actualmente é possível proteger adequadamente os computadores contra o acesso não autorizado a partir do exterior através do « isolamento », ou seja, através da aplicação de medidas organizativas e físicas convencionais. O mesmo se aplica às comunicações electrónicas num grupo fechado de utilizadores funcionando numa rede dedicada. A situação é muito diferente caso a informação seja partilhada entre grupos de utilizadores ou transferida através de uma rede pública ou de acesso generalizado. Tanto a tecnologia, os terminais e os serviços como as normas e procedimentos associados são, em geral, incapazes de oferecer um nível comparável de segurança dos sistemas de informação nestes casos.

3.2. *Objectivo*

O objectivo deve ser o de fornecer, a curto prazo, soluções que possam responder às necessidades mais urgentes dos utilizadores, dos prestadores de serviços e dos fabricantes, o que implica a aplicação de critérios comuns de avaliação da segurança das IT. Estes devem ser concebidos de modo aberto às futuras necessidades e soluções.

3.3. *Situação e tendências*

Alguns grupos de utilizadores desenvolveram técnicas e procedimentos para uso próprio que respondem, nomeadamente, às necessidades de autenticação, integridade e não repúdio. São utilizados, em geral, cartões magnéticos ou cartões inteligentes. Por vezes utilizam-se técnicas mais ou menos sofisticadas de criptografia. Muitas vezes isto implica a definição de « autoridades » específicas de grupos de utilizadores. Contudo, é difícil generalizar estas técnicas e métodos por forma a responderem às necessidades de um ambiente aberto.

A ISO está a trabalhar na segurança dos sistemas de informação OSI (ISO DIS 7498-2), tal como o CCITT no contexto do X400. É também possível inserir segmentos de segurança nas mensagens. A autenticação, a integridade e o não repúdio estão a ser tratados como parte das mensagens (EDIFACT) e do X400 MHS.

Actualmente, o quadro jurídico da Electronic Data Interchange (EDI) está ainda em fase de concepção. A Câmara de Comércio Internacional publicou regras de conduta uniformes para a transferência de dados comerciais através de redes de telecomunicações.

Vários países (por exemplo, Alemanha, França, Reino Unido e Estados Unidos da América) desenvolveram ou estão a desenvolver critérios para avaliação da fiabilidade dos produtos e sistemas de TI e os procedimentos correspondentes para a realização das avaliações. Esses critérios foram coordenados com os fabricantes nacionais e conduzirão a um número crescente de produtos e sistemas fiáveis, a começar por produtos simples. A criação de organizações nacionais que efectuem avaliações e emitam certificados constituirá um apoio a esta linha de esforços.

A garantia da confidencialidade é considerada pela maioria dos utilizadores como menos importante no imediato. Contudo, no futuro esta situação irá provavelmente mudar, na medida em que se generalizem os serviços de comunicações avançados, nomeadamente os serviços móveis.

3.4. *Necessidades, opções e prioridades*

É essencial desenvolver o mais rapidamente possível os procedimentos, normas, produtos e instrumentos adequados para garantir a segurança tanto dos sistemas de informação em si (computadores, periféricos), como das redes públicas de comunicações. Deve ser dada uma prioridade à autenticação, integridade e não repúdio. Devem realizar-se projectos-piloto destinados a verificar a validade das soluções propostas. O programa *Tedis* procura soluções para necessidades prioritárias em matéria de EDI, soluções estas coordenadas no âmbito mais geral do presente plano de acção.

4. Linha de acção IV — Desenvolvimento de especificações, normalização, avaliação e certificação no que se refere à segurança dos sistemas de informação

4.1. *Tema*

As necessidades em matéria de segurança dos sistemas de informação vão-se generalizando e, como tal, é crucial a existência de especificações e normas comuns. A ausência de normas e especificações aprovadas em matéria de segurança das TI pode constituir uma grande barreira ao avanço dos processos e serviços baseados na informação tanto na economia como na sociedade. São igualmente necessárias medidas que acelerem o desenvolvimento e a utilização de tecnologias e normas em diversos domínios interrelacionados ligados às redes de comunicação e de computadores, que são de importância crítica para os utilizadores, a indústria e as administrações.

4.2. *Objectivo*

São necessários esforços para fornecer meios de suporte e realização de funções de segurança específicas nas áreas gerais de OSI, ORE, RDSI/IBC e gestão de redes de segurança específicas nas áreas gerais de OSI, ORE, RDSI/IBC e gestão de redes. As técnicas e abordagens necessárias para a verificação, incluindo a certificação conducente ao reconhecimento mútuo, estão intrinsecamente ligadas à normalização e especificação. Sempre que possível, deverão apoiar-se soluções adoptadas a nível internacional. Deverão igualmente ser fomentados o desenvolvimento e a utilização de sistemas de computadores com funções de segurança.

4.3. *Situação e tendências*

Os Estados Unidos da América (EUA), em especial, tomaram importantes iniciativas dirigidas à segurança dos sistemas de informação. Na Europa, o assunto é tratado no contexto da normalização das TI e telecomunicações no âmbito do ETSI e do CEN/Cenelec, em preparação dos trabalhos do CCITT e da ISO neste domínio.

Dadas as preocupações crescentes, os trabalhos nos EUA estão a intensificar-se rapidamente e tanto vendedores como prestadores de serviços estão a aumentar os seus esforços neste domínio. Na Europa, a França, a Alemanha e o Reino Unido iniciaram, independentemente, actividades similares, mas só lentamente se está a desenvolver um esforço comum correspondente ao verifiado nos EUA.

4.4. *Necessidades, opções e prioridades*

Na segurança dos sistemas de informação existe intrinsecamente uma relação muito estreita entre os aspectos de regulamentação, operacionais, administrativos e técnicos. As regulamentações devem reflectir-se em normas e as disposições relativas à segurança dos sistemas de informação devem satisfazer, de forma verificável, as normas e regulamentações. As regulamentações exigem, em vários aspectos, especificações que ultrapassam o âmbito convencional da normalização, ou seja, incluem códigos de conduta. As exigências em matéria de normas e códigos de conduta estão presentes em todas as áreas da segurança dos sistemas de informação, devendo fazer-se uma distinção entre as exigências de protecção que correspondem aos objectivos de segurança e algumas das exigências técnicas que podem ser confiadas aos organismos de normalização europeus competentes (CEN/ /Cenelec/ETSI).

As especificações e normas devem abranger os domínios dos serviços de segurança dos sistemas de informação (autenticação de pessoas e empresas, protocolos de não repúdio, prova electrónica legalmente aceitável, controlo de autorização), dos respectivos serviços de comunicação (privacidade na comunicação de imagens, privacidade nas comunicações móveis de voz e dados, protecção de bases de dados e de imagens, segurança dos serviços integrados), da gestão da comunicação e segurança (sistema de chaves públicas/privadas para funcionamento de redes abertas, protecção da gestão da rede, protecção do prestador de serviços) e da certificação (critérios e níveis de garantia, procedimentos de garantia da segurança sistemas de informação).

5. Linha de acção V — Evolução tecnológica e operacional no campo da segurança dos sistemas de informação

5.1. *Tema*

O estudo e o desenvolvimento sistemáticos da tecnologia a fim de possibilitar soluções economicamente viáveis e funcionalmente satisfatórias para uma gama de exigências actuais e futuras no domínio da segurança dos sistemas de informação constituem um pré-requisito para o desenvolvimento do mercado de serviços e da competitividade da economia europeia no seu conjunto.

Qualquer desenvolvimento tecnológico na segurança dos sistemas de informação terá de incluir simultaneamente os aspectos da segurança dos computadores e da segurança das comunicações, dado que a maioria dos sistemas actuais são sistemas distribuídos, obtendo-se o acesso a estes sistemas através de serviços de comunicações.

5.2. *Objectivo*

Estudo e desenvolvimento sistemáticos da tecnologia a fim de possibilitar soluções economicamente viáveis e funcionalmente satisfatórias para uma gama de necessidades actuais e futuras no domínio da segurança dos sistemas de informação.

5.3. *Necessidades, opções e prioridades*

Os trabalhos em matéria de segurança dos sistemas de informação deverão abordar estratégias de desenvolvimento e realização, tecnologias e ainda integração e verificação.

Os trabalhos de I&D estratégica deveriam abordar modelos conceptuais de sistemas seguros (segurança contra alterações não autorizadas e recusa de prestação de serviços), modelos de exigências funcionais, modelos de riscos e arquitecturas para a segurança.

Os trabalhos de I&D orientada para a tecnologia deveriam incluir autenticação do utilizador e da mensagem (por exemplo, através da análise da voz e de assinaturas electrónicas), interfaces e protocolos técnicos para cifragem, mecanismos de controlo de acesso e métodos de realização de sistemas seguros comprováveis.

Através de projectos de integração e verificação deveria estudar-se a verificação e validação da segurança do sistema técnico e sua aplicabilidade.

Para além da consolidação e desenvolvimento da tecnologia da segurança, são necessárias diversas medidas de acompanhamento ligadas à criação, manutenção e aplicação coerente de normas e à validação e certificação de produtos das TI e telecomunicações no que respeita às suas propriedades de segurança, incluindo a validação e certificação de métodos de concepção e realização de sistemas.

O terceiro programa-quadro comunitário de IDT poderá ser utilizado para promover projectos de cooperação nos níveis pré-competitivo e pré-normativo.

6. Linha de acção VI — Garantia de segurança dos sistemas de informação

6.1. *Tema*

Em função da natureza exacta das características de segurança dos sistemas de informação, deverão incorporar-se as necessárias funções nas diferentes partes dos sistemas de informação, incluindo terminais/computadores, serviços, gestão da rede até aos dispositivos criptográficos, cartões inteligentes, chaves públicas e privadas, etc. Algumas destas funções estarão, previsivelmente, incorporadas nos equipamentos ou suportes lógicos fornecidos pelos vendedores, enquanto outras podem fazer parte de sistemas distribuídos (por exemplo, gestão das redes), estar na posse dos utilizadores individuais (por exemplo, cartões inteligentes) ou ser fornecidas por uma organização especializada (por exemplo, chaves públicas/privadas).

A maior parte dos produtos e serviços de segurança podem, previsivelmente, ser fornecidos por vendedores, prestadores de serviços ou operadores. Para funções específicas, por exemplo, oferta de chaves públicas/privadas, autorização do acesso, pode vir a ser necessário identificar e mandatar organizações adequadas.

O mesmo se aplica à certificação, avaliação e verificação da qualidade do serviço, funções que devem estar a cargo de organizações independentes dos interesses de vendedores, prestadores de serviços ou operadores. Estas organizações poderão ser privadas, públicas ou mandatadas pelo Estado para exercer funções por delegação.

6.2. *Objectivo*

Para facilitar o desenvolvimento harmonioso da garantia de segurança dos sistemas de informação na Comunidade para protecção do público e dos interesses comerciais, será necessário desenvolver uma abordagem coerente da respectiva oferta de segurança. Sempre que haja necessidade de mandatar organizações independentes, as suas funções e condições de funcionamento deverão ser definidas, acordadas e, se necessário, incluídas no quadro regulamentar. O objectivo será a obtenção de uma repartição de responsabilidades claramente definida e acordada entre os diferentes intervenientes a nível comunitário, como pré-requisito para o reconhecimento mútuo.

6.3. *Situação e tendências*

Actualmente, a garantia de segurança dos sistemas de informação está bem organizada apenas em áreas específicas e limita-se a responder a necessidades específicas. A organização a nível europeu é, em geral, informal e o reconhecimento mútuo da verificação e certificação ainda não existe fora de grupos fechados. Com a crescente importância da segurança dos sistemas de informação, a necessidade de definição de uma abordagem coerente da garantia de segurança dos sistemas de informação a nível europeu e internacional está a tornar-se urgente.

6.4. *Necessidades, opções e prioridades*

Dado o número de intervenientes envolvidos e as relações estreitas com questões de regulamentação e legislativas, é especialmente importante chegar-se a um consenso sobre os princípios que devem reger a garantia de segurança dos sistemas de informação.

Ao desenvolver uma abordagem coerente deste problema, há que tratar os aspectos de identificação e especificação de funções que exigem, pela sua natureza, as intervenções de organizações independentes (ou organizações que trabalhem em conjunto). Tal poderia abranger funções como a administração de um sistema de chaves públicas/privadas.

Além disso, é necessário identificar e especificar, desde logo, as funções que, no interesse público, devem ser confiadas a organizações independentes (ou organizações que trabalhem em conjunto). Poderá aqui incluir-se, por exemplo, a auditoria, a garantia da qualidade, a verificação, a certificação e funções similares.