UNISYS
Imagine it. Done.

UMIC
Agência para a Sociedade do Conhecimento, IP

ANACOM

FCCN
Fundação para a Computação Científica Nacional

GNS
Gabinete Nacional de Segurança

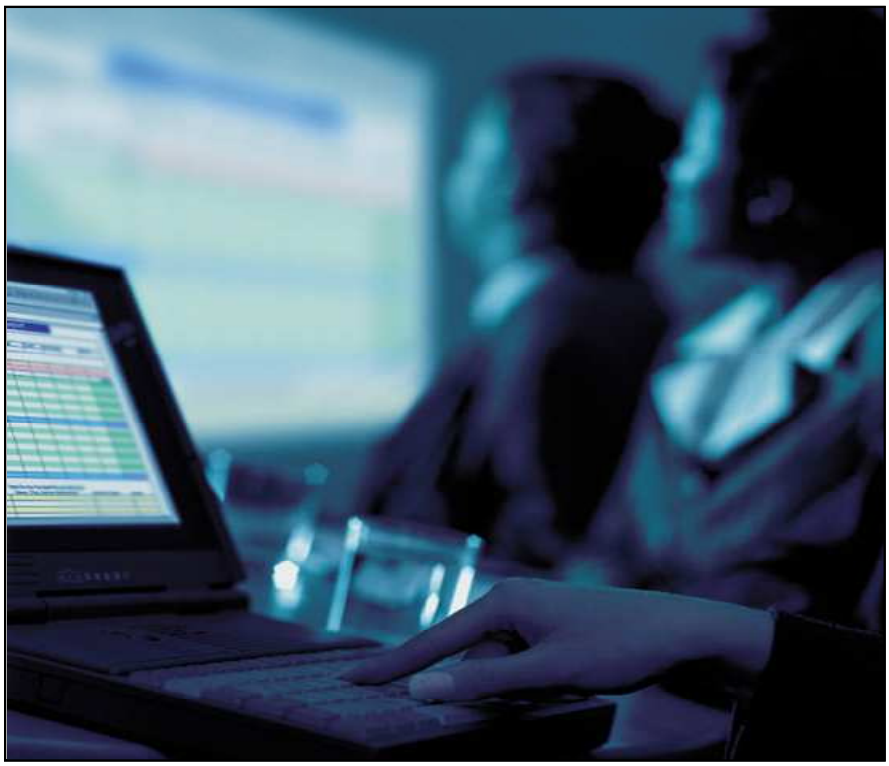
Estrutura Nacional de Segurança da Informação (ENSI)

Política de Segurança da Informação da Entidade

Fevereiro 2005

Versão 1.0

Público



ÍNDICE

1 Prefácio

A Política de Segurança da Informação da Entidade (PSIE) apresenta a Estrutura Nacional de Segurança de Informação (ENSI) a ser aplicada pelas entidades públicas portuguesas.

Cada entidade deverá desenvolver a sua própria Política de Segurança de Informação (PSIE) de modo a assegurar a confidencialidade, integridade e disponibilidade dos seus recursos.

Este documento descreve os princípios gerais que devem ser aplicados por cada entidade, e encontra-se definido do seguinte modo:

- Audiência
- Valor da Informação
- Importância da Segurança da Informação
- Definição do nível de Segurança da Informação
- Objectivos da Política Nacional de Segurança da Informação
- Responsabilidade na Segurança da Informação
- Organização da Segurança da Informação
- Recomendações para a Implementação

Este documento não deverá ser utilizado tal como está mas sim adaptado às actividades desenvolvidas pelas entidades. No entanto, é importante que a Politica de Segurança de Informação da Entidade (PSIE) se mantenha em conformidade com a Política Nacional de Segurança da Informação (PNSI).

2 Audiência

A Política de Segurança da Informação da Entidade destina-se a todos os colaboradores de uma entidade – independentemente do seu vínculo (empregados, fornecedores, consultores, temporários, voluntários, etc.) – têm de estar em conformidade com a Política de Segurança de Informação da Entidade e com os demais documentos relacionados com a Segurança de Informação. Os colaboradores que deliberadamente violem esta ou outras políticas devem ser sujeitos a acções disciplinares, que podem ir até à cessação do contrato de trabalho.

3 Valor da Informação

O acesso à informação é um aspecto importante da nossa operação. A nossa eficiência dependente da disponibilidade dos Sistemas e infra-estruturas de informação. A segurança e protecção do tratamento e transmissão de informação são um factor vital para manter a nossa força.

Qualquer interrupção do serviço ou fuga de informação para partes não autorizadas ou modificação de dados não autorizada pode levar a uma perda de confiança e/ou violar as obrigações para com a entidade e os cidadãos.

Associado a crescente dependência dos utilizadores em utilizarem as redes surge o paradigma da mudança. A mudança leva-nos de sistemas de processamento clássicos em *mainframes* baseados em centros informáticos fechados, para as mais variadas formas de processamento de dados distribuídos em ambientes abertos e heterogéneos cliente/servidor. Esta mudança traz riscos adicionais que necessitam de ser geridos de forma a assegurar os nossos objectivos, uma vez que a informação de segurança relevante e as aplicações estão a aumentar e são utilizadas em locais cujo controlo é difícil ou mesmo impossível.

Para atingir os objectivos as entidades públicas, privadas e os cidadãos estão dependentes do funcionamento ininterrupto da tecnologia de informação e comunicações. Isto apenas é possível com a implementação de medidas de segurança, com a utilização correcta e com criação da alta disponibilidade de todos os sistemas de tecnologias de informação acompanhados por uma supervisão e formação de todas as pessoas que lidam com dados e recursos sensíveis.

4 Importância da Segurança da Informação

A informação, os seus processos de suporte, sistemas, aplicações e redes são activos valiosos para as nossas entidades e cidadãos. A perda de confidencialidade, integridade e/ou disponibilidade podem levar a uma futura perda de credibilidade dos nossos serviços.

Hoje em dia, as organizações e os seus sistemas de informação e redes encontram-se expostos a muitas ameaças de segurança. Alguns dos exemplos são: fraude, espionagem, sabotagem, vandalismo, incêndio ou inundações. Alguns perigos como os vírus, *hackers* e ataques do tipo Negação de Serviço estão a tornar-se mais frequentes, criativos e complexos de gerir.

A informação é armazenada e transferida sob várias formas. Pode ser transferida, escrita em papel, como uma impressão, através do correio tradicional ou electrónico, filmes ou passada verbalmente. Esta informação deve ser protegida, independentemente do meio, uso ou suporte.

- A protecção da informação tem de estar ajustada à sua importância e valor, que são determinados pelo detentor da informação, sendo que apenas este pode permitir o acesso à mesma;

- A Segurança da Informação, num projecto, (inserção/colecta, processamento, armazenamento, transferência, relacionamento e resultado/pesquisa da informação) é tão importante quanto a funcionalidade e o cumprimento de objectivos;

- A Segurança da Informação deve alcançar e manter de forma permanente um nível de qualidade elevada, de forma a evitar o descontentamento ou eventuais queixas dos detentores da informação. Para isso deverá ser criada uma equipa de gestão de segurança da informação;

- A Segurança da Informação é um pré requisito fundamental para o sucesso dos serviços e é da responsabilidade de todos os funcionários, fornecedores ou pessoas que têm acesso à informação;

- Através das orientações da Direcção das entidades da Administração Pública e disponibilização de material de formação adequado, todos os funcionários e parceiros têm de conseguir compreender e agir em conformidade com os requisitos da Estrutura Nacional de Segurança da Informação (ENSI);

- As ameaças à Segurança da Informação estão em constante evolução, o que torna necessário adaptar continuamente as medidas de segurança de modo a acompanhar alterações à tecnologia e/ou sociais.

- As medidas de segurança devem ser técnica e economicamente viáveis e não devem limitar de forma inadequada a produtividade da empresa pública/privada ou do cidadão. Os riscos residuais devem ser conhecidos e explicitamente aceites pelas Direcções das entidades;

- A Segurança da Informação tem implicações estratégicas para Portugal e representa uma parte integral dos objectivos do país.

5 Organização da Segurança da Informação

A Estrutura Nacional de Segurança da Informação (ENSI) é apresentada para descrever a forma como a Segurança da Informação se encontra organizada de acordo com os princípios definidos em Portugal.

A organização da segurança de informação da entidade não é apresentada aqui uma vez que está demasiado dependente da própria entidade. Contudo, é recomendado que siga os princípios definidos pela ENSI e que têm de estar reflectidos na Politica de Segurança da Informação Detalhada da Entidade (PSIDE).

6 Definição do Nível de Segurança da Informação

A Segurança da Informação é baseada em 3 factores:

a) **Confidencialidade**: garantia de que a informação está acessível apenas por pessoas que têm autorização para tal;

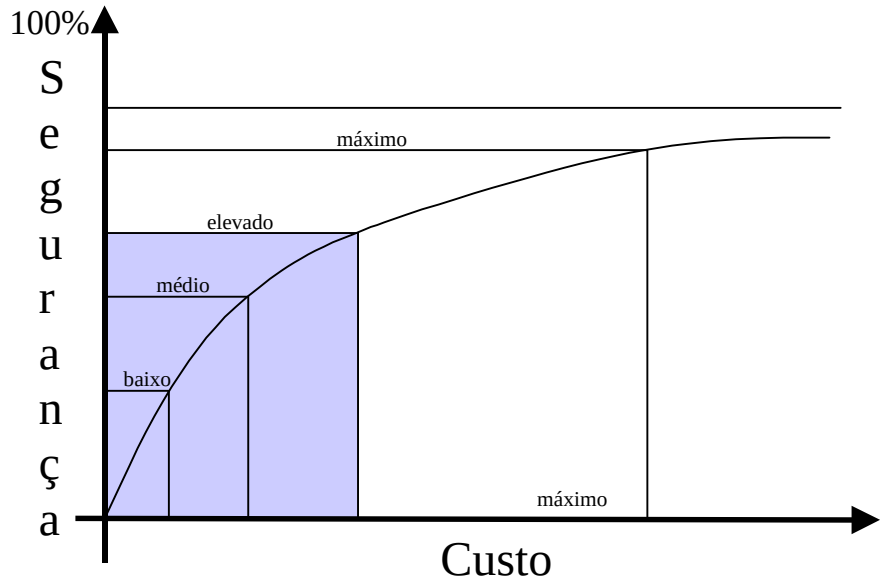
b) **Integridade**: salvaguarda da exactidão da informação e dos métodos de processamento;

c) **Disponibilidade**: garantia de que utilizadores autorizados tenham acesso à informação e activos correspondentes sempre que necessário.

A informação é um bem tão importante como qualquer outro bem da organização pelo que tem de ser protegido da forma mais apropriada. A Segurança da Informação protege a informação contra uma multiplicidade de ameaças, entre as quais compreende: assegurar a continuidade do negócio, minimizar os efeitos negativos no negócio e maximizar a rentabilização dos investimentos e as oportunidades de negócio.

O nível atingido de Segurança da Informação depende do esforço dispendido. No entanto, o esforço ou o investimento dispendido não é proporcional às melhorias a alcançar. Atingir um nível de segurança de 100% não é possível.

Deverá existir um compromisso na definição do nível de segurança pretendido. Nestas condições e de acordo com o gráfico apresentado a seguir recomenda-se o nível de segurança elevado a adoptar para a Entidade. Esta orientação geral permite ajudar na selecção dos meios para a criação da Segurança da Informação.



7 Objectivos da Política Nacional de Segurança da Informação

Em baixo relembramos os objectivos de segurança de informação do governo e apontamos as principais acções a tomar para os cumprir.

Objectivo 1: *Ser parte integral dos objectivos da Administração Pública e servir de orientação ao sector privado.*

Os objectivos da Administração Pública incluem não só qualidade e tecnologia como também justiça, economia e flexibilidade. Para atingir estes objectivos é necessário um elevado nível de Segurança da Informação em todos os processos da Administração Pública. Como tal, a Segurança da Informação deverá ser tida em conta durante a fase de desenho de todos os processos.

Objectivo 2: *Proteger os interesses do estado e seus cidadãos, as entidades públicas e privadas e seus clientes e os parceiros e seus empregados.*

Este objectivo de segurança tem influência no desenvolvimento dos processos e sua implementação. As medidas e controlos técnicos de Segurança da Informação estão a ser actualizadas para que os cidadãos, entidades públicas e privadas e seus clientes, parceiros e seus empregados encontrem-se protegidos enquanto perseguem os seus interesses legítimos.

Objectivo 3: *Assegurar que todos os requisitos legais e da Indústria são cumpridos e de que existe o registo de evidências para efeitos de auditoria de todos os processos TIC relevantes em cada entidade do sector público ou privado.*

A adesão aos requisitos legais e afins relativamente à Segurança da Informação, além de ser obrigatória, contribui não só para o cumprimento dos objectivos da entidade, como também para a protecção do país, da entidade, dos seus clientes, parceiros e seus empregados. Deste modo, as alterações à legislação e outros regulamentos relevantes para a segurança encontram-se a ser constantemente monitorizadas, e as consequências destas para a Segurança da Informação a serem identificadas. Os controlos apropriados são implementados utilizando métodos ou ferramentas de segurança adequados. A protecção dos dados é uma preocupação constante e importante.

Os registos de evidências para efeitos de auditoria devem permitir uma reconstrução de como a informação foi recebida, tratada e/ou modificada. No mínimo, os requisitos de auditoria da Lei de Protecção de Dados necessitam ser cumpridos, se possível devem ser estendidos a toda a informação sujeita à Política de Privacidade da Entidade.

Objectivo 4: *Assegurar que a Política de Segurança da Informação da Entidade é implementada por uma equipa de Segurança da Informação, de acordo com as normas de Segurança da Informação mandatárias. As entidades do sector privado são incentivadas a proceder da mesma forma.*

As normas de segurança da entidade cobrem e definem as funções, responsabilidades e competências da gestão da Segurança da Informação para todos os tópicos relevantes de segurança. A definição de normas é assegurada por um conselho/fórum de segurança, que define objectivos de segurança (incluindo risco aceitável), estratégias, requisitos, medidas e serviços que estão integrados numa estrutura da entidade. Isto assegura a implementação coordenada da Política de Segurança da Informação da Entidade e garante que o nível de Segurança da Informação pretendido seja atingido e mantido.

Objectivo 5: *Consciencializar para a segurança todos os funcionários públicos e empregados de empresas do sector privado que fornecem serviços de infra-estrutura crítica.*

A consciencialização para a segurança e qualidade de todos os funcionários públicos e empregados de empresas do sector privado é um pré requisito para o cumprimento dos controlos de Segurança da Informação e o seu contínuo aperfeiçoamento, bem como a introdução de serviços de Segurança da Informação modernos. A consciencialização de segurança permite a Portugal fornecer serviços de qualidade para benefício do Estado e seus cidadãos, das entidades públicas e privadas e seus clientes, parceiros e seus empregados.

Objectivo 6: *Assegurar a protecção de dados e recursos das TIC através de iniciativas adequadas a tomar por cada membro da Sociedade da Informação.*

A informação e dados pertencentes ou confiados a qualquer membro da Sociedade da Informação de acordo com os contractos estabelecidos, bem como os recursos de TIC utilizados para inserir, transferir, processar ou armazenar dados serão protegidos contra a divulgação ou modificação não autorizada. Medidas rigorosas de Segurança da Informação, quer de origem técnica, quer de origem organizacional são implementadas, de modo a garantir a adequada confidencialidade, integridade e disponibilidade dos dados e recursos sensíveis.

Os incidentes de Segurança de Informação são registados e analisados através de meios adequados no sentido de precaver uma recorrência futura. A equipa de Segurança da Informação é incentivada a identificar lacunas no Sistema de Gestão da Segurança da Informação (SGSI) e a eliminar qualquer fragilidade em cooperação com os responsáveis dos departamentos afectados.

A Administração Pública de Portugal assegura que todas as actividades e incidentes relacionados com a segurança são registados, no sentido de reforçar a responsabilidade pela sua rede, sistemas e bases de dados.

Objectivo 7: *Assegurar um elevado nível de Segurança da Informação durante todo o ciclo de vida dos sistemas de informação.*

No sentido de se obter serviços de segurança com qualidade, todo o ciclo de vida dos sistemas de informação está sujeito a uma gestão de qualidade. Para este fim, são definidos procedimentos seguros para o desenvolvimento e a introdução de novas aplicações, a gestão de recursos, a avaliação da segurança dos produtos, a operação e manutenção de recursos de TIC e a desactivação controlada.

Objectivo 8: *Garantir a continuidade do negócio.*

Todas as entidades da Administração Pública e empresas do sector privado que fornecem serviços de infra-estrutura crítica têm um plano de continuidade do negócio de forma a salvaguardar interrupções deste e proteger os processos críticos do mesmo contra os efeitos de erros e desastres. O conselho/fórum de segurança da entidade define as normas base dos planos de recuperação em caso de emergência. Estes especificam localizações alternativas e os procedimentos de armazenamento de dados *off-site*.

Os planos de recuperação contêm toda a informação necessária para uma rápida recuperação das aplicações e serviços. Os planos de recuperação são testados regularmente de acordo com a criticidade do serviço que protegem, dos requisitos legais, das expectativas dos clientes e/ou dos Acordos dos Níveis de Serviço.

Objectivo 9: *Honrar a confiança de todos os membros da Sociedade da Informação.*

As entidades do sector público e privado dependem não só de tecnologias cada vez mais sofisticadas e complexas utilizadas no ciclo de desenho e desenvolvimento, como também na relação próxima com o cidadão, fornecedores, clientes e outros membros da Sociedade da Informação. Portanto, cada entidade do sector público ou privado garante a salvaguarda adequada de todos os seus dados. Toda a informação pessoal armazenada pode ser vista, modificada ou apagada pelo cidadão ou pela entidade proprietária dos dados. A menos que indicado em contrário na legislação, os dados armazenados apenas podem ser utilizados para a finalidade para a qual foram recolhidos. Existem excepções à lei definidas em regulamentação própria (e.g. Polícia Judiciária no âmbito de uma investigação).

8 Responsabilidades na Segurança da Informação

A Politica de Segurança da Informação da Entidade (PSIE) é implementada pela entidade em conformidade com a Estrutura Nacional de Segurança da Informação (ENSI). A PSIE define os objectivos de controlo tal como são aplicados a toda a entidade.

Será definida uma estrutura de gestão para iniciar e controlar a implementação da Segurança da Informação dentro da entidade. Esta terá de aprovar a PSIE, a Politica de Segurança da Informação da Entidade em Detalhe (PSIED), atribuir funções e coordenar a implementação da Segurança da Informação em toda a entidade.

A estrutura de gestão inclui uma função de gestão de risco responsável pela definição de prioridades nas implementações de segurança da informação e assegurar um compromisso entre o custo e o risco associado.

9 Recomendações para a Implementação

1. *Cada entidade da administração pública deverá desenvolver e implementar uma politica de segurança de informação que seja apropriada às funções e riscos associados da entidade.*

   A Direcção é responsável pela integração dos princípios e planos de uma estrutura coordenada e sistematizada para identificar, avaliar e tratar os riscos de Segurança da Informação na entidade. A política de Segurança da Informação será baseada numa avaliação da estratégia e contexto da entidade. A política de Segurança da Informação suporta as metas e os objectivos definidos pela entidade.

2. *A política de Segurança da Informação deverá identificar os activos da informação da entidade.*

   Cada bem de informação, ou grupo de classes de bens de informação requerido pela entidade publica precisa de ser listado na política juntamente com a identificação dos grupos de pessoas ou organizações que estão autorizados a aceder e para que propósito.

3. *Cada entidade pública deverá realizar análises de risco de segurança da informação de forma regular.*

   Avaliações de risco de segurança de informação regulares cobrindo ameaças à disponibilidade, confidencialidade e integridade dos bens de informação da entidade, são utilizadas para o desenvolvimento e revisão da política de segurança de informação da entidade.

4. *A politica de Segurança da Informação da entidade deverá ser monitorizada e revista de forma a minimizar os riscos.*

   Para assegurar que as medidas de segurança são relevantes para as alterações das condições, a politica de segurança de informação da entidade vai necessitar de ser analisada e sujeita a um processo contínuo de revisão e avaliação.

   Os incidentes de segurança de informação necessitam de ser investigados atempadamente. A investigação deve identificar as causas, minimizar as consequências adversas e recomendar acções que permitam que incidentes similares não se repitam. Caso seja necessário, deve ser criado uma área de investigação e processos criminais e/ou civis.

5. *Deverão ser protegidos os recursos de informação, nomeadamente os sistemas TIC, de serem comprometidos ou indevidamente utilizados – ou seja, o conjunto de meios pelos quais poderia ser comprometida a informação, especialmente perda, corrupção, fuga, quer sejam deliberados ou acidentais.*

   A informação recolhida e gerada pelas entidades públicas é valiosa quer para a Administração Pública quer para os indivíduos ou entidades privadas. Recursos de informação valiosos devem ser identificados e protegidos, e fundamentados numa avaliação de risco formal.

6. *As pessoas contratadas para desempenharem funções governamentais têm de ser idóneas e integras.*

   A segurança da informação de uma entidade depende da integridade e honestidade das pessoas que trabalham para esta. Portanto, as entidades públicas necessitam de assegurar que os princípios de idoneidade descrevem as responsabilidades a serem atribuídas aos empregados, que os empregados são informados das suas responsabilidades, e que os empregados estão em conformidade com a sua responsabilidade e regulamentações governamentais relevantes.

7. *Quando se faz outsourcing de uma função, as entidades públicas deverão manter a capacidade de avaliar o desempenho em termos de segurança dessa mesma função.*

   Cada entidade deve assegurar que a segurança é estabelecida de forma apropriada para todas as funções e recursos oficiais do governo. Isto é igualmente importante se a função da entidade for contratada fora. É necessário garantir que os a fornecedores contratados são informados das políticas e recomendações da Segurança da Informação da entidade.

8. *Os recursos de informação utilizados num ambiente de tele-trabalho ou móvel deverão ser adequadamente seguros.*

   A entidade pública é responsável por assegurar as medidas de segurança apropriadas de forma a permitir um manuseamento correcto da informação pelos funcionários da entidade no desempenho das suas funções. De forma a assegurar a Segurança de Informação nos ambientes de tele-trabalho e móvel, a entidade deve apoiar o empregado na identificação e gestão dos potenciais riscos de Segurança da Informação tendo em atenção o seu ambiente de trabalho.