Carta de Princípios de Segurança Informática e Privacidade

Lisboa, 3 de Julho de 2008

Versão 1.1

Histórico de Alterações

Versão	Data	Descrição	Autor
1.0	18-05-2006	Versão Inicial	Auditoria Externa / António Pina
1.1	03-07-2008	Adaptação às novas Unidades Orgânicas	Pedro Madeira da Fonseca

Controlo do documento

Revisto por:

Nome	Unidade Orgânica	Data	Rubrica
António Pina	GSIN	2006-05-17	
António Pina	DSAQ	04-07-2008	

Versão 1.1 aprovada por:

Nome	Unidade Orgânica	Data	Rubrica
Manuela Leamaro	DSAQ	06-07-2008	
Mário Campos	DSAQ	06-07-2008	

Palavras-chave: segurança, política, privacidade.

Áreas com interesse neste documento: DSAQ; DSOD; DSOS; DSEP; DSGR; Direcção

Data de impressão:

Localização física: Intranet:

Índice

1 Visão Geral

O propósito deste documento é dar a conhecer a Política de Segurança Informática e Privacidade (PSIP) que o Instituto de Informática do Ministério das Finanças e Administração Pública (IIMFAP) segue no desenvolvimento das suas actividades, por forma a definir, aprovar e implementar um sistema adequado de controlo e monitorização, suportado por uma Organização de Segurança Informática, envolvendo todos os colaboradores e definindo medidas, regras e responsabilidades.

O Instituto de Informática do Ministério das Finanças e Administração Pública (IIMFAP) é um serviço do Ministério das Finanças dotado de autonomia administrativa e com personalidade jurídica, criado em 11 de Novembro de 1977, e que tem a sua orgânica regulamentada pelo Decreto-Lei n.º 83/2007, de 29 de Março, e tem como missão apoiar a definição das politicas e estratégias das tecnologias de informação e comunicação (TIC) do Ministério das Finanças e da Administração Pública (MFAP) e garantir o planeamento, concepção, execução e avaliação das iniciativas de informatização e actualização tecnológica dos respectivos serviços e organismos, assegurando uma gestão eficaz e racional dos recursos disponíveis.

A Política de Segurança Informática e Privacidade (PSIP) serve como guia para todas as questões relativas à Segurança da Informação e pretende assegurar a confidencialidade, integridade e disponibilidade dos seus recursos.

Este documento descreve os princípios gerais que devem ser aplicados pelo IIMFAP e encontra-se definido do seguinte modo:

- Visão Geral
- Âmbito e Audiência
- Introdução
- Importância das TIC
- Importância da Segurança da Informação
- Organização da Segurança da Informação
- Objectivos da Política de Segurança Informática e Privacidade

É importante que a Política de Segurança Informática e Privacidade Detalhada (PSIPD) e os procedimentos do IIMFAP se mantenham em conformidade com a Política de Segurança Informática e Privacidade (PSIP).

2 Âmbito e Audiência

A Política de Segurança Informática e Privacidade destina-se a todos os colaboradores do Instituto de Informática, independentemente do seu vínculo (colaboradores, fornecedores, consultores, temporários, voluntários, etc.).

É responsabilidade de todos assegurar um elevado nível de segurança, no sentido de apoiar e proteger os interesses do IIMFAP e permitir o funcionamento adequado de todos os sectores de actividade, assegurando assim a realização de serviços e negócios de maneira segura e eficaz.

Os colaboradores que deliberadamente violem esta ou outras políticas devem ser sujeitos a sanções disciplinares ou outras previstas na lei.

O ambiente físico e lógico que envolve uma entidade tem um impacto significativo no nível de Segurança da Informação. O IIMFAP possui uma gestão de risco, através da qual, é possível avaliar o risco associado à utilização das Tecnologias de Informação e Comunicação (TIC) e recomendar medidas adequadas.

3 Introdução

A Segurança da Informação define-se como a preservação de:

a) **Confidencialidade**: garantia de que a informação é acedida 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 os 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: assegurar a continuidade do serviço (negócio), minimizar os efeitos negativos no negócio, maximizar a rentabilização dos investimentos e melhorar a qualidade do serviço.

A Segurança da Informação é obtida através da implementação de um conjunto de controlos que podem ser: políticas, práticas, procedimentos, estruturas organizacionais e funções de *software*.

Os controlos são necessários em toda a Segurança da Informação, que é baseada na norma internacional ISO/IEC 27002:2005 (Ex 17799) e composta pelos seguintes domínios:

- Política de segurança
- Organização da segurança da informação
- Gestão dos activos
- Segurança dos recursos humanos
- Segurança física e ambiental
- Gestão de comunicações e operações
- Controlo de acessos
- Aquisição, desenvolvimento e manutenção dos sistemas de informação
- Gestão de incidentes de segurança da informação
- Gestão de continuidade de negócio
- Conformidade

A política de topo e qualquer controlo centralizado implementado garantem a qualidade do nível de serviço prestado, permitindo gerir o risco de forma eficaz.

4 Importância das TIC

A recolha, arquivo, processamento e transmissão de informação são processos relevantes para o Instituto de Informática. Estas funções estão dependentes de sistemas e infra-estruturas de Tecnologias de Informação e Comunicações (TIC). Para garantir a segurança e protecção da informação do IIMFAP é necessário utilizar TIC seguras, tolerantes a falhas, com alta disponibilidade e garantir a correcta supervisão e formação de todas as pessoas que lidam com recursos e dados sensíveis.

A perturbação nos serviços (prestados pelas TIC), a revelação de dados confidenciais a terceiros não autorizados ou alterações não autorizadas/intencionais de dados podem violar as leis nacionais; podem igualmente levar a uma perda de confiança ou violação de obrigações contratuais para com fornecedores, clientes ou parceiros.

A crescente utilização de sistemas distribuídos em ambientes abertos e heterogéneos de tipo cliente-servidor e Internet implica uma dependência das redes cada vez maior, o que as torna uma infra-estrutura crítica. Esta dependência traz riscos adicionais que têm de ser geridos de forma a salvaguardar a infra-estrutura crítica do Instituto de Informática.

Uma situação emergente é a questão de aplicações TIC que utilizam informação que requer medidas de segurança, mas que se encontram em ambientes difíceis ou impossíveis de controlar. É aqui que a consciencialização planeada de todos os colaboradores do Instituto de Informática é pertinente, pelo que o IIMFAP implementa uma cultura de segurança que cobre todos os seus activos.

5 Importância da Segurança da Informação

A informação, os seus processos de suporte, sistemas, aplicações e redes são activos valiosos para as entidades e cidadãos. A perda de confidencialidade, integridade e/ou disponibilidade podem levar a uma perda de confiança nos serviços prestados.

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 inundação. Alguns perigos como os vírus, *hackers* e ataques do tipo Negação de Serviço (DoS) estão a acontecer mais frequentemente e têm-se tornado cada vez mais criativos e complexos de gerir.

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

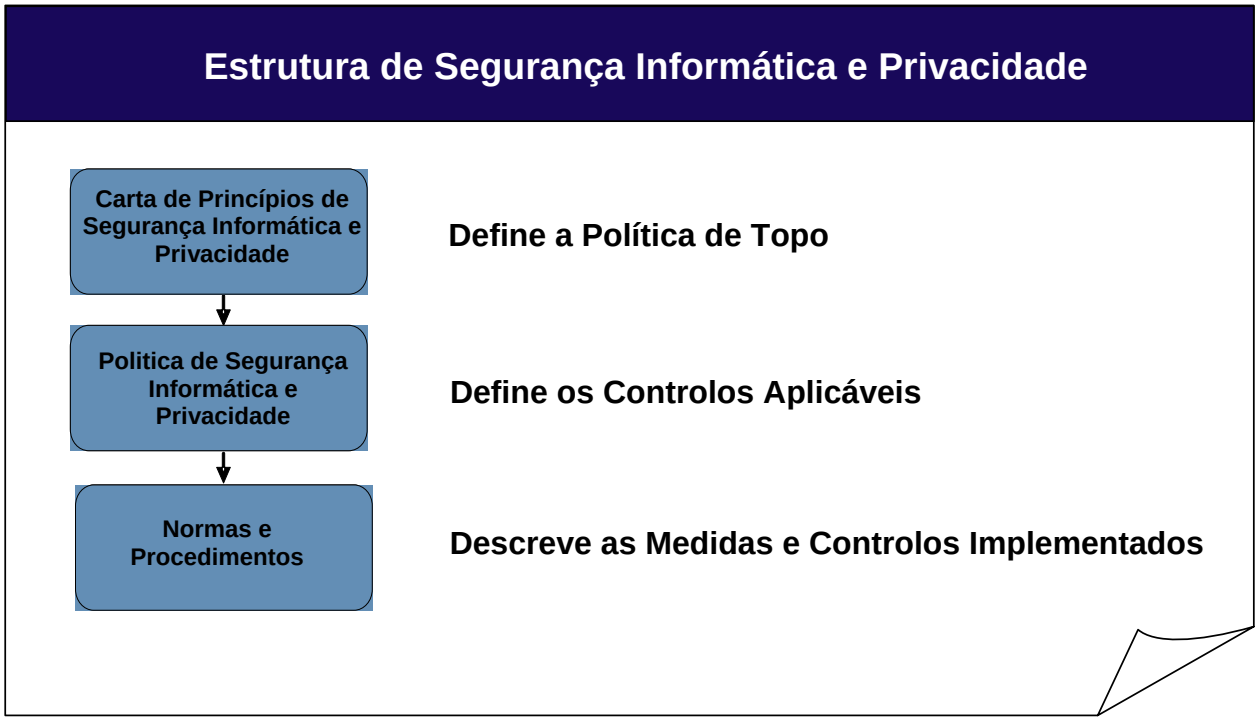
- A protecção da informação está ajustada à sua importância e valor, que são determinados pelo detentor da informação, sendo que apenas este pode permitir o acesso à mesma;
- A Segurança da Informação, num projecto, (inserção/recolha, processamento, armazenamento, transferência, relacionamento e resultado/pesquisa da informação) é tão importante quanto a funcionalidade e o cumprimento de objectivos;
- A Segurança da Informação permite alcançar e manter, de forma permanente, um nível de qualidade elevado, de forma a evitar o descontentamento ou eventuais queixas dos detentores da informação. Para isso foi 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 colaboradores, fornecedores ou pessoas que têm acesso à informação;
- Através das orientações do Director-Geral e da disponibilização de material de formação adequado, todos os colaboradores e parceiros têm de compreender e agir em

conformidade com os requisitos da Política de Segurança Informática e Privacidade (PSIP);

- 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 tecnológicas e/ou sociais;
- As medidas de segurança são técnica e economicamente viáveis e não limitam, de forma inadequada, a produtividade do Instituto de Informática.

6 Organização da Segurança da Informação

A estrutura da Segurança da Informação e Privacidade que o IIMFAP implementa contém 3 níveis. Cada nível está em conformidade com o nível anterior e, ao mesmo tempo, especifica as expectativas e objectivos para o(s) nível(eis) abaixo:



Existe apenas uma Política de Segurança Informática e Privacidade (PSIP). A PSIP define os objectivos de segurança da política para a Segurança da Informação.

7 Objectivos da Política de Segurança Informática e Privacidade

Objectivo 1: *Ser parte integrante dos objectivos do Instituto de Informática.*

Os objectivos do Instituto de Informática incluem qualidade, tecnologia, justiça, economia e flexibilidade na prestação de serviços. Para atingir estes objectivos é necessário um elevado nível de Segurança da Informação em todos os processos. Como tal, a Segurança da Informação é 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 colaboradores.*

Este objectivo de segurança tem influência no desenvolvimento dos processos e sua implementação. As medidas e controlos técnicos de Segurança da Informação estão actualizados para que os cidadãos, entidades públicas e privadas e seus clientes, parceiros e seus colaboradores se encontrem protegidos.

Objectivo 3: *Assegurar que todos os requisitos legais e da Indústria são cumpridos e que existe o registo de evidências, para efeitos de auditoria, de todos os processos TIC relevantes no Instituto de Informática.*

A adesão aos requisitos legais e afins, relativamente à Segurança da Informação, além de ser obrigatória, contribui não só para o cumprimento dos objectivos do IIMFAP, como também para a protecção deste, dos seus colaboradores e parceiros. Deste modo, as alterações à legislação e outros regulamentos relevantes para a segurança são constantemente monitorizados e as consequências destes para a Segurança da Informação 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 permitem uma reconstrução de como a informação foi recebida, tratada e/ou modificada. Os requisitos da Lei de Protecção de Dados são cumpridos e são estendidos a toda a informação sujeita à Política de Segurança Informática e Privacidade do IIMFAP.

Objectivo 4: *Assegurar que a Política de Segurança Informática e Privacidade (PSIP) é implementada por uma equipa de Segurança da Informação, de acordo com as normas de Segurança da Informação mandatárias.*

As normas de segurança do IIMFAP 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 pelo Conselho de Segurança Informática e Privacidade do IIMFAP, que define objectivos de segurança (incluindo risco aceitável), estratégias, requisitos, medidas e serviços que estão integrados na estrutura do IIMFAP. Isto assegura a implementação coordenada da Política de Segurança Informática e Privacidade e garante que o nível de Segurança da Informação pretendido é atingido e mantido.

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

A consciencialização, para a segurança e qualidade, de todos os colaboradores do IIMFAP 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 e fiáveis. A consciencialização de segurança permite ao IIMFAP fornecer serviços de qualidade para o seu próprio benefício, dos seus colaboradores, clientes, parceiros e seus empregados.

Objectivo 6: *Assegurar a protecção de dados e recursos das TIC através de iniciativas adequadas a tomar por cada colaborador do Instituto de Informática.*

A informação e dados pertencentes ou confiados a qualquer colaborador do IIMFAP, de acordo com os contratos estabelecidos, bem como os recursos de TIC utilizados para inserir, transferir, processar ou armazenar dados, são 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 da 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 hiatos no Sistema de Gestão da Segurança da Informação (SGSI) e a eliminar qualquer fragilidade, em cooperação com os responsáveis dos departamentos afectados.

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***.**

O IIMFAP possui serviços de infra-estrutura críticos e, consequentemente, tem um plano de continuidade do negócio de forma a salvaguardar interrupções destes e proteger os processos críticos dos mesmos contra os efeitos de erros e desastres. O plano abrange os mecanismos de redundância e recuperação de serviços necessários. O Conselho de Segurança Informática e Privacidade do IIMFAP define as normas base dos planos de recuperação em caso de emergência. Estes especificam localizações alternativas e os procedimentos de armazenamento de dados em local remoto.

Objectivo 9: *Honrar a confiança de todos os colaboradores do Instituto de Informática.*

O IIMFAP depende não só de tecnologias cada vez mais sofisticadas e complexas, utilizadas no ciclo de desenho e desenvolvimento, como também da relação próxima com os seus colaboradores, clientes e parceiros. Portanto, garante a salvaguarda adequada de todos os seus dados. Toda a informação pessoal armazenada pode ser vista, modificada ou apagada pelo colaborador 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.

8 Responsabilidades na Segurança da Informação

Existe uma estrutura de gestão para promover e controlar a implementação da Segurança da Informação dentro do Instituto de Informática designada Conselho de Segurança Informática e Privacidade (CSIP), formada por representantes de todas as Direcções de Serviços/Projectos do IIMFAP, é presidida por um elemento da Direcção. Este, é responsável por elaborar e propor a aprovação, pela Direcção, da Carta de Princípios de Segurança Informática e Privacidade, da Politica de Segurança Informática e Privacidade (PSIP), normas e procedimentos bem como, atribuir funções e coordenar a implementação da Segurança da Informação em todo o IIMFAP.

À DSAQ incumbe, no domínio da segurança da informação, estudar e propor as normas e procedimentos de segurança informática; realizar acções de auditoria, acompanhamento e avaliação do cumprimento das normas e procedimentos de segurança.

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