Segurança da Informação
Política

Versão 8.0

Índice

1. Introdução

1.1 Objetivo

Esta política tem como objetivo definir os princípios gerais a ser aplicados pelo Organismo aos ativos de informação por si geridos, considerando as normas, *standards* e requisitos legais aplicáveis, permitindo a adoção de padrões de segurança e de boas práticas na gestão da segurança da informação.

A última versão aprovada deste documento encontra-se disponível na intranet.

1.2 Âmbito

A política de segurança de informação aplica-se a todas as atividades do Organismo.

.

1.3 Audiência

Este documento é destinado a todos os colaboradores que prestam serviço no Organismo, independentemente do seu vínculo laboral.

1.4 Glossário

Consultar o "Glossário de Definições e Acrónimos" (REG139) na Intranet, em: Espaço e-Qualidade > Sistema de Gestão Integrado > Procedimentos do Sistema de Gestão Integrado > Controlo de Documentos e Registos.

2. Descrição

O organismo compromete-se a proteger a informação gerida por si e à sua salvaguarda, qualquer que seja o seu formato, contra o acesso por pessoas não autorizadas, a garantir que a informação está acessível sempre que necessário e que a mesma é confiável e autêntica. Para o efeito, organismo compromete-se a estabelecer, implementar, manter e melhorar, de forma contínua, um Sistema de Gestão de Segurança de Informação, considerando os ativos de informação que detém à sua guarda e responsabilidade, em alinhamento com a análise de risco realizada e revista periodicamente, com os objetivos estratégicos do organismo e os traçados para a segurança da informação.

O Sistema de Gestão de Segurança de Informação deve assim garantir a confidencialidade, integridade e disponibilidade da informação, pela implementação dos controlos necessários, e pela definição clara das responsabilidades, papeis e atividades a realizar no âmbito da segurança da informação.

3. Princípios gerais

O Organismo **deve** definir as políticas, processos e procedimentos necessários à garantia da confidencialidade, integridade e disponibilidade dos ativos de informação acedidos e geridos pelo Organismo.

As políticas, processos e procedimentos definidos **devem** ser aprovados pela gestão de topo e divulgados a todas as partes interessadas.

O organismo **deve** definir os objetivos a prosseguir no âmbito da segurança da informação, bem como os papéis e responsabilidades a atribuir.

É **recomendado** que o organismo garante a independência e a segregação de funções.

É **recomendado** que seja estabelecido, implementado e gerido um sistema de gestão da segurança da informação, integrado com os processos da organização e com a estrutura de gestão global do Organismo, garantindo uma abordagem multidisciplinar ao tema.

Todos os colaboradores do Organismo **devem** ser responsáveis pela segurança da informação contribuindo proactivamente para a proteção da mesma.

É **recomendado** que os requisitos de segurança da informação sejam conhecidos e acordados com todas as partes interessadas.

3.1 Violação das políticas

Caso se verifique incumprimento desta ou outras políticas por parte de um colaborador do Organismo, que coloquem em risco a segurança dos ativos de informação, o organismo **deve** despoletar procedimentos disciplinares de acordo com legislação aplicável.

4. A Segurança da Informação

O organismo recolhe, armazena, processa e transmite informações de variados formatos (físicos e eletrónicos). Estes ativos de informação, à semelhança de outros ativos do Organismo, têm valor para o negócio da organização e, consequentemente, **devem** ser protegidos contra várias ameaças, tanto acidentais como deliberadas, internas ou externas, que podem colocar riscos de segurança a estes ativos.

A segurança da informação **deve** reduzir a exposição do Organismo a estas ameaças e vulnerabilidades, protegendo a confidencialidade, integridade e disponibilidade dos ativos de informação, onde se entende por:

- **Confidencialidade**: garantia de que a informação está acessível apenas por colaboradores devidamente autorizadas para o efeito;
- **Integridade**: garantia da exatidão da informação e dos métodos de processamento; e
- **Disponibilidade**: garantia de que utilizadores autorizados têm acesso à informação sempre que necessário.

4.1 Valor da Informação

O valor de informação **deve** ser definido pelo impacto da eventual quebra da integridade, confidencialidade e disponibilidade da mesma nos objetivos e missão do Organismo, assim como legislação vigente e regulamentação específica. A perda de confidencialidade, integridade e/ou disponibilidade de ativos de informação podem levar à perda de credibilidade dos serviços prestados pelo Organismo.

Assim, o Organismo **deve** proteger os ativos de informação contra as ameaças e vulnerabilidades a que estão sujeitos,

É **recomendado** que as medidas de proteção dos ativos de informação sejam ajustadas à sua importância e valor.

4.2 Políticas

O Organismo **deve** definir a política de segurança da informação, identificando:

- A definição da segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;
- A atribuição de responsabilidades, gerais e específicas, para a gestão da segurança da informação.

É **recomendado** que o Organismo defina e aprove, políticas detalhadas de segurança da informação de acordo com a Figura 1. Devem ser adotadas as políticas detalhadas relevantes para a missão e atividades do Organismo.

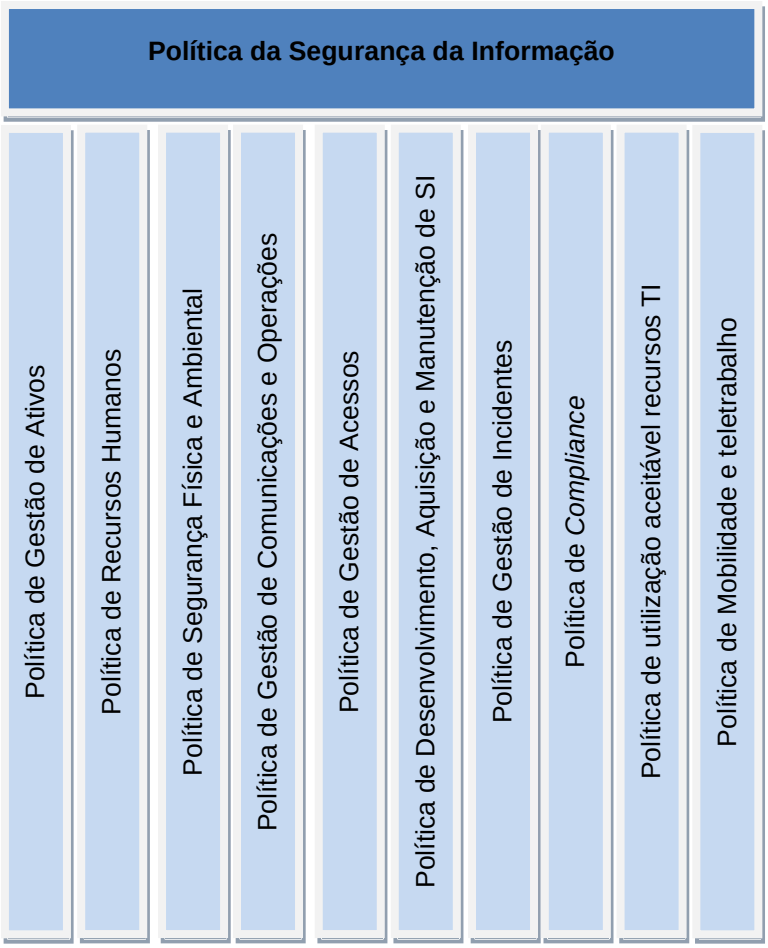

Figura 1 - Políticas de Segurança da Informação

As políticas **devem** ser revistas sempre que houver alterações organizacionais ou técnicas significativas, garantindo que continuam a ser relevantes e adequadas.

O organismo **deve** garantir a comunicação efetiva das políticas a todos os colaboradores, de modo a que estes fiquem cientes das obrigações individuais quanto à temática da segurança da informação.

5. Organização da Segurança da Informação

5.1 Sistema de Gestão

Recomenda-se que a organização da segurança da informação no Organismo seja suportada num sistema de gestão que permita planear, desenhar, controlar, avaliar e melhorar todo o processo de implementação da segurança da informação, de forma transversal, considerando três vertentes de atuação: “pessoas”, “tecnologia” e “processos”.

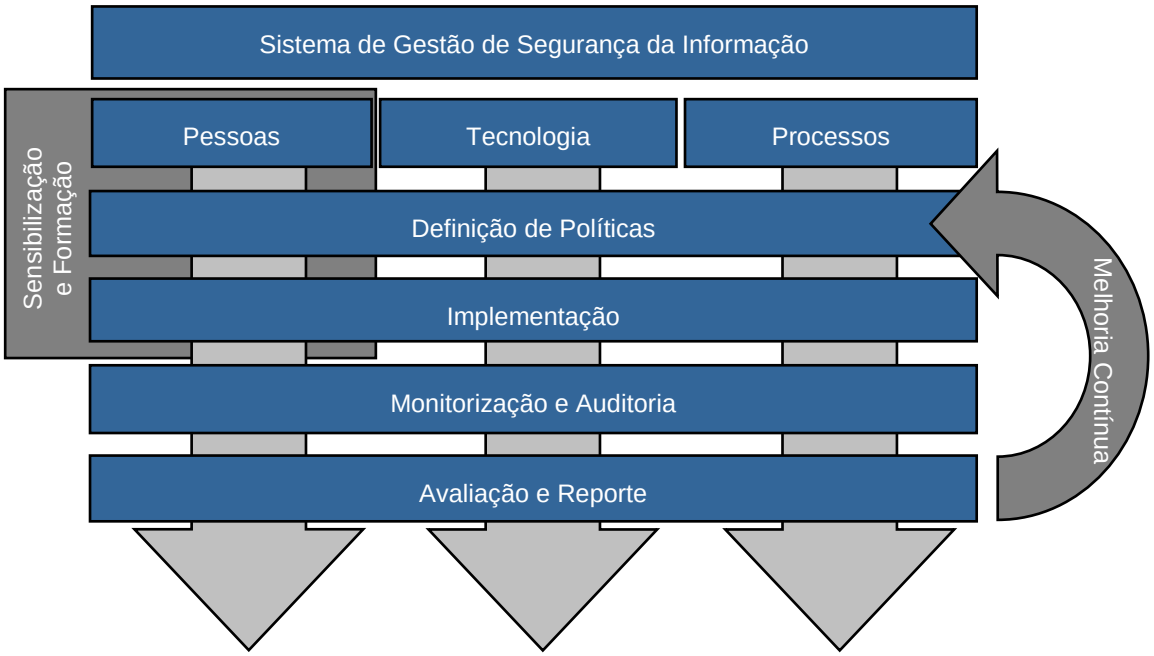

Figura 2 - Framework para Sistema de Gestão de Segurança da Informação

(Adaptado de Information Security Framework - Forrester Research, Inc)

A gestão do Sistema de Gestão de Segurança da Informação **deve** ser constituída por um conjunto de processos que visam suportar a *framework* apresentada e desenvolver um plano de segurança da informação no Organismo, o qual deve ser entendido como um ciclo evolutivo e interligado, que conduzirá ao aperfeiçoamento constante do mesmo, de acordo com as melhores práticas do mercado aplicáveis.

As atividades inerentes ao processo de gestão da segurança da informação **devem** ser realizadas de uma forma coordenada por todos os responsáveis com funções e responsabilidades atribuídas no âmbito da segurança da informação.

5.2 Responsabilidades e papéis

Recomenda-se que o organismo, para uma adequada proteção dos ativos de informação, defina uma estrutura de relacionamento entre pessoas, processos e ativos.

É **recomendado** a definição de uma estrutura de gestão e coordenação no Organismo, que garanta que os processos operacionais salvaguardam a confidencialidade, integridade e disponibilidade da informação, apoiando a tomada de decisões ágil sobre os riscos e investimentos a realizar no âmbito da segurança de informação e na conformidade com requisitos externos (legais, regulamentares ou contratuais), de forma articulada com processos internos do Organismo.

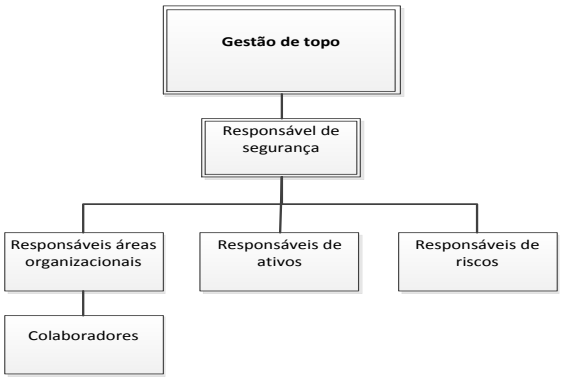

Figura 3 - Responsabilidade da Segurança da Informação

A Gestão de topo do Organismo **deve** ter a responsabilidade máxima de promover, controlar e monitorizar a segurança da informação do Organismo, nomeadamente através da:

- Liderança e compromisso com o sistema de gestão da segurança da informação,
- Aprovação da política de segurança da informação, e
- Identificação e nomeação de responsáveis para as funções relevantes para a segurança da informação, assegurando a conformidade da mesma e reporte do desempenho do sistema de gestão a segurança da informação.

O Responsável de Segurança **deve** ser responsável pelo alinhamento dos objetivos de Segurança da Informação com os objetivos estratégicos do Instituto de Informática, definindo e mantendo atualizadas as políticas de segurança da informação, apoiando e monitorizando a implementação e melhoria contínua dos procedimentos internos de suporte. Cabe ao responsável de segurança a responsabilidade global de desenvolver, implementar e melhorar a segurança da informação no organismo.

Os responsáveis das áreas organizacionais do Organismo **devem** ser responsáveis por promover, no âmbito suas competências e valências próprias, o cumprimento das políticas, processos e procedimentos, identificando proactivamente as ameaças e vulnerabilidades que coloquem em risco a segurança da informação, potenciando uma cultura de segurança transversal.

Os responsáveis dos ativos **devem** garantir a classificação dos ativos de que são responsáveis bem como a definição e implementação dos controlos adequados à proteção dos mesmos, assegurando a integridade, confidencialidade e disponibilidade dos ativos de informação que suportam.

Os responsáveis dos riscos **devem** garantir a aplicação das medidas (técnicas, materiais, organizativas e procedimentais) adequadas que permitam atenuar, eliminar ou transferir os riscos associados aos ativos de informação, reduzindo a possibilidade de uma ameaça específica explorar as vulnerabilidades que comprometam um ativo de informação. Os responsáveis dos riscos devem avaliar o impacto das medidas implementadas e em consequência da análise de riscos realizada, periodicamente, reavaliar a necessidade de implementar medidas adicionais/complementares.

Todos os colaboradores **devem** ter o dever de zelar pelo cumprimento das políticas de segurança da informação.

O organismo **deve** definir responsabilidades e papéis adicionais, de acordo com o seu modelo organizacional e requisitos legais/de conformidade a que esteja obrigado.

É **recomendado** a definição de responsáveis para estabelecer contatos com grupos de interesse especial, associações profissionais ou outros fóruns especializados em segurança da informação.

É **recomendado** a definição de responsáveis para estabelecer contatos com autoridades (por exemplo, corpo de bombeiros, autoridades fiscalizadoras, entidades policiais, entidades regulatórias).

5.3 Contacto com grupos de interesse especial

É recomendado a promoção de contactos adequados com os fóruns de especialistas de segurança e associações profissionais, que permitam assegurar o acompanhamento das tendências, *standards*, melhores práticas e notícias relacionadas com a segurança da informação.
A participação ativa nestes grupos deverá permitir:

- Aumentar o conhecimento sobre melhores práticas e a obtenção de informação de segurança atualizada e relevante;

- Garantir que o entendimento do contexto global de segurança da informação se encontra atualizado e completo;
- Receber os primeiros avisos sobre alertas, conselhos, e mitigações para ataques e vulnerabilidades;
- Obter aconselhamento de especialistas sobre segurança da informação;
- Partilhar e trocar informação sobre novas tecnologias, produtos, ameaças ou vulnerabilidades;
- Estabelecer pontos de contacto adequados para o tratamento de incidentes de segurança da informação.

5.4 Contacto com as autoridades

O organismo **deve** manter contactos adequados com as autoridades civis que permitam assegurar uma resposta atempada das mesmas face a um incidente de grandes dimensões.
O Organismo **deve** manter uma lista atualizada dos contactos das autoridades relevantes a contactar em caso de necessidade, no âmbito de planos de emergência, nomeadamente com:

- Polícia;
- Bombeiros;
- Proteção Civil;
- Segurança das instalações físicas.

5.5 Acordos de confidencialidade

Os acordos de confidencialidade **devem** ser estabelecidos de forma individual entre o organismo e os colaboradores, independentemente do seu vínculo, com o objetivo de responsabilizar os envolvidos, quanto à proteção, utilização e divulgação da informação sob a responsabilidade do Organismo. Neste sentido, é **recomendado** a revisão dos acordos de confidencialidade periodicamente.

O organismo **deve** ser assegurar que todos os colaboradores conhecem e se comprometem com as seguintes obrigações, cuja violação deve ser suscetível de originar responsabilidade disciplinar, civil e/ou criminal, conforme apropriado:

- Deveres decorrentes da legislação laboral, dos quais decorre a obrigação de não divulgação da informação;

- Especial dever de sigilo e confidencialidade, obrigando-se a não divulgar nem fazer uso de qualquer informação a que venha a ter acesso no decurso da sua colaboração no Organismo, com especial relevo para dados pessoais, salvo e na medida em que tal seja necessário para o exercício das suas funções, dever esse que subsistirá mesmo após a cessação do contrato de trabalho;
- Manter a confidencialidade e respeitar os direitos sobre produtos que resultem de aquisição, investigação e desenvolvimento propriedade do organismo, não fazendo cópias, integrais ou parciais dos mesmos.

Estas obrigações **devem** prevalecer pelo período de tempo legalmente previsto para a proteção dos dados a que respeitem, mesmo após a extinção dos contratos com o Organismo, sem prejuízo dos prazos de proteção dos direitos de propriedade intelectual ou outros legalmente fixados.

6. Relação com terceiros

É **recomendado** que, sempre exista uma necessidade de trabalhar com entidades externas que acedam a recursos de processamento ou ativos de informação do organismo, seja feita uma análise dos riscos envolvidos para determinar se os controlos de segurança existentes são adequados. O mesmo deve ser aplicado na obtenção ou no fornecimento de um produto / serviço de ou para uma entidade externa.

É **recomendado** que todos os requisitos/controlos de segurança da informação relevantes sejam estabelecidos e acordados com cada entidade externa para aceder, processar, armazenar ou transferir ativos de informação do organismo.

A presente política abrange todos os diferentes tipos de entidades externas como, por exemplo:

- Fornecedores de serviços de suporte (p.ex., ISP's, fornecedores de redes de dados, telecomunicações e serviços de apoio e manutenção);
- Externalização de operações e/ou de recursos (p.ex., sistemas de TI, serviços de recolha de dados, operação de callcenter, atendimento, etc.);
- Consultores de negócio e gestão, e auditores;
- Implementadores e fornecedores de serviços/produtos de sistemas de informação;
- Serviços de limpeza, refeitório, segurança, ou outros serviços de apoio externalizados;
- Pessoal temporário, estagiários e outras contratações de curta duração.

6.1 Identificação dos Riscos

É **recomendado** que sempre que exista necessidade de conceder a uma entidade externa acesso aos recursos de processamento ou a ativos de informação, seja efetuada uma análise de riscos para identificar eventuais requisitos de controlos específicos, tendo em consideração os seguintes aspetos:

- Os recursos de processamento e a informação a que a entidade externa irá aceder;
- O valor e a sensibilidade da informação envolvida e a sua criticidade para o Organismo;
- A necessidade de acesso:
    - As instalações físicas;
    - Lógico às bases de dados e aos sistemas de informação sob responsabilidade do Organismo;
    - A redes de comunicação ou acesso remotos a ativos de processamento através

de ligação entre as redes de comunicação do Organismo e a entidade externa (por exemplo, link dedicado, acesso remoto) e controlos de segurança a aplicar;

- Os controlos necessários para proteger a informação que não possa ser acedida pelas entidades externas;
- Os diferentes meios e controlos usados pela entidade externa para armazenar, processar, comunicar, partilhar e reencaminhar informação;
- As práticas e os procedimentos para tratar os incidentes de segurança da informação (e os seus eventuais danos) causados pela entidade externa, e os termos e condições para manter o acesso após a ocorrência de um incidente;
- Os requisitos legais e regulamentares e outras obrigações contratuais relevantes para a entidade externa.

É **recomendado** que sempre que os ativos de informação tenham especial criticidade/sensibilidade, seja formalizado o acesso com acordos de não-divulgação.

6.2 Relacionamento com terceiros

O acesso à informação **deve** ser concedido à entidade externa apenas quando os controlos definidos e acordados estiverem implementados.
Antes de conceder a terceiros acesso a quaisquer ativos de informação do Organismo **é recomendado** que seja definido e comunicado:

- Descrição do produto ou serviço a fornecer;
- Procedimentos para proteger a informação e software, gestão de vulnerabilidades conhecidas e comunicação de incidentes;
- Restrições em relação a cópias e divulgação da informação;
- Procedimentos para descrição, notificação e investigação de informações imprecisas, incidentes de segurança da informação e quebras de segurança;
- Direito do Organismo monitorizar e revogar qualquer atividade relacionada com os seus ativos de informação;
- As responsabilidades civis do Organismo e das partes interessadas;
- As responsabilidades legais e requisitos de privacidade de dados, direitos de propriedade intelectual, direitos de autor e a proteção de qualquer trabalho colaborativo ou propriedade intelectual.

Os acordos com as partes envolvidas que envolvam outras terceiras partes **devem** incluir a autorização explícita para a designação de outras partes elegíveis (subcontratadas) e as

condições para o seu acesso e envolvimento.

6.3 Acordos com Terceiros

É **recomendado** que os acordos com entidades terceiras incluam, quando aplicável:

- Política de segurança da informação do Organismo;
- Controlos para assegurar a proteção dos ativos do Organismo:
- Formação dos utilizadores e administradores de sistemas, redes e BDs dos terceiros nos métodos, procedimentos e segurança;
- Assegurar a sensibilização dos utilizadores nas questões e responsabilidades pela segurança da informação;
- Restrições relativas à instalação e manutenção de software e hardware;
- Comunicação dos processos internos do Organismo de desenvolvimento e entrega de serviços, assim como de resolução e gestão/controlo da mudança
- Os níveis de serviços acordados e os níveis de serviços inaceitáveis;
- Definição de critérios de desempenho verificáveis, sua monitorização e descrição;
- Direito de monitorizar e revogar qualquer atividade relacionada com os ativos do Organismo;
- Direito de auditar as responsabilidades definidas no acordo, de essas auditorias serem realizadas por uma terceira parte e de poder enumerar os direitos estatutários dos auditores;
- Estabelecimento de um processo de escalada/litígio para resolução de problemas;
- Responsabilidades legais e a forma de assegurar que estas são atendidas, considerando os sistemas legais de outros países, caso o acordo envolva organizações estrangeiras;
- Direitos de propriedade intelectual e de autor e proteção de qualquer trabalho colaborativo;
- Condições de renegociação ou finalização de acordos.

7. Referências

A seguinte lista identifica outros documentos relacionados com o presente.

Não são incluídos documentos controlados pelo Sistema de Gestão Integrado do Instituto de Informática, sendo estes identificados na Tabela de Controlo de Documentos (REG125).

Referência	Título do Documento	Responsável pelo Documento	Versão
(1)	ISO 27001		2013
(2)			
(3)			
(4)			

8. Histórico de Alterações

Descrição resumida das principais alterações de cada versão.

Data	Versão	Descrição	Autor
Maio 2005	1.0	Versão Inicial PSISS	
23-09-2009	2.0	Atualização da PSISS com base na análise de risco	Gestor da Conformidade
25-05-2010	3.0	Atualização da PSISS na sequência da auditoria interna integrada de Abril de 2010	Gestor da Conformidade
25-08-2011	4.0	Atualização da PSISS na sequência da auditoria interna integrada de seguimento de Julho de 2010	Gestor da Conformidade
19-10-2011	5.0	Atualização do logótipo do Instituto de Informática, alteração para Glossário na Intranet, Referências deixa de incluir documentos controlados do SGI	Gestor da Conformidade
20-01-2015	6.0	Atualização de Imagem do Instituto de Informática, normalização de texto de cópias, e normalização de cabeçalho.	Gestor da Conformidade
18-08-2015	7.0	Atualização do nome do Instituto de Informática, normalização de texto com acordo ortográfico, atualização para normas recentes ISO/EIC/27001:2013; ISO/EIC/27002:2013, substituição de referência de “registos” e “documentos”, por “informação documentada”	Gestor da Conformidade
18-07-2017	8.0	Reestruturação da política, permitindo a sua generalização a outros organismos. Adaptação ao Modelo MOD112-V4.0 Consolidação com Politica de Organização nesta política	Responsável SGSI