REPÚBLICA PORTUGUESA
CULTURA

dgARTES
DIREÇÃO-GERAL DAS ARTES

Homologo

Assinado de forma digital por Américo Rodrigues
DN: c=PT, title=Diretor Geral, ou=Direção Geral, o=Direção-Geral das Artes, cn=Américo Rodrigues
Dados: 2022.05.23 09:14:19 +01'00'

POLITICA DE SEGURANÇA DA INFORMAÇÃO

FICHA TÉCNICA

Título: Politica de Segurança de Informação

Edição Direção-Geral das Artes

Elaboração:

Direção-Geral das Artes

Direção de Serviços de Gestão Financeira e Patrimonial

Data de Publicação: 1.ª versão - março de 2022

Índice

1. Introdução

A presente Política de Segurança da Informação (PSI), segue o disposto na Politica de Privacidade e de Proteção de Dados da Direção-Geral das Artes (DGARTES) e define a aplicação dos princípios e critérios de segurança, ao tratamento dos dados pessoais que sejam levados a cabo pela DGARTES enquanto responsável pelo tratamento.

O Diretor-Geral, ao estabelecer a PSI, assume os compromissos nela definidos, a integração dos seus requisitos nos processos que decorrem da atividade da Direção-Geral e assegura a disponibilidade dos recursos necessários à sua implementação.

2. Objetivos

O objetivo da PSI é garantir que os dados pessoais são recolhidos, tratados, disponibilizados e eliminados de forma segura, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental através daimplementação de medidas técnicas e organizativas.

É ainda objetivo da PSI manter a confidencialidade, garantindo que a informação não seja alterada ou perdida e que esteja disponível quando for necessário, ou seja, comprometer a DGARTES com a aplicação dos dispostos no RGPD no que concerne à garantia da integridade, confidencialidade, disponibilidade e resiliência dos sistemas e dos serviços de tratamento de dados.

Para cumprimento dos objetivos da PSI concorrem os seguintes membros:

2.1. Diretor-Geral;

2.2. Subdiretor-Geral;

2.3. Encarregado de Proteção de Dados ou equiparado;

2.4. Direção de Serviços de Gestão Financeira e Patrimonial (DSGFP) (vertente administração das infraestruturas eletrónicas e informáticas);

2.5. Dirigentes e trabalhadores/as da DGARTES;

2.6. Prestadores de serviços no âmbito das suas contratualizações.

3. Compromisso

Na observância da PSI, a DGARTES compromete-se a:

- Agir em conformidade com os dispostos legais em matéria de segurança da informação, cumprindo e fazendo cumprir os requisitos neles inscritos[1];
- Garantir a confidencialidade, integridade e disponibilidade da informação nos seusprocessos;
- Assegurar uma comunicação efetiva das políticas e procedimentos de segurança dainformação;
- Implementar um processo contínuo de sensibilização e formação da segurança dainformação;
- Demonstrar ser uma entidade segura em matéria de segurança da informação.

4. Âmbito

A PSI destina-se a todas as partes interessadas[2], às quais se acomete a obrigatoriedade de conhecer e agir em conformidade com o nela disposto, bem como com os demais documentos[3] relacionados com a segurança da informação, conforme aplicável e adequado, nomeadamente as políticas, regulamentos, normas e manuais internos com relevância para a gestão da segurança na recolha, tratamento, guarda, partilha e eliminação dos dados pessoais sob responsabilidade da DGARTES

É da responsabilidade de todas as partes interessadas contribuírem proactivamente para a segurança da informação.

Todas as partes interessadas que estão abrangidas pela PSI e que deliberadamente violem esta ou outra política decorrente da atividade da DGARTES, ficam sujeitas a sanções e outras ações, que podem ir até à cessação de contrato e/ou à participação às autoridades policiaisou judiciais das situações que indiciem a prática de crime.

5. Definição de responsabilidades

A PGSI determina a existência de níveis de responsabilidade atribuídos do seguinte modo:

- Ao Diretor-Geral cabe a responsabilidade de controlar e avaliar a implementação

[1] *Exemplo: Resolução do Conselho de Ministros (RCM) 41/2018 que define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais; RCM 91/2012 que aprova o Regulamento Nacional de Interoperabilidade Digital (RNID) na versão atualizada publicada através do Decreto-lei 83/2018;*

[2] *Partes interessadas correspondem a todos os elementos que de alguma forma se relacionam com a DGARTES (cidadãos, empresas, entidades públicas, trabalhadores, prestadores de serviços, subcontratantes, …)*

[3] *2 Exemplos: Manual de utilização do correio eletrónico; Política de Utilização Aceitável da internet; Declaração de Consentimento; Código de Conduta para o Tratamento de Dados Pessoais; Notas Internas sobre Cibersegurança; …*

da PSI, bem como nomear e exonerar os membros da Equipa de Segurança da Informação;

- A Equipa de Segurança da Informação deverá ter um mínimo de 3 elementos trabalhadores da DSGFP ou em caso de contratação de serviços especializados externos, ser coordenada e monitorizada por 1 elemento da DSGFP;
- A Equipa de Segurança da Informação deverá ser nomeada no despacho de entrada em vigor da presente PSI (ponto 10);
- O Diretor-Geral é autónomo na intenção de exoneração parcial ou total dos membros da Equipa de Segurança da Informação, promovendo a sua substituição sempre que verifique não estarem observadas as responsabilidades que acometem a referida equipa no âmbito da PSI;
- Com a exoneração parcial ou total dos membros da Equipa de Segurança da Informação, não obstante o inscrito no ponto 10, há lugar à revisão obrigatória da PSI.;
- Ao Encarregado de Proteção de Dados, ou equiparado, cabe a responsabilidade de promover ativamente a privacidade e segurança das informações coincidentes com implicações na proteção dados pessoais, através da monitorização das vulnerabilidades dos sistemas de informação e do recurso a avaliações do impacto sobre o tratamento dos dados pessoais decorrentes da atividade da DGARTES;
- À Equipa de Segurança da Informação cabe a responsabilidade pela implementação dos mecanismos de segurança da informação, independentemente do seu suporte eletrónico e do perfil de utilização, nomeadamente:
    - criação, monitorização e eliminação de perfis de acesso aos sistemas informáticos da DGARTES, coincidente com as práticas de segurança dos sistemas de informação definidos na RCM 41/2018;
    - monitorização das plataformas informatizadas da DGARTES (manutenção, registo, armazenamento e backup dos dados produzidos, coincidente com as práticas de segurança dos sistemas de informação definidos na RCM 41/2018);
    - gestão e monitorização das informações geradas ou partilhadas, através dos sistemas informáticos da DGARTES, no decurso das suas atividades;
    - formulação e implementação de procedimentos conducentes à mitigação de risco informático;
        - adoção de software e hardware coincidente com as práticas de segurança dos sistemas de informação definidos na RCM 41/2018;
        - elaboração de planos e conteúdos formativos, com vista ao

esclarecimento dos demais serviços sobre os riscos associados à segurança da informação, com incidência em práticas de secretária e ecrã limpo e sobre o uso de dispositivos amovíveis de dados;

- promoção da eliminação ou reutilização segura de suportes de dados e equipamentos;
- observação das práticas elencadas no ponto 8.2. da PSI.

- Aos dirigentes e trabalhadores/as da DGARTES, cabe a responsabilidade pelo cumprimento do exposto na PSI, bem como nos demais normativos a ela associados ou que a ela se referem, na prossecução dos objetivos definidos.

6. Valor e importância da segurança da informação

A importância da segurança da informação decorre do facto de ser uma obrigação legal, pelo que a falta dela coloca os sistemas e os serviços em risco e pode implicar danos aos titularesde dados (exemplos: roubo de identidade pessoal e/ou fraude bancária).

A informação gerada ou recolhida pela DGARTES, bem como os seus processos de suporte, sistemas, aplicações e redes representam ativos[4] de grande valia e interesse para a sociedade, pelo que a garantia de confidencialidade, integridade e disponibilidade da informação assegura a credibilidade dos serviços prestados.

A importância da segurança da informação também se reflete na gestão estratégica da DGARTES, através da construção de uma política que demonstre, entre outros aspetos, conformidade financeira e permita a monitorização, da implementação das medidas de segurança, pela tutela e organismos de controlo.

Assim, as medidas organizativas implementadas devem garantir que as diversas formas adotadas pela informação (escrita ou impressa, armazenada eletronicamente ou em arquivo físico, transmitida por correio ou meios eletrónicos, entre outras) são adequadamente protegidas independentemente do seu meio, utilização e suporte.

A segurança da informação deve, ainda, ser aplicada em todas as fases do ciclo de vida das atividades e processos prosseguidos pela DGARTES, implicando uma manutenção e adaptação contínua ao desenvolvimento tecnológico e legislativo.

Garante-se, assim, que os dados são tratados, alterados, divulgados ou apagados apenas por aqueles que estão autorizados a fazê-lo e que se mantêm disponíveis e acessíveis na

[4] Por ativo entende-se qualquer componente que sustenta um ou mais processos de negócio no âmbito da segurança da informação (exemplo: dados, hardware, software, datacenter, cofre, …)

eventualidade de ocorrer um incidente físico ou técnico, por forma a que a DGARTES consiga salvaguardar os dados afetados e prevenir qualquer dano aos seus titulares.

7. Nível de segurança exigido

O RGPD exige um nível de segurança apropriado aos riscos apresentados pelo tratamento, o qual é determinado através da aplicação de uma avaliação de impacto aos dados pessoais tratados pela DGARTES e comporta a identificação da tipologia de dados, a extensão do seu eventual comprometimento, o grau de risco associado e a natureza dos sistemas (informáticos ou físicos) que os suportem.

Para a determinação do nível de segurança, há também que considerar o número de trabalhadores/acessos aos dados pessoais e a eventualidade desses dados serem tratados por um subcontratante.

A manutenção do nível de segurança da informação, implica que as partes interessadas, com especial relevância nos trabalhadores da DGARTES, saibam reconhecer as possíveis tentativas de violação dos dados pessoais (exemplo: a possibilidade de cometerem atos ilícitos se, voluntariamente, tentarem aceder ou divulgar dados sem autorização; os perigos decorrentes de tentativas de obtenção de dados pessoais por terceiros que se façam passarpelos próprios titulares de dados; etc) e estar devidamente informadas sobre as restrições internas ao uso dos sistemas da DGARTES, nomeadamente os que sejam potenciadores de disseminação de vírus informático.

O nível de segurança da informação deve permitir restaurar a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico, como por exemplo através da manutenção de *backups* estáveis;

Constitui uma falha grave no nível de segurança da informação, qualquer violação de dados pessoais, manifestada, de modo acidental ou ilícito, na destruição, perda, alteração, divulgação ou acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

8. Medidas técnicas de segurança da informação

8.1. Quanto à segurança física:

8.1.1. qualidade das portas e das fechaduras (instalações, gabinetes e mobiliário de escritório);

8.1.2. proteção das instalações por meio de alarmes, luzes de segurança ou CCTV[5];

8.1.3. controlo do acesso às instalações e supervisão de visitantes;

8.2. Quanto à segurança informática:

8.2.1. Segurança dos sistemas com especial relevância para o sistema de redes,

[5] Closed-Circuit Television (Circuito Fechado de Televisão) corresponde aos sistemas de videovigilância.

tráfego de dados, encriptação e sistemas operacionais com manifesta recolha de dados pessoais;

8.2.2. Segurança dos dados contidos nos sistemas da DAGRTES, garantindo que há controlos de acesso apropriados e que os dados são conservados de forma segura, observado o seu armazenamento e *backup*;

8.2.3. Segurança do sítio web da DGARTES e de qualquer aplicação ou serviço a ele associado ou que para ele conflua;

8.2.4. Segurança dos dispositivos correspondentes a políticas de BYOD (*bring your own device*);

9. Linhas orientadoras da PSI

9.1. Recursos Humanos:

A PSI é aplicável a todos os trabalhadores:

a) A PGSI assegura que todos os trabalhadores conhecem, entendem e cumprem as responsabilidades na área da segurança da informação em conformidade com as suas funções;

b) A PSI assegura que os interesses da DGARTES e dos seus trabalhadores são protegidos como parte do processo de início, mudança ou cessação de funções:

9.2. Gestão dos acessos:

A PSI assegura a gestão e o controlo dos acessos às instalações, à informação e aos sistemas informáticos da DGARTES, responsabilizando os utilizadores pela proteção das suas credenciais de acesso e a intransferibilidade dos direitos atribuídos através delas.

9.3. Gestão da Informação:

A PSI assegura a gestão da informação através do cumprimento das medidas técnicas e organizativas em termos de dados pessoais, adaptando-se à elaboração do Regulamento de Arquivo e respetiva classificação documental, bem como através das demais normas internas no âmbito de políticas de utilização aceitável dos recursos disponibilizados pela DGARTES associados à recolha, partilha e armazenamento da informação, independentemente do suporte utilizado.

9.4. Gestão do sistema informático:

a) A PSI garante a operacionalização segura e a adequada proteção dos recursos de processamento da informação, através da monitorização dos seus sistemas informáticos;

b) A PSI permite, com a monitorização permanente dos sistemas, a rastreabilidade e, por conseguinte, a análise, controlo e mitigação de eventuais riscos informáticos, que representem vulnerabilidades na segurança da informação interna e na transmissão entre DGARTES e entidades externas;

c) A PSI subentende a implementação de medidas de gestão de acesso, armazenamento e backup dos dados decorrentes da informação gerada ou partilhada pela DGARTES.

10. Entrada em vigor e revisão

A PGSI entra em vigor na data do despacho do Diretor-Geral e será revista sempre queseja considerado necessário.