Política de Segurança da Informação

Uso Interno (I)

20190211_CSM_RGPD_1_PolíticadeSegurançadaInformação_I_1.0

Classificação: Uso Interno (I)

Versão: 1.0

Data: 11/02/2019

Identificador do Documento: 20190211_CSM_RGPD_1_PolíticadeSegurançadaInformação_I_1.0
Palavras-chave: Política; Segurança da Informação; RGPD; CSM
Tipologia Documental: Política
Título: Política de Segurança da Informação
Tema: Segurança da Informação; Proteção de Dados Pessoais; RGPD
Idioma Original: Português
Idioma de Publicação: Português
Classificação: Uso Interno
Data: 11/02/2019
Versão Atual: 1.0

Autor: Equipa RGPD **Data de Aprovação:** 26/02/2019

Aprovador: Conselho Plenário do CSM

Lista de Distribuição

Função
Todos os colaboradores do CSM

Histórico de Versões

Nº de Versão	Data	Detalhes	Autor(es)
1.0	11/02/2019	Draft	Equipa RGPD

Documentos Relacionados

ID Documento	Detalhes	Autor(es)

Apêndices

ID Documento	Detalhes	Autor(es)

Aceitação do Documento

Cargo	Nome
Vice-Presidente	Juiz Conselheiro Mário Belo Morgado
Chefe do GAVPM	Juíza Desembargadora Ana Isabel de Azeredo Rodrigues Coelho Fernandes da Silva
Juiz Secretário	Juiz de Direito Carlos Gabriel Donoso Castelo Branco

Aprovação do Documento

Cargo	Nome
Plenário	Data: 26/02/2019

Índice

Política de Segurança da Informação

1. INTRODUÇÃO

A segurança da informação é uma preocupação do Conselho Superior da Magistratura (CSM), que se compromete a manter permanentemente um processo organizado e estruturado para esse efeito e que permita preservar os seguintes aspetos basilares:

i) **Confidencialidade da informação**, assegurando que a informação é acessível somente por pessoas devidamente autorizadas, sendo o acesso à informação -restrito a utilizadores legítimos;

ii) I**ntegridade da informação**, garantindo a integral veracidade e completude da informação, bem como os seus métodos de processamento, não podendo o conteúdo da informação ser modificado de forma inesperada;

iii) **Disponibilidade da informação**, assegurando o acesso à informação e a bens associados, por quem esteja devidamente autorizado para tal e sempre que necessário.

Ao nível da responsabilidade pela segurança da informação existente no CSM, **todos os detentores de informação são responsáveis pela segurança da mesma**, bem como, em concreto, pela proteção dos dados pessoais tratados, sem prejuízo da existência no CSM, nos termos legalmente previstos, dos responsáveis especializadas e dedicadas à segurança da informação e à proteção dos dados pessoais.

Os referidos responsáveis especializados em matéria de segurança da informação e dos dados pessoais são o Chefe de Divisão da DDIJ do CSM e o Juiz Secretário do CSM, este na qualidade de responsável pelo tratamento de dados[1], que em concreto assumem a proteção da informação contra quebras de confidencialidade, integridade e disponibilidade da mesma.

Para a concretização, com sucesso, das medidas de segurança da informação em geral, e dos dados pessoais em particular, foi elaborada a presente Política de Segurança da Informação, sendo essencial a colaboração e o envolvimento de todos trabalhadores e colaboradores do CSM, independentemente do respetivo vínculo legal.

2. PRINCÍPIOS GERAIS DE SEGURANÇA DA INFORMAÇÃO

A proteção eficaz e adequada da informação e dos sistemas de informação contra quebras de confidencialidade, de integridade e de disponibilidade garante a continuidade da produção da organização, promove a confiança, bem como salvaguarda uma imagem junto dos magistrados judiciais e do público em geral que interage com o CSM nos mais diferentes âmbitos, que se quer de rigor e de cumprimento escrupuloso das medidas técnicas e das obrigações legais.

Nessa medida, o CSM rege-se pelos seguintes princípios gerais de segurança da informação:

a) Adequação do tratamento da informação face às finalidades da mesma;

b) Proteção da informação própria do CSM e da que lhe é confiada, não permitindo a sua divulgação e alteração contrárias à Lei;

c) Resposta imediata e adequada a eventuais situações de violação da segurança;

d) Disponibilidade dos sistemas de informação com base nas concretas exigências identificadas;

e) Implementação de procedimentos adequados à não interrupção da atividade;

[1] Na aceção do Regulamento Geral de Proteção de Dados (RGPD).

f) Adequada publicitação e divulgação das regras de segurança da informação aos colaboradores do CSM, bem como fornecedores e prestadores de serviços subcontratados;

g) Implementação de procedimentos sistemáticos que visam a redução dos riscos;

h) Adequada formação e sensibilização em matéria de responsabilidade pela segurança da informação;

i) Estabelecimento de medidas adequadas à estrutura orgânica e ao funcionamento do CSM para garantir a segurança da informação;

j) Verificação periódica e regular do cumprimento e da eficácia das medidas de segurança de informação.

3. MEDIDAS CONCRETAS PARA A SEGURANÇA DA INFORMAÇÃO

3.1. Acesso a informação apenas pelos utilizadores autorizados para tal

i. O acesso ao sistema só pode ser concedido a quem tiver concluído, com sucesso, o procedimento de registo.

ii. Os pedidos de criação ou modificação de um perfil de utilizador, incluindo conta de e-mail, são efetuados através de formulários próprios, devidamente preenchidos e assinados.

iii. O Juiz Secretário aprova todos os pedidos relacionados com os perfis dos utilizadores.

iv. Quando a aprovação é concedida, é gerada automaticamente uma nova conta individual para o utilizador e uma palavra-passe inicial (a qual deve também obedecer às regras definidas para as palavra-passe) que lhe irão permitir aceder às funções do sistema para as quais foi autorizado.

v. O acesso às funções do sistema é refletido em perfis de acesso diferenciados em razão da necessidade de conhecer e da segregação de funções.

vi. Os privilégios de acesso (perfis) são devidamente especificados e explicados ao utilizador.

vii. As credenciais de autenticação de cada utilizador são únicas e intransmissíveis.

viii. Não são permitidas contas compartilhadas.

ix. Para comunicações no âmbito do exercício de funções no CSM, os trabalhadores e colaboradores utilizarão exclusivamente a conta de e-mail institucional.

x. No caso de autenticação ser também efetuada por userID/palavra-passe, no primeiro acesso ao sistema, ao utilizador deverá ser solicitado a alteração da palavra-passe inicial, cabendo-lhe a escolha da sua própria palavra-passe.

xi. As contas dos utilizadores serão automaticamente bloqueadas após 3 tentativas de autenticação mal sucedidas e bloqueadas manualmente se se suspeitar que a conta está a ser usada incorretamente.

xii. As contas dos utilizadores serão automaticamente bloqueadas após 90 dias de inatividade.

xiii. O desbloqueio de contas com acesso a dados pessoais deve requerer a intervenção do Responsável pelo tratamento de dados ou a quem ele delegar essa função.

xiv. É criada e mantida atualizada uma lista de utilizadores autorizados e dos respetivos perfis e acesso.

xv. O sistema está configurado para alertar os utilizadores de que devem alterar as respetivas palavras-passe, com uma antecedência adequada (máxima de 30 dias).

xvi. Como regra, o bloqueio automático do ecrã da estação de trabalho fica ativado após 5 minutos de inatividade.

xvii. No final de cada ciclo de trabalho do utilizador, a respetiva sessão deve ser encerrada.

xviii. Verifica-se o encerramento automático da sessão de trabalho do utilizador em caso de inatividade por tempo superior a 3 horas, e o encerramento automático da estação de trabalho em caso de inatividade superior a 5 horas (excecionam-se necessidades de sessões ativas para efeitos de manutenção e administração de sistemas).

3.2. As palavras passe e o acesso à informação

i. As palavras passe dos utilizadores dos sistemas de informação do CSM devem manter-se confidenciais e reservadas, sendo conhecidas apenas pelo próprio.

ii. Não deverá ser selecionada a opção de gravação automática das palavras passe nos sistemas.

iii. Recomenda-se a não utilização das mesmas palavras passe para os sistemas do CSM e para os sistemas de usos pessoais;

iv. As palavras passe definidas deverão ser únicas, seguras e fáceis de memorizar (mas difíceis de adivinhar).

v. A palavra passe deve ter no mínimo 9 caracteres e ser complexa, devendo exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a..z), letras maiúsculas (A..Z), números (0..9) e caracteres especiais (~! @ # $ % ^ & * () _ + | `- = \ {} []:"; '<>?,. /), e podendo, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de "espaço".

vi. Deverão ser mudadas as palavras passe regularmente, mesmo nos sistemas que não obriguem a fazê-lo. Como tal, a palavra passe deve ser alterada, no máximo, a cada 180 dias para perfis de utilizador e 90 dias para perfis de administradores de sistemas e bases de dados, ou quando for comprometida ou se espera que venha a ser comprometida.

vii. A reutilização de palavras passe anteriores deverá ser evitada, recomendando-se que não seja igual às últimas 4 palavras passe.

viii. As palavras passe deverão ser memorizadas e não escritas em papéis ou locais visíveis.

ix. As palavras passe são guardadas em *softwares* encriptados (ex. *KeePass Safe*).

3.3. Posto de trabalho e salas de reuniões

i. O posto de trabalho de cada colaborador deve estar sempre arrumado e cumprir o princípio "*clean desk",* devendo manter as suas mesas de trabalho limpas e organizadas e garantindo que nenhuma informação confidencial ou reservada é deixada à vista, seja em formato papel ou em quaisquer outros formatos ou meios eletrónicos.

ii. Os espaços físicos, designadamente armários, salas ou outros, que contenham informação confidencial ou reservada, deverão estar fechados nos períodos de ausência dos colaboradores a quem estão confiados esses espaços.

iii. Durante as reuniões, com temas confidenciais ou sensíveis, deve verificar se a sala está corretamente fechada e protegida para que a informação seja partilhada de forma confidencial.

iv. Após a realização das reuniões ou eventuais visitas externas, todo o material utilizado deverá ser retirado das salas de reuniões, incluindo anotações.

v. Quando não se está a utilizar o computador, o mesmo deverá ser manualmente bloqueado, sem prejuízo de, em caso de omissão de tal procedimento, ser acionado o bloqueio automático da sessão.

vi. Cada um dos computadores pessoais e portáteis disponibilizados pelo CSM apenas poderá ter *software*

autorizado e devidamente licenciado.

vii. É obrigatória a verificação regular de atualização do *software* antivírus e *antispam* de cada estação de trabalho devendo o utilizador, em caso contrário, comunicar de imediato essa situação ao responsável do departamento de informática, bem como reportar a situação ao responsável pelo tratamento de dados;

viii. Caso se observe algum comportamento suspeito do sistema, o utilizador deve parar imediatamente qualquer processamento em curso, desconectar o sistema (potencialmente) infetado da rede e notificar o Chefe de Divisão da DDIJ do CSM.

ix. O armazenamento de dados em pastas locais deve ser evitado e todos os documentos de trabalho devem estar armazenados nas pastas da rede.

x. Os documentos, impressões, agendas e blocos de apontamentos com dados confidenciais devem ser tratados de forma a garantir que terceiros não possam ter conhecimento do seu conteúdo, pelo que em caso de ausência física do posto de trabalho deverão ser colocados dentro de armários ou gavetas devidamente trancadas.

xi. As impressões devem ser recolhidas da impressora no mais curto espaço de tempo.

xii. Quando se imprimem documentos confidenciais deve ser acompanhada presencialmente a saídas das folhas, garantindo-se que todas são recolhidas da impressora.

3.4. Regras de segurança relativas a dispositivos móveis

i. Todos os dispositivos portáteis (v.g. telemóvel, computador portátil, PEN USB, pasta de documentos) estão protegidos com palavra passe nos termos definidos na presente política de segurança de informação.

ii. Os dispositivos portáteis devem ter os dados encriptados sempre que tal seja tecnicamente possível.

iii. O *software* deverá estar atualizado, pelo que sempre que possível o equipamento móvel deverá ser ligado à rede da organização para receber as devidas atualizações (pelo menos a cada 15 dias).

iv. Todos os equipamentos móveis devem ter instalado um antivírus e uma *firewall*.

v. Devem ser feitas cópias de segurança dos dados e os dados relativos à atividade desenvolvida no CSM devem ser colocados nas pastas da rede.

vi. Em locais públicos, designadamente em transportes públicos, os equipamentos devem estar sob vigilância do respetivo utilizador, para prevenir eventuais furtos.

vii. O trabalho em locais públicos com equipamentos móveis deve garantir o princípio "*clear screen*", salvaguardando que os dados apresentados no ecrã não são acessíveis a terceiros não autorizados.

viii. Os equipamentos móveis não devem ser deixados nos veículos automóveis.

ix. É proibido desbloquear equipamentos com recurso a ferramentas ou sistemas operativos não autorizados (ex. *Jailbreak* ou *Root*).

x. *Home-office* - os documentos que são levados para trabalhar em casa devem estar protegidos contra acesso indevido.

3.5. Regras e boas práticas relativas a parceiros externos (por fase contratual)

Fase pré-contratual:

i. Os parceiros que processam ou armazenam dados da responsabilidade do CSM recebem um *briefing* de segurança da informação.

ii. São definidos os dados a serem trocados e os canais seguros para a troca.

iii. São definidos os interlocutores do CSM e os do parceiro, sendo acordado entre ambos a forma de comunicar incidentes de segurança.

iv. Se forem trocados dados críticos (pessoais ou da atividade do CSM) os interlocutores devem garantir que foram tomadas as medidas de proteção técnicas e funcionais adequadas.

v. O prestador de serviço apresenta um plano de segurança claro e atualizado.

vi. É assinada uma minuta de contrato-tipo disponibilizada pela DSAF, contendo cláusula expressa e validada pelo EPD, relativa à proteção de dados pessoais e cumprimento do RGPD.

vii. Em todos os contratos deve ser assegurado o direito de auditoria de segurança da informação aos parceiros e fornecedores, as quais podem ser realizadas pelo CSM ou por um parceiro escolhido pelas partes e devem ter lugar no âmbito da prestação de serviço.

Durante a execução do contrato e correspondente prestação de serviços:

i. São atribuídos acessos locais ou remotos aos parceiros de acordo com princípio do "Mínimo acesso permitido".

ii. São definidos os espaços físicos de circulação dos prestadores de serviços;

iii. Os sistemas dos subcontratados e prestadores de serviços apenas podem ser instalados nas infraestruturas do CSM se existirem comprovadas razões técnicas ou económicas.

iv. Não é permitido instalar o *software* do CSM em equipamentos de subcontratados e prestadores de serviços.

v. Os sistemas do CSM apenas podem ser colocados nas instalações dos subcontratados e prestadores de serviços após aprovação formal do Chefe de Divisão da DDIJ do CSM.

Terminada a relação contratual:

i. O interlocutor do CSM informa todas as entidades envolvidas do fim da relação contratual.

ii. Todos os privilégios e acessos são imediatamente eliminados.

iii. Todos os equipamentos inerentes à relação contratual são desligados e recolhidos.

4. REGULAMENTO DE GESTÃO DE DADOS PESSOAIS (RGPD)

Os princípios e regras aplicáveis em matéria de segurança de dados pessoais e cumprimento do RGPD encontram-se melhor descritos e detalhados na Política Geral de Proteção de Dados Pessoais do Conselho Superior da Magistratura, aprovada em reunião do Conselho Plenário do CSM.

Não obstante, importa primordialmente reter os seguintes aspetos:

i. O que são dados pessoais (todas as informações relativas a uma pessoa identificada ou identificável como nome, morada, património, vencimento, datas, números de cartões, n.º de telefone, IP, vídeos, imagem, raça, dados biométricos, folhas de presença, avaliações, *curriculum vitae*, etc).

ii. Não devem ser reunidos dados pessoais em papel ou em formato eletrónico sem informar o EPD.

iii. Ao enviar dados pessoais deve estar garantido que os mesmos estão encriptados ou protegidos.

iv. Qualquer operação de destruição ou eliminação de dados pessoais deve garantir que fiquem definitivamente apagados ou eliminados de forma a não serem recuperados por terceiros.

v. Deverá ter-se especial atenção aos dados pessoais transmitidos com subcontratantes e fornecedores, em especial se para fora da EU.

vi. Quaisquer documentos com dados médicos, dados de menores, classificativos, inspetivos, e outros definidos como tal no RGPD, são muitos sensíveis pelo que deve ter-se um cuidado redobrado na sua utilização e meios de transmissão.

vii. Em caso de perda ou violação ilícita de dados pessoais informa-se de imediato o EPD do CSM, para o e-mail: **dpo.csm@csm.org.pt**.

viii. O responsável pelo tratamento de dados cumprirá a obrigação de comunicar às autoridades todas as violações ou perdas de dados pessoais e procede à documentação das mesmas, nos termos previamente aprovados.

5. DESTRUIÇÃO DE DADOS E IMPRESSÕES

A informação pode existir no CSM sob várias formas, como por exemplo: em suportes de papel (folhetos, jornais, cartolinas, posters, etc.) ou suportes eletrónicos designados por *media* (CDs, disquetes, tapes, microfilme, discos rígidos, PEN USB, cartões de memória, etc.).

i. A destruição de informação confidencial ou reservada deve ser realizada de acordo com regras de segurança e procedimentos adequados, nas instalações do CSM e nos destruidores de papel disponibilizados pelo CSM.

ii. Os equipamentos eletrónicos *media* em fim de vida só podem ser destruídos ou ter os dados apagados pela DDIJ.

6. EM RESUMO: AS DEZ REGRAS ELEMENTARES DE SEGURANÇA

1) É interdita a introdução de dispositivos USB de proveniência desconhecida no computador de trabalho.

2) O computador pessoal não deverá permanecer desbloqueado.

3) Em contexto de trabalho em curso, é recomendada a realização frequente de *backups*.

4) É obrigatório garantir que o *software* antivírus está ativo.

5) São proibidas práticas de *phishing* ou outras práticas ilícitas no domínio do tratamento da informação.

6) Verificando-se algum comportamento suspeito do sistema, o utilizador deve parar imediatamente qualquer processamento em curso, desconectar o sistema (potencialmente) infetado da rede e reportar ao responsável pela segurança.

7) É responsabilidade de todos a aplicação das medidas de segurança da informação e de prevenção contra os ciberataques.

8) Todo o trabalho será preferencialmente executado e armazenado em ambientes de redes seguras.

9) É interdita a partilha de palavras passe e de códigos de acesso.

10) As atualizações requeridas pelos sistemas serão executadas com a maior brevidade e mesmo aos dias de fim de semana e feriados.

7. DISPOSIÇÕES FINAIS

7.1. Aplicação da Política e incumprimento

Todos os colaboradores do Conselho Superior da Magistratura, independentemente do respetivo vínculo legal, têm a obrigação de conhecer o conteúdo da presente Política e das suas atualizações posteriores.

Os colaboradores estão obrigados a cumprir a presente Política e a colaborar na sua aplicação.

O não cumprimento das presentes regras pode conduzir à instauração de ação disciplinar, nas situações legalmente previstas, e o desconhecimento da presente Política não justifica qualquer tipo de incumprimento.

Os colaboradores deverão abster-se de qualquer comportamento sobre o qual tenham dúvidas, podendo solicitar ao Juiz Secretário quaisquer esclarecimentos.

Em caso de desconformidade entre a presente Política de Segurança da Informação e a legislação, a legislação prevalece sobre a Política de Segurança da Informação.

7.2. Revisão e acompanhamento da Política

A presente Política será revista periodicamente ou sempre que, por força das necessidades decorrentes das atribuições do Conselho Superior da Magistratura, factos, ou alterações legislativas, assim o obriguem.

7.3. Comunicação e divulgação

Após aprovação, procede-se à divulgação da presente Política a todos os colaboradores do Conselho Superior da Magistratura, independentemente do respetivo vínculo legal.

7.4. Entrada em vigor

A presente Política é de aplicação imediata.

As atualizações à Política constante do presente documento serão válidas a partir da data da respetiva aprovação.

Aprovação do documento

Este documento é aprovado formalmente por:

Aprovado Por:	
26/02/2019	Conselho Plenário do CSM