SISTEMA DE INFORMAÇÃO DA SAÚDE
GOVERNANÇA E GESTÃO

Política de Segurança da Informação da Unidade Local de Saúde de Matosinhos, E.P.E.

ULSM-SGSI-PSI

VERSÃO:	1.0
DATA DA ÚLTIMA REVISÃO:	28 - 05 – 2018
VÁLIDO ATÉ:	31 – 12 – 2019
ESTADO:	
RESPONSÁVEL:	Comissão Local de Proteção de Dados Pessoais
APROVADO POR:	Conselho de Administração
CLASSIFICAÇÃO DO DOCUMENTO:	Interno

Controlo de Versões e Aprovação

Registo das Revisões

REVISÃO	DATA DE ELABORAÇÃO	MOTIVO DA REVISÃO	ELABORADO POR
1.0	28-05-2018	Primeira versão do documento	CISO

Classificação do Documento

CLASSIFICAÇÃO	AUTORIZAÇÃO DE DISTRIBUIÇÃO
Interno	Este documento deve ser distribuído e assinado por todos os colaboradores da ULSM, incluindo voluntários e estagiários. Este documento deve ser publicado no *site* http://www.ulsm.dom/ Qualquer alteração a esta definição de Autorização de Distribuição tem de ser aprovada pelo Conselho de Administração.

Responsabilidades

ELABORAÇÃO, ATUALIZAÇÃO	Chief Information Secutiry Officer (CISO)
APROVAÇÃO	Conselho de Administração (CA)
REVISÃO	Comissão Local de Proteção de Dados Pessoais (CLPDP)

SPMS – Serviços Partilhados do Ministério da Saúde, EPE . Av. João Crisóstomo, nº 11 - 5º piso | 1049-062 Lisboa | Tel.: 211 545 600 | Fax: 211 545 649

Índice

SPMS – Serviços Partilhados do Ministério da Saúde, EPE . Av. João Crisóstomo, nº 11 - 5º piso | 1049-062 Lisboa | Tel.: 211 545 600 | Fax: 211 545 649

1 Introdução

1.1 Enquadramento do Documento

A "Política de Segurança da Informação (PSI) da Unidade Local de Saúde de Matosinhos, E.P.E. (ULSM)" é um documento que se enquadra no nível Estratégico da "*Framework* da Documentação no âmbito da Segurança da Informação" e está alinhado com os "Princípios de Segurança da Informação".

Todos os documentos dos níveis Tático e Operacional da *Framework,* nomeadamente políticas operacionais, normas internas e procedimentos, devem ser baseados ou refletir as preocupações e considerações estabelecidas por este documento.

1.2 Âmbito do Documento

A "Política de Segurança da Informação" (PSI) aplica-se a todos os colaboradores da ULSM (independentemente da sua função, posição hierárquica e vínculo contratual), a fornecedores e parceiros, bem como a todas as outras pessoas que tenham acesso a um posto de trabalho ou sistema de informação da ULSM. As entidades externas com acesso a sistemas de informação da ULSM devem considerar esta Política como recomendação para aplicação interna na sua entidade.

1.3 Finalidade do Documento

a) Definir a Segurança da Informação, alinhada com os princípios de Segurança da Informação, para orientar todas as atividades relacionadas com a Segurança da Informação na ULSM;
b) Enquadrar o modelo de Organização de Segurança da Informação;
c) Identificar os processos para tratamento de desvios e exceções da Política de Segurança da Informação da ULSM.

1.4 Responsabilidades Associadas ao Documento

Todos os colaboradores e parceiros/fornecedores devem estar familiarizados e cumprir com a PSI definida nos pontos seguintes, bem como com as políticas, normas e procedimentos relevantes em cada caso, de forma a garantir a proteção da informação de negócio da ULSM, bem como da infraestrutura que a suporta.

A PSI deve ser:

- **Aprovada** pelo Conselho de Administração (CA) da ULSM;
- **Publicada** para consulta de todos os colaboradores na Intranet, para utentes e parceiros/fornecedores da ULSM no site http://www.ulsm.min-saude.pt/;

SPMS – Serviços Partilhados do Ministério da Saúde, EPE . Av. João Crisóstomo, nº 11 - 5º piso | 1049-062 Lisboa | Tel.: 211 545 600 | Fax: 211 545 649

- **Comunicada** internamente e externamente pelo *Chief Information Security Officer* (CISO);
- **Revista** pela Comissão Local de Proteção de Dados Pessoais (CLPDP) pelo menos uma vez por ano ou quando ocorrem mudanças significativas para garantir a sua melhoria contínua;
- **Atualizada** pelo CISO.

1.5 Termos e Acrónimos

Tabela 1 – Termos e Acrónimos

TERMO OU ACRÓNIMO	DESCRIÇÃO
CA	Conselho de Administração
CISO	*Chief Information Security Officer*
CLPDP	Comissão Local de Proteção de Dados Pessoais
PSI	Política de Segurança da Informação
SNS	Serviço Nacional de Saúde
SGSI	Sistema da Gestão de Segurança da Informação
TIC	Tecnologias de Informação e Comunicação
ULSM	Unidade Local de Saúde de Matosinhos, E.P.E.

1.6 Documentos de Referência

[1] *Framework* de referência de Governação, Gestão e Operação do eSIS;

[2] Estruturas Organizacionais de suporte ao Risco e Segurança da Informação na ULSM;

[3] Plano Estratégico da ULSM.

[4] Estrutura Organizacional do Departamento de Tecnologias de Informação.

1.7 Boas Práticas de Referência

[1] **COBIT® 5.** *A Business Framework for the Governance and Management of Enterprise IT.*

[2] **ISO/IEC 27000:2016.** *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

[3] **ISO/IEC 27001:2013.** *Information technology – Security techniques – Information security management systems – Requirements*.

[4] **ISO/IEC 27002:2013.** *Information technology – Security techniques – Code of practice for information security controls.*

[5] **ISO 27799:2008.** *Health informatics – Information security management in health using ISO/IEC 27002.*

SPMS – Serviços Partilhados do Ministério da Saúde, EPE . Av. João Crisóstomo, nº 11 - 5º piso | 1049-062 Lisboa | Tel.: 211 545 600 | Fax: 211 545 649

2 Princípios de Segurança da Informação da ULSM

2.1 Definição de Segurança da Informação

A informação e respetivos repositórios são ativos relevantes e críticos para a ULSM e para o Serviço Nacional da Saúde (SNS) em geral. Qualquer que seja a forma e o meio de transmissão, recolha e armazenamento de informação, esta deve ser adequadamente protegida.

A Segurança da Informação é a proteção de informação de um amplo conjunto de ameaças através de um processo de gestão de riscos, garantindo a continuidade de negócio e maximizando o retorno em investimentos efetuados.

Em conformidade com a norma ISO/IEC 27000:2016, a Segurança da Informação pode ser formalmente definida como a "preservação da **confidencialidade, da integridade e da disponibilidade**" da informação.

Figura 1 - Princípios fundamentais de Segurança da Informação

Para melhor compreensão importa esclarecer que confidencialidade, integridade e disponibilidade são propriedades da informação e dos ativos de informação:

Confidencialidade – Propriedade em que a informação não está disponível ou que não é revelada a indivíduos, entidades ou processos não autorizados.

Integridade – Propriedade de exatidão e completude.

Disponibilidade – Propriedade de ser acessível e utilizável, sob pedido, por uma entidade autorizada.

A extensão na qual a confidencialidade, disponibilidade e integridade (incluindo não-repúdio, autenticidade e rastreabilidade/auditabilidade) da informação da ULSM deve ser protegida, depende da natureza da informação, das utilizações a que se encontra colocada e dos riscos a que se encontra exposta.

O número crescente de ameaças provenientes de várias fontes aumenta os riscos para os nossos recursos e bens.

O aparecimento e inclusão de um número cada vez maior de formas de comunicação oferecem novas oportunidades de acesso não-autorizado a recursos, nomeadamente informação. As medidas de segurança são consideravelmente menos onerosas e de implementação mais eficaz durante a elaboração dos seus requisitos e da conceção de processos e de sistemas. Assim, quanto mais célere for a adoção de ações para proteger e salvaguardar a nossa informação, mais rentáveis serão estas ações.

Na área da Saúde, a privacidade dos utentes depende da manutenção da confidencialidade da informação pessoal de saúde. Para manter a confidencialidade, bem

SPMS – Serviços Partilhados do Ministério da Saúde, EPE . Av. João Crisóstomo, nº 11 - 5º piso | 1049-062 Lisboa | Tel.: 211 545 600 | Fax: 211 545 649

como para garantir a segurança e evitar os impactos negativos na saúde e na vida dos utentes, devem ser tomadas medidas para manter a integridade dos dados, bem como para garantir a sua conformidade, fiabilidade, eficácia e eficiência.

A Segurança da Informação deve ser salvaguardada nos seus diferentes tipos, nomeadamente:

- Segurança Física;
- Segurança Informática;
- Cibersegurança.

2.2 Compromisso com o Sistema de Gestão de Segurança da Informação

A visão estratégica da Segurança da Informação na ULSM vai para além da implementação de controlos pontuais. As ações no âmbito de Segurança da Informação devem ser alinhadas com os objetivos de Segurança da Informação da ULSM (enquadrados nos objetivos do Sistema de Informação) e geridas de forma integrada.

Para assegurar o cumprimento dos objetivos estratégicos da organização o Conselho de Administração da ULSM assume o compromisso de:

- Assegurar o cumprimento dos requisitos legais e normativos no âmbito da Segurança da Informação;
- Garantir o alinhamento da "Framework de referência do Risco e Segurança da Informação" com a framework de referência para a governança, gestão e operação do Sistema de Informação da ULSM;
- Estabelecer, implementar e melhorar continuamente a Segurança da Informação na ULSM.

Os benefícios de estabelecimento da Segurança de Informação traduzem-se na redução dos riscos para o negócio, no aumento da conformidade com a legislação e regulamentação aplicável, na proteção da reputação, na maior confiança dos clientes e parceiros e na gestão eficaz dos recursos na ULSM.

A PSI está alinhada com os "Princípios de Segurança da Informação", os quais servem de guias-orientadoras para o desenvolvimento de qualquer documento do nível Estratégico, Tático e/ou Operacional.

Para garantir a operacionalização da "Política de Segurança da Informação da ULSM" deverão ser definidos e formalizados os seguintes documentos:

- "Objetivos de Segurança da Informação", alinhados com os objetivos estratégicos da ULSM e os objetivos do Sistema de Informação;
- "Framework da Documentação no âmbito da Segurança da Informação", com identificação dos documentos estratégicos, tácitos e operacionais relacionados com a Segurança da Informação na ULSM.

SPMS – Serviços Partilhados do Ministério da Saúde, EPE . Av. João Crisóstomo, nº 11 - 5º piso | 1049-062 Lisboa | Tel.: 211 545 600 | Fax: 211 545 649

2.3 Gestão de Risco

A ULSM deve assegurar um processo de gestão de risco baseado na identificação de vulnerabilidades que podem ser alvo de ameaças e/ou ataques, tendo em conta a probabilidade e o impacto da ameaça/ataque, com o objetivo de calcular e priorizar os riscos identificados.

2.4 Tratamento de não conformidades

As ações que violem a PSI, bem como as políticas operacionais, procedimentos e regras, que quebrem os controlos de Segurança da Informação são passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas de forma isolada ou cumulativamente.

As penalidades são aplicadas proporcionalmente à ação praticada em conformidade com os procedimentos para processos disciplinares. Dependendo do tipo de contraordenação, as ações disciplinares podem incluir, por exemplo, a suspensão ou a interrupção da relação entre a ULSM e as partes envolvidas.

Em todos os casos aplica-se o previsto no Código Penal e no Código Civil, bem como as normas e procedimentos internos da ULSM.

2.5 Tratamento de exceções

Os objetivos de Segurança da Informação são facilmente alcançados se os requisitos de Segurança da Informação e os respetivos processos, políticas e procedimentos forem idênticos para todas as unidades de negócio, incluindo áreas clínicas.

Entretanto, há noção que os procedimentos e políticas padronizadas nem sempre são viáveis para uma unidade específica, projeto a decorrer, novo equipamento ou aplicação instalados.

É previsível que, no âmbito de atividades da ULSM, surjam situações ou cenários que não podem ser tratados de forma eficaz dentro dos requisitos estabelecidos na "Política de Segurança da Informação da ULSM" ou nas políticas operacionais, normas e procedimentos de Segurança da Informação.

Embora o desvio de políticas e procedimentos estabelecidos centralmente seja desencorajado, nalguns momentos os procedimentos e processos estabelecidos na ULSM, podem e devem ser alterados, desde que a alternativa apresentada seja suportada por uma justificação forte e provida de recursos suficientes para implementar adequadamente e manter o procedimento/política/tecnologia alternativo.

Para tratar atempadamente este tipo de situações e paralelamente garantir a segurança de infraestrutura e dos dados da ULSM é obrigatório cumprir com o processo de gestão de alterações do Sistema de Informação da ULSM.

SPMS – Serviços Partilhados do Ministério da Saúde, EPE . Av. João Crisóstomo, nº 11 - 5º piso | 1049-062 Lisboa | Tel.: 211 545 600 | Fax: 211 545 649

3 Organização de Segurança da Informação

3.1 Estrutura Organizacional de Segurança da Informação

Para assegurar a gestão efetiva de Segurança da Informação deve ser criada uma estrutura responsável pela orientação, planeamento, implementação, manutenção e melhoria das práticas de Segurança da Informação. Esta estrutura deverá abranger os níveis estratégico, tático e operacional para considerar a necessidade de descentralizar as responsabilidades da gestão da Segurança da Informação pelas várias áreas da ULSM:

Nível Estratégico

Neste nível é assegurada a governação da Segurança da Informação através de orientações estratégicas que garantam o atingimento dos objetivos de Segurança da Informação, a gestão adequada do risco, a disponibilização e a utilização otimizada dos recursos da ULSM (Conselho de Administração e Comissão Local de Proteção de Dados Pessoais).

Nível Tático

Neste nível é assegurada a gestão da Segurança da Informação que inclui práticas e atividades que endereçam as áreas de responsabilidade de planeamento, definição, execução e acompanhamento (*Chief Information Security Officer, Chief Security Officer* e área TIC).

Nível Operacional

Neste nível é assegurada a operacionalização e monitorização das práticas de Segurança da Informação (áreas de negócio/funcionais e área TIC).

3.2 Responsabilidades de Segurança da Informação

As responsabilidades e autoridades específicas no âmbito de Gestão da Segurança da Informação são detalhados no documento das “Estruturas Organizacionais de suporte ao Risco e Segurança da Informação”.

Adicionalmente, os utilizadores (incluindo a gestão de topo e todos aqueles que fazem parte da estrutura organizacional de Gestão de Segurança da Informação) têm a responsabilidade de manter um comportamento responsável e consistente com “Objetivos de Segurança da Informação”. Para tal, os utilizadores devem conhecer as instruções, regras e penalidades de funcionamento do serviço que utilizam, devendo ainda:

1. Aceitar plenamente as regras e responsabilidades definidas neste documento e de normas e procedimentos internos da ULSM sobre a utilização dos recursos de tratamento da informação, incluindo, em especial, os recursos de TIC da ULSM.
2. Cumprir com os códigos de ética profissional, bem como com os requisitos da legislação em vigor relacionados com as atividades no setor da Saúde, em particular com a legislação em vigor de proteção de dados pessoais;

SPMS – Serviços Partilhados do Ministério da Saúde, EPE . Av. João Crisóstomo, nº 11 - 5º piso | 1049-062 Lisboa | Tel.: 211 545 600 | Fax: 211 545 649

3. Responder por atos que violem as regras de utilização dos recursos computacionais, estando, portanto, sujeito às penalidades definidas na política de uso desses recursos e também, se for o caso, às penalidades impostas pela legislação em vigor;
4. Comunicar imediatamente qualquer falha ou não conformidade identificada na Segurança da Informação de acordo com o procedimento de notificação de incidentes;
5. Não se fazer passar por outra pessoa ou dissimular sua identidade enquanto a utilizar os recursos computacionais;
6. Responsabilizar-se pela sua identidade eletrónica, *passwords*, credenciais de autenticação, autorização ou outro dispositivo de segurança, não partilhando com ninguém esta informação;
7. Responder pela utilização indevida da sua conta e os recursos computacionais em qualquer circunstância;
8. Divulgar informação interna e/ou confidencial apenas nas situações previstas na lei, devendo, para tal efeito, recorrer a aconselhamento deontológico e jurídico (Comissão de Ética e Responsável do Acesso à Informação).

Fim de Documento

SPMS – Serviços Partilhados do Ministério da Saúde, EPE . Av. João Crisóstomo, nº 11 - 5º piso | 1049-062 Lisboa | Tel.: 211 545 600 | Fax: 211 545 649