MISERICÓRDIA DO PORTO

DECLARAÇÃO DE SEGURANÇA CORPORATIVA

2018

SANTA CASA DA MISERICÓRDIA DO PORTO

Data: 01/06/18 - v01 ; Classificação Doc.: Pública

VISÃO GERAL

Mais próximos, mais solidários e **mais seguros.**

A Santa Casa da Misericórdia do Porto (SCMP) está comprometida em garantir a segurança de todas as operações, pessoas, infraestruturas, informação, equipamentos e todos os ativos que representem valor para a Instituição. Assim, e dada a importância crescente que a segurança representa, a SCMP está a implementar políticas, controlos e procedimentos, em todas as suas áreas de negócio.

Este documento estabelece o compromisso da SCMP e representa um breve resumo das políticas e controlos já definidos.

POLÍTICA DA SEGURANÇA

A SCMP definiu um conjunto de políticas para a segurança organizacional, aprovado pela Gestão de Topo, publicado e comunicado aos colaboradores e partes externas relevantes.

A Política de Segurança Organizacional da Misericórdia do Porto constitui uma base comum a todos estabelecimentos, departamentos, gabinetes e serviços, que define padrões de segurança organizacional e de práticas eficazes na gestão da segurança e privacidade. Para isto, os ativos tangíveis e intangíveis, bem como os processos de negócio, devem estar adequadamente protegidos contra riscos, ameaças e vulnerabilidades.

O objetivo da segurança organizacional é a proteção dos ativos, minimização do risco, prevenção dos incidentes de segurança, reduzindo o seu potencial impacto e assegurar a continuidade do negócio da Instituição.
De forma a cumprir este objetivo, a Política de Segurança Organizacional assume e promove os seguintes objetivos específicos para a gestão da segurança:

- Desenvolver uma estratégia de segurança alinhada com os objetivos da Instituição;
- Estar em conformidade com as normas e regulamentos aplicáveis;
- Assegurar que os recursos necessários para o sistema de gestão da segurança estão disponíveis;
- Garantir a proteção dos ativos, das pessoas, conhecimento e informação da SCMP;
- Desenvolver planos de tratamento que garantam a efetiva proteção da informação;
- Estabelecer controlos para a entrada e saída de informação, de forma a prevenir fugas ou roubo de informação sensível, seja acidental ou intencionalmente;
- Identificar os pontos críticos relacionados com a segurança da SCMP, definindo ações para a prevenção e melhoria contínua;
- Garantir formação, boas práticas e sensibilização em segurança, a todos os colaboradores;
- Contribuir para a criação de uma cultura de segurança na SCMP, através de redes de comunicação.

Adicionalmente, e para suportar os processos de gestão da segurança organizacional, a SCMP definiu um modelo de gestão, cujo objetivo prende-se com a dinamização deste modelo, assegurando-se o cumprimento dos objetivos enumerados anteriormente, com base nos seguintes princípios orientadores:

- Responsabilidades da Organização;
- Alinhamento com o negócio;
- Gestão do Risco;
- Formação e Sensibilização;
- Proteção e privacidade.

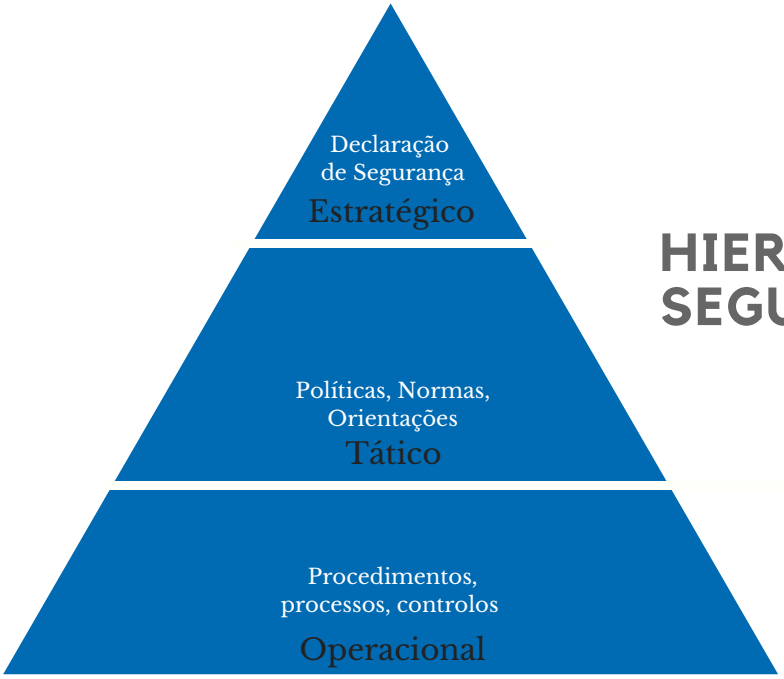
ORGANIZAÇÃO DA SEGURANÇA

Modelo de organização

A SCMP tem uma estrutura orgânica de segurança corporativa, inserida no Gabinete de Segurança, Risco e Compliance (GSRC), responsável pelas questões de segurança, em articulação com os diversos departamentos e gabinetes.

O Departamento de Sistemas e Informação (DSI) assegura a proteção dos equipamentos TI, assim como todos os sistemas aplicacionais que dão suporte às atividades da SCMP.

Ao nível operacional, estão nomeados SRC managers, que têm a responsabilidade por, entre outras, identificar e monitorizar controlos de segurança, bem como o reporte de ocorrências. Os SRC Managers asseguram a articulação entre o GSRC e o negócio, e em matérias de proteção de dados, entre o negócio e o DPO (Data Protection Officer) da SCMP.



HIERARQUIA DA SEGURANÇA

ACORDO DE CONFIDENCIALIDADE

Estão previstas cláusulas de confidencialidade para os colaboradores da SCMP, demonstrando o seu compromisso com a Instituição e com a segurança da informação.

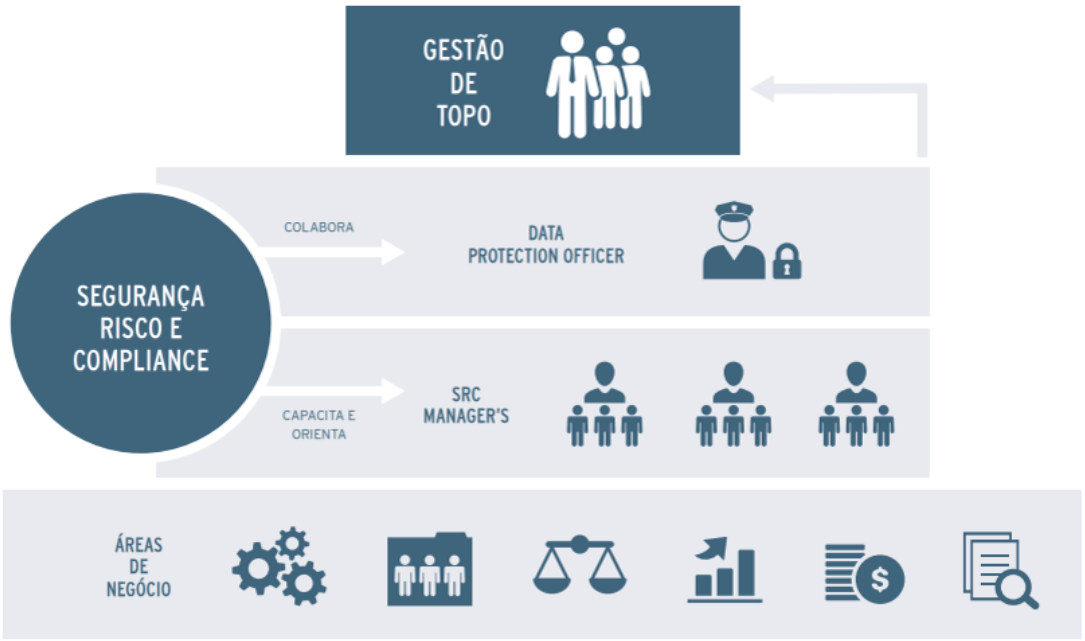
PROTEÇÃO DE DADOS PESSOAIS

A proteção da privacidade e dos dados pessoais constitui um compromisso fundamental da Misericórdia do Porto para com os seus clientes, utilizadores dos seus serviços, colaboradores e outros interessados. Neste contexto, a SCMP definiu uma Política de Proteção de Dados Pessoais, com o objetivo de estabelecer e manter um determinado nível de proteção de dados pessoais que:

- Esteja de acordo com as disposições legais aplicáveis sobre proteção de dados;
- Esteja de acordo com as necessidades dos clientes, parceiros e dos colaboradores;
- Permita realizar os processos de negócio de forma eficaz;
- Permita à Instituição manter uma imagem externa positiva no mercado.

A proteção de dados é uma função central, pelo que foi nomeado um DPO que deverá reportar à Comissão Executiva, o desenvolvimento das atividades realizadas no âmbito da Política. Desde modo, foi nomeada a Comissão de Proteção de Dados, cuja função é de coordenar a implementação do Regulamento Geral de Proteção de Dados (RGPD) e prestar apoio à Mesa Administrativa em questões relacionadas com a proteção da informação.

No âmbito do RGPD, foi definida uma Política de Privacidade, com a finalidade de demonstrar o seu compromisso e respeito para com as regras de privacidade e de proteção de dados pessoais.



ÉTICA E COMPLIANCE

A SCMP tem um Departamento de Auditoria Interna, responsável pela avaliação das operações internas, incluindo a segurança e os sistemas de informação.

A SCMP assumiu um forte compromisso em estabelecer uma cultura firme de cumprimento e, por isso, transmite uma mensagem sólida de oposição à prática de qualquer ato ilícito a todos os seus colaboradores (representantes, fornecedores e outros terceiros que prestem serviços para a SCMP). Todos os colaboradores são responsáveis por realizar as suas atividades, cumprindo com a legislação em vigor e os princípios corporativos de atuação presentes no código de ética e conduta da Instituição.

SEGURANÇA DOS RECURSOS HUMANOS

O plano de segurança das pessoas tem como objetivo definir os princípios de segurança e responsabilidades relativamente à gestão da relação com os recursos humanos, desde o momento do recrutamento até ao da cessação de funções e responsabilidades com a SCMP.

FORMAÇÃO E SENSIBILIZAÇÃO

Todos os colaboradores, fornecedores e terceiros devem receber formação apropriada, bem como ações de sensibilização, no âmbito desta temática.
Para além disso, deverão, ainda, receber receber atualizações regulares sobre as políticas e procedimentos relevantes para as suas funções.
Foram criados planos de formação específicos, de forma a garantir os níveis adequados de conhecimento e responsabilidade estabelecidos na Política de Segurança.

GESTÃO DE ACESSOS

A política de controlo de acesso de colaboradores, prestadores de serviços, terceiros e viaturas, tem como objetivo, proporcionar um ambiente de trabalho seguro a todos os indivíduos, bem como definir os critérios necessários para o acompanhamento e controlo da disciplina interna, entrada e saída de indivíduos e de veículos, nos Estabelecimentos da SCMP.
Independentemente da natureza do acesso às instalações da SCMP, todos as pessoas devem utilizar cartão de identificação e ser responsáveis pelo mesmo.

A política de passwords não só define as obrigações que os utilizadores dos sistemas de informação da SCMP devem respeitar na utilização das suas passwords, como também especifica as regras que o Departamento de Sistemas de Informação deverá seguir para a correta gestão das mesmas.

GESTÃO DE OPERAÇÕES

O DSI estabelece e mantém procedimentos que garantem a proteção dos equipamentos TI, como todos os sistemas aplicacionais que dão suporte às atividades da SCMP, e a título de exemplo:

- Regulamento para utilização do equipamento informático: normas para a utilização de todos os equipamentos informáticos existentes na SCMP, deveres e obrigações dos utilizadores, controlo de acesso a equipamentos e programas, instalação de software, manutenção dos equipamentos, utilização de serviços informáticos e acesso à Internet;
- Regular a Utilização da Computação Pessoal na Instituição: regula a Utilização da Computação Pessoal na Instituição garantindo que a informação proveniente dos diversos ambientes aplicacionais, são utilizadas de maneira adequada;
- Regular a Utilização das Bases de Dados na Instituição: regula os pedidos de Utilização da Computação Pessoal na Instituição provenientes dos Departamentos/Serviços da SCMP;
- Norma de Configurações de Segurança: define as regras para estabelecer, implementar e gerir a configuração de segurança de laptops, servidores e estações de trabalho usando um rigoroso processo de gestão e controlo de configurações para evitar que atacantes possam explorar serviços e configurações vulneráveis;
- Gestão de acesso lógico: define os princípios relativamente ao controlo de acessos à informação e sistemas de informação da SCMP, baseado nos requisitos operacionais e de segurança;
- Política de Gestão de Classificação da Informação: define os critérios de classificação da Informação na SCMP, de forma a garantir que a Informação recebe um nível de proteção adequado, consoante o seu valor e sensibilidade para a organização;
- Política de Segurança de Rede e Comunicações: define os princípios de segurança relativamente ao acesso e uso dos serviços de rede da SCMP;
- Norma de utilização de serviços TI: define orientações, regras e boas práticas para o acesso e uso dos equipamentos, software, serviços TI e informação corporativa da SCMP por parte dos colaboradores e terceiros (fornecedores, visitantes e parceiros), bem como consciencializar relativamente à temática da segurança da informação;
- Gestão de Incidentes de Segurança: promove que os incidentes de segurança da informação são endereçados de forma completa, correta e alinhada com a Política de Segurança da Informação da SCMP e outros normativos internos e externos;
- Política de Gestão de Operações de Segurança: define os requisitos para a gestão das infraestruturas TI e gestão de alterações aos sistemas de informação da SCMP;
- Metodologia de Avaliação de Risco SI/TIC: define a metodologia utilizada pela SCMP para a identificação e avaliação dos seus Risco SI/TIC à garantia da confidencialidade, integridade e disponibilidade da informação. A metodologia apresentada é baseada na ISO 27005:2011, norma que fornece orientações para a gestão do Risco SI/TIC de segurança da informação das organizações.

PLANO DE CONTINUIDADE DE NEGÓCIO

Existe um Plano Estratégico para a Continuidade de Negócio, que visa estabelecer as orientações base para a criação das fundações de um programa de continuidade de negócio, de acordo com as melhores práticas e standards internacionais. Os objetivos do programa são os seguintes:

- Definir e implementar medidas de prevenção;
- Dotar a SCMP dos meios necessários para fazer face a eventos não previstos que provoquem interrupções dos serviços e processos;
- Capacitar a SCMP e os seus recursos humanos dos meios necessários para desencadear os planos definidos e previstos;
- Mobilizar a organização para uma cultura de prevenção efetiva, incrementando a sua capacidade de resposta a emergências, com o mínimo de consequências físicas, técnicas operacionais e financeiras.

GESTÃO DO RISCO

Um processo de gestão de risco eficaz necessita de decisões estratégicas eficientes, bem como, para uma condução eficaz, eficiente e robusta dos processos organizacionais, permitindo à SCMP identificar e usufruir de oportunidades enquanto cumpre com os requisitos de compliance. A SCMP compromete-se a gerir as suas oportunidades e riscos, como componente do sistema de gestão, e simultaneamente, reduzir a exposição aos riscos inerentes para níveis aceitáveis, assegurando a continuidade dos processos chave.

O propósito da Política da Gestão do Risco é:
- Desenvolver a consciencialização da cultura do risco, mantendo a inovação organizacional e agilidade para a identificação e concretização das oportunidades;
- Assegurar a conformidade com os processos de gestão do risco;
- Integrar e alinhar o sistema de gestão do risco com as atividades e processos de negócio da SCMP;
- Encorajar a revisão e a melhoria contínua dos processos de gestão.

Os objetivos da Política de Gestão do Risco são:
- Ter em conta os riscos corporativos no processo de tomada de decisão estratégica;
- Integrar o processo de gestão de riscos operacionais nos processos de gestão organizacional;
- Promover a responsabilização dos colaboradores pela gestão do risco.