

## Política de Segurança da Informação

---

### 1. Referência ACSA

---

S 09.08

S 03.03

S 03.07

### 2. Objetivo

---

Definir a segurança da informação, alinhada com os princípios de Segurança da Informação, para orientar todas as atividades relacionadas neste âmbito no Hospital Santa Maria Maior, EPE (HSMM) e enquadrar assim modelo de Organização da Segurança da Informação.

**Dados a proteger:** Informação relativa a uma entidade identificada ou identificável.

### 3. Destinatários

---

A Política de Segurança da Informação (PSI) aplica-se a todos os colaboradores do HSMM, independentemente da sua função, posição hierárquica e vínculo contratual, bem como a fornecedores e parceiros, e ainda outras pessoas que tenham acesso a um posto de trabalho ou sistema de informação do Hospital.

As entidades externas com acessos a sistemas de informação do Hospital devem considerar esta política como recomendação, para aplicação interna na sua instituição.

Todos os colaboradores são responsáveis pela segurança da informação e todos têm a responsabilidade de proteger os respetivos dados próprios ou os que lhes são confiados.

### 4. Definições

---

**Confidencialidade** – assegurar que a informação é acessível somente por pessoas devidamente autorizadas. O acesso à informação é, por conseguinte, restrito a utilizadores considerados legítimos.

**Integridade** – garantir a veracidade, autenticidade e exatidão da informação, bem como os seus métodos de processamento ao longo de todo o processo, garantindo que o conteúdo não seja adulterado.

**Disponibilidade** - assegurar o acesso à informação, a quem se encontre devidamente credenciado e legitimamente autorizado. A informação está acessível quando se revelar necessária.

**Legitimidade** - a recolha da informação é feita nos estritos limites da lei que é aplicável ao objeto da recolha.

### 5. Política

---

#### 5.1. Segurança da Informação no HSMM

##### 5.1.1. Enquadramento

A informação e respetivos repositórios são ativos relevantes e críticos para o Hospital e para o Serviço Nacional de 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 da informação de um amplo conjunto de ameaças, através de um processo de gestão de riscos, garantindo a continuidade do negócio e maximizando o retorno em investimentos efetuados.

## Política de Segurança da Informação

---

A conformidade da Segurança da Informação pode ser formalmente definida como a “prevenção da confidencialidade, da integridade e da disponibilidade da informação, obtida legitimamente”.

A extensão na qual a confidencialidade, integridade e a disponibilidade da informação da instituição deve ser protegida, depende da natureza da mesma, das utilizações a que se encontra alocada e dos riscos a que se encontra exposta, face às ameaças tecnológicas que surgem em numero crescente, provenientes de várias fontes.

O aparecimento e inclusão de um número cada vez maior de formas de comunicação, oferecem novas oportunidades de acesso não-autorizadas a recursos, bens e sistemas de informação, que necessariamente têm que ser acauteladas.

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 informação, mais rentáveis serão estas ações.

### 5.1.2. Princípios Gerais da Segurança da Informação

Deve ser garantida a proteção que se tenha por adequada face ao risco existente, garantindo a inviolabilidade da confidencialidade, a disponibilidade da informação, garantindo igualmente a continuidade da vida da organização, fomentado e garantindo a confiança dos seus utilizadores, quer de utentes quer de colaboradores.

Nesta conformidade, a informação é tratada de forma adequada à finalidade a que se destina, implementando procedimentos sistemáticos que visem a redução do risco de quebra da confidencialidade, reforçando princípios e inculcando em todos os que com ela contactam o sentido da responsabilização.

Assim, para além de se estabelecer medidas visando e garantindo a segurança dos dados que compõem a informação, é também verificado regularmente o respetivo cumprimento e o seu grau de eficácia.

A Informação que a todos é confiada, é por definição protegida, estando impedida a sua adulteração, violação ou divulgação.

As regras de segurança de informação são comunicadas a todos os que contactam com os dados inerentes a esta, através de divulgação de regras, procedimentos e ações formativas.

As passwords e as modalidades de acesso à informação são objeto de procedimento próprio, cujo principal objetivo é garantir a segurança dos dados, os quais são por inerência confidenciais, nestes se incluindo os dados pessoais nominativos.

Os acessos de cada utilizador, designadamente correio eletrónico e passwords diversas de acesso a sistemas de informação, são pessoais e intransmissíveis.

## Política de Segurança da Informação

---

O computador de cada utilizador apenas pode conter software devidamente credenciado pelo administrador do sistema de informação, devendo ser de imediato encerrado ou bloqueado sempre que se encontre a ser utilizado software não autorizado.

O correio eletrónico, é uma ferramenta de trabalho, que terá de ser utilizada para os estritos fins a que se destina, de forma cuidada e adequada.

São implementados procedimentos de medidas de segurança de acessos a postos de trabalho, protegendo a informação inerente aos mesmos.

Deve ser cumprido o compromisso com o sistema de Gestão de Segurança da Informação.

O objetivo Segurança da Informação vai para além da implementação de controlos pontuais e sistemáticos.

As ações no âmbito de Segurança da Informação devem ser alinhadas com os objetivos de segurança da informação do Hospital (enquadrados nos objetivos do Sistema de Informação) e geridas de forma integrada.

Para assegurar o cumprimento dos objetivos de Segurança da Informação, o HSMM, enquanto detentor da informação, assume o compromisso de:

- Assegurar o cumprimento dos requisitos legais e normativos no âmbito da segurança da informação.
- Estabelecer, implementar e melhorar continuamente a segurança da informação.

Os benefícios do estabelecimento de parâmetros de segurança da informação, traduzem-se na redução dos riscos para a atividade, no aumento da conformidade com os normativos legais e regulamentação aplicável, na proteção da reputação, na maior confiança dos utentes e colaboradores, bem como de todos os que privam com a entidade no âmbito da sua atividade, traduzindo-se naturalmente numa gestão mais eficaz dos recursos e serviços prestados.

A PSI está alinhada com os princípios gerais de segurança da informação, os quais servem de guias e orientações para o desenvolvimento de qualquer documento de nível estratégico, tático e/ou operacional.

### 5.1.3. Tratamento de não conformidades

Todos os atos que violem a segurança da informação, bem como as políticas organizacionais que implementam procedimentos, normas, diretivas, em suma, regras às quais obedece a segurança dos dados confiados e contidos nos registos da entidade, sob qualquer suporte, e que quebrem os controlos de Segurança da Informação, são passíveis de sanções, disciplinares, judiciais e extrajudiciais, designadamente ao abrigo da lei civil, penal, administrativa, ou o que em concreto se aplique, incluindo legislação de regulamentos originados pelo espaço comunitário europeu diretamente aplicáveis ao ordenamento jurídico nacional, conforme a legislação em vigor do estado nacional ou da união europeia, que podem ser aplicadas de forma isolada ou cumulativamente.

## Política de Segurança da Informação

---

Os respetivos procedimentos e consequentes as penalidades, são aplicadas proporcionalmente à ação ou omissão praticada, que coloque em risco a conformidade da segurança da informação, neste se incluindo processos disciplinares, ou contraordenacionais.

Em todos os casos aplica-se o previsto nos normativos legais, bem como as normas e os procedimentos internos da entidade.

### 5.1.4. Tratamentos das exceções ao padronizado para a segurança da informação estabelecida

Os objetivos de Segurança da Informação são alcançados se os requisitos de Segurança da Informação e os respetivos processos, políticas, procedimentos, normativos, forem idênticos em todo o circuito do HSMM.

Contudo, os procedimentos e as políticas padronizados, nem sempre são viáveis para uma unidade específica, projeto a decorrer, novo equipamento ou aplicação instalados.

É previsível que, no âmbito do desenvolvimento de atividades do HSMM, surjam situações ou cenários que não podem ser tratados de forma eficaz dentro dos requisitos estritos e tramitações reguladas, estabelecidos na PSI ou nas políticas operacionais, normas e procedimentos de segurança da Informação.

Embora o desvio de políticas e procedimentos estabelecidos centralmente seja desaconselhado, nalguns momentos os procedimentos e processos estabelecidos no HSMM, podem e devem ser alterados, desde que a alternativa apresentada seja suportada por uma justificação forte e provida de recursos suficientes para a implementar adequadamente e manter o procedimentos/política/tecnologia alternativos.

Para tratar atempadamente este tipo de situações e paralelamente garantir a segurança de infraestruturas e dos dados do HSMM, recomenda-se documentar a exceção através de procedimento de gestão de alterações do Sistema de Gestão de Segurança da Informação.

## 5.2. Organização de Segurança da Informação

### 5.2.1. Estrutura Organizacional de Segurança da Informação

Para assegurar a gestão efetiva de Segurança da Informação deve ser criada uma estrutura que permita e responsabilize o HSMM ou serviço a quem esta responsabilidade é deferida, estabelecendo orientações, 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 entidade.

## Política de Segurança da Informação

### 5.2.2. Responsabilidades de Segurança da Informação

As responsabilidades específicas no âmbito de Gestão da Segurança da Informação são detalhadas em documentos internos específicos, designadamente, na “*Garantia e Confidencialidade e Proteção de Dados*”, na “*Política de Confidencialidade*”, na “*Política de Segurança de Dados*”, e outros que surjam no âmbito dos normativos que possam a vir a ser elaborados, perante as imposições de proteção de dados do RGPD.

Os utilizadores, nestes se incluindo todos aqueles que fazem parte da estrutura institucional, têm a responsabilidade de manter um comportamento responsável e consistente com os objetivos de Segurança da Informação.

Neste sentido deverão ser conhecidos de todos, os normativos e regras que regulam internamente o sistema de gestão da segurança da informação, cumprindo ainda com:

- A aceitação plena das regras e responsabilidades definidas neste documento e nas normas e procedimentos internos do HSMM sobre a utilização dos recursos de tratamento da informação, incluindo, em especial, os recursos de TIC.
- O cumprimento dos códigos de ética vigentes a nível institucional do Hospital e externo e ainda profissional, bem como os requisitos da legislação em vigor relacionados com as atividades no setor da saúde, com a especial atenção à legislação de proteção de dados, nesta se incluindo o RGPD e a lei da especialidade que vierem a ser aprovadas que regulem em matéria de estado Português a proteção de dados no âmbito da Política da Segurança da Informação e em especial setor da Saúde.
- Respondendo por atos que violem as regras de utilização dos recursos informáticos, quer a nível de utilização de equipamentos computacionais quer de sistemas ou web sites de entidades de saúde, ou dentro das áreas com que se tenham de articular, ou ainda do próprio HSMM, estando, portanto, sujeito às penalidades impostas pela legislação em vigor;
- Comunicando imediatamente qualquer falha ou não conformidade identificada na segurança da informação, de acordo com o procedimento de notificações de incidentes;
- Não se fazer passar por outra pessoa, usurpando ou dissimular a sua identidade enquanto utilizar os recursos computacionais;
- Responsabilizando-se pela sua identidade eletrónica, palavras-passe, credenciais de autenticação, autorização ou outro dispositivo de segurança, não partilhando com ninguém esta informação.
- Respondendo pela utilização indevida da sua conta e dos recursos informáticos, que contenham informação incluindo os físicos e computacionais em qualquer circunstância;
- Divulgando informação confidencial e interna apenas nas situações previstas na lei, devendo, para tal efeito, recorrendo aconselhamento deontológico e jurídico.

## Política de Segurança da Informação

### 6. Referências

- Documento de Garantia de Confidencialidade e proteção dos Dados (0099\_Pro\_Pros)
- Documento de Política de Confidencialidade dos Dados (0102\_Pol\_Pros)
- Documento de Política de Segurança de Dados (0100\_Pol\_Pros)
- Política de Segurança de Informação dos SPMS

### 7. Anexos

Não aplicável.

### 8. Alterações em relação à última revisão

Não aplicável.

### 9. Edições / Revisões

| Edição          | Revisão | Elaborado / Revisto | Aprovado              | Data       | Homologado           | Data       |
|-----------------|---------|---------------------|-----------------------|------------|----------------------|------------|
| 1               | 0       | EPD - Ana Santos    | PCA – Joaquim Barbosa | 30.05.2018 | CA – Joaquim Barbosa | 30.05.2018 |
| Próxima Revisão |         | 31/05/2021          |                       |            |                      |            |