# Circular Normativa N.º 7/2018/SPMS

Para: **Administrações Regionais de Saúde, Unidades Locais de Saúde, Hospitais EPE, Hospitais SPA, Hospitais PPP e Institutos Públicos do SNS**

Assunto: **Medidas de Reforço de Segurança**

O Decreto-Lei n.º 108/2011, de 17 de novembro, atribuiu à SPMS, E.P.E. competências no domínio dos sistemas de informação e comunicação, com inerente responsabilidade sobre a operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação do Ministério da Saúde (MS).

É por isso missão da SPMS, E.P.E. a prossecução de formas de cooperação, partilha de conhecimento e informação, bem como, o desenvolvimento de atividades de prestação de serviços nas áreas dos sistemas de informação e comunicação, garantindo a operacionalidade, disponibilidade, integridade e confidencialidade das infraestruturas de base e dos sistemas de informação do Ministério da Saúde.

Considerando o Despacho n.º 1348/2017, publicado em Diário da República nº28/2017, Série II de 2017-02-08, que visa reforçar a coordenação e monitorização da implementação e operacionalização das boas práticas e da resposta a ciber-riscos, no setor da saúde, bem como o disposto no Despacho n.º 8877/2017, publicado em Diário da República n.º 194/2017, Série II de 2017-10-09, importa agora operacionalizar indicações e medidas concretas em relação a resiliência e segurança dos sistemas de informação da saúde.

O despacho n.º 8877/2017, estabelece o modelo de governação relativo à implementação da política de cibersegurança da saúde, sendo aplicável aos estabelecimentos, serviços e organismos do Serviço Nacional de Saúde (SNS) e do Ministério da Saúde, bem como às entidades do setor empresarial do Estado da área da saúde.

Este Despacho define um conjunto de responsabilidades às entidades por ele abrangidas, entre as quais se destacam:

- A adoção de medidas relativas ao Programa de Gestão de Risco e Segurança do eSIS;
- A elaboração de relatórios regulares sobre o perfil evolutivo da implementação das políticas e controlos de segurança na entidade, de forma a permitir avaliar e comparar níveis de maturidade;
- A necessidade de garantir a disponibilização dos recursos humanos, tecnológicos e financeiros, necessários para assegurar o cumprimento dos níveis de serviço definidos pela SPMS, E. P. E.;
- Assumir um papel participativo e colaborativo na partilha de boas práticas e de melhoria contínua para responder à dinâmica evolutiva dos diversos contextos de cibersegurança;
- Cumprir as medidas e procedimentos na área da cibersegurança;
- Promover em tempo útil a disponibilidade dos meios de proteção, deteção, resposta e recuperação reportando aos órgãos competentes, sempre que confrontada com situações que comprometam a segurança;
- Acompanhar, apoiar e monitorizar o desenvolvimento de medidas de proteção, deteção, resposta e recuperação dos recursos críticos locais;





SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

- Adotar o modelo de avaliação para a gestão e monitorização das medidas de segurança;
- Colaborar com a SPMS, E. P. E., no processo de definição normativo e nos modelos de gestão da segurança a implementar.

Nesse sentido, é publicada a presente Circular normativa, com o objetivo de concretizar, em termos operacionais, as responsabilidades das Partes em matéria de segurança da informação e cibersegurança na saúde.

## 1. Considerações

Face à exposição a que o Ministério da Saúde, incluindo todas as entidades do seu ecossistema funcional, estão sujeitas por força da sua atividade, e à criticidade dos tratamentos de categorias especiais de dados pessoais («dados sensíveis») de que são responsáveis, revela-se essencial que, no âmbito da Segurança da Informação e em observação das obrigações legais impostas pelo Regulamento Geral de Proteção de Dados – RGPD, sejam adotadas medidas organizacionais e tecnológicas para minimizar o risco de perda de dados, e garantir a qualidade dos serviços prestados.

A Segurança da Informação deverá ser uma preocupação de todos os que compõem o "Ecossistema Saúde". A solidez desse Ecossistema faz-se com a responsabilização individual de cada uma das entidades, incluindo a SPMS, E.P.E., com o comprometimento, de todos, na promoção e, principalmente, na adoção de boas práticas que reforçam a CiberSegurança, garantindo, assim, uma estrutura organizacional mais forte e robusta contra o Cibercrime.

A utilização de meios tecnológicos e sistemas de informação na saúde tem vindo a assumir um papel preponderante, criando um enorme benefício na prestação contínua de cuidados de saúde. No entanto, há preocupações crescentes relacionadas com a segurança de informação, nomeadamente, com os dispositivos de saúde, dado que o aumento da conectividade a redes de computadores existentes expõe estas plataformas a novas vulnerabilidades de CiberSegurança. Este tema torna-se ainda mais crítico quando vários estudos demonstram que os registos clínicos são altamente valorizados por *hackers*, atendendo à criticidade das informações pessoais e sensíveis que contêm.

Nesse sentido, as *firewall* são uma ferramenta base de toda a segurança da uma rede, prevenindo várias ameaças existentes na *internet* como *malwares* potencialmente perigosos e acessos não autorizados e possibilitando, simultaneamente, uma monitorização do tráfego e dos tipos de ataques que a rede está a receber.

Atento os vários tipos de *firewall*, dever-se-á considerar *Firewall* do tipo *layer* 7 atentas as capacidades de análise da camada aplicacional.

## 2. Responsabilidades da SPMS

A SPMS -Serviços Partilhados do Ministério da Saúde, E. P. E. (SPMS), nos termos do Decreto-Lei n.º 19/2010, de 22 de março, alterado pelos Decretos-Leis n$^{os}$108/2011, de 17 de novembro, 209/2015, de 25 de setembro, 32/2016, de 28 de junho, 69/2017 , de 16 de junho, e 38/2018 , de 11 de junho, no âmbito dos serviços partilhados de sistemas e tecnologias de informação, tem por missão a cooperação, a partilha de conhecimentos e informação e o desenvolvimento de atividades de prestação de serviços nas áreas dos sistemas e tecnologias de informação e de comunicação, garantindo a operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação do Ministério da Saúde e promovendo a definição e utilização de normas, metodologias e requisitos que garantam a





SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

interoperabilidade e interconexão dos sistemas de informação da saúde, entre si e com os sistemas de informação transversais à Administração Pública.

Neste pressuposto, no âmbito das tecnologias de informação e comunicação (TIC) constitui responsabilidade da SPMS:

1. Emitir normas e pareceres no âmbito de sistemas e tecnologias de informação.
2. Colaborar na revisão dos contratos realizados no âmbito TIC;
3. Acompanhar as intervenções técnicas no âmbito TIC.
4. Realizar junto das entidades, recolha de dados/auditorias aos sistemas de informação sempre que tal se revele conveniente.
5. Promover junto das entidades a partilha e gestão dos sistemas de informação.
6. Promover junto de todas as entidades do Ministério da Saúde a adoção de boas práticas na área TIC.

## 3. Responsabilidade das entidades

Constitui responsabilidade das entidades:

a) Garantir a necessária proteção do seu perímetro devendo para o efeito implementar um sistema defensivo em redundância, num prazo máximo de seis (6) meses após a publicação da presente circular, que assegure os controlos enumerados e detalhados em anexo desta Circular; a título de exemplo, devem ser assegurados controlos tais como:

- Intrusion Prevention System
- Visibilidade e Controlo Aplicacional
- Host Detection e Capacidades de Profiling
- Network Discovery e Capacidades de profiling de Tráfego
- Deteção de Anomalias e Correlação
- Políticas de Controlo de Acessos
- Solução de gestão centralizada
- Diversos outros controlos, conforme detalhado em anexo

b) A solução em causa deve estar a coberto de um contrato de manutenção, suportado pelo fabricante, cujo SLA não pode ser inferior a 24x7x4.

c) Garantir no prazo máximo de seis (6) meses após publicação da presente Circular, a existência de recursos internos ou por subcontratação externa para a gestão e operação da solução.

d) Promover no prazo máximo de seis (6) meses, após publicação da presente Circular, formação adequada (reciclagem), através de entidades especializadas, aos recursos humanos que gerem a solução em apreço, garantindo assim as melhores práticas e técnicas na gestão, operação e manutenção da mesma.

e) Remeter à SPMS, no prazo máximo de oito (8) meses, após a publicação da presente circular, os resultados da monitorização ativa que executam com a solução ora instalada, de forma a que o





SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

Ministério da Saúde possa partilhar estes resultados com o Centro Nacional de Cibersegurança (CNCS).

f) As medidas de segurança preconizadas nesta Circular entram em vigor no dia seguinte à sua publicação, ressalvando-se, todavia, os prazos de adaptação nela previstos, quanto à aquisição, implementação e gestão ativa da solução preconizada.

Lisboa, 30 outubro de 2018

O Presidente do Conselho de Administração

Henrique Manuel Gil Martins

Assinado de forma digital por Henrique Manuel Gil Martins
Dados: 2018.10.30 18:57:40 Z



Anexo A: Requisitos da Solução de Segurança a Adotar



SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

# Anexo A:

# Requisitos da Solução de Segurança a Adotar

## Nota Introdutória

Este Anexo é referente à Circular Normativa n.º 7/2018/SPMS – Medidas de Reforço de Segurança, de 30 de outubro 2018, detalhando os requisitos e informação técnica para a solução de segurança de perímetro (vulgo, firewall de tipo layer 7) que as entidades estão obrigadas a implementar e gerir, no âmbito das suas responsabilidades ao nível de medidas de segurança da informação e cibersegurança.

Os requisitos apresentados em baixo reúnem um conjunto básico de boas práticas e de medidas consideradas elementares para uma solução desta tipologia, face aos atuais níveis de riscos e ameaças no sector da saúde. Complementarmente, estes requisitos beneficiam, também, da incorporação de contributos recebidos de um conjunto alargado de entidades da saúde, cuja revisão de versão preliminar deste Anexo desde já agradecemos.

Pretende-se, assim, fazer evoluir a defesa de perímetro ao nível da rede e dos centros de dados das entidades do SNS e do MS, adquirindo, implementando e gerindo soluções de firewalls harmonizadas com os requisitos emanados nesta Circular.

## Princípios Gerais

### *A. Integração com as melhores práticas da Segurança de Informação*

Devem ser adotadas soluções com abordagens e metodologias que seguem as melhores práticas do mercado, para obter resultados eficazes e eficientes, de forma a monitorizar e melhorar os processos implementados e não apenas direcionar mais tecnologia para o problema.

### *B. Gestão de risco*

Devem ser adotadas soluções e práticas, designadamente, programas de gestão de risco, que permitam identificar, minimizar e erradicar as ciber-ameaças, garantir os requisitos de conformidade dos processos e acelerar os objetivos de negócio, incluindo serviços que vão do planeamento à execução e à eficácia operacional na gestão de risco, segurança de identidade e operações de segurança.

### *C. Resposta a Incidentes*

A deteção precoce e resposta rápida são cruciais para proteger os ativos digitais, o que requer acesso a competências específicas. Devem ser garantidas soluções que permitam o acesso a peritos forenses competentes que circunscrevam e corrijam ataques conduzidos por adversários cada vez mais sofisticados.

### *D. Proteção avançada de ataques*



SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

As entidades continuam a ser alvo de ataques direcionados. Adversários sofisticados e determinados conseguem contornar mesmo as defesas mais robustas. Uma equipa dedicada à ciberdefesa ajuda as entidades a identificar os estados de maturidade atuais e desejados, e a traçar um rumo de segurança que evolui consoante as ameaças no ambiente e protege a missão da organização.

Uma lógica de serviços orientados para a segurança da informação e cibersegurança permite que as entidades reforcem a sua preparação, acelerem a resposta e mantenham a resiliência.

### *E. Deteção de ameaças e resposta a eventos*

Agregação de dados de registo, proteção de terminal e visibilidade de rede são elementos cruciais de um programa de segurança eficaz. A existência de equipas de deteção de ameaças e resposta ajuda as entidades a aplicar as capacidades e a detetar ameaças avançadas.

### *F. Arquitetura de Software*

De forma a potenciar uma arquitetura aberta, o *software* do sistema tem que ter a flexibilidade para correr diferentes *suites* de *software* em conjunto.

Nesse sentido, o código do supervisor do sistema deve ser capaz de gerir os componentes de *hardware*, automatizar a implementação de *software* e seus *updates*, assim como orquestrar as operações dos módulos de *software* de segurança e *hardware*. O sistema de supervisão deve suportar *'flow-offload'*, fazer QoS para o tráfego do *control plane* e ter capacidade de fazer *'packet captures'.*

## Funcionalidades de Segurança do Software

### *1. Identidade de Firewall*

A firewall deve ser capaz de autenticar utilizadores através de LDAP ou grupos de Active Directory como condição nas políticas de controlo de acessos.

A firewall deve utilizar Security Group Tags dos utilizadores, perfis de dispositivos (tipo de dispositivo) e localização de dispositivos (NAD ID) nas políticas de controlo de acesso.

### *2. Intrusion Prevention System*

- O sistema deve ter um mecanismo IPS.
- O mecanismo IPS deve ser compatível com assinaturas *snort* e suportar regras customizadas.
- O mecanismo IPS deve suportar diferentes políticas para cada política de acesso.
- Deve permitir atualização de assinaturas automatizada através de um motor de atualizações remoto.
- As políticas de configuração IPS devem suportar uma abordagem por camadas. Modificações no *set* de regras devem ser colecionados em cima das camadas base providenciadas pelo fabricante. Estas camadas podem ser eliminadas ou copiadas entre políticas.
- O sistema deve ter as seguintes políticas de IPS por defeito: Conectividade sob segurança, *balancing*, Segurança sob Conectividade e Máxima deteção.
- O sistema deve suportar regras de configuração aplicacional.



SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

- O sistema deve suportar um nível máximo global de eventos IPS.
- O sistema deve sugerir automaticamente regras de IPS a aplicar de acordo com os dispositivos existentes na rede e as vulnerabilidades conhecidas para esses dispositivos
- O sistema de ser capaz de prioritizar os eventos do IPS de acordo com a relevância dos eventos para a infraestrutura do cliente e do perigo que representam.
- Os alertas IPS devem ser reportados no sistema de gestão central ou encaminhados em SNMP *traps* ou publicados através de uma API segura que deve ser suportada entre os principais fornecedores de SIEMs (gestão e correlação de eventos de segurança).
- Deve ser suportado *'Dynamic Rule State'* ou funcionalidade similar que permita modificação de regras de ação baseadas em taxa de credibilidade por Origem, Destino ou ambos.
- Suporte de pacotes com limites de latência que podem cessar a inspeção de pacotes quando o limite de latência é excedido.
- O sistema deve suportar *updates* de assinaturas automáticas de IPS.

### *3. Visibilidade e Controlo Aplicacional*

- O sistema deve ser capaz de reconhecer e controlar mais de 4000 aplicações e micro aplicações por defeito.
- O sistema deve suportar OpenAppID e importar detetores de formatação OpenAppID.
- O sistema deve suportar a criação de detetores de aplicações simples através de um GUI com parâmetros estáticos e reconhecimento de características aplicacionais através da importação de pacotes capturados.
- Aplicação ou categorização aplicacional deve estar disponível como uma condição nas políticas de controlo de acessos.
- O mecanismo AVC deve suportar permitir a otimização de performance com inteligência aplicacional de 'Bypass'. Esta tecnologia deve permitir o bypass seguro do mecanismo de IPS. Um certo fluxo processual só pode sofrer bypass de inspeção adicional de IPS quando:
    - Pertencer a um reconhecido set aplicacional ou grupo aplicacional.
    - O sistema estiver sob uma intensa carga (utilização configurável em CPU, latência de Pacotes, 'flow rate' e percentagem de perdas de thresholds);
    - O flow excede um rácio configurável.

O sistema deve ter visibilidade sobre os dispositivos e aplicações existentes na rede, nomeadamente:

- Aplicações usadas pelo cliente
- Sistema operativo e respetiva versão de servidores e computadores utilizados na rede
- Dispositivos móveis
- Browsers
- Máquinas virtuais

### *4. Host Detection e Capacidades de Profiling*



SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

- O sistema deve ser capaz de detetar o perfil do utilizador com métodos passivos e ativos (ex. NMAP)
- O sistema de gestão deverá conter uma database de vulnerabilidade que possa ser automaticamente comparada aos perfis de Host.
- O perfil de host deve incluir: endereços IP, MAC addresses, Last Seen timestamp, User (se disponível), Sistema Operativo, Serviços de Servidor, Aplicações vistas, Protocolos de Host, vulnerabilidades relevantes.
- O sistema deve ser capaz de correlacionar eventos ativos com indicação de compromisso (IoC) e os perfis de host.
- Os perfis de host devem conter características custodiáveis.

### *5. Network Discovery e Capacidades de profiling de Tráfego*

O Sistema deve ser capaz de descobrir redes e criar perfis de tráfego por redes e zonas.

Os perfis de tráfego devem ser criados com base no tráfego de rede inspecionado na firewall e baseados na informação de Netflow através de exportadores externos de Netflow.

### *6. Deteção de Anomalias e Correlação*

O sistema deve ser capaz de detetar anomalias nos perfis de tráfego e nos perfis dos utilizadores

O sistema deve ser capaz de correlacionar eventos de IPS, *Malware*, ficheiros, *hosts* e novas conexões com eventos relacionados com alterações dos perfis de *hosts* e dos perfis de tráfego, e com isto aplicar automaticamente medidas para prevenir estes cenários.

No caso de ocorrerem eventos de correlação, o sistema deve ser capaz de ativar automaticamente medidas de remediação *stardard* e custodiáveis.

O sistema deve ser capaz de fazer quarentena automaticamente a um *host* quando usado em conjunto com o *Identity Services Engine* (ISE).

### *7. Filtragem por reputação, DNS sinkhole and Geolocalização*

- O sistema deve suportar feeds de reputação disponibilizados pelo vendedor assim como feeds customizáveis.
- O sistema deve suportar e processar feeds de reputação através de URL, domínio e IP
- A reputação do domínio deve ser verificada antes de a comunicação ser iniciada entre um utilizador interno e outro externo.
- O sistema deve ser capaz de fazer drop ou modificar records A e AAAA quando um pedido é feito para domínios bloqueados ou suspeitos.
- O feed disponibilizado pelo fornecedor deve ter múltiplas categorias, incluindo as seguintes:
  - Attackers
  - Bogon
  - Bots
  - CnC



SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

- Dga
- Exploitkit
- Malware
- Open_proxy
- Open_relay
- Phishing
- Spam
- Suspicious
- Global Blacklist
- Global Whitelist

- O sistema deve ser capaz de utilizar a informação de geolocalização para criar relatórios, como condição para as políticas de controlo de acessos e em políticas de correlação.

### *8. URL Filtering Dinâmico*

O sistema deve ser capaz de determinar a categoria e o nível de risco de URLs.

O sistema deve ter atualizações automáticas à base de dados de URLs e permitir que o sistema consulta uma plataforma na *cloud* no caso de um URL não ser conhecido.

### *9. Proteção contra Malware e Controlo de Ficheiros*

O sistema deve ser capaz de voltar a montar arquivos e descompactar arquivos compactados.

Inspeção de ficheiros e *malware* têm de suportar os protocolos HTTP, FTP, SMTP, POP3, IMAP e NetBIOS.

O motor de inspeção de ficheiros deve ser capaz de reconhecer dinamicamente tipos de ficheiros.

Deve suportar a capacidade de firewall sandboxing, para execução de ficheiros e binários suspeitos.

A funcionalidade de deteção de *malware* deve suportar:

- Verificação da estrutura de ficheiros executáveis e verificação da sua estrutura contra o serviço de cloud do fornecedor.
- Anti-virus tradicional baseado em assinaturas.
- Serviço de cloud que verifica apenas hashes no serviço de cloud do fornecedor.
- Deve ser capaz de enviar ficheiros para sandboxing na cloud ou através de appliances dedicadas de sandboxing.
- O sistema deve ser capaz de integrar-se com a solução de endpoints do próprio fornecedor.
- O sistema deve ser capaz de visualizar dinamicamente a trajetória dos ficheiros dentro da rede através de um gráfico temporal.
- A consola de gestão central deve reportar o resultado de ficheiros enviados para a plataforma de sandboxing.



SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

- O sistema deve suportar eventos retrospetivos. O sistema deve ser capaz de categorizar um ficheiro como malware no caso de este ter passado pelo sistema sem ser detetado, e posteriormente for identificado como malware. Devem ser gerados alertas e deve ser possível visualizar os eventos através de um gráfico onde seja possível identificar o ponto de entrada na rede e a trajetória do ficheiro dentro da rede.

### *10. Gestão de eventos e Assets*

O Sistema deve ter *widgets*, devendo estes serem customizáveis.

O sistema deve ser capaz de manter um mapa de rede dinâmico.

O sistema deve ser capaz de registrar eventos de conexão com base no tráfego inspecionado e nos dados de *Netflow* exportados a partir de dispositivos de redes externas.

O sistema de gestão deve ter páginas com dados em tempo real (ou quase) sobre:

- Eventos de malware
- Eventos de ficheiros
- Eventos de ficheiros capturados
- Eventos de conexões
- Eventos de indicações de comprometimento para hosts e rede
- Filtragens baseadas em reputação
- Perfis dos hosts da rede
- Análise das aplicações
- Análise ao comportamento dos utilizadores
- Análise de vulnerabilidades

### *11. Políticas de Controlo de Acessos*

As políticas de controlo de acesso devem incluir:

- Zonas de origem e destino
- Redes de origem e destino
- Portos de origem e destino
- Aplicações
- Reputação de URLs e Ips
- Categorias de URLs e níveis de risco
- Atributos do ISE
- VLAN Tag (para implementações inline)
- Geolocalização

### *12. Desencriptação SSL/TLS*



SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

O aparelho proposto deve ser capaz de fazer desencriptação, inspecionar e voltar a encriptar os dados.

Desencriptação SSL/TLS deve ser controlada por uma política que é reutilizável e permite exceções definidas em regras.

Desencriptação SSL/TLS não deve ser limitada a HTTPS, outros protocolos que utilizam criptografia SSL ou TLS devem ser suportados.

### *13. Solução de gestão centralizada*

- A solução de gestão centralizada deve ter um GUI, devendo esta apresentar capacidade de gestão e manutenção através de uma única consola de gestão simplificada;
- Consola de gestão assente em tecnologia web-based, ressalvando-se a existência de linha de comando para a introdução global de configurações;
- A solução de gestão deve suportar ambientes – multi-tenant, multi-domain
- A solução de gestão deve suportar RBAC (Role-Based Access Control)
- A solução de gestão deve suportar autenticação através de RADIUS ou LDAP para os administradores.
- A plataforma de gestão deve permitir upgrade de firmwares de forma centralizada para todas as plataformas geridas por ela.
- A plataforma de gestão deve gerir centralmente as licenças.
- A plataforma de gestão deve aplicar políticas de monitorização. Estas políticas devem incluir, entre outras, as seguintes:
    - Monitorização de CPU
    - Monitorização dos módulos de hardware
    - Monitorização do status do cluster
    - Monitorização do uso dos discos
    - Monitorização dos links e interfaces
    - Monitorização dos eventos de intrusão e de ficheiros
    - Monitorização dos feeds de informação reputacional recolhidos da cloud
    - Monitorização da sincronização de tempo

### *14. Partilha e Interoperabilidade de Dados e Logs*

O sistema deve possibilitar a exportação e partilha segura (por ex., API seguro e com base em standards de interoperabilidade que permitam encriptação) de dados e *logs* para um sistema ou plataforma central, devendo os níveis de granularidade e detalhe a exportar ou partilhar ser configurável.

### *15. QoS e Traffic-Shapping*

Deverá ter a capacidade de implementar o Qualidade de Serviço(QoS) e ter a funcionalidade de traffic-shaping;



SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

### *16. Capacidade de gestão de plataformas Wireless*

Deve suportar a gestão de Wireless Access points, devendo efectuar funções de Wireless Security Switch, para redes de Guesting.



SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61, 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649