

Orientações de Segurança para o Projeto

Exames sem Papel



Data de publicação 14-12-2017

Este trabalho não pode ser reproduzido ou divulgado, na íntegra ou em parte, a terceiros nem utilizado para outros fins que não aqueles para que foi fornecido sem a autorização escrita prévia ou, se alguma parte do mesmo for fornecida por virtude de um contrato com terceiros, segundo autorização expressa de acordo com esse contrato. Todos os outros direitos e marcas são reconhecidos.



Os direitos de autor deste trabalho pertencem à SPMS e a informação nele contida é confidencial.

As cópias impressas não assinadas representam versões não controladas.

Índice

1. Introdução	3
2. Âmbito	4
3. Enquadramento	5
4. Camada de transporte	6
a. Plataforma de Dados da Saúde (PDS)	6
b. Portuguese National Broker (PNB)	6
c. Pressupostos	7
5. <i>Compliance</i> dos sistemas	8
6. Controlo do Documento	8
a. Histórico de Alterações	8
b. Lista de Distribuição	8
c. Documentos Relacionados	8
d. Outros Documentos Relevantes	8
e. Acrónimos	9

1. Introdução

Nos últimos 6 meses e, no âmbito do programa **Exames Sem Papel**, a SPMS tem trabalhado conjuntamente com todos os *stakeholders* envolvidos no circuito de Meios Complementares de Diagnóstico e Terapêutica (MCDT), privados e públicos, por forma a testar o conceito da desmaterialização de resultados de MCDT. Verificou-se que a publicação do Despacho 4751/2017 (procedimento para partilha de resultados) e do Despacho 8018/2017 (consentimento informado) imprimiu uma dinâmica positiva para o avanço do projeto, sendo que atualmente já existem 3 Hospitais do SNS que disponibilizam os resultados dos exames dos seus utentes através do Registo de Saúde Eletrónico. No setor privado já há igualmente laboratórios que respeitando a vontade do utente, facultam de forma eletrónica os resultados dos seus MCDT na sua área do cidadão.

Não obstante o gáudio originado pelo *kick off*, são números ainda insuficientes para o desiderato do projeto. O avanço do projeto, ao nível no setor privado, nomeadamente na área das análises clínicas, não progrediu mais acentuadamente devido a questões técnicas e de segurança.

Neste contexto, existe a necessidade de regulamentar a comunicação eletrónica entre a Plataforma de Dados da Saúde (PDS)/Portuguese National Broker (PNB) e os sistemas de informação dos Laboratórios convencionados, onde são realizados os MCDT.

2. Âmbito

A necessidade de confidencialidade, integridade e disponibilidade da informação, requer que todas as transações informacionais entre os sistemas sejam realizadas de forma segura e expedita, não colocando assim em causa a utilidade da informação.

O presente documento é de âmbito claramente definido e restrito às comunicações externas à RIS, entre os Laboratórios convencionados e PNB/PDS, sendo que, a SPMS reserva-se o direito de efetuar a sua revogação por um documento de âmbito mais abrangente alicerçado na estratégia de segurança da informação.

Todas as entidades que integrem ou pretendam integrar o projeto Exames sem Papel, ficam sujeitas à regulamentação plasmada no presente documento.

3. Enquadramento

O programa Exames sem Papel, pretende efetuar a desmaterialização de todas as requisições de MCDT. Parte desse projeto consiste em estabelecer comunicação com os Laboratórios Convencionados através da INTERNET, permitindo assim que os resultados dos exames realizados nos referidos laboratórios, possam nesta fase, ser consultados através de um documento em PDF, armazenado no sistema de informação do laboratório. Prevê-se que num curto espaço de tempo esses exames sejam disponibilizados também em formato de dados estruturados para que possam ser integrados nos vários sistemas de informação do SNS.

No momento, estão a ser desenvolvidas duas formas de integração, uma via PDS, através da WEBAPI e outra, que será a solução definitiva, através do PNB.

Foi solicitado ao Núcleo de CiberSegurança que especificasse de que forma as comunicações entre os sistemas de informação do SNS, dentro da RIS, poderiam comunicar de forma segura com os sistemas de informação dos laboratórios convencionados que se encontram fora da RIS.

Para responder a estas questões, foram tidas em conta as seguintes premissas:

- A INTERNET é por definição uma rede insegura;
- A RIS é por definição uma rede segura;
- As comunicações devem ser realizadas de forma segura garantindo confidencialidade, integridade e disponibilidade da informação;
- Devem ser utilizados protocolos *standard* garantindo compatibilidade;
- Associar vários mecanismos de proteção garantindo maior segurança;

4. Camada de transporte

As comunicações realizadas no âmbito do programa Exames sem Papel entre PNB/PDS e os Laboratórios convencionados, externos à Rede Informática da Saúde (RIS), por definição são consideradas comunicações de risco, uma vez que, são realizadas através de uma rede não segura, a INTERNET.

Existem, contudo, mecanismos de proteção e mitigação do risco que utilizados em conjunto, conferem às comunicações níveis de proteção adicionais.

Atentas à necessidade de confidencialidade, integridade, disponibilidade e segurança da informação a transmitir entre os vários sistemas envolvidos, as comunicações devem obrigatoriamente cumprir os seguintes requisitos:

a. Plataforma de Dados da Saúde (PDS)

- Utilização do protocolo HTTPS (TLS 1.2) na porta 443;
- Utilização de certificados válidos e emitidos por entidades credenciadas com chave RSA 2048bits e algoritmo de assinatura SHA256withRSA;
- Bloqueio de qualquer acesso via HTTP;
- Utilização de *Access Lists* (ACL) para permitir conectividade aos *WebServices*, apenas aos IPs autorizados no âmbito do programa.
- Utilização do *standard* OAuth2.0 para o processo de autorização na utilização dos serviços da WebAPI, cujo tempo de validade deve ser de 5 minutos.

b. Portuguese National Broker (PNB)

- Utilização do protocolo HTTPS (TLS 1.2) na porta 443;
- Utilização de certificados válidos e emitidos por entidades credenciadas com chave RSA 2048 bits e algoritmo de assinatura SHA256withRSA;
- Bloqueio de qualquer acesso via HTTP;



- Utilização de *Access Lists* (ACL) para permitir conectividade aos *WebServices*, apenas aos IPs autorizados no âmbito do programa.
- Utilização do *standard* WS-Security (Digest) para o processo de autorização na utilização dos serviços, cujo tempo de validade deve ser de 5 minutos.

c. Pressupostos

- Cada entidade, terá ainda que garantir a utilização de um IP fixo válido no espaço de endereçamento da INTERNET por forma a garantir a conectividade ao programa Exames sem Papel.
- O publicador da SPMS, deve suportar publicações WSDL e REST.





5. Compliance dos sistemas

A adaptação dos sistemas de abrangidos por estas recomendações de segurança, entidades do SNS e prestadores convencionados com o SNS, deve ocorrer no prazo máximo de 90 dias após a publicação do presente documento.

6. Controlo do Documento

a. Histórico de Alterações

Versão	Data	Autores	Revisores	Alterações	Aprovação
V1.1	12/12/2017	NCS - SPMS	Nuno Lucas		
V2.0	14/12/2017	ESP - SPMS	Cristina Santos	Capítulo 5	

b. Lista de Distribuição

Nome	Organização	Cargo / Responsabilidade
Plataforma de Dados da Saúde	SPMS	
Portuguese National Broker	SPMS	
Operação Segurança Infraestrutura	SPMS	

c. Documentos Relacionados

Relatório precedente	Início	Fim

d. Outros Documentos Relevantes

Referência	Título
------------	--------



SPMS_SGSI_PLTSI_PSI_Política SegInfo

Política de Segurança da Informação

e. Acrónimos

Sigla	Significado
ESP	Exames Sem Papel
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
MCDT	Meios Complementares de Diagnóstico e Terapêutica
OSI	Operação Segurança Infraestrutura
PDS	Plataforma de Dados da Saúde
PNB	Portuguese National Broker
RIS	Rede Informática da Saúde
SNS	Serviço Nacional de Saúde
SPMS	Serviços Partilhados do Ministério da Saúde, E.P.E.

Fim de Documento