Circular Normativa N.º 07/2017/SPMS

Para: **Unidades Locais de Saúde, Hospitais EPE, SPA, PPP do SNS**

Assunto**: Medidas de reforço de infraestruturas e operação de sistemas**

Através do Decreto-Lei n.º 108/2011, de 17 de novembro, foram acometidas à SPMS, EPE competências no domínio dos sistemas de informação e comunicação, com inerente responsabilidade sobre a manutenção e operação dos vários sistemas de informação na área da saúde.

É por isso missão da SPMS, EPE 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 e segurança das infraestruturas tecnológicas e dos sistemas de informação do Ministério da Saúde.

1. Considerações

A presente circular, tem em consideração a atual conjuntura no âmbito da segurança informática, e a exposição a que o Ministério da Saúde e as suas entidades estão sujeitas por força da sua atividade.

O risco de segurança informática do conjunto das entidades do Ministério da Saúde, é equivalente ao risco de segurança da entidade menos protegida, pelo que é responsabilidade individual de cada entidade, inclusive da SPMS EPE, promover e adotar todas as boas práticas garantindo assim um Ministério da Saúde mais forte e robustecido contra o cibercrime.

Pretende-se também, fomentar e incrementar o desempenho geral dos sistemas de informação das entidades, e garantir uniformização e coerência no âmbito das infraestruturas e parque informático.

2. Responsabilidade das entidades

a. Infraestrutura de rede

i. É da responsabilidade das entidades garantir o correto funcionamento das redes locais (LAN). Devem por isso as entidades realizar regularmente, idealmente com uma frequência anual mas obrigatoriamente pelo menos de dois (2) em dois (2) anos, auditorias externas a toda 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

infraestrutura de rede para identificar eventuais problemas de performance ou configuração que estejam a degradar o seu desempenho.

ii. Devem ser garantidas pelas entidades, no prazo máximo de 6 meses, após assinatura da presente Circular, formação (e reciclagem) adequada, aos recursos humanos que gerem e mantêm a infraestrutura de rede, garantindo assim as melhores práticas e técnicas na gestão, operação e manutenção da mesma.

iii. No que diz respeito aos switchs de *Core* (*core* de rede), as entidades devem garantir no prazo máximo de 1 ano após assinatura da presente Circular, que os mesmos são redundantes e que dispõem de interfaces suficientes para interligar, também de forma redundante, os ativos de rede de acesso.

iv. As ligações entre os switchs de *Core* e os swichs de acesso (*backbone)*, devem ser garantidas, por meio de fibra ótica com velocidade de 10Gb no acesso principal, sendo que, no acesso de *backup* são aceites velocidades inferiores até um mínimo de 1Gb também em fibra ótica.

v. As ligações dos servidores à infraestrutura de rede, devem estar asseguradas a velocidades superiores a 1Gb, pelo que, deve a entidades realizar todos os esforços para garantir velocidades de 10Gb.

vi. A entidade deve garantir no prazo máximo de 6 meses, após assinatura da presente Circular, que não tem em produção nenhum equipamento ativo de rede, cujo suporte já não seja assegurado pelo fabricante do equipamento.

vii. É desejável que toda a infraestrutura de rede seja homogénea para garantir compatibilidade e fiabilidade, pelo que, devem as entidades garantir todos os esforços no sentido de uniformizar toda a infraestrutura de rede em marca e modelo – ressalva-se neste caso os switchs de *core* cujo modelo será/poderá ser diferente dos switchs de acesso.

viii. Deve a entidade garantir no prazo máximo de 6 meses, após assinatura da presente Circular, a existência de um software específico para a gestão, manutenção, operação e geração de alertas da infraestrutura rede, adequado aos equipamentos existentes ou a adquirir.

ix. No que diz respeito aos contratos de manutenção, deve a entidade garantir que no prazo máximo de 6 meses, após assinatura da presente Circular, todos os equipamentos que compõem a infraestrutura de rede estão cobertos por um contrato de manutenção válido, e suportado pelo fabricante, cujo SLA não pode ser inferior a 24X7X4.

b. Infraestrutura de sistemas

i. No que diz respeito à infraestrutura de servidores e storage (armazenamento), é da responsabilidade das entidades garantir o seu correto funcionamento bem como aprovisionar em tempo útil recursos suficientes para fazer face às necessidades da entidade. Devem por isso as entidades realizar regularmente, idealmente com uma frequência anual mas obrigatoriamente pelo menos de dois (2) em dois (2) anos, auditorias externas a toda a infraestrutura para identificar eventuais problemas de performance, configuração ou falta de recursos como sendo disco, memória, processamento, etc.

ii. Devem ser garantidas pelas entidades, no prazo máximo de 6 meses após assinatura da presente Circular, formação (e reciclagem) adequada, aos recursos humanos que gerem e mantêm a infraestrutura de sistemas, garantindo assim as melhores práticas e técnicas na gestão operação e manutenção da mesma.

iii. Com vista à otimização dos recursos financeiros, por definição sempre escassos, devem as entidades promover a adoção de infraestruturas robustas e redundantes, com capacidade de albergar vários sistemas efetuando assim uma otimização dos recursos disponíveis. Excetua-se neste caso o sistema SONHO V.x que, pela sua especificidade e particularidade, deve permanecer numa infraestrutura dedicada.

iv. Deve a entidade promover a adoção da virtualização de sistemas, em detrimento da aquisição de infraestruturas físicas, salvo nos casos em que exista contraindicação técnica.

v. Deve a entidade no prazo máximo de 6 meses, após assinatura da presente Circular, garantir que todos os equipamentos produtivos (servidores, storages, SAN switchs, etc.) que compõem a infraestrutura de sistemas estão cobertos por um contrato de manutenção

válido, e suportado pelo fabricante, cujo SLA não pode ser inferior a 24X7X4 no caso dos sistemas que prestam serviço 24 horas por dia. Os equipamentos que não sejam suportados pelos fabricantes, devem ser incluídos num plano de substituição no máximo de um (1) ano após assinatura da presente Circular.

c. DataCenter e salas de sistemas

i. Deve a entidade garantir no prazo máximo de um (1) ano, após assinatura da presente Circular, o cumprimento dos requisitos do standard TIA-942 Telecommunications Infrastructure Standard for Data Centers para o Rated-2/Tier 2.

Para os devidos efeitos, a presente Circular refere-se neste ponto a mecanismo eletrónico de controlo a indicar e/ou a remessa de documento de controlo checklist_tia942.xlsx que será enviado via correspondência direta da DSI da SPMS ás referidas entidades e cujo feedback deve ser remetido (um por cada DataCenter/sala de sistemas de cada entidade) para a SPMS EPE, 30 dias após recepção da comunicação dessa informação. Para o efeito devem utilizar-se o e-mail ticadm@spms.min-saude.pt com o assunto "TIA942-2017".

ii. Deve a entidade remeter para a SPMS, um (1) ano após assinatura da presente Circular, feedback atualizado através de via informática e/ou versão atualizada do documento de controlo checklist_tia942.xlsx devidamente atualizado à data do seu envio para o e-mail referido no ponto anterior (i) com o assunto "TIA942-2018".

d. Competências técnicas

i. Devem as entidades garantir no prazo máximo de seis (6) meses, após assinatura da presente Circular, a existência de recursos internos ou externos com os seguintes perfis técnicos:

1. Administrador de sistemas;
2. Segurança informática;
3. Administrador de redes informáticas;
4. Administrador de base-de-dados;

ii. Devem as entidades proporcionar um plano de formação (e reciclagem) anual para cada um dos perfis elencados acima, de no mínimo de 35 horas anuais, tal como legalmente previsto, e adaptado ao exercício das suas funções.

e. Segurança

i. No âmbito da segurança, a SPMS emite circulares de âmbito próprio para o efeito. Neste sentido, recorda-se que até ao momento foram emitidas 4 Circulares Normativas, que se anexam à presente Circular. Reforçamos, ainda, a necessidade imperiosa do seu cumprimento.

f. Operação

i. Neste domínio, a SPMS, EPE para a prossecução eficaz das suas competências e responsabilidades, tem que conhecer de forma atempada e, em articulação com as entidades, agendar qualquer intervenção nos sistemas informáticos locais, quer na área da infraestrutura, quer na área aplicacional ou base-de-dados, suscetível de comprometer o sistema ou a interoperabilidade dos sistemas da saúde e/ou segurança e integridade de dados. Estão também abrangidas as intervenções nos respetivos DataCenters ou Salas de Sistemas.

Assim, cumpre-nos solicitar a Vossa atenta e especial colaboração no cumprimento rigoroso do seguinte circuito comunicacional, para além dos legalmente exigidos.

Qualquer intervenção com alcance e trato sensível, descrito na presente missiva, deverá ser previamente agendada para que possa usufruir de um acompanhamento técnico por parte da SPMS, EPE com 30 dias de antecedência através do Portal Self-Service, com a seguinte informação, sem prejuízo de outra que seja essencial para o sucesso da intervenção:

- Assunto deve conter obrigatoriamente o texto: “Aviso de Agendamento de Intervenção Local”;
- Entidade responsável pela intervenção;

- Data e hora prevista da intervenção;
- Tempo previsto para a intervenção;
- No caso de a entidade responsável ser externa, o âmbito contratual do qual existem salvaguardas de segurança e legais;
- Sistemas e aplicações que serão intervencionadas;
- Sistemas e aplicações que podem ser afetadas de forma direta ou indireta;
- Detalhe técnico da intervenção;
- Contacto de e-mail e telefónico do responsável pela intervenção da entidade;

Nos casos em que se verifique uma situação de ausência de comunicação, ou que a mesma não cumpra os pressupostos acima referidos, enquadrável na violação genérica do disposto do artigo 4º do Decreto-Lei n.º 108/2011 de 17 de novembro, não pode esta entidade, assumir ou aceitar quaisquer responsabilidades emergentes do processo.

Caso os pressupostos anteriormente descritos não sejam cumpridos, a SPMS, EPE não poderá intervir na resolução de qualquer evento técnico uma vez que não poderá assegurar em tempo útil, os meios e recursos técnicos necessários.

Salienta-se ainda que, no caso de estarem em causa aplicações suportadas e/ou fornecidas pela SPMS, EPE, tal ocorrência consubstancia uma situação típica de uso indevido de base-de-dados ou aplicativo, para todos os efeitos legais.

ii. A entidade tem a responsabilidade de garantir que todas as intervenções realizadas, quer no âmbito da infraestrutura, quer no âmbito aplicacional, têm suporte contratual legal com o prestador do serviço.

iii. Deve a entidade promover a documentação atualizada da arquitetura aplicacional e de infraestrutura existentes, submetendo-a até dia 31 de dezembro de 2017 para a SPMS, EPE através do e-mail ticadm@spms.min-saude.pt, com o assunto “Documentação de arquitetura - 2017”.

3. Responsabilidades da SPMS

A SPMS tem por Missão a prestação de serviços partilhados específicos na área da saúde em matéria de compras e de logística, de serviços financeiros, de recursos humanos, de sistemas e tecnologias de informação e comunicação e demais atividades complementares e subsidiárias, a todos os estabelecimentos e serviços do SNS, independentemente da respetiva natureza jurídica, sejam entidades EPE´s, sejam entidades do Sector Público Administrativo (SPA), bem como aos órgãos e serviços do Ministério da Saúde e a quaisquer outras entidades quando executem atividades na área da saúde.
Neste pressuposto e cingindo a presente Circular ao âmbito TIC,

i. É responsabilidade da SPMS EPE, emitir normas e pareceres no âmbito de sistemas e tecnologias de informação.
ii. É responsabilidade da SPMS EPE, colaborar na revisão dos contratos realizados no âmbito TIC;
iii. É responsabilidade da SPMS EPE, acompanhar as intervenções técnicas no âmbito TIC.
iv. É responsabilidade da SPMS EPE, sempre que achar conveniente, realizar junto das entidades, recolha de dados/auditorias aos sistemas de informação.
v. É da responsabilidade da SPMS, EPE promover junto das entidades a partilha e gestão dos sistemas de informação.
vi. É da responsabilidade da SPMS EPE, promover junto de todas as entidades do Ministério da Saúde a adoção de boas práticas na área TIC.

4. Contingência e situações de crise

a. Devem as entidades remeter até 30 dias após assinatura da presente Circular, o Plano de Contingência da área TIC.
   Sem prejuízo de outra informação relevante, o Plano de Contingência deve ter:

   1. Identificação de toda a equipa e estrutura TIC bem como contactos e áreas de responsabilidade;
   2. Plano de comunicação que inclua:
      a. Clientes internos dos serviços;
      b. Clientes externos dos serviços;
      c. A tutela;

d. Entidades terceiras com dependência (*stakeholders*);

3. Identificação de um ponto único de contacto;
4. Identificação clara dos departamentos da entidade considerados críticos em caso de falha dos sistemas de informação.
5. Circuitos e plano de redundância do ponto de vista funcional para a:
    a. Urgência;
    b. Cuidados Intensivos;
    c. Bloco Operatório;
    d. Cirurgia de Ambulatório
    e. Outro departamento que seja considerado crítico pela entidade;

b. Mecanismos de contacto da SPMS

i. Sem prejuízo de outro contacto mais direto em casos urgentes ou emergentes de indisponibilidade de serviços de sistemas críticos, devem as entidades sempre e em primeiro lugar utilizar a plataforma Self-Service, divulgada pela Circular Normativa n.º 6 de 2017.

ii. No caso de eventual indisponibilidade do acesso à plataforma referida no ponto anterior (i), podem recorrer a formas de contacto alternativas como sendo o e-mail servicesk@spms.min-saude.pt ou o contacto telefónico através do número +351 220 129 818.

c. Ações e informação a remeter

i. Deve a entidade, no prazo máximo de 20 minutos após o inicio de um incidente, informar a SPMS pelos canais referidos no ponto 4b).
ii. Antes de qualquer reporte, deve a entidade realizar os despistes necessários para a identificação da causa raiz de um incidente;
iii. Sem prejuízo de informação relevante para a resolução do incidente, o reporte deve conter a seguinte informação:
    1. Identificação do(s) sistema(s) afetado(s);
    2. Descrição detalhada do incidente;
    3. Identificação das últimas ações realizadas no sistema em causa antes e depois do incidente;

4. Existência de indisponibilidade de serviço ou não;
5. Impacto e criticidade;
6. Identificação e contactos (e-mail e telemóvel) do técnico da entidade que acompanha o incidente.

d. Simulacros

i. Devem as entidades entre outubro e dezembro de 2017 elaborar e executar um plano de simulacro, pelo menos, para as seguintes situações:

1. Falha da climatização do DataCenter entre as 03:00 e 04:00 da manha;
2. Falha do *core* de rede entre as 10:00 e as 12:00;
3. Falha da energia elétrica geral entre a 01:00 e as 02:00 durante 1 hora;
4. Paragem não programa de uma *storage* crítica, por exemplo que aloja o SONHO ou o sistema de virtualização da entidade.

ii. Após a aprovação do plano de simulacro pelo Conselho de Administração da entidade, o mesmo deve ser remetido para a SPMS EPE, através do e-mail ticadm@spms.min-saude.pt no mínimo com 30 dias de antecedência à sua execução, tal como solicitado no ponto (i).

iii. O plano de simulacro deve ser revisto e executado uma vez por ano, sendo os resultados do mesmo comunicados à SPMS pelo e-mail referido no ponto anterior, no máximo 10 dias após a sua execução.

5. Recomendações

a. As entidades devem garantir a atualização da infraestrutura de suporte - servidores, storages (armazenamento), ativos de rede, entre outros - em tempo útil, não permitindo que atinjam graus de obsolescência que coloquem em risco todo o sistema de informação;

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

Considera-se, para todos os efeitos, que um equipamento informático, por exemplo um servidor ou *storage*, atingiu o seu fim de vida útil a partir do quarto (4) ano de utilização, sendo por isso recomendada a sua substituição.
Considera-se, ainda, que os equipamentos devem ser atempadamente substituídos quando o fabricante anuncia o fim de suporte do mesmo, caso não o tenham sido em tempo útil.

Nos dias de hoje, muitas organizações, quando enfrentam desafios orçamentais, adiam as despesas de capital (CAPEX) e prolongam os ciclos de vida dos equipamentos, produzindo alguns benefícios no imediato; contudo, se o adiamento se prolongar, os equipamentos ficam desfasados em relação aos níveis de desempenho e eficiência desejáveis. O conceito "*buy and hold*" vai, na realidade, acrescentar custos diretos e indiretos em toda a infraestrutura:

- Os custos de manutenção de hardware aumentam com o tempo, e o desempenho fica atrás do desempenho de equipamentos mais atuais, impactando diretamente com a produtividade da entidade;

- A eficiência energética não é tão otimizada em modelos de equipamentos mais antigos, levando a custos mais elevados de energia e climatização nos anos posteriores ao ciclo de vida útil dos equipamentos;

- Horas de inatividade não planeada devido a avarias nos sistemas e componentes dos mesmos;

- Incremento exponencial da complexidade de gestão, administração e suporte dos sistemas;

b. É da competência da entidade garantir que toda a infraestrutura de suporte aos sistemas de informação se encontram no seu perfeito estado de funcionamento e que os mesmos são suportados por contratos de manutenção e suporte, com especial enfase para a exigência de contratos back-to-back com os fabricantes por parte dos fornecedores, garantindo SLAs que não excedam 24x7 com tempos de resposta de 4 horas para os

sistemas considerados críticos e que coloquem em causa o funcionamento da entidade, como por exemplo, o SONHO, SClínico, ou sistemas similares, storages, infraestrutura de rede, apenas para referir alguns.

Os contratos celebrados devem também prever manutenção corretiva, upgrades de versão de firmware, correções de *bugs,* patchs de segurança, e uma ou duas visitas anuais de verificação geral do sistema.

c. As entidades, devem assegurar os meios técnicos e humanos necessários para garantir os backups dos sistemas existentes, não devendo os backups realizados permanecer nos próprios sistemas, pelo que, é fortemente recomendável a existência de sistemas específicos com as condições adequadas e que respondam às exigências legais no âmbito do General Data Protection Regulation (GDPR).

   Adicionalmente, deve a entidade criar condições para efetuar testes de reposição de backups fora dos ambientes produtivos para os vários sistemas, garantindo assim a sua qualidade ou deteção prévia de falhas.

d. As entidades devem assegurar que, nos servidores afetos aos sistemas SClínico e SONHO, não existe qualquer outro aplicativo ou base-de-dados. Excetuam-se obviamente os sistemas considerados indispensáveis para o correto funcionamento dos aplicativos em causa, bem como os sistemas de segurança e proteção. A partilha de infraestrutura não é contraindicada, contudo, devem estar salvaguardados todos os meios técnicos para o correto funcionamento e salvaguarda da performance dos sistemas em causa.

e. As entidades devem garantir que, antes de qualquer alteração ao modelo de dados das aplicações produzidas pela SPMS, devem ter recebido a devida autorização e aceitação por escrito. É ainda de referir que não deve a entidade utilizar utilizadores previamente criados no SONHO para realizar outras integrações, ou seja, sempre que exista lugar a uma integração nova, deve ser solicitada à SPMS a criação de um utilizador adequado a esse fim.

Lisboa, 13 de setembro de 2017

O Presidente do Conselho de Administração

Henrique Manuel Gil Martins

Assinado de forma digital por Henrique Manuel Gil Martins
Dados: 2017.09.13 13:32:52 +01'00'

Henrique Martins