**Circular Normativa N.º 06**

Para: **Administrações Regionais de Saúde (ARS) e Unidades Locais de Saúde (ULS)**

Assunto**: Medidas de Reforço de Infraestruturas, Operações e Comunicações nos Cuidados de Saúde Primários**

# 1. CONTEXTO

A SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. tem como atribuições a prestação de serviços partilhados específicos da área da saúde em matéria de compras e logística, de serviços financeiros, de recursos humanos e de sistemas e tecnologias de informação e comunicação aos estabelecimentos e serviços do Serviço Nacional de Saúde (SNS), independentemente da sua natureza jurídica, bem como aos órgãos e serviços do Ministério da Saúde e a quaisquer outras entidades, quando executem atividades específicas da área da saúde.

No âmbito dos serviços partilhados de sistemas e tecnologias de informação e comunicação, a SPMS, E.P.E., 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 interoperabilidade e interconexão dos sistemas de informação da saúde, entre si e com os sistemas de informação transversais à Administração Pública.

Neste contexto, compete à SPMS promover, junto das entidades do SNS, a disseminação das melhores práticas, de acordo com normas e orientações nacionais e internacionais no domínio dos sistemas de informação e comunicação. Através do Decreto-Lei nº 108/2011, de 17 de novembro, que procedeu à primeira alteração ao Decreto-Lei n.º 19/2010, de 22 de março, foram concedidas à SPMS, E.P.E 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, designadamente:

- Emitir normas e definição de requisitos no âmbito de sistemas e tecnologias de informação;
- Colaborar na revisão dos contratos realizados no âmbito TIC;
- Acompanhar as intervenções técnicas no âmbito TIC;
- Realizar junto das entidades, recolha de dados/auditorias aos sistemas de informação, sempre que achar conveniente e que seja solicitado pelas entidades;
- Promover junto das entidades a partilha e gestão dos sistemas de informação;
- Promover ainda, junto de todas as entidades do SNS e Ministério da Saúde, a adoção de boas práticas no âmbito das Tecnologias de Informação e Comunicação (TIC).





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 ecossistema de informação em saúde está mais complexo, apresentando um conjunto de desafios, em resultado, quer de uma crescente rede de interdependências, de partilha de recursos, distribuição de acessos, quer da necessidade de assegurar meios económicos para a sustentabilidade da infraestrutura de suporte. Estes desafios carecem de permanente análise, planeamento e resolução por parte dos responsáveis das entidades que prestam cuidados de saúde.

A transformação digital no Serviço Nacional de Saúde e, em particular, no setor dos Cuidados de Saúde Primários (CSP), implica a adequada informação e aconselhamento especializado. Assim, atento o papel da SPMS, E.P.E. nesta matéria, importa divulgar recomendações que promovam a sustentabilidade dos serviços e sistemas digitais que, de forma cada mais crítica, suportam o dia-a-dia das unidades funcionais nos cuidados de saúde primários do SNS.

Neste contexto, a presente circular tem por objetivo documentar e divulgar as boas práticas, processos, procedimentos, normas e *standards* que deverão ser adotados para promover a operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação do Ministério da Saúde e SNS, garantindo, desta forma, a estandardização na operacionalidade e segurança das respetivas infraestruturas tecnológicas.

Assim, revelou-se fundamental proceder à caracterização da realidade e do modelo de governação atual das Tecnologias de Informação e Comunicação (TIC), por forma a obter uma visão abrangente de todas as componentes do seu ecossistema.

Para o efeito, foi enviado, a todas as entidades do SNS, um questionário tipo, que permitirá caraterizar de forma detalhada a generalidade das componentes, melhor identificadas na Figura 1 - Diagrama de Sistemas de Informação.


*Figura 1 – Diagrama Sistemas de Informação*

Este levantamento permite, assim:

- Identificar e sugerir a priorização de projetos e ações da SPMS, E.P.E, no âmbito de um plano de evolução tecnológico, por forma a apoiar os organismos na modernização dos seus serviços aos cidadãos/utentes que estão suportados por TIC;
- Definir, por um lado, as estratégias para as aquisições de bens e serviços TIC, mas também a de capacitação de Recursos Humanos próprios (que melhor se apliquem), considerando os custos, riscos e benefícios;
- Definir níveis de maturidade a serem alcançados para os processos de gestão de TI, para que a SPMS, E.P.E. possa perceber onde poderá apoiar, por forma a garantir continuidade, assegurando a não disrupção sobre o que já existe e está a ser levando a cabo nestas matérias pelas entidades do MS;
- Definir melhorias a ser implementadas nos processos de gestão e de serviços partilhados;
- Garantir um Modelo Corporativo para uma melhoria da prestação dos serviços comuns;
- Garantir que o Programa de Implementação está dotado das ações e medidas de evolução tecnológicas, com uma equipa de apoio à execução destas ações, por forma a garantir a sua execução em tempo útil.

## 2. RESPONSABILIDADES DAS ENTIDADES

A implementação das melhores práticas, de acordo com normas e orientações nacionais e internacionais, deverá ser um desígnio comum às diversas entidades e serviços do SNS e MS, por forma a promover otimização dos respetivos sistemas e recursos, no tocante aos serviços que lhe estão subjacentes.

Neste contexto, tendo por base o Diagrama de Sistemas de Informação (Fig. 1) apresenta-se, de seguida, o detalhe de cada um dos pontos que o compõem, a fim de documentar as entidades a operar no setor dos Cuidados de Saúde Primários com um conjunto de premissas e requisitos anteriormente referidos.

## 3. INFRAESTRUTURAS

Garantir a correta operacionalização das infraestruturas que suportam o funcionamento dos seus sistemas é um compromisso geral das organizações. A realização com regularidade de auditorias (com uma frequência anual e por entidades certificadas para o efeito) a toda a infraestrutura, para identificar eventuais vicissitudes funcionais, designadamente, problemas de performance, configurações, falta de recursos que estejam a degradar o seu desempenho, riscos de segurança de informação, entre outras, deverá ser uma preocupação.

A entidade deve garantir que todos os equipamentos produtivos críticos, nomeadamente, ao nível das infraestruturas de sistemas (equipamentos ativos de rede, servidores, *storages*, *firewalls*, servidores, entre outros), estão cobertos por contratos de manutenção válidos e suportados pelos respetivos

fabricantes. Paralelamente, se não for assegurada internamente, a gestão e manutenção e operação deve ser assegurada por contrato de prestação de serviços, de acordo com a realidade da entidade, por forma a não colocar em causa o funcionamento da instituição.

Em termos de níveis de serviço, deverá ser considerado, para os serviços muitos críticos, que exista um racional ponderador, designadamente:

- Infraestruturas em Alta Disponibilidade[1];
- Infraestrutura em Redundância[2];
- Infraestrutura em *Single Instance*[3].
- Neste contexto recomendamos:
    - Se a entidade tiver uma infraestrutura em Alta Disponibilidade ou em Redundância, opte por um nível de reposição de 4 horas até 24 horas;
    - Se a entidade tiver uma infraestrutura em *Single Instance*, opte por níveis de reposição inferiores a 4 horas.
    - Em relação à operação deverá ser considerado um SLA de 24X7X4:
    - Assegurado na integra por um prestador de serviços, caso a entidade não consiga assegurar o mesmo;
    - Complementado por um prestador, caso a entidade consiga assegurar a parcialidade do tempo.
- Os contratos celebrados devem também prever manutenção corretiva designadamente:
- Upgrades de versão de firmware;
- Correções de erros (bug);
- *Patchs* de segurança;
- Uma verificação global dos sistemas, anualmente.

Os equipamentos que se encontrem identificados pelo fabricante como estando em fim de vida (*end of life*), ou seja, com data definida para o suporte ser descontinuado, devem ser incluídos num plano de substituição no máximo de um (1) ano após publicação da presente Circular.

Pela entidade devem ser garantidos planos de formação continuados, em conformidade com as tecnologias instaladas e em produção.

[1] **Infraestrutura em Alta Disponibilidade** – infraestruturas em redundância (2N) mas com funcionamento ativo-ativo, em que qualquer um assegura o funcionamento da mesma em caso de paragem do outro.

[2] **Infraestrutura em Redundância** – infraestrutura em (2N), no entanto o funcionamento é ativo passivo. Em caso de paragem o redundante assegura o funcionamento da infraestrutura.

[3] **Infraestrutura em Single Instance** – A infraestrutura é composta por um equipamento (1N) que assegura o seu funcionamento. Neste cenário, a entidade está perante um SPOF – Single Point of Failure, o que implica num risco muito elevado, pois, em caso de avaria, a entidade ficará "parada".

Deve a entidade garantir, no prazo máximo de 6 meses após publicação da presente Circular, a existência das ferramentas adequadas para a gestão e/ou operação, bem como monitorização e geração de alertas das infraestruturas dos equipamentos existentes.

## 3.1. CENTRO DE DADOS E SALAS DE SISTEMA

As entidades que gerem Centros de Dados sedeados nas suas infraestruturas físicas, devem observar alguns dos requisitos da norma TIA 942[4].

Para efeitos de conformidade, o Anexo I – 1.1 NORMA TIA 942 caracteriza em termos exemplificativos os requisitos da norma para as salas de Centro de Dados.

Existe um sistema de avalia e classifica a infraestrutura de Centro de Dados, com base num formato padrão denominado de *Tier*, tendo como objetivo comparar a funcionalidade, capacidade e disponibilidade do Centro de Dados. O padrão descreve critérios para diferenciar as classificações de topologias de infraestruturas, baseadas em níveis crescentes de redundância.

O Anexo I – 1.2 Níveis TIER e Requisitos, densifica e caracteriza os *Tiers*, devendo a entidade considerar como uma boa prática a conformidade com *Tier II*, e, como excelente, a conformidade com *Tier III*.

Os espaços ou salas onde existem equipamentos ativos de rede ou outro tipo de sistemas (sistemas isolados que pela sua especificidade não estão centralizados), devem estar dotados de sistema de energia ininterrupto (UPS) e de refrigeração adequada aos equipamentos.

## 3.2. PASSIVOS DE REDE LOCAL

Deve a entidade garantir que a cablagem é, no mínimo, de categoria 6 e que se encontra certificada, de forma a garantir o bom funcionamento dos postos de trabalho. A revalidação da certificação deve ser efetuada, pelo menos, de dois em dois anos ou sempre que existam tomadas que se encontrem em mau estado de conservação.

Em resumo, as infraestruturas de passivos de rede local deverão ter em consideração quatro imperativos:

- Performance – A solução a implementar deverá ter em consideração não só as necessidades atuais da entidade, mas também, e tendo em conta a evolução dos sistemas e/ou aplicações, as suas necessidades futuras;
- Escalabilidade – A solução a implementar deverá ser aberta e com capacidade de crescimentos, quer ao nível de número de equipamentos/utilizadores quer ao nível da infraestrutura de Core;
- Disponibilidade – A solução a implementar deverá garantir o máximo de disponibilidade de serviço (Uptime) com mecanismos de redundância e resiliência;
- Gestão e Operação – A solução a implementar deverá garantir funcionalidades de gestão, monitorização e operação remota.

[4] Standard for Telecommunications Infrastructure Standard for Data Centers

O Anexo I – 2. INFRAESTRUTURA - PASSIVOS DE REDE LOCAL reflete os requisitos técnicos para a componente de passivos de rede local.

Os passivos da rede local que não cumpram os requisitos indicados devem ser incluídos num plano de substituição no máximo de dois (2) anos após publicação da presente Circular.

# 4. COMUNICAÇÕES

## 4.1. INFRAESTRUTURAS DE ATIVOS DE REDE

A infraestrutura de rede deverá funcionar sobre *standards* para garantir a interoperabilidade, compatibilidade e fiabilidade, pelo que, devem as entidades uniformizar toda a infraestrutura de rede em marca e modelo. Ressalvam-se neste caso os equipamentos ativos de rede de *Core* cujo modelo será/poderá ser diferente dos equipamentos ativos de rede de acesso/distribuição.

No que diz respeito aos equipamentos ativos de rede de *Core* (designados tecnicamente por *Switch* de *Core*), as entidades devem garantir, no prazo de 1 ano e após a publicação da presente Circular, que os mesmos estão em alta disponibilidade (ativo-ativo) ou que têm redundância (ativo-passivo). Pela sua especificidade (interligam os Sistemas e Sistemas de Informação críticos, e a infraestrutura da rede de dados), necessitam de garantir interfaces suficientes para interligar, também e de forma redundante, os ativos de rede de acesso/distribuição.

O Anexo II – 1. INFRAESTRUTURAS DE ATIVOS DE REDE reflete os requisitos técnicos para a componente da infraestrutura de rede local.

# 5. SISTEMAS

## 5.1. INFRAESTRUTURAS DE SISTEMAS

Com vista à otimização dos recursos financeiros, 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 SINUS que, pela sua especificidade e particularidade, deve permanecer numa infraestrutura dedicada.

Deve a entidade adotar a virtualização de sistemas, em detrimento da aquisição de infraestruturas físicas, salvo nos casos em que exista contraindicação técnica, garantindo assim a centralização de sistemas.

Devem as entidades instituir como uma boa prática, a realização regular (preferencialmente anualmente, mas obrigatoriamente de 2 em 2 anos) de auditorias à infraestrutura, para identificar eventuais situações (*v.g.*: problemas de performance; problemas nas configurações; falta de recursos no sistema, como disco, memória, processamento, ...), por forma a aprovisionar, em tempo útil, recursos efetivos e a reduzir riscos operacionais, bem como contribuir para o correto funcionamento das suas infraestruturas de sistemas.





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 Anexo III – 1. INFRAESTRUTURAS DE SISTEMAS reflete os requisitos técnicos para a componente da infraestrutura de sistemas.

# 6. SEGURANÇA

## 6.1. SEGURANÇA (MEDIDAS EXCECIONAIS DE SEGURANÇA)

No âmbito das suas competências em matéria de segurança da informação, a SPMS, EPE emite circulares para o efeito, tendo neste contexto sido emitidas 4 Circulares Normativas.

## 6.2. SEGURANÇA FÍSICA E MONITORIZAÇÃO

Até ao momento foram emitidas 4 Circulares Normativas no âmbito da segurança da informação, reforçando-se assim a necessidade imperiosa do seu cumprimento.

Sempre que ocorram atualizações das infraestruturas a entidade deve garantir a compatibilidade com os sistemas de segurança física e monitorização.

As soluções de segurança física devem cumprir o disposto na Lei n.º 58/2019, de 8 de agosto, diploma que assegura a execução na ordem jurídica nacional do RGPD, relativamente à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

As soluções de videovigilância existentes ou a implementar, além de cumprirem com a legislação em vigor em matéria de proteção de dados, devem também cumprir integralmente a Lei n.º 34/2013, de 16 de maio, bem como a Portaria n.º 273/2013, de 20 de agosto, na redação atual, cujo Anexo I define os requisitos mínimos dos sistemas de videovigilância. As soluções de videovigilância deverão ser IP e suportadas por plataformas abertas.

Assim, deverá evitar-se a aquisição de soluções de um só fabricante (câmaras e sistema de gravação), que quase sempre limitam a adoção de equipamentos de terceiros.

As câmaras deverão suportar analíticas de vídeo a correr diretamente no próprio equipamento, podendo ser analíticas do próprio fabricante ou de terceiros.

O sistema de videovigilância deverá estar suportado por um ou mais servidores de gravação com solução de redundância de discos (RAID 5 ou equivalente) para suportar a totalidade das câmaras da entidade.

Todas as câmaras deverão suportar gravação para cartão de memória como backup em caso de falha no envio do(s) fluxo(s) de vídeo para o servidor de gravação. O sistema de gravação deverá ter a capacidade de solicitar automaticamente o envio das gravações retidas nos cartões de memória das câmaras assim que estiver retomada a ligação e apagar automaticamente essas imagens dos cartões de memória.

As soluções de videovigilância deverão possuir a capacidade de anonimizar as imagens (ao vivo e gravadas) dinamicamente através de analítica de vídeo, protegendo assim a privacidade dos indivíduos cujas imagens forem capturadas, mas sem limitar a visualização das ações e os movimentos na imagem,

garantindo o acesso controlado e protegido aos dados originais (ao vivo ou gravados) para efeitos de operação e eventual utilização das imagens como prova.

As soluções de Controlo de Acessos deverão ser baseadas em controladores IP e suportadas por plataformas abertas. Assim, deverá evitar-se a aquisição de soluções de um só fabricante (controladores e sistemas de gestão), que quase sempre limitam a adoção de equipamentos de terceiros.

Os sistemas de Controlo de Acesso com utilização de cartões de proximidade, deverão suportar tecnologias mais recentes que evitem a fácil clonagem de cartões.

Os leitores de exterior não poderão ser leitores e controladores num só equipamento.

Os leitores que controlam o acesso ao edifício pelo exterior, para além de suportarem cartões de proximidade e/ou biometria, deverão possuir teclado numérico. Assim, no controlo de acessos fora de horas, deverá ser necessária dupla autenticação: cartão de proximidade e biometria, cartão de proximidade e código PIN, ou biometria e código PIN.

A existirem sistemas de anti-intrusão, deverão permitir o envio de alarmes por IP a uma CRA (Central Recetora de Alarmes), seja essa central interna ou externa (num prestador de serviços de segurança).

De modo a garantir uma operação coerente e fluída entre os vários módulos de segurança (videovigilância, controlo de acessos, intrusão, analítica de vídeo, etc.), deverá ser implementada uma solução unificada de segurança (como um PSIM - *Physical Security Information Management*, ou uma plataforma de Unificação) que garanta a ligação entre os vários módulos de segurança.

O anexo IV – 1. SEGURANÇA FÍSICA E MONITORIZAÇÃO reflete os requisitos técnicos para a componente de segurança física e monitorização.

# 7. APLICACIONAL

As boas práticas no desenvolvimento aplicacional são atualmente uma preocupação transversal às Organizações. Não só os standards evidenciam a necessidade de conformidade no âmbito da Segurança da Informação, designadamente a Framework ISO 27001, mas também a legislação Nacional e Europeia, nomeadamente:

- A Lei nº 58/2019, de 8 de agosto, que assegura a execução na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;
- RCM Nº 41/2018, de 28 de março, que define as orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais;

Estes aspetos têm contribuído para uma sensibilização generalizada sobre a componente de desenvolvimento aplicacional, sendo que acresce a esta consciencialização universalizada, a necessidade de responsabilização por parte das entidades, por forma a garantir os desígnios funcionais da

interoperabilidade (característica essencial na troca e partilha de informação), acrescidos das premissas, cada vez mais exigentes ao nível da confidencialidade, integridade e privacidade.

Consequentemente, as entidades do SNS devem considerar um conjunto de boas práticas no desenvolvimento aplicacional que garantam:

- Uma resposta eficaz às necessidades identificadas;
- Um controlo eficiente no desenvolvimento aplicacional; e,
- A conformidade com as principais diretrizes de segurança e privacidade de dados.

Paralelamente, o desenvolvimento aplicacional deve:

- Ser precedido de um levantamento rigoroso dos requisitos funcionais dos processos e atividades a que a aplicação irá dar suporte, sendo necessário efetuar um levantamento da situação atual, a identificação de constrangimentos e respetivos impactos, a análise e decisão sobre a implementação das oportunidades de melhoria identificadas e o desenho do modelo futuro, cuja aplicação será uma componente chave;
- Ser observada a arquitetura funcional e de que forma a aplicação será integrada na mesma;
- A implementação do modelo futuro deverá ser suportada por um roadmap de implementação onde são identificadas iniciativas, responsáveis, duração, estimativa de investimento e indicadores de medição da concretização das mesmas;
- Ser acompanhado por uma gestão de projeto efetiva através da utilização da metodologia de gestão de projeto do PMI – Project Management Institute, uma metodologia de gestão de projetos reconhecida mundialmente. De acordo com o PMI, o desenvolvimento de um plano de projeto inclui a definição e confirmação das metas/objetivos do projeto, e como é que esses objetivos serão alcançados, identificação de tarefas, quantificação dos recursos necessários e determinação dos orçamentos e prazos para a sua conclusão. Inclui ainda os mecanismos para implementar ações de recuperação sempre que necessário. Os projetos são limitados por requisitos de qualidade do produto e qualidade do processo. Os processos de gestão de projeto abrangem as ferramentas e técnicas envolvidas na aplicação das habilidades e capacidades para assegurar o fluxo eficaz do projeto através do seu ciclo de vida. Em cada uma das fases a metodologia deverá ser adequada às necessidades específicas da mesma, tendo em conta a exigência do trabalho a efetuar e das interligações com outras fases, projetos ou equipas.

Deverá ser uma preocupação da entidade a manutenção da componente aplicacional, por forma a garantir a sua atualização, que acompanha os desenvolvimentos tecnológicos e que atualiza os requisitos funcionais, observando as melhores práticas e os requisitos de segurança subjacentes às aplicações do SNS.

## 8. COMPETÊNCIAS TÉCNICAS

A existência de recursos humanos qualificados garante uma operacionalidade mais eficaz dos recursos tecnológicos nas entidades. Por consequência, as entidades deverão assegurar a existência de recursos internos ou externos (certificados) com os seguintes perfis técnicos:

- Administrador de sistemas;
- Segurança informática;
- Administrador de redes informáticas;
- Administrador de base-de-dados;
- Administrador aplicacional.

Em relação aos recursos internos, deverão as entidades prever um plano anual de formação (e reciclagem) para cada um dos perfis elencados, conforme prevê a legislação, e adaptado ao exercício das suas funções.

## 9. OPERAÇÃO

Neste domínio, a SPMS, EPE, para a prossecução eficaz das suas atribuições e responsabilidades, tem de conhecer de forma atempada e agendar, em articulação com as entidades, 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 Centros de Dados ou Salas de Sistemas.

Assim, importa que as entidades garantam o cumprimento rigoroso do seguinte circuito comunicacional, para além dos legalmente exigidos.

Qualquer intervenção com alcance e trato sensível, deverá ser agendada com 30 dias de antecedência, através do Portal Self-Service, para que possa usufruir de acompanhamento técnico por parte da SPMS, EPE, devendo para o efeito incluir 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;
- Equipa de intervenção com comprovativo de certificação;
- No caso de a entidade responsável ser externa, o âmbito contratual do qual resultam salvaguardas de segurança;

- Sistemas e aplicações que serão intervencionadas;
- Sistemas e aplicações que podem ser afetadas de forma direta ou indireta;
- Detalhe técnico da intervenção;
- Contato de e-mail e telemóvel do responsável pela intervenção da entidade;
- Risco para as diversas componentes intervencionadas na ação que se pretende executar.

Não se cumprindo o procedimento suprarreferido, não será possível à SPMS, EPE 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, estando em causa aplicações suportadas e/ou fornecidas pela SPMS, EPE, tal ocorrência consubstancia uma situação anómala e indesejada, com as consequências daí decorrentes.

A entidade tem a responsabilidade de garantir que todas as intervenções realizadas, quer no âmbito da infraestrutura, quer no âmbito aplicacional, têm suporte contratual com o prestador do serviço. Não se verificando este suporte, deverá, junto da SPMS, EPE, procurar apoio no sentido de uma possível resolução.

A entidade deve manter a documentação atualizada da arquitetura aplicacional e de infraestrutura existentes, submetendo-a até dia 31 de dezembro de 2019 para a SPMS, EPE através do e-mail ticadm@spms.min-saude.pt, com o assunto “Documentação de arquitetura - 2019”. (Validar se já enviaram alguma coisa para o atlas)

# 10. CONTINGÊNCIA E SITUAÇÕES DE CRISE

## 10.1. PLANO DE CONTINGÊNCIA

Independentemente da situação, será documentada e criada uma base de conhecimento que será posteriormente disponibilizada às entidades do SNS.

Neste contexto, devem as entidades ter aprovado, e pronto para ser partilhado com a SPMS, até 90 dias após publicação da presente Circular, o Plano de Contingência da área TIC.

Sem prejuízo de outra informação que a entidade considere relevante, o Plano de Contingência deve:

- Identificar a equipa e estrutura TIC, contatos da mesma e as áreas de responsabilidade;
- Incluir o plano de comunicação, prevendo:
    a. os clientes internos dos serviços;
    b. os clientes externos dos serviços;
- Tutela:
    a. as entidades terceiras com dependência (stakeholders);
- Indicar o ponto de contacto e os meios de contacto;

- Identificação, em caso de falha dos sistemas de informação:
    a. das unidades que funcionam 24X7;
    b. dos departamentos que sejam considerados críticos pela entidade.

## 10.2. MECANISMOS/MEIOS DE CONTACTO DA SPMS

Sem prejuízo de outro contacto mais direto, para os casos urgentes ou emergentes de indisponibilidade de serviços de sistemas críticos, devem as entidades privilegiar a utilização da plataforma *Self-Service*, divulgada pela Circular Normativa n.º 6 de 2017.

Alternativamente, para os casos que se verifique uma indisponibilidade de acesso à plataforma *Self-Service*, deverão usar o e-mail servicesk@spms.min-saude.pt ou o contato telefónico através do número +351 220 129 818.

## 10.3. AÇÕES E INFORMAÇÃO A REMETER

Qualquer incidente deve ser comunicado à SPMS, EPE através dos mecanismos/meios de contacto previstos e protocolados pela SPMS para o efeito, após a constatação do mesmo.

Qualquer reporte deve ser antecedido de um diagnóstico, identificando a causa raiz de um incidente, preferencialmente. No entanto, a participação do incidente antes de qualquer diagnóstico viabilizará, previsivelmente, uma resolução mais célere.

Sem prejuízo de informação relevante para a resolução do incidente, o reporte deve conter a seguinte informação:

- Identificação do(s) sistema(s) afetado(s);
- Descrição detalhada do incidente;
- Identificação das últimas ações realizadas no sistema em causa antes e depois do incidente;
- Identificação de um ponto único de contacto;
- Identificação clara dos departamentos da entidade considerados críticos em caso de falha dos sistemas de informação;
- Circuitos e plano de redundância do ponto de vista funcional;
- Existência de indisponibilidade de serviço ou não;
- Impacto e criticidade;
- Identificação e contatos (e-mail e telemóvel) do técnico da entidade que acompanha o incidente.

Sem prejuízo de outra informação que a entidade considere relevante, o reporte inicial deverá indicar, obrigatoriamente:

- Identificação e contatos (e-mail e telemóvel) do técnico da entidade que acompanha o incidente;
- o impacto e criticidade do incidente;
- um resumo sumário e a identificação, previsível, do(s) sistema(s) afetado(s).

A resolução dos incidentes deverá ser documentada com um reporte, devendo o mesmo incluir, além da informação incluída no reporte inicial:

- O histórico do incidente desde a sua abertura até à sua resolução;
- Identificação dos sistemas envolvidos;
- Identificação da causa raiz;
- Plano de remediação ou resolução;
- Histórico ou informação de contexto qua a entidade considere relevante.

## 11. SIMULACROS

Os simulacros são uma das boas práticas a adotar por forma a aferir o estado da componente das *facilities* do Centro de Dados da entidade. Por consequência as entidades devem prever anualmente um simulacro.

Nesse sentido, deverá ser elaborado um plano de simulacro, incluindo as seguintes situações:

- Falha da climatização do DataCenter;
- Falha do core de rede;
- Falha da(s) UPS(s) do DataCenter;
- Falha da energia elétrica geral e de geração da entidade;
- Paragem não programada de uma storage crítica, por exemplo, que aloja o SINUS ou o sistema de virtualização da entidade.

Após a aprovação do plano de simulacro pelo Conselho de Administração/ Conselho Diretivo da entidade, o mesmo deve ser remetido à SPMS, EPE, através do e-mail ticadm@spms.min-saude.pt, com o mínimo de 30 dias de antecedência relativamente à sua execução.

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

A falha de um dos componentes deverá ser reportada como um incidente, acompanhada de reporte.

## 12. LICENCIAMENTO

Os contratos de licenciamento geridos pela SPMS, como é o caso da Microsoft e Oracle, suportam apenas as componentes de software necessárias ao funcionamento dos sistemas centrais do Sistema de Informação de Saúde geridos pela SPMS. São exemplo o RNU, a PEM, o SICO, o SISO, etc. Nos sistemas locais apenas estão abrangidas, pelos mesmos contratos, as infraestruturas de servidores aplicacionais onde assentam sistemas de informação da SPMS.

No caso das licenças de Sistema Operativo Microsoft para os postos de trabalho, concedidas através do contrato de licenciamento gerido pela SPMS, são apenas licenças de atualização. Isto obriga a que todos os computadores adquiridos pelos organismos tragam pré-instalado o Sistema Operativo OEM suite Professional para que possam beneficiar das atualizações ao abrigo do contrato de licenciamento. Estas licenças são intransmissíveis de máquina para máquina, assim como as licenças de upgrade. Ferramentas colaborativas, como Office, Project, Viso, VisualStudio, Power BI, ou similares, não estão previstas no contrato. A SPMS inclui uma quantidade mínima de licenciamento para cobrir necessidades pontuais e urgentes nas entidades, mas que devem ser regularizadas pelas mesmas na sua devida altura. O Office 365, componente de Exchange Online, é assegurado às entidades mediante as políticas de utilização do serviço.

Relembramos a todos os organismos que os contratos de licenciamento que são geridos pela SPMS com parceiros externos, como por exemplo Microsoft, Oracle e outros, não suportam a manutenção ou a aquisição de licenciamento que não se enquadre nos pressupostos acima referidos. Cabe às entidades zelar para que todo o licenciamento sob a sua responsabilidade esteja regularizado e licenciado.

Face ao exposto, para que seja possível uma gestão atempada das necessidades de licenciamento, a SPMS recomenda aos organismos que, com a devida antecedência, prevejam estes valores nos seus orçamentos e informem a SPMS. Desta forma, torna-se possível efetuar agregação de necessidades, assegurando às Entidades a aquisição de licenciamento a preços acordados com os Fornecedores para a SPMS e o cumprimento dos prazos de entrega.

## 13. NOTAS

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.

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.

No caso dos Postos de Trabalho, ferramenta essencial do utilizador para acesso às aplicações, as Entidades devem evitar a sua obsolescência, promovendo revisões regulares e upgrades que possam promover o desempenho adequado à utilização dessas aplicações.

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, no que concerne aos Postos

de trabalho considera-se o seu fim de vida útil a partir do quinto (5) ano. Para ambos os casos é recomendada a sua substituição.

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 seu desempenho ficará aquém do desempenho de equipamentos mais atuais, impactando assim 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.

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

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.

As entidades devem garantir que, antes de qualquer alteração ao modelo de dados das aplicações produzidas pela SPMS, EPE, 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, EPE, a criação de um "utilizador" adequado a esse fim.

Lisboa, 25 de outubro 2019

O Presidente do Conselho de Administração

Henrique Manuel Gil Martins

Assinado de forma digital por Henrique Manuel Gil Martins
Dados: 2019.10.25 15:53:52 +01'00'

(Henrique Martins)

# ANEXO I

## 1. INFRAESTRUTURA - CENTRO DE DADOS E SALAS DE SISTEMA

### 1.1 NORMA TIA 942

A especificação ANSI / TIA-942 faz referência a requisitos de Centro de Dados no âmbito do domínio público e privado para as temáticas de âmbito e procedimentos, nomeadamente:

- Arquitetura de rede;
- Componente elétrica (projeto e cabelagem estruturada);
- *Storage*, backup e arquivo;
- Redundância dos sistemas;
- Controlo e segurança de acesso à rede;
- Gestão de Base de Dados;
- *Web Hosting;*
- *Application Hosting;*
- Distribuição de conteúdo;
- Controlo ambiental do Espaço do Centro de Dados (componente de *facilities*);
- Proteção contra riscos físicos (incêndio, inundação, tempestade);
- Gestão de energia.

A norma define ainda a topologia física dos espaços, por forma a segregar, sempre que possível, os equipamentos e infraestruturas de suporte (*facilities*). Paralelamente, recomenda uma segregação lógica por tipologia de ativo (*networking*, Computação, *Storage*), na disposição da sala.

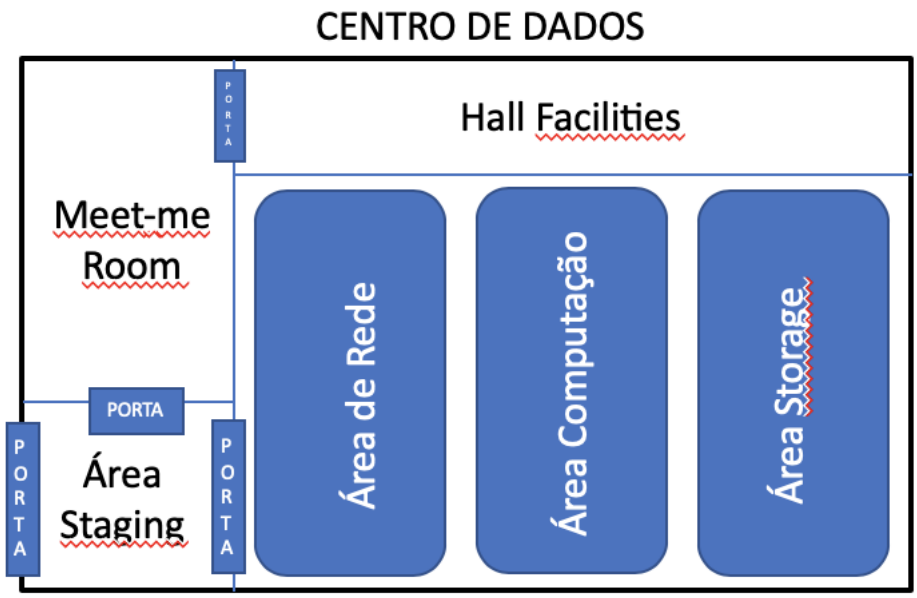


*Figura 2 - Tipologia física e lógica do Centro de Dados*

### 1.2 Níveis TIER e Requisitos

| Nível (Tier) | Requisitos |
|---|---|
| I | • Caminho de distribuição (elétrico; de Rede) único, não-redundante, que serve os equipamentos de TI;<br>• Infraestrutura do local com **componentes de capacidade não-redundantes** (quer seja ao nível das *facilities* (elétrica; Geração; *Uninterruptible Power Supply* - UPS; Aquecimento Ventilação e Ar Condicionado – AVAC), quer seja ao nível ao nível dos componentes de Tecnologias de Informação);<br>• Infraestrutura do local básico garantindo disponibilidade 99,671% (corresponde ter durante um ano o centro de dados indisponível até 1 dia, 4 horas, 50 minutes e 22 segundos). |
| II | • Cumpre todos os requisitos do Tier 1;<br>• Infraestrutura do local com componentes de capacidade redundante (quer seja ao nível das *facilities* (elétrica; Geração; *Uninterruptible Power Supply* - UPS; Aquecimento Ventilação e Ar Condicionado – AVAC), quer seja ao nível ao nível dos componentes de Tecnologias de Informação)<br>• Garante a disponibilidade de 99,741% (corresponde ter durante um ano o centro de dados indisponível até 22 horas, 4 minutes e 20 segundos). |
| III | • Cumpre todos os requisitos Tier 1 e Tier 2;<br>• Múltiplos caminhos de distribuição (elétrico; de Rede) mas independentes, que servem os equipamentos de TI;<br>• Todos os equipamentos de TI devem ter fonte de alimentação redundante e totalmente compatíveis com a topologia da arquitetura do local;<br>• Infraestrutura local paralelamente sustentável, garantindo a disponibilidade de 99,982% (corresponde ter durante um ano o centro de dados indisponível até 1 horas, 34 minutes e 44 segundos). |
| IV | • Cumpre todos os requisitos Tier 1, Tier 2 e Tier 3;<br>• Infraestrutura do local com componentes de capacidade totalmente redundantes (ao nível das *facilities* (elétrica; Geração; *Uninterruptible Power Supply* - UPS; Aquecimento Ventilação e Ar Condicionado – AVAC)<br>• Infraestrutura local tolerante a falhas, com instalações de armazenamento para distribuição de energia elétrica (depósitos de combustível de grande capacidade para alimentação dos geradores e contratos de abastimento de combustível com operadores de fuel), garantindo a disponibilidade de 99,995% (corresponde ter durante um ano o centro de dados indisponível até 26 minutes e 18 segundos). |

## 1.3 INFRAESTRUTURA - PASSIVOS DE REDE LOCAL

Os passivos das LAN devem cumprir com a legislação nacional, nomeadamente:

- ITED3 (Infraestruturas de telecomunicações em edifícios) e ITUR (Infraestruturas de telecomunicações em loteamentos, urbanizações e conjuntos de edifícios);
- O standard internacional IEEE 802.3 de 2018 (é um standard sobre ethernet atualizado em 2018);

Em relação ao tipo de cabelagem a usar, na componente de Cobre deverão ser usados cabos CAT 6. Em termos de fibras óticas deverão ser usadas fibras OM4 multimodo otimizado de 50 µ/125 µ, que garante uma velocidade de até 10 Gigabit Ethernet em distâncias até 550m (Comprimento de onda: 850nm).

Em relação à topologia das infraestruturas de rede LAN deverão ser implementas em estrela e hierarquizada. As soluções a implementar deverão ter em consideração as seguintes hierarquias:

| Nível (Tier) | Requisitos |
|---|---|
| II | • Implementação de um sistema de *Core* que também poderá ter funções de distribuição onde serão ligados os equipamentos de acesso que irão garantir a conectividade aos utilizadores. |
| III | • Implementação de um sistema de *Core* que deverá ligar a sistemas de *Core* de distribuição, e este, por sua vez, ligar aos equipamentos de acesso que irão garantir a conectividade aos utilizadores. |

# ANEXO II

## 1. INFRAESTRUTURAS DE ATIVOS DE REDE

As ligações entre os *switchs* de *Core* e os *switchs* de acesso (*backbone*) devem ser garantidos 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.

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 e sempre em redundância.

Relativamente aos *switchs* de distribuição na LAN, devem estar asseguradas velocidades a 1Gb e com suporte PoE (*Power over Ethernet*) por porta, garantindo que as ligações entre *switchs* serão no mínimo a 10Gb em fibra ótica de última geração.

A interligação dos *switchs* de distribuição (nos casos em que existem vários *switchs* no mesmo espaço físico de bastidor) deverá ser feita, preferencialmente, em cascata, através dos cabos específicos e proprietários, para interligar equipamentos do mesmo fabricante) e a ligação ao *core* por fibras redundantes e a partir de equipamentos distintos.

Lista exemplificativa de protocolos standards do *Institute of Electrical and Electronics Engineers* – IEEE

| Característica | Especificação |
|---|---|
| Protocolos Standard | • IEEE 802.1d,<br>• IEEE 802.1p,<br>• IEEE 802.1q,<br>• IEEE 802.1s,<br>• IEEE 802.1w,<br>• IEEE 802.3x,<br>• IEEE 802.3ad,<br>• IEEE 802.3z,<br>• IEEE 802.3ab,<br>• IEEE 802.3ae,<br>• IEEE 802.3ak,<br>• IEEE 802.3aq, e<br>• IEEE 802.3an |

# ANEXO III

## 1. INFRAESTRUTURAS DE SISTEMAS

Garantir que não existem sistemas com um desfasamento superior a 2 versões de antiguidade.

Garantir a aplicação de *patchs* periodicamente, observando a criticidade dos mesmos por forma a escrutinar os mais ou menos críticos.

A utilização, em postos de trabalho, de sistema operativos *legacy*, designadamente, Windows 7 e Windows vista, só deverão ser autorizados com a ressalva específica de exceção, para as aplicações que exigem esse tipo de sistema operativo para funcionarem.





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 IV

## 1. SEGURANÇA FÍSICA E MONITORIZAÇÃO

As soluções de videovigilância deverão cumprir adicionalmente os seguintes requisitos:

- A alimentação das câmaras de videovigilância - fixas ou móveis – deverá ser feita por PoE (802.3af, 802.3at ou 802.3bt)[5];
- No caso de câmaras instaladas no exterior dos edifícios, deverá ser considerada cablagem STP, devidamente ligada à terra;
- Câmaras fixas ou móveis, com um mínimo de resolução 1080p e codificação H.264 ou H.265 e com capacidade de correr analíticas diretamente na câmara;
- No caso dos locais onde se pretende o reconhecimento e/ou identificação de pessoas ou matrículas (entrada/saída de edifícios ou de estacionamentos, datacenter, etc.), deverão considerar-se as seguintes métricas:
    - reconhecimento: 17 pixels por face (ou 100 pixels/metro);
    - identificação: 40 pixels por face (ou 250 pixels/metro);
    - leitura de matrículas: 150 pixels por matrícula.
- O sistema de gravação deverá estar dimensionado para a gravação por movimento de todas as câmaras do sistema por um período de 30 dias, com os seguintes requisitos mínimos:
    - Resolução 1080p (1920x1080);
    - 6 imagens por segundo;
    - Codificação H.264 ou H.265;
    - Compressão máxima de 30%.

As soluções de Controlo de Acessos deverão cumprir adicionalmente os seguintes requisitos:

- No que diz respeito à infraestrutura de suporte aos controladores, deverá ser em UTP Categoria 6 (ou STP, no caso de haver controladores no exterior);
- A ligação dos controladores deverá ser exclusivamente IP (ou seja, não devem ser utilizadas ligações em BUS RS-485, ressalvando apenas o caso da ligação dos leitores aos controladores, quando os leitores não forem IP) e alimentação por PoE (802.3af, 802.3at ou 802.3bt);
- Sempre que necessário, deverá ser reforçada essa alimentação para suportar os equipamentos de abertura (testas elétricas, retentores, eletroimans, etc.), com cablagem de energia adequada. Nestes casos, cada circuito deverá estar protegido por disjuntor diferencial adequado junto ao

[5] No caso da PoE 802.3bt, em particular o tipo 4 (100W), é necessário que a cablagem seja no mínimo Cat6A, devido à capacidade de melhor dissipação de calor;

quadro elétrico mais próximo, e devidamente identificado com "SISTEMA DE CONTROLO DE ACESSOS";

- Os leitores deverão ser IP (ou seja, com controlador incluído) e/ou ligação ao controlador por protocolo OSDP[6]. Deverão suportar cartões ISO/IEC 14443.[7]

De modo a garantir uma operação coerente e fluída entre os vários módulos de segurança (videovigilância, controlo de acessos, intrusão, analítica de vídeo, etc), deverá ser implementada uma solução unificada de segurança que garanta essa ligação entre os vários módulos de segurança.

[6] Relativamente ao antigo protocolo Wiegand, o OSDP permite encriptação, comunicação bidirecional, uma maior distância de cabo até ao controlador (até 500 metros) e suporte bidirecional para comunicação de dados biométricos;

[7] 13.56 MHz (Mifare/Desfire ou iClass). Os cartões mais antigos funcionavam nos 125Khz e são muito fáceis de clonar