SONHO
Sistema de Cuidados de Saúde Hospitalares

SClínico
Sistema de Cuidados de Saúde Hospitalares

BOAS PRÁTICAS

GESTÃO E MONITORIZAÇÃO DE ACESSOS AO SONHO E SCLÍNICO HOSPITALAR

REPÚBLICA PORTUGUESA
SAÚDE

SNS
SERVIÇO NACIONAL DE SAÚDE

SPMS EPE
Serviços Partilhados do Ministério da Saúde

1 | CONSIDERAÇÕES GERAIS
1.1 | PRINCÍPIOS BASE

Na disponibilização de acessos aos sistemas de informação que se revelem necessários ao exercício de funções pelos trabalhadores, fornecedores e partes interessadas, devem ser observados os seguintes princípios:

IDENTIDADE

Os utilizadores dos sistemas devem ser únicos, individuais e intransmissíveis. Os colaboradores são responsáveis pela respetiva conta e devem proteger a identidade que lhes seja atribuída. Salvo quando tal resulte necessário em virtude de imperativos de negócio ou operacionais extraordinários e devidamente identificados na documentação da conta, é proibida a criação de utilizadores genéricos ou de grupo. Deve ser vedado aos referidos utilizadores o acesso a informação confidencial ou secreta ou a informação pessoal de outros colaboradores, utilizadores, partes interessadas ou utentes.

RESTRIÇÃO DE CONTAS PRIVILEGIADAS

A atribuição de contas privilegiadas (*e.g. administrador*, *super-user*, *root*, *gestor de sistema ou similares*) deve ser controlada e restringida ao mínimo necessário. Este tipo de contas não deve ser atribuído por defeito. Ademais, a atribuição de contas privilegiadas deve ser limitada aos trabalhadores responsáveis pelas administração e gestão das aplicações e sujeita a processo de aprovação que inclua responsáveis pelos sistemas respetivos e pela área de segurança. Este processo deverá contemplar, também, o registo dos privilégios especiais concedidos.

ACESSOS MÍNIMOS

Apenas devem ser atribuídos aos colaboradores os acessos necessários à execução das respetivas funções. Aconselha-se a catalogação dos diferentes perfis de acesso necessários à condução das atividades de negócio, de acordo com as funções existentes na instituição. Esta catalogação deverá refletir os acessos aos sistemas de informação disponibilizados na Instituição, independentemente do fornecedor, com menção dos respetivos titulares e das ações passiveis de serem realizadas.

SEGREGAÇÃO DE FUNÇÕES

Deve ser evitada a acumulação de funções críticas no sistema pelo mesmo trabalhador, sob pena de aumentar a probabilidade de comportamentos maliciosos e/ou fraudes;

AUDITORIA

Os sistemas de informação devem compreender um registo das atividades relacionadas com acessos, que permita escrutinar todas as operações de gestão, administração e acessos de utilizadores, incluindo tentativas de login e ações realizadas pelos mesmos.

ACESSOS EM CONTEXTO

Os profissionais devem aceder exclusivamente à informação necessária ao exercício das respetivas funções e apenas quando se verifique um motivo válido para o efeito.

1.2 | ORIENTAÇÕES

Os principais objetivos da gestão de acessos poderão ser atingidos através do cumprimento das seguintes premissas:

- Os sistemas de informação apenas podem ser objeto de acessos autorizados;
- Os acessos não autorizados a serviços disponíveis nos sistemas de informação devem ser impedidos;

- O comprometimento ou roubo de informação devem ser impedidos;

De forma a garantir o cumprimento destas premissas, devem ser definidas e seguidas orientações que permitam:

- Identificar e registar os utilizadores dos sistemas de informação;
- Restringir e gerir a atribuição de acessos privilegiados;
- Rever periodicamente os utilizadores existentes e os respetivos privilégios e permissões;
- Gerir credenciais de acesso atribuídas aos utilizadores;
- Identificar os serviços e informação a disponibilizar aos trabalhadores, de acordo com as funções respetivas;
- Identificar controlos de acessos a implementar nos sistemas de informação;
- Formar e instruir trabalhadores em matéria de gestão de acessos; e
- Controlar e monitorizar os acessos e ações efetuadas pelos colaboradores nos sistemas de informação, com recurso aos instrumentos de auditoria disponíveis ou a disponibilizar.

2 | GESTÃO DE ACESSOS DE UTILIZADORES

A identificação unívoca de cada trabalhador deve obedecer a uma nomenclatura-tipo.
Todos os utilizadores dos sistemas devem estar registados com informação relativa ao seu perfil de utilizador.
Devem ser definidas regras relativas à gestão e utilização de palavras-passe dos utilizadores. Às palavras-passe de utilizadores com contas privilegiadas (e.g. administradores de sistemas) devem aplicar-se regras mais rígidas. A atribuição de privilégios deve ser efetuada ao abrigo de um processo formal de autorização e numa base de privilégios mínimos para desempenho de funções de acordo com o modelo de funções em vigor.
Para além do processo de autorização, deve ainda existir um processo de revisão periódica dos direitos de acesso dos utilizadores. Os resultados da referida revisão devem ser documentados e armazenados centralmente.

As contas de utilizador devem ser imediatamente desativadas após o término ou a suspensão do vínculo contratual ou de colaboração.

A criação de contas de teste deve ser evitada. As atividades de formação contínua devem recorrer aos ambientes de teste existentes nas instituições, ou ao ambiente centralizado disponibilizado pela SPMS a todas as instituições.

3 | CONTROLO DE ACESSOS AOS SISTEMAS

Os sistemas operativos devem contemplar mecanismos de segurança que permitam restringir ou prevenir o acesso não autorizado aos computadores.

O sistema de gestão de palavras-passe de acesso aos sistemas deve ser interativo e garantir a qualidade das mesmas. O uso de aplicações que se sobreponham e permitam contornar os mecanismos de segurança dos sistemas deve ser totalmente proibido.

Deve ser considerada a implementação de controlos de tempo das ligações, especialmente no caso de sistemas situados em localizações de alto risco.

A gestão de acessos deve ser efetuada de acordo com o ciclo de vida da gestão de acessos: atribuição, alteração, revisão e remoção de acessos.

A criação de contas de utilizador deve ser efetuada mediante autorização explícita do superior hierárquico ou estar prevista como etapa na admissão de novos profissionais, sendo a gestão dos perfis

atribuídos da responsabilidade de cada instituição, assegurando que os privilégios dos mesmos são prontamente atribuídos, alterados ou removidos conforme a necessidade e com recurso a um ciclo de aprovações definido. Para os colaboradores já vinculados, devem as mesmas ser revistas no que concerne a conformidade com as boas práticas emanadas.

Sempre que se verifique a cessação dos fundamentos que determinaram a concessão de acesso a um sistema de informação, o referido acesso deverá ser removido. Cada instituição deverá proceder a uma revisão periódica dos acessos concedidos, que permita identificar a existência de eventuais acessos não justificados. A referida revisão deverá ter lugar, pelo menos, duas vezes por ano e resultar na produção de evidências suficientes para comprovar a respetiva efetividade.
Os direitos de acesso aos sistemas de informação deverão ser removidos quando a conta de utilizador:

- Esteja em risco ou tenha sido comprometida;
- Esteja, ou possa vir a, estar inativa por um período de 90 (noventa) dias consecutivos.

As contas que não se encontrem associadas a um trabalhador deverão ser prontamente apagadas ou desabilitadas de forma a impedir o respetivo uso.

4 | REGRAS RELATIVAS A PALAVRAS-PASSE

No acesso aos sistemas de informação, os utilizadores autorizados deverão autenticar-se através de um procedimento seguro de entrada nos sistemas (i.e. *login*), com recurso a palavras passe individuais.

Este procedimento deverá ser desenhado de forma a minimizar as hipóteses de entrada não autorizada no sistema, cumprindo os seguintes critérios mínimos:

O sistema deverá exibir um aviso geral de que o computador apenas pode ser acedido por utilizadores autorizados para o efeito;
O sistema deverá limitar o número permitido de tentativas de entradas no sistema (i.e. tentativas de *login*) sem sucesso;
As credenciais de acesso introduzidas pelo utilizador não deverão ser exibidas ou, em alternativa, o sistema deverá ocultar os caracteres das credenciais substituindo-os por símbolos;
As informações introduzidas no sistema deverão ser validadas apenas quando todos os dados estiverem completos. Caso ocorra uma condição de erro, o sistema não deverá indicar o segmento de informação correta ou incorretamente introduzido; e
As credenciais de acesso não deverão ser transmitidas sem encriptação na rede.
Deverá ser contemplada, quando possível, a configuração de um tempo máximo de ligação e de desconexão por inatividade do utilizador ou terminal caso esse limite seja atingido.

4.1 | ESCOLHA DE PALAVRA-PASSE

A cada utilizador deverá estar associada uma palavra-passe forte, ou seja, uma palavra-passe desenhada de forma a que seja improvável o respetivo roubo ou deteção. Os sistemas de gestão de palavras-passe devem forçar a boa qualidade das mesmas.

Na criação de palavras-passe fortes deverão ser seguidas as seguintes regras:

- Nunca deverão ter valor nulo;
- Mínimo de 8 (oito) caracteres;
- Verificação dos requisitos previstos nas alíneas seguintes:
    - Letras maiúsculas (*i.e.* A-Z);
    - Letras minúsculas (*i.e.* a-z);
    - Caracteres numéricos (*i.e.* 0-9);
    - Caracteres especiais (*e.g.* !#$%&)

Não deverão ser utilizadas palavras únicas do dicionário, datas ou outros elementos facilmente associáveis ao trabalhador.

A seleção ou utilização incorreta da palavra-passe poderá colocar em risco a segurança e comprometer a confidencialidade, integridade e disponibilidade dos sistemas de informação da instituição. Independentemente da validação, à partida, pelos sistemas, do cumprimento dos critérios invocados, devem os utilizadores zelar pelo cumprimento destes requisitos aquando da definição das suas credenciais.

4.2 | PROTEÇÃO DE PALAVRA-PASSE

As palavras-passe devem ser protegidas durante todo o respetivo tempo de vida. Devem, assim, observar-se as seguintes regras relativas a contas de utilizador:

- As palavras-passe atribuídas por *default*, i.e., atribuídas automaticamente pelos sistemas de informação, devem ser objeto de alteração antes da realização de qualquer ação pelo respetivo utilizador;
- As palavras-passe de cada utilizador devem ser objeto de alteração a cada 90 (noventa) dias;
- A alteração de palavras-passe deve compreender a possibilidade de não repetição das últimas utilizadas.

Sem prejuízo do acima referido, deverão ser seguidas pelos utilizadores as seguintes regras para todo o tipo de contas:

- Não revelar palavras-passe;
- Encerrar todas as sessões antes de abandonar o local de trabalho;
- Não registar palavras-passe em qualquer tipo de suporte;
- Não armazenar palavras-passe em locais de onde as mesmas possam ser subtraídas;
- Não utilizar partes do nome de utilizador na palavra-passe;
- Não utilizar a mesma palavra-passe em aplicações dentro e fora do contexto profissional;
- Não utilizar a funcionalidade "lembrar palavra-passe" disponível nos browsers;
- Cumprir com os critérios de complexidade de palavra-passe mencionados.

As palavras-passe devem ser objeto de alteração imediata caso se verifique uma fundada suspeita de que as mesmas foram comprometidas.

REPÚBLICA PORTUGUESA
SAÚDE

SNS
SERVIÇO NACIONAL DE SAÚDE

SPMS EPE
Serviços Partilhados do Ministério da Saúde