MANUAL DE CIBERSEGURANÇA
para Farmacêuticos

REPÚBLICA PORTUGUESA
SAÚDE
SNS SERVIÇO NACIONAL DE SAÚDE
SPMS EPE Serviços Partilhados do Ministério da Saúde
CIBERSEGURANÇA SNS

INTRODUÇÃO

Não é novidade que o cibercrime é um negócio global rentável e os ataques a setores que envolvem dados pessoais sensíveis, como o da Saúde, mostram ser ainda mais lucrativos pois contêm dados permanentes de identificação, como o nº de Utente.

Um ataque de *Ransomware* (vírus que provoca impedimento de acesso a registos, sistemas ou dispositivos até ao pagamento de resgate) poderá impossibilitar a consulta da terapêutica a administrar ao utente e, em certos casos, ser decisivo na sua saúde.

QUAIS OS RISCOS?

- Impressão de fichas de utentes em farmácias;
- Computadores desbloqueados no atendimento ao público;
- Partilha das mesmas credenciais de acesso entre colegas de trabalho;
- Clicar em hiperligações de origem duvidosa.

NÃO SE ESQUEÇA: A SEGURANÇA DO UTENTE TAMBÉM DEPENDE DA SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA!

Assim como no dia-a-dia do farmacêutico, quer trabalhe em farmácia comunitária quer em hospitalar, o tratamento eficiente do utente depende da administração correta da terapêutica, também faz parte do papel do farmacêutico proteger os utentes da exposição dos seus dados pessoais a terceiros, bem como do acesso indevido, alterações, destruição ou impossibilidade de acesso.

COMO AGIR?

TAL COMO...

Verificamos diariamente o *stock* dos medicamentos, damos entrada dos pedidos e retiramos lotes por questões de qualidade

DEVEMOS TAMBÉM...

Confirmar que não existe nenhuma atualização de sistema por executar ou mensagens de erro por validar.

TAL COMO...

Damos baixa dos medicamentos através da leitura do código de barras

DEVEMOS TAMBÉM...

Terminar sempre a nossa sessão após determinada utilização do sistema.

TAL COMO...

Existe uma norma para identificar os medicamentos (p.e. o nome da substância ativa, a dosagem, o lote, validade)

DEVEMOS TAMBÉM...

Basear-nos nas boas práticas da criação de *passwords* como usar uma frase-passe longa que inclua números e caracteres especiais.

TAL COMO...

Aconselhamos os nossos doentes a respeitarem a posologia prescrita de antibióticos para evitar o aparecimento de resistências

DEVEMOS TAMBÉM...

Ter a noção que todos os dias surgem vírus diferentes e por isso temos de manter os sistemas atualizados.

TAL COMO...

Não partilhamos a bata com os nossos colegas nem partilhamos as tiras e agulhas usadas na medição de parâmetros bioquímicos

DEVEMOS TAMBÉM...

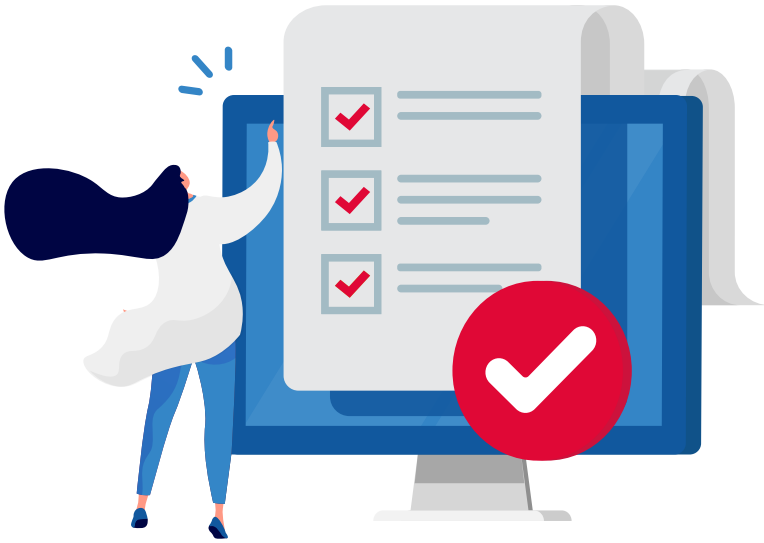
Utilizar apenas as nossas credenciais de acesso nos sistemas e nunca as de colegas.

TAL COMO...

Antes de dispensarmos uma medicação a um utente confirmamos se existem contraindicações que desaconselhem o seu uso

DEVEMOS TAMBÉM...

Verificar a lista de *software* autorizado antes de instalar algo no computador profissional pois pode estar em causa a instalação de vírus que poderá comprometer os dados existentes nesse PC.



TAL COMO...

Ouvimos com atenção os sintomas do utente e fazemos um aconselhamento individual e personalizado

DEVEMOS TAMBÉM...

Cumprir a boa-prática de utilizar uma *password* diferente para cada sistema e dispositivo, minimizando o possível roubo de *passwords* e respetivas consequências.

TAL COMO...

Protegemos a saúde dos nossos utentes ao informarmos como deve ser realizada a toma da medicação

DEVEMOS TAMBÉM...

Proteger os sistemas ao não abrirmos ou clicarmos em hiperligações de origem desconhecida.

TAL COMO...

Revemos o historial clínico do doente e contactamos o médico caso exista uma interação medicamentosa potencialmente prejudicial ao utente

DEVEMOS TAMBÉM...

Contactar o Departamento Informático/Suporte Técnico caso tenhamos alguma dúvida relacionada com a segurança da informação e Cibersegurança ou caso queiramos reportar um incidente.

TAL COMO...

Em hospital, manipulamos e preparamos de forma individualizada alguma medicação com base nas necessidades especiais de cada utente sempre na Câmara de Fluxo Laminar, por questões de esterilidade e segurança

DEVEMOS TAMBÉM...

Garantir que não conectamos nenhum dispositivo pessoal, seja uma *pen USB* ou telemóvel, aos computadores de trabalho e às redes da organização.

TAL COMO...

Fazemos formação para administrar injetáveis a utentes e estamos atualizados sobre novas opções terapêuticas

DEVEMOS TAMBÉM...

Fazer ações de sensibilização em Segurança da Informação e Cibersegurança e conhecer o procedimento a adotar em caso de incidente.

TAL COMO...

Antes de medirmos a tensão a um utente falamos um pouco com ele para o deixar mais relaxado e não interferir com os resultados

DEVEMOS TAMBÉM...

Ler calmamente cada e-mail e desconfiar sempre se este tiver origens e objetivos maliciosos.

10 MANDAMENTOS DA CIBERSEGURANÇA

Hardware

Não colocarás pens alheias
no PC de trabalho

Não deixarás o teu PC desbloqueado,
mesmo entre amigos ou colegas

Software

Não esquecerás os *backups*
e apostarás na redundância

Não esquecerás o antivírus

PeopleWare

Não cobiçarás *phishing* alheio

Assumirás o papel de melhor linha
de defesa contra os ciber-ataques

LocalWare

Não desejarás trabalhar fora
de ambientes e redes seguras

Não partilharás *passwords*
e códigos de acesso

IntegraWare

Amarás as medidas de segurança
sobre todas as coisas

Não procrastinarás as atualizações,
mesmo aos domingos e feriados