MANUAL DE CIBERSEGURANÇA

para os Enfermeiros

REPÚBLICA PORTUGUESA SAÚDE
40 ANOS SNS SERVIÇO NACIONAL DE SAÚDE 1979-2019
SPMS Serviços Partilhados do Ministério da Saúde
Cibersegurança SNS

INTRODUÇÃO

Sabia que a saúde é um dos setores mais aliciantes para os *hackers*? Para além dos dados de saúde serem mais sensíveis e lucrativos do que os dados bancários no mercado negro (por conterem dados permanentes de identificação, como o nº de Utente), também é o setor mais vulnerável a ataques.

Se para um melhor e mais eficiente cuidado ao utente, é necessário que os profissionais de saúde tenham hábitos e procedimentos de higiene, também os hábitos de ciberhigiene são essenciais!

QUAIS OS RISCOS?

- Divulgação de informação em carros de terapêutica ou salas abertas/comuns;
- Computadores desbloqueados nos serviços;
- Partilha das mesmas credenciais de acesso entre colegas de trabalho;
- Clicar em hiperligações de origem duvidosa.

Salvaguardar os dados pessoais do utente e impedir a sua exposição a acessos indevidos é um dever de todos nós. A segurança do utente também depende da Segurança da informação e cibersegurança!

Ao longo dos anos tem havido um aumento considerável de ataques informáticos na saúde. O meio mais comum de ataque é por e-mail, através de *phishing* (roubo de informação) ou *ransomware* (um tipo de ataque que impede o acesso a informações, sistemas ou dispositivos, até que seja pago o valor exigido como resgate). Em 2026 Estados Unidos da América, um ataque de *ransomware,* ao Hollywood Presbyterian Medical Center, desligou a rede por 10 dias, impediu (PASSADO) o *staff* de aceder a registos médicos ou de usar equipamentos médicos até ser pago o suborno. Já em 2017, no Reino Unido, o vírus WannaCry custou ao NHS (National Health System) 92 milhões de libras e causou o cancelamento de 1900 tratamentos e o redireccionamento dos utentes.

COMO AGIR?

TAL COMO...

Quando começamos um turno, mudamos o calçado, vestimos a bata e pegamos no material de trabalho.

DEVEMOS TAMBÉM...

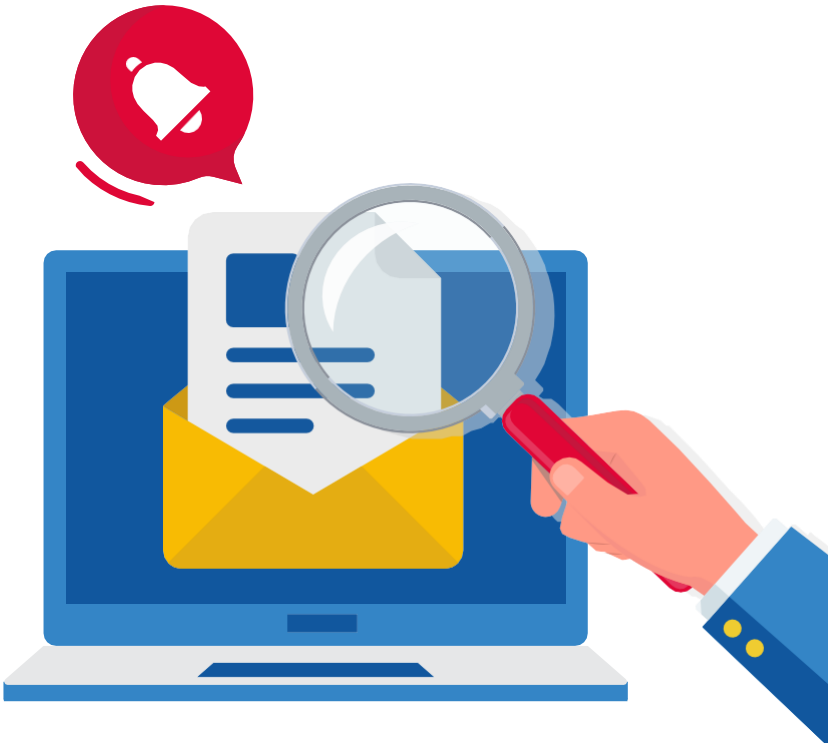
Garantir que não conectamos nenhum dispositivo pessoal, seja uma *pen drive* ou telemóvel, aos computadores de trabalho e às redes da organização.

TAL COMO...

Fechamos a cortina para proteger a privacidade do utente.

DEVEMOS TAMBÉM...

Minimizar janelas ou separadores com informação dos utentes e bloquear os computadores, mesmo que por breves períodos de ausência.

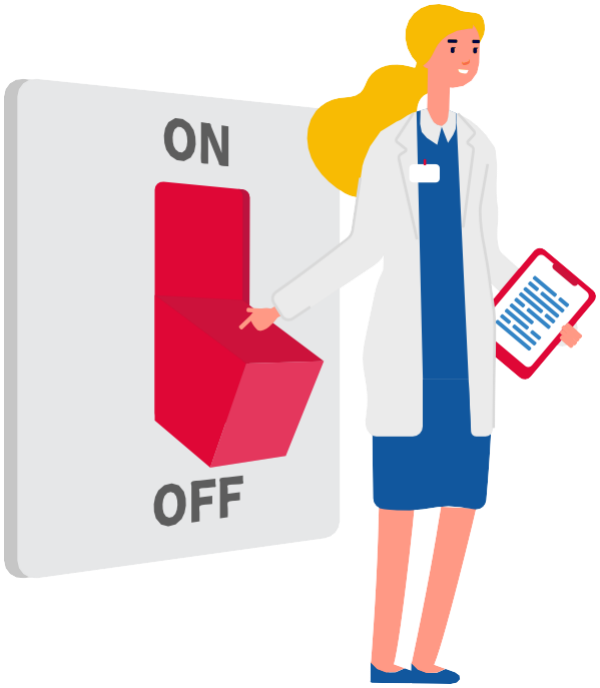


TAL COMO...

Recebemos o utente e analisamos com cuidado os seus sintomas.

DEVEMOS TAMBÉM...

Ler atentamente cada e-mail e desconfiar sempre quando tiver origens e objetivos maliciosos.



TAL COMO...

Ajudamos a certificar que as operações são concluídas com sucesso.

DEVEMOS TAMBÉM...

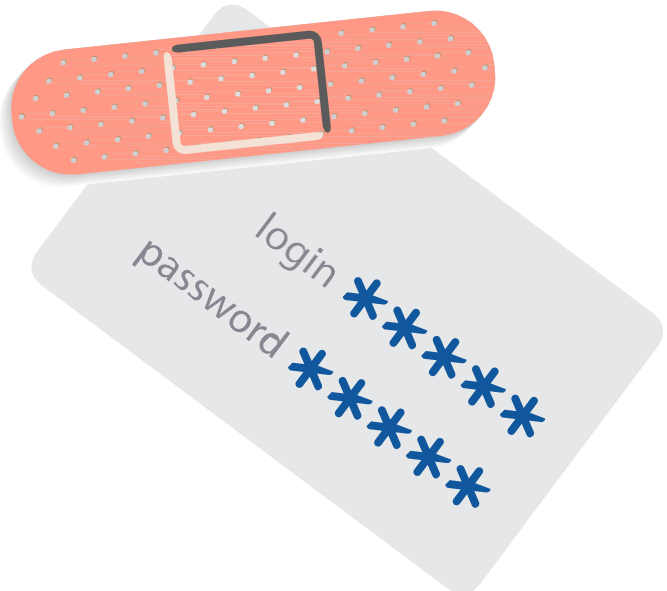
Compreender que, ao partilharmos um computador de trabalho, devemos sempre terminar a sessão após uma determinada utilização do sistema.

TAL COMO...

Não utilizamos o mesmo material de realização de penso para utentes diferentes.

DEVEMOS TAMBÉM...

Usar apenas a nossa credencial de acesso aos sistemas e nunca a de colegas.



TAL COMO...

Limpamos e desinfetamos as feridas, e fazemos um penso para prevenir a contaminação por bactérias externas aos nossos utentes.

DEVEMOS TAMBÉM...

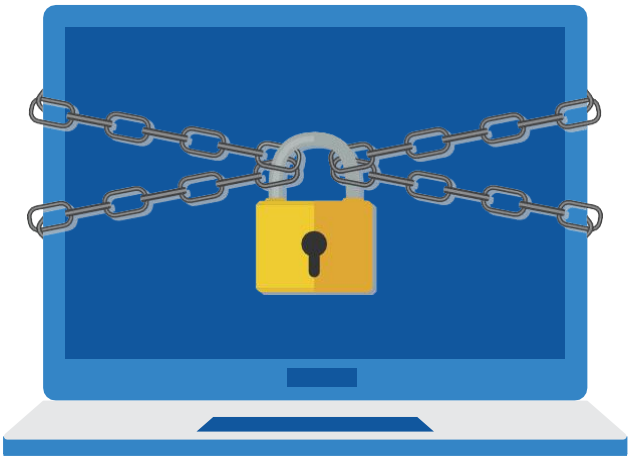
Estar alerta para possíveis anomalias dos antivírus e *firewall,* e, se detetadas, reportar ao Departamento Informático.

TAL COMO...

Contactamos o médico responsável em caso de dúvida.

DEVEMOS TAMBÉM...

Contactar o Departamento Informático caso tenhamos alguma dúvida relacionada com a segurança de informação ou reportar um incidente.



TAL COMO...

Na passagem de turno, partilhamos informação clínica com os nossos colegas num local privado.

DEVEMOS TAMBÉM...

Verificar que a informação partilhada digitalmente é feita de uma forma segura e que apenas os destinatários pretendidos têm acesso.

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