

CARTILHA DOS GUARDIÕES DE DADOS



AINDA NÃO CONHECE OS

**10 PASSOS DA SEGURANÇA
DA INFORMAÇÃO?**

Comitê de Segurança da Informação - CSI



CH-UFC / HU BRASIL

CARTILHA DOS GUARDIÕES DE DADOS

SEGURANÇA DA INFORMAÇÃO

OS GUARDIÕES DE DADOS DO CH-UFC/HU BRASIL

Proteger dados é proteger vidas!

Bem-vindo à Cartilha dos Guardiões de Dados do CH-UF-C / HU Brasil.

Aqui você encontrará orientações simples para proteger informações, preservar a privacidade dos pacientes e contribuir para um ambiente mais seguro para todos.

**Segurança da Informação é
responsabilidade de todos!**



Você sabia?

No CH-UFC / HU Brasil, todos os dias lidamos com informações importantes.



Dados de pacientes



Prontuários



Exames



Sistemas institucionais



Pesquisas



Documentos

Quando essas informações não são protegidas, podem ocorrer:



Vazamentos de dados



Fraudes



Interrupção de serviços



Danos aos pacientes e
à instituição

Por isso, cada trabalhador é um **Guardião de Dados**



CH-UFC / HU BRASIL

SEGURANÇA DA INFORMAÇÃO

OS 10 PASSOS DO GUARDIÃO

Um guia prático para proteger dados e vidas dentro do nosso CH-UFC/HU Brasil.

- 1 Proteja dados de pacientes
- 2 Guarde documentos só em locais autorizados
- 3 Nunca compartilhe senha
- 4 Use canais institucionais seguros
- 5 Acesse apenas o necessário
- 6 Bloqueie a tela ao se afastar
- 7 Desconfie de links suspeitos
- 8 Evite Wi-Fi público ou desconhecido
- 9 Notifique incidentes rapidamente
- 10 Segurança é missão de todos



No CH-UFC/HU Brasil, cada trabalhador é **parte essencial da proteção das informações**

PASSOS 1, 2 E 3

1

Não espalharás dado de paciente, nem por acidente!

Informações de pacientes são sigilosas. Mesmo comentários aparentemente inocentes podem causar exposição indevida.



Pense antes de falar ou compartilhar!



2

Não guardará prontuário no pendrive da vida, isso é furada garantida!

Utilize apenas locais autorizados para armazenar documentos institucionais. Pendrives podem ser perdidos, roubados ou contaminados por vírus.



Use os repositórios institucionais autorizados



3

Não passará tua senha pra ninguém, nem pro amigo "gente boa também".

Sua senha é pessoal e intransferível!



Pense antes de falar ou compartilhar!



PASSOS 4, 5 E 6

4

Não mandarás laudo no “zap” ou e-mail pessoal, isso é cilada digital!

Utilize apenas os canais autorizados pelo hospital para enviar informações institucionais e documentos sensíveis.



Na dúvida, confirme o canal correto



5

Não bisbilhotarás prontuário alheio, curiosidade aqui é devaneio!

Acesse somente informações necessárias para o seu trabalho.
Consulta sem finalidade profissional compromete a privacidade do paciente.



Acesso deve ter necessidade e finalidade



6

Não deixarás tela aberta, computador sem trava vira festa!

Ao sair da estação de trabalho, pressione **Windows + L** e bloqueie sua sessão.
Proteja as informações mesmo durante ausências rápidas.



Levantou? Bloqueou!



PASSOS 7 E 8

7

Não clicarás em link duvidoso, vírus chega sorrateiro e perigoso!

Antes de clicar, confira o remetente, verifique o endereço do site e desconfie de urgências excessivas.

✓ Na dúvida, não clique!



8

Não usarás Wi-Fi esquisito, aberto demais é sempre esquisito!

Evite acessar sistemas institucionais em redes públicas ou desconhecidas. A segurança começa pela conexão.

📶 Prefira redes confiáveis e autorizadas!



Links e redes desconhecidas são portas comuns para golpes. Pare, confira e peça orientação quando necessário.

PASSOS 9 E 10

9

Notificarás na hora se algo estranho acontecer!

Recebeu um e-mail suspeito? Perdeu um equipamento? Percebeu atividade incomum? Comunique imediatamente a equipe responsável.



Quanto mais rápido o aviso, menor o impacto



10

E lembrarás sempre com o coração: proteger dados é nossa missão!

A tecnologia ajuda, as normas orientam, mas a segurança depende principalmente das pessoas. Você faz a diferença!



Quanto mais rápido o aviso, menor o impacto



Proteger dados é proteger vidas!

CH-UFC / HU BRASIL

MARQUE SIM OU NÃO

TESTE RÁPIDO DO GUARDIÃO

Você é um Guardião de Dados?

Use este checklist para reforçar atitudes seguras no dia a dia.

☐

Eu bloqueio a tela ao me afastar.

SIM ☐NÃO ☐☐

Eu nunca compartilho minha senha.

SIM ☐NÃO ☐☐

Eu verifico os destinatários antes de enviar informações.

SIM ☐NÃO ☐☐

Eu desconfio de links desconhecidos.

SIM ☐NÃO ☐☐

Eu reporto situações suspeitas.

SIM ☐NÃO ☐

Se você marcou SIM para todas as opções, parabéns!
Você já atua como um verdadeiro Guardião de Dados.



CH-UFC / HU BRASIL

COMPROMISSO DO GUARDIÃO

EU SOU UM GUARDIÃO DE DADOS

Meu compromisso é:

✓ Proteger informações

✓ Respeitar a privacidade dos pacientes

✓ Utilizar os sistemas de forma segura

✓ Comunicar incidentes rapidamente

✓ Contribuir para um CH-UFC/HU Brasil mais seguro

✓ Agir com atenção, sigilo e responsabilidade

**"Segurança da Informação:
uma atitude de todos, um benefício para todos."**



**COMITÊ DE SEGURANÇA DA INFORMAÇÃO - CSI
COMPLEXO HOSPITALAR DA UFC/HU BRASIL**

E lembre-se sempre:

Em caso de vazamento de dados ou situações de risco,
comunique imediatamente à Ouvidoria do nosso
CH-UFC/HU Brasil, nosso **encarregado de dados**.

