MARSH

12 dicas de segurança cibernética para Home Office.

MARSH

Dica #1

Habilite

o acesso remoto à rede através de um canal seguro, quando for necessário (por exemplo:VPN).

MARSH

Dica #2

Exija

o duplo fator de autenticação, sempre que possível.

MARSH

Dica #3

Utilize

serviços remotos somente em protocolos seguros (HTTPS).

MARSH

Dica
#4

Limite

os acessos remotos unicamente aos serviços permitidos e a zonas isoladas de rede.

MARSH

Dica #5

Valide

os controles dos dispositivos
(por exemplo: antivírus, atualizações,
configurações de segurança, etc.)

MARSH

Dica #6

Valide

as capacidades de limpeza e bloqueio remoto nos dispositivos.

MARSH

Dica #7

Assegure-se

de que seus dispositivos sejam criptografados e valide os controles de prevenção de vazamento de informação.

MARSH

Dica #8

Realize

um backup das informações importantes.

MARSH

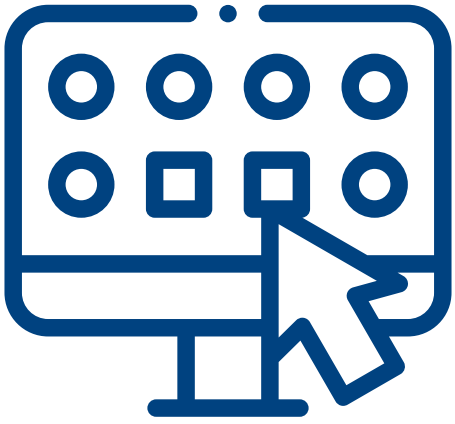
Dica #9

Conscientização, conscientização, conscientização

por exemplo: como detectar um phishing, e-mails maliciosos, etc

MARSH

Dica #10



Informe

aos usuários os protocolos para reportar qualquer situação suspeita ou incomum.

MARSH

Dica #11

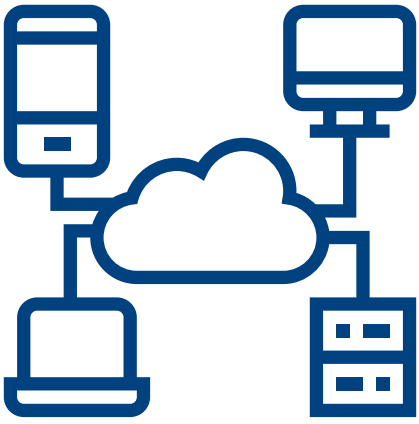
Incremente

os níveis de monitoramento de eventos de segurança. Alguns exemplos:

- Falhas e tentativas de autenticação bem-sucedidas.
- Acesso de um mesmo usuário em múltiplos endereços de IP.
- Tráfego de rede suspeito.
- Conexões em localidades incomuns (por exemplo: países não usuais).

MARSH

Dica #12



Aconselha-se

evitar o uso de redes públicas ou inseguras para a conexão.

MARSH

Leve em consideração que a aplicação de políticas de home office podem saturar os acessos à internet.

Revise a capacidade e monitore constantemente os acessos para assegurar a continuidade dos serviços.