CARTILHA DE BOAS PRÁTICAS E POLÍTICAS DE MITIGAÇÃO DE RISCOS DE INVASÃO

SEGURANÇA DA INFORMAÇÃO É COISA SÉRIA

SAFECYBER

SEGURANÇA EM TI DESCOMPLICADA

NESTE MATERIAL, VAMOS TE DAR DICAS IMPORTANTES SOBRE BOAS PRÁTICAS DA SEGURANÇA DA INFORMAÇÃO

Fique ligado e deixe sua empresa ainda mais protegida.
Para facilitar, dividimos a cartilha em 2 partes:

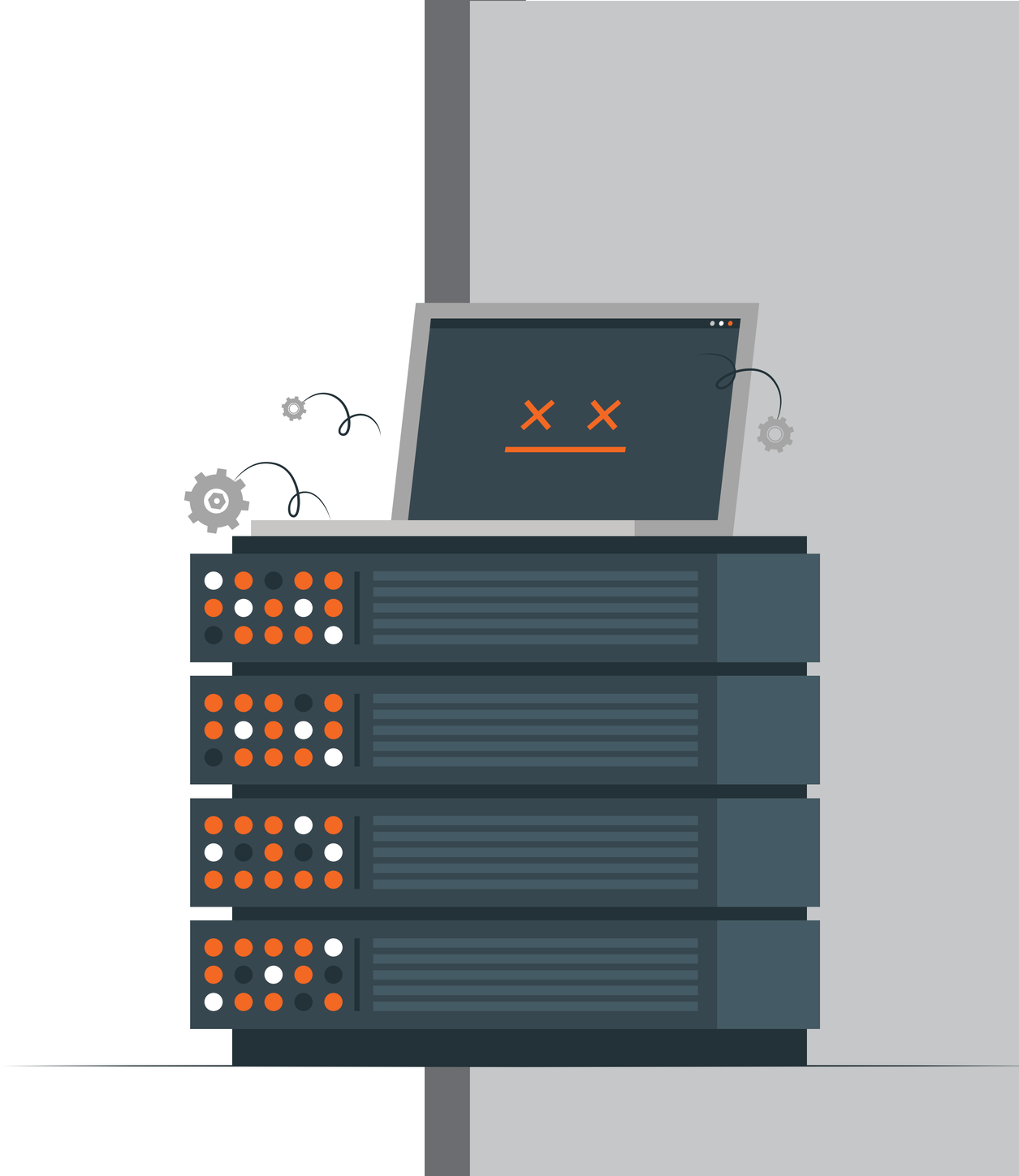
- melhores práticas a serem adotadas antes de um evento de infestação por malware;
- o que fazer em caso de invasão.

MELHORES PRÁTICAS | CENÁRIO

Em um passado recente, possuir backups e ser capaz de restaurá-los integral e rapidamente era o suficiente para sanar problemas de invasão por ransomware.

Hoje, com o advento da LGPD (Lei Geral de Proteção de Dados), da GDPR (Regulamentação Geral de Proteção de Dados) e suas implicações legais, multas, destruição de imagem e reputação de empresas, restaurar já não é mais suficiente, as empresas e organizações devem MITIGAR, ao máximo, as infestações.

Apresentamos um roteiro de providências que podem reduzir estes riscos, algumas ofertadas pela solução Safe Cyber e outras de contratação externa.



MELHORES PRÁTICAS | CHECKLIST

1. Conte com um firewall de borda (NGFW), gerenciado, monitorado e atualizado.
Firewall é um dispositivo de segurança da rede de dados que monitora o tráfego de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com as regras de segurança definidas.

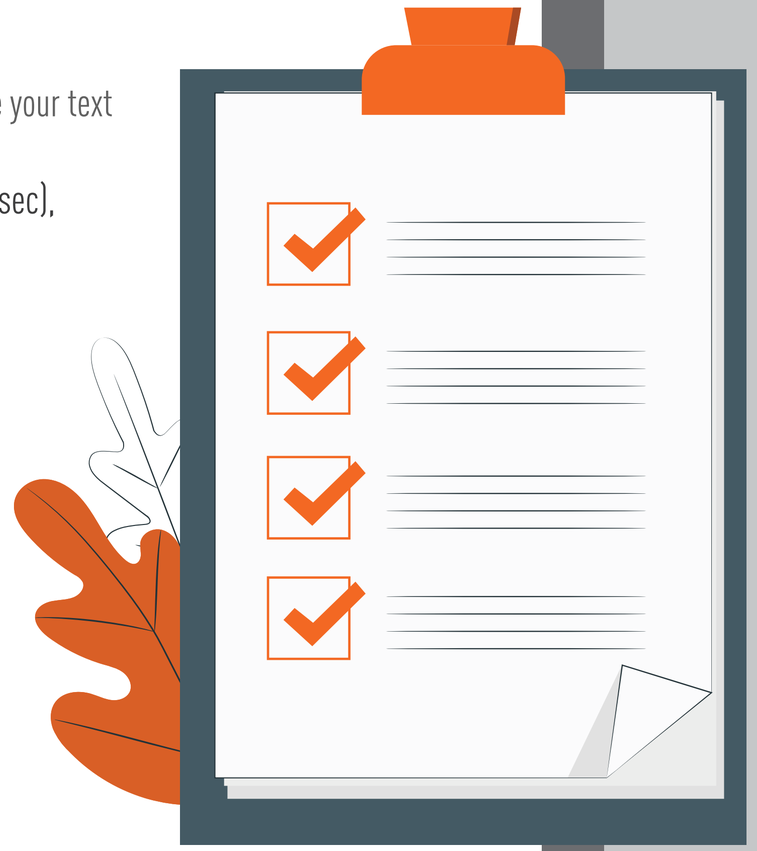
2. Tenha uma política consistente, frequente e monitorada de backups.
De preferência, armazene os dados em mais de um meio e, pelo menos, em um ambiente separado da rede local.

Type your text

3. Faça acessos remotos controlados de colaboradores
Além de prestadores, fornecedores, entre outros, somente por meio de VPN com protocolos seguros (ex,: OpenVPN, IPsec), fator múltiplo de autenticação (MFA) e regras do que pode ser acessado.

4. Tenha um conjunto de soluções complementares de segurança, externas à Safe Cyber, como:

. Antivírus gerenciado, em todos os servidores, desktops, notebooks e mobiles com atualização diária programada automaticamente;
. ANTISPAM e ANTIPHISHING;
. SIEM (Gerenciamento e Correlação de Eventos de Segurança);
. DLP (Prevenção de Perda de Dados);
. FIM (Monitoramento de integridade de arquivos).



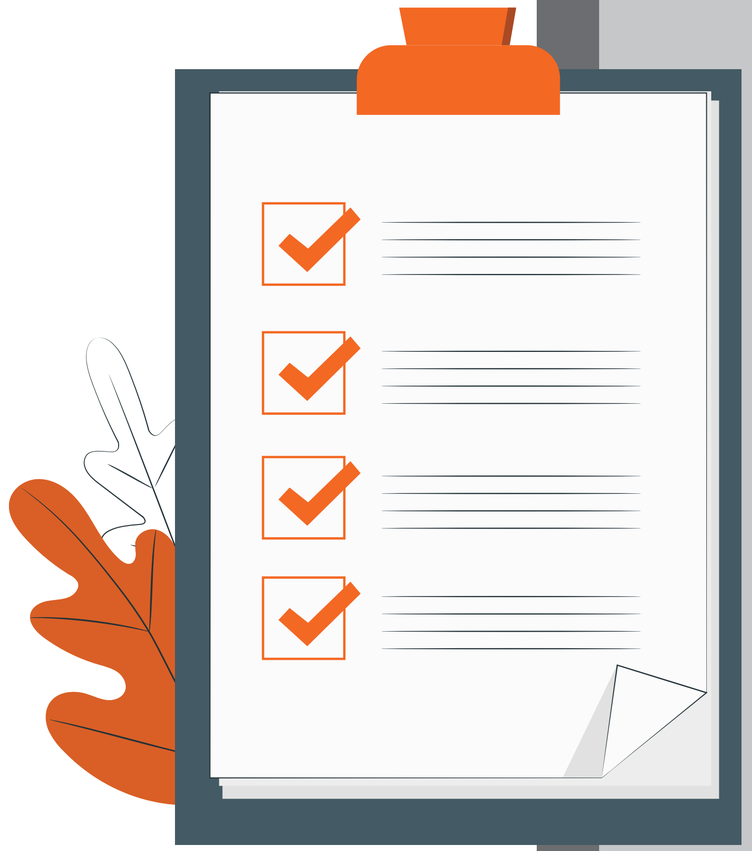
MELHORES PRÁTICAS | CHECKLIST

5. Tenha uma política de segurança da informação para empregados e colaboradores.

. Crie e implemente um time de respostas a incidentes.
. Crie e implemente um plano de respostas a incidentes.
. Crie um plano para avaliação de riscos.
. Crie e implemente um plano de continuidade de negócios.

6. Senhas

. Implante um sistema centralizado e segregado de gerenciamento de senhas (passwords manager);
Exemplos: TeamPass, SAML-Security Assertion Markup Language, entre outros.
. Implante política de SSO (Single Sign On), uma forma de autenticação que permite o acesso
a diferentes aplicativos e plataformas utilizando um só cadastro;
. Prefira senha longas, com o mínimo de 10 caracteres, e complexas mesclando números,
letras maiúsculas e minúsculas além de caracteres especiais (Ex.: !@#$%ˆ&*()+-=[];’../);
. Force a troca de senhas com intervalos de, no máximo, 30 (trinta) dias;
. Tenha um padrão de gestão de mudanças com o seu RH para revogação de acessos aos recursos da empresa
em caso de desligamento ou férias de colaboradores e terceiros.



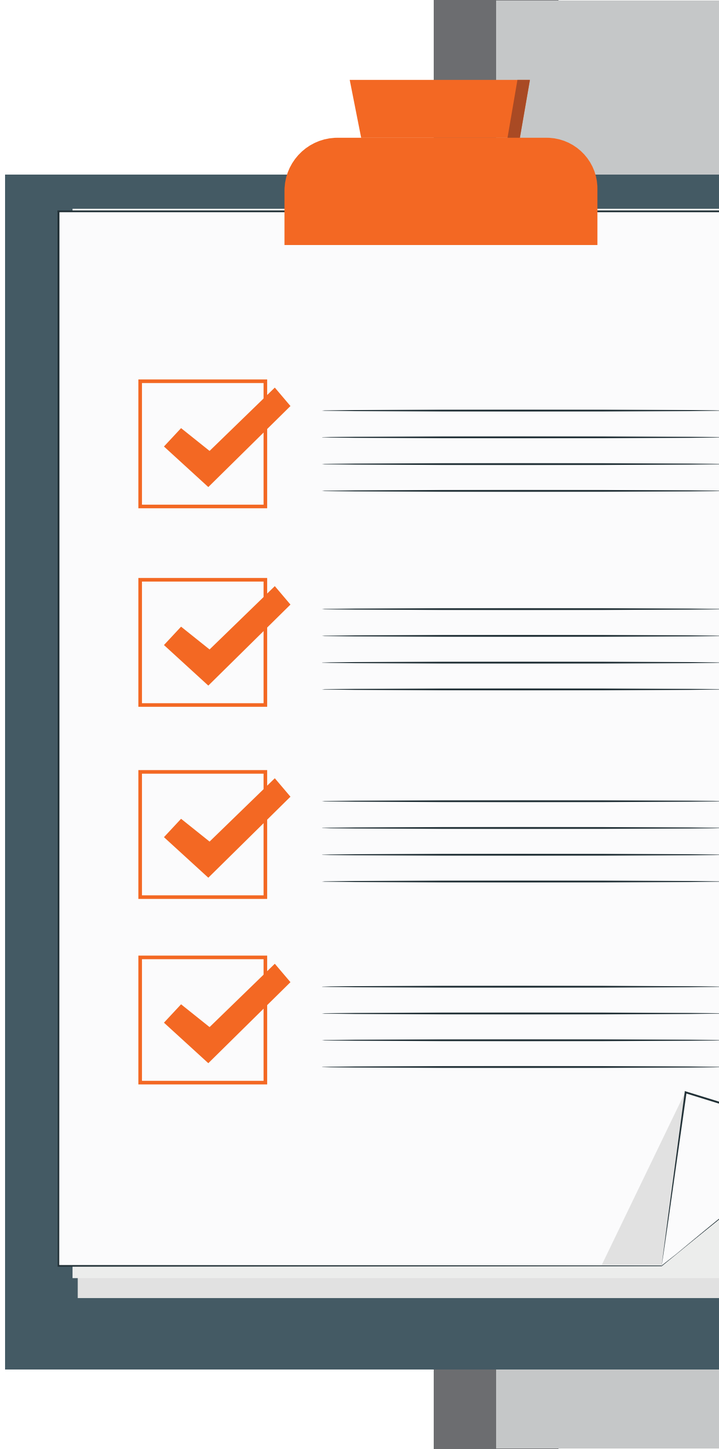
MELHORES PRÁTICAS | CHECKLIST

7. Acesso Privilegiado

. Remova acesso administrativo em todos os desktops e, principalmente, notebooks que entram e saem da rede local de sua empresa;
. Bloqueie usuários Administrador/Administrator/root em servidores, elegendo outros usuários para gestão dos servidores.

8. Servidores e Rede local

. Implemente um sistema de gestão de atualizações, como o o WSUS e confira diariamente se estão sendo feitas;;
. Isole suas redes locais em VLANs separadas da rede de desktops e notebooks;
. Crie uma DMZ (sub-rede) no Firewall e produza regras rígidas de acesso aos recursos destes servidores para a rede local e externa;
. Bloqueie no Firewall protocolos de acessos externos via Remote Desktop Protocol, Terminal Service (TS), Remote Desktop Connection (RDC) e serviços/produtos como TeamViewer, LogMeIn e afins.
. Implemente a segmentação de redes (VLANs) por departamentos em seu Switch;
. Implemente amarração de MAC Address por porta de Switch;
. Crie e mantenha uma política de EOL (Fim de Vida Útil) dos ativos de rede.



MELHORES PRÁTICAS | CHECKLIST

9. WebFilter (filtro de conteúdo) e Proxy (intermediário entre usuário e servidor)

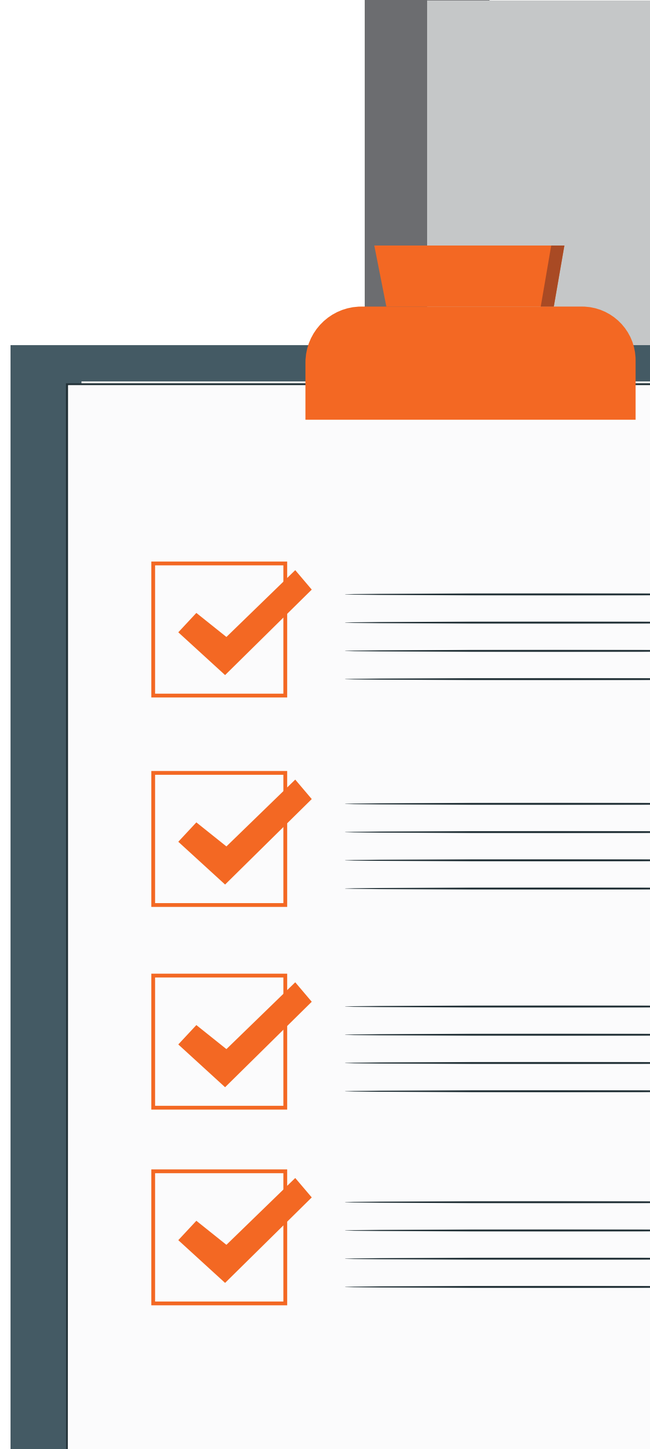
. Obrigue, via firewall, a navegação pelo proxy;
. Tenha regras rígidas de bloqueios a sites de categorias não permitidas ou indevidas (Ex.: Jogos, pornografia, Torrents);
. Publique, via WPAD (protocolo de detecção automática de proxy), o acesso à navegação de acordo com a sua política de política de grupo (GPO);
. Aplique a política de proxy separada por setor, até mesmo para diretores e para quem tiver acesso total;
. Adote o uso de Serviços de Diretórios, tais como Microsoft AD ou OpenLDAP.

10. E-mails e DNS

. Mantenha configurados e atualizados os registros de propriedade dos e-mails para evitar fraudes:
. DMARC - Mensagem Baseada em Domínio de Autenticação, Relatório e Conformidade
. DKIM - Autenticação que adiciona assinaturas de criptografia digital para as mensagens de correio eletrônico.

11. Bloqueie no firewall todos os protocolos não necessários para os serviços indispensáveis para a rede local.

12. Sanitize todos os dispositivos que propagam protocolos não necessários, como por exemplo, IPX/SPX e Appletalk.



RESPOSTA A UM ATAQUE | CHECKLIST

☑ **1. Desconecte tudo imediatamente:**

. Remova os cabos de rede de todos os PCs, notebooks, servidores, etc;
. Desligue o Switch core;
. Desligue a rede WiFi, APs, routers WiFi, etc;
. Desconecte discos externos ou NAS (Network Attached Storages) plugados por cabo de rede ethernet e/ou cabo USB;
. Desconecte pendrives, carregadores de celular USB, carregadores de câmeras e qualquer dispositivo USB plugado em servidores ou estações de trabalho.

☑ **2. Identifique e isole os alvos atacados:**

. Servidores de arquivos locais (Ex.: Windows Server, Samba, etc);
. Diretórios/pastas compartilhadas/mapeadas de desktops e notebooks;
. Discos externos/NAS/pendrives/etc;
. Backup na nuvem, tais como: OneDrive, Google Drive, DropBox, etc;
. Utilize um analisador de protocolos de rede para identificar os pontos disseminadores.

RESPOSTA A UM ATAQUE | CHECKLIST

☑ **3. Identifique o tipo/variante do ataque e quais os dados foram sequestrados e/ou criptografados:**

. Busque na internet informações, com base no banner de infecção, procurando orientações em sites confiáveis;
. Procure por grandes arquivos estranhos/inesperados que estejam compactados (Ex.: Zip, ARJ, RAR, etc) ou por inúmeros arquivos com nomes similares e também compactados;
. Analise os LOGs dos servidores de arquivos (Windows Server, Samba, etc);
. Aplique nos servidores e desktops ferramentas de busca de malwares do seu antivírus corporativo, exemplo: KVRT, Stinger, etc;
. Analise os logs do antivírus gerenciado e de suas ferramentas de DLP e SIEM.

☑ **4. Limpeza e Desinfecção:**

. Instale novos servidores de arquivos (Windows Server, Samba, etc). Se não for possível, remova os discos (HDs) do servidores infectados e reinstale o sistema operacional e serviços de compartilhamento de arquivos em novos HDs.
. Desinfecte pelo antivírus gerenciado notebooks e desktops. Caso não seja possível, reinstale os sistemas operacionais.

☑ **5. Restauração**

. Analise os seus backups em uma máquina virtual (VM) ou em um novo computador não participante da rede infectada e livre de infecções em um ambiente já desinfectado ou reinstalado, restaure os backups.

RESPOSTA A UM ATAQUE | CHECKLIST

A implementação das dicas desta cartilha é de baixo investimento e esforço e pode fazer a diferença no salvamento dos seus arquivos e informações.

Para finalizar, ressaltamos que aqui não tratamos sobre negociação de resgate com os sequestradores, porém, este assunto é controverso e pede análise mais profunda, pois "cada caso é um caso", não havendo um roteiro simples para abordar o tema.

APROVEITE ESTA CARTILHA E COMPARTILHE TAMBÉM COM OUTRAS PESSOAS QUE PODEM SER AJUDADAS.

Para continuar apreendendo mais sobre segurança da informação, conte conosco e siga nossas redes sociais.

Belo Horizonte | MG | São Paulo | SP

safecyber.com.br

SAFECYBER
SEGURANÇA EM TI DESCOMPLICADA