trinity ti

SOLUÇÕES
TECNOLÓGICAS

SEU MANUAL DE SEGURANÇA DA INFORMAÇÃO

Objetivos e benefícios da implementação de medidas de segurança da informação na sua empresa

ÍNDICE



02 Introdução

03 Antivírus corporativo

04 Inventário

05 Autenticação de dois fatores para e-mail e acesso web

06 Controle de compartilhamento de arquivos

07 Login do Windows, Bloqueio de Tela e Complexidade Mínima de Senha

08 Nossos contatos

INTRODUÇÃO

Você já parou para pensar na importância da segurança da informação em sua empresa?
Com a crescente ameaça de ataques e vazamentos de dados, é essencial adotar medidas de proteção para garantir a segurança das informações confidenciais.

Este manual de segurança da informação foi criado para fornecer orientações e melhores práticas que ajudarão você a proteger seus dados e manter a integridade das informações em sua organização.

Com o objetivo de fornecer orientações claras e abrangentes sobre as melhores práticas de segurança da informação. Abordaremos uma variedade de tópicos, desde a proteção de dispositivos e redes até a conscientização dos funcionários e a conformidade regulatória.



ANRIVÍRUS CORPORATIVO



Premissa

Ter um antivírus corporativo padrão com dashboard para gerenciamento e visibilidade.

Isso significa que todos os dispositivos da organização devem ter instalado um software de antivírus confiável e atualizado. Além disso, é importante ter um dashboard, ou painel de controle, que permita o gerenciamento centralizado e a visibilidade das atividades de segurança em todos os dispositivos.

Risco

Contaminação por vírus e ransomware, com possibilidade de contaminação de outras máquinas na mesma rede e do grupo de trabalho.

Esses tipos de malware podem infectar os dispositivos da empresa, comprometendo a segurança dos dados e a continuidade dos negócios. Além disso, uma máquina infectada pode contaminar outras máquinas na mesma rede e até mesmo afetar o grupo de trabalho, causando um impacto ainda maior.

Solução Sugerida

Adotar o Antivírus com licenciamento anual ou mensal

Adotar um antivírus com licenciamento anual ou mensal é fundamental para garantir a segurança e proteção do seu dispositivo contra ameaças cibernéticas. Ele fornece atualizações regulares, detecção e remoção eficazes de malware, proteção em tempo real, atualizações de segurança e suporte técnico para ajudá-lo a manter-se protegido contra as ameaças.

INVENTÁRIO



Premissa

Ter um controle dos equipamentos pertencentes à empresa, incluindo os equipamentos dos funcionários utilizados para produzir, e saber as configurações de hardware e softwares instalados.

É essencial ter um controle efetivo dos equipamentos pertencentes à empresa, bem como dos dispositivos utilizados pelos funcionários para realizar suas atividades.

Risco

Perda de equipamentos por falta de controle, alto risco de compliance de software (instalação de programas não autorizados) e ausência no planejamento de renovação do parque.

O risco associado à falta de controle de inventário é significativo. Sem um controle adequado, há maior probabilidade de perda de equipamentos, o que pode resultar em prejuízos financeiros e de produtividade.

Solução Sugerida

Adotar uma ferramenta de RMM para mapear todas essas informações

Essa ferramenta pode fornecer uma visão abrangente de todos os equipamentos da empresa, incluindo detalhes de hardware e software. Com uma ferramenta de RMM, é possível ter um inventário atualizado e preciso, facilitando a gestão dos ativos da empresa.

AUTENTICAÇÃO DE DOIS FATORES PARA EMAIL E ACESSO WEB



Premissa

Ter mais segurança no acesso ao ambiente em nuvem, seja através de email ou compartilhamento de arquivos, utilizando autenticação de dois fatores.

A autenticação de dois fatores é uma camada adicional de segurança que requer não apenas uma senha, mas também um segundo fator de autenticação, como um código enviado por SMS ou gerado por um aplicativo de autenticação.

Risco

Facilidade de invasão, baixo nível de proteção e comprometimento dos dados e dos emails da empresa.

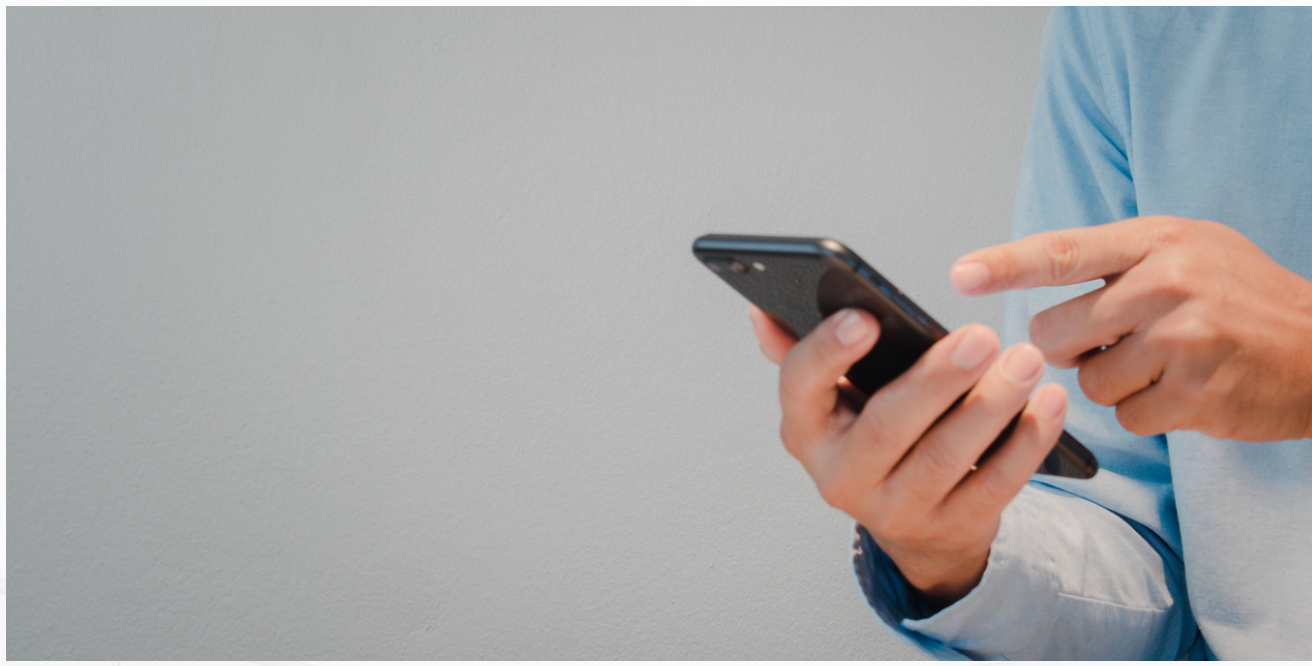
Com apenas uma senha, os invasores têm mais facilidade em violar a segurança do ambiente em nuvem, o que pode levar ao comprometimento dos dados e dos emails da empresa. Além disso, a falta de autenticação de dois fatores resulta em um nível de proteção mais baixo, tornando a empresa mais vulnerável.

Solução Sugerida

Adotar a autenticação de dois fatores para serviços como Google, Microsoft ou qualquer outro utilizado para arquivos e emails na web

Ao adotar a autenticação de dois fatores, você estará aumentando significativamente a segurança do acesso ao ambiente em nuvem, reduzindo a facilidade de invasão e protegendo os dados e os emails da empresa contra comprometimento.

CONTROLE DE ARQUIVOS COMPARTILHADOS



Premissa

Ter um controle efetivo de quem pode acessar seus arquivos

A premissa deste tópico é que é essencial ter um controle efetivo sobre quem pode acessar os arquivos da empresa. Isso envolve garantir que apenas as pessoas autorizadas tenham acesso aos arquivos e que as permissões de acesso sejam configuradas corretamente.

Risco

Qualquer pessoa da organização acessar arquivos inadequados. Qualquer pessoa FORA da organização ter acesso aos seus dados.

Se qualquer pessoa dentro da organização tiver acesso a arquivos inadequados, isso pode resultar em violações de privacidade, vazamento de informações confidenciais ou acesso não autorizado a dados sensíveis.

Solução Sugerida

Usar ferramentas ou recursos que permitam o controle, como AdMicrosoft, Google Drive (Shared Drives) ou SharePoint (OneDrive). Adotar política de revisão de permissionamento de forma recorrente.

Exemplos de ferramentas incluem o Active Directory da Microsoft, o Google Drive (compartilhamento de drives) ou o SharePoint (OneDrive). Essas ferramentas oferecem recursos avançados de gerenciamento de permissões, permitindo que você defina quem pode acessar, visualizar, editar ou compartilhar os arquivos.

LOGIN DO WINDOWS, BLOQUEIO DE TELA E COMPLEXIDADE MÍNIMA DE SENHA



Premissa

Ter uma forma de garantir o controle de quem pode entrar nos computadores corporativos, bloquear a tela após algum tempo de inatividade e aplicar complexidade mínima de senha.

Isso visa aumentar a conscientização sobre as ameaças cibernéticas e educar os funcionários sobre as melhores práticas de segurança que devem ser seguidas no ambiente de trabalho.

Risco

Sem a gestão de identidades ou sem garantir que uma senha seja exigida ao abrir o computador, qualquer pessoa com posse do equipamento pode entrar e acessar os arquivos da empresa.

A falta de conhecimento e conscientização dos funcionários pode tornar a empresa mais vulnerável a ataques cibernéticos, como phishing, malware e engenharia social.

Solução Sugerida

Adotar o uso do Active Directory da Microsoft (Azure ou on-premise), Google Cloud Passwords ou Intune.

Gerenciar apenas com Gmail ou Office 365 protege apenas o acesso online, mas não protege o computador e os arquivos armazenados nele. Essa é uma área importante a ser trabalhada para fortalecer a segurança da empresa.

contato@trinityti.com

www.trinityti.com

(21) 4062-7800

CLIQUE PARA ACESSAR