CÂMARA MUNICIPAL DE Manaus

SEGURANÇA DA INFORMAÇÃO

O QUE É? COMO APLICÁ-LA?

MANAUS - AMAZONAS
2022

MESA DIRETORA - 18ª LEGISLATURA

PRESIDENTE DA CÂMARA
Ver. David Reis

1º VICE-PRESIDENTE
Ver. Wallace Oliveira

2º VICE-PRESIDENTE
Ver. Diego Afonso

3º VICE-PRESIDENTE
Ver. Caio André

SECRETÁRIO(A) - GERAL
Ver. Glória Carratte

1º SECRETÁRIO(A)
Ver. Bessa

2º SECRETÁRIO(A)
Ver. Eduardo Alfaia

3º SECRETÁRIO(A)
Ver. João Carlos

CORREGEDOR(A)
Ver. Jaildo Oliveira

OUVIRDOR(A)
Ver. Amom Mandel

VEREADORES - 18ª LEGISLATURA

Allan Campelo
Amom Mandel
Bessa
Caio André
Capitão Carpê Andrade
Daniel Vasconcelos
David Reis
Diego Afonso
Dione Carvalho
Dr. Eduardo Assis
Eduardo Alfaia
Elan Alencar
Everton Assis
Fransuá
Gilmar Nascimento
Glória Carratte
Ivo Neto
Jaildo Oliveira
Jander Lobato
João Carlos
Joelson Silva
Kennedy Marques
Lissandro Breval
Marcel Alexandre
Marcelo Serafim
Márcio Tavares
Mitoso
Peixoto
Professor Samuel
Professora Jacqueline
Raiff Matos
Raulzinho
Rodrigo Guedes
Rosinaldo Bual
Rosivaldo Cordovil
Sassá da Construção Civil
Thaysa Lippy
Wallace Oliveira
Wanderley Monteiro
William Alemão
Yomara Lins

Segurança da Informação: O que é? Como aplicá-la?

Hoje em dia, a informação é o ativo mais valioso para qualquer organização. Seja ela governamental ou privada.

Mantê-la segura é uma obrigação de todos, dentro e fora da organização, mas como podemos fazer isso? Através da Segurança da Informação.

A segurança da informação é um conjunto de normas e boas práticas para manter os dados seguros, preservando o seu valor para a organização.

A seguir vamos conhecer as ameaças e como podemos nos prevenir aplicando as dicas para mantermos a Segurança da Informação na CMM.

De quais ameaças estamos falando?

Quando falamos das ameaças que rondam os pilares da segurança da informação, fazemos referência a diversos tipos entre digitais e humanas.

Tais como:

Ataques a software

Por meio de vírus, e-mails e websites;

Phishing

Responsáveis por roubar dados e senhas;

Golpes de engenharia social

Que manipulam pessoas para roubar informações privadas;

Roubos dispositivos móveis

Que manipulam pessoas para roubar informações privadas;

Ataques de negação de serviço (DoS e DDoS)

Que sobrecarregam os servidores.

Para proteger as informações dessas ameaças vamos entender melhor os pilares da segurança da Informação.

I- Integridade - é responsável por manter as características originais dos dados, a informação não pode ser alterada sem autorização. Existindo uma modificação indevida nos dados, significa que houve perda da integridade, portanto se faz necessária a implementação de mecanismos de controle, com o intuito de impedir a alteração não autorizada das informações.

II- Confidencialidade - protege a informação dos acessos não autorizados estabelecendo a privacidade para os dados da sua empresa, evitando situações de ataques cibernéticos ou espionagem. A base desse pilar é controlar o acesso por autenticação de senha, podendo ser também por verificação biométrica e criptografia

III- Disponibilidade – é a disponibilidade dos dados para o que for necessário, garantindo o acesso dos usuários em tempo integral. Isso exige a estabilidade e acesso permanente aos dados do sistema, através de manutenções rápidas, atualizações constantes e eliminação de falhas.

Considerando as diversas ameaças existentes, como podemos proteger as informações com que lidamos no nosso dia-a-dia na organização?

1. Sempre desconfiar de e-mails não solicitados

- Atualmente, uma das principais formas dos cibercriminosos agirem é por meio de ataques phishing que contaminam os emails recebidos pelos usuários. Portanto, antes de abrir qualquer mensagem, é importante refletir “Eu solicitei algum serviço deste remetente?”
- É muito comum hackers se passarem por bancos ou outras instituições mandando cobranças, boletos, multas e afins. Por isso, é necessário identificar se a mensagem é verdadeira ou não e, assim, não abrir o email, eliminando a ameaça.
- Muitos emails recebidos parecem ser verídicos e direcionado para os usuários. Por isso, uma das primeiras coisas a serem feitas ao receber um email é verificar o remetente. O usuário estava esperando por aquele email? Conhece a pessoa que está enviando?
- É necessário verificar se o endereço de email está correto, pois muitas vezes os hackers se passam por empresas conhecidas, mas trocam algumas letras no nome. Este é o primeiro alerta que é falso, portanto, jogue-o na lixeira rapidamente.

2. Não baixar arquivos suspeitos

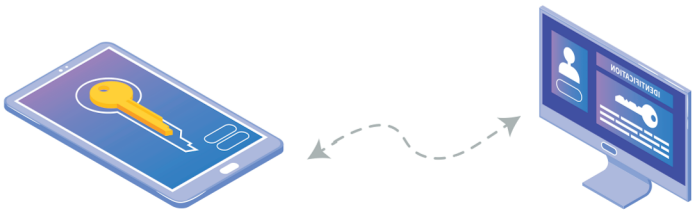
- Os links para download recebidos requerem atenção extra eles podem ser um grande problema se não levados a sério.
- Quando um link infectado é aberto por um colaborador que está conectado à rede corporativa, todos as outras máquinas passam a estar em perigo, pois ao ser instalado o vírus, o acesso dos criminosos é liberado na rede.
- Para evitar que isso aconteça, os usuários devem evitar baixar qualquer arquivo e, quando duvidarem de algum link, devem bloqueá-lo.

3. Checar o domínio em sites.

- Assim como nos emails, muitos sites maliciosos possuem o mesmo layout dos verdadeiros, com apenas algum detalhe diferente. Com isso, acabam conseguindo facilmente enganar os usuários.
- Portanto, antes de acessá-lo e preencher qualquer informação pessoal nele, é necessário verificar seu domínio. É importante pesquisar na internet sobre aquele site, caso seja malicioso, outras pessoas podem estar comentando sobre ele e emitindo alertas.

4. Manter dispositivos atualizados

- Quando um software está trabalhando em versões anteriores, os cibercriminosos podem se aproveitar de brechas que não foram corrigidas para invadirem o aparelho e roubar dados importantes.
- Dessa forma, é crucial manter todos os aparelhos e aplicativos atualizados, pois seus fornecedores sempre fazem as correções necessárias para que eles estejam mais seguros.

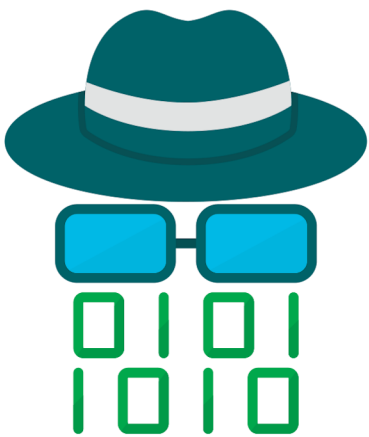


5. Cuidados com suas senhas

- Não divulgue e nem compartilhe – a senha é sua e de mais ninguém.
- Não escreva sua senha em local público ou de fácil acesso.
- Não deixe sua senha visível ao digitá-la, muito menos na presença de desconhecidos.
- Nunca use palavras de dicionários ou dados pessoais como senha.
- Crie senhas com mais de oito caracteres e que misture letras maiúsculas, minúsculas, números e caracteres especiais.
- Mude de senha regularmente, principalmente se utilizar máquinas administradas por pessoas que não sejam de sua confiança.
- Utilize um gerenciador de senhas.

6. Antivírus e antispyware

- Configure seu antivírus para procurar por atualizações sempre que seu computador estiver conectado à Internet.
- Faça pelo menos uma varredura completa no sistema por semana.
- Use seu antivírus em todo arquivo baixado antes de executá-lo, assim como em toda mídia removível conectada. Se possível, configure essas verificações para que sejam feitas automaticamente, bem como as demais verificações passíveis de execução pelo software.
- Use o antispyware como uma ferramenta auxiliar do antivírus, pois muitas aplicações maliciosas conseguem burlar o antivírus para espionar e acessar seus dados. Prevenção nunca é demais!
- Não utilize mais de um software antivírus simultaneamente, pois as aplicações podem entrar em conflito e o resultado pode acabar sendo exatamente o oposto do pretendido



7. Proteja seus dados pessoais

- Nunca forneça informações sensíveis em sites sem que você tenha solicitado o serviço que o exige, e o faça somente se confiar no site e se o mesmo estiver utilizando criptografia (procure pelo cadeado no navegador e um informativo de certificado digital).
- Evite fazer cadastros em sites de venda desconhecidos pela Internet, especialmente fornecendo seus dados pessoais, pois muitas pequenas e médias empresas possuem pouco ou nenhum tipo de segurança para armazenar e proteger seus dados.
- Cuidado aos disponibilizar informações muito pessoais em sites de relacionamento (telefones móveis, endereços, etc).

8. Faça backups

- Agende regularmente cópias de reserva (backup) de todos os seus dados importantes.
- Pense nas coisas que realmente lhe fariam falta caso perdesse tudo e cuide para que isso não aconteça.
- Discos rígidos, pendrives e CDs também dão defeito! Tenha sempre cópias redundantes e jamais confie em apenas uma mídia para armazenar seus dados mais importantes.

9. Segurança Física

- Tenha um filtro de linha com suporte a queda de energia (no-break). Se não for possível, use ao menos um filtro de linha comum.
- Mantenha seu computador e cabos protegidos contra quedas e esbarrões.
- Mantenha seu computador e suas mídias (como pendrives, DVDs e HDs externos) em local seco, arejado, longe do calor, e sempre protegidos de fontes eletromagnéticas fortes.

10. Chamar a TI quando necessário

- Mesmo tomando todos os cuidados possíveis, os usuários ainda podem cometer erros e suspeitar de que alguma ameaça está afetando seus dispositivos. Nesses momentos, é crucial avisar a equipe de TI o mais rápido possível.
- Quando os profissionais certos sabem sobre o problema ainda no início, as chances de prejuízos são menores. Assim, podem tomar as medidas necessárias para eliminar a ameaça.

LEMBREM-SE A SEGURANÇA DA INFORMAÇÃO É UMA RESPONSABILIDADE DE TODOS.

FAÇA A SUA PARTE!!!!

CÂMARA MUNICIPAL DE
Manaus

MANAUS - AMAZONAS
2022