PREFEITURA MUNICIPAL DE DUQUE DE CAXIAS
SECRETARIA MUNICIPAL DE GOVERNO
SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E MODERNIZAÇÃO ADMINISTRATIVA

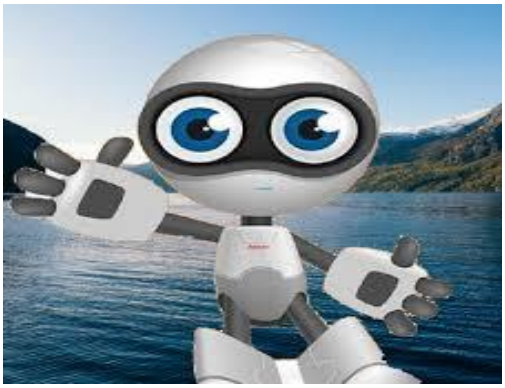
6 DE DEZEMBRO 2021

Prefeitura Municipal de Duque de Caxias
Criado por:
Fernando Felipe Corrêa
Henrique dos Santos Cardozo
Pedro Oliveira Felix
Graziela do Nascimento Silva

Sumário

Cartilha de Segurança da informação: 3
O que é segurança da informação? 4
Física 5
Lógica....5
Humana 5
Por que é importante cuidar da segurança da informação?....6
Confira 10 importantes dicas de segurança na internet 7
Ações implementadas pelo setor TI: 10

Cartilha de Segurança da informação:



Diversas informações circulam diariamente nas redes e saber como se proteger de roubos de dados e fraudes é muito importante atualmente. Pensando nisso, criamos a cartilha de segurança da informação para saber como atuar.

A segurança da informação é um conceito importante e que é fundamental para qualquer empresa e até mesmo para a vida pessoal.

Mais do que estratégica, a segurança da informação é essencial para proteção dos dados corporativos e pessoais, evitando perdas e prejuízos que podem causar danos enormes.

Quando bem aplicada, é capaz de blindar as empresas de ataques digitais, desastres tecnológicos e falhas humanas. Por isso, é fundamental que os gestores compreendam a importância desse tipo de investimento.

Você sabe como se proteger digitalmente? Continue lendo e saiba algumas boas dicas importantes em nossa cartilha de segurança da informação!

O que é segurança da informação?

Segurança da informação nada mais é do que a união de esforços e medidas voltadas para a defesa dos dados, principalmente aqueles mais sensíveis, de usuários e organizações. Em síntese, o grande cerne da segurança da informação está em manter o acesso aos dados sempre protegido. Ou seja, livre de invasões e outras ações maliciosas que podem comprometer o sigilo, a integridade e o valor das informações.

A segurança da informação é importante porque protege todas as categorias de dados contra roubo e danos. Isso inclui dados confidenciais, informações de identificação pessoal, informações de saúde, propriedade intelectual, dados e sistemas de informações, tanto corporativas como governamentais.

Sem uma estratégia de segurança cibernética, sua organização não pode se defender contra ações maliciosas de violação de dados.

Já se foi o tempo em que firewalls simples eram as únicas medidas de segurança. Hoje, é preciso de mais. Por isso, os gestores não podem mais deixar a segurança da informação em segundo plano. Esse entendimento é essencial, já que o cibercrime e as ameaças digitais exigem que cada vez mais as empresas adotem medidas de proteção.

Só para você ter noção, de acordo com o 2020 Webroot Threat Report, 93,6% dos malwares analisados eram considerados polimórficos.

Você sabe o que isso significa? Um malware polimórfico possui a habilidade de constantemente mudar seu código para fugir dos mecanismos de detecção.

A boa notícia é que existem diversas maneiras de garantir uma comunicação segura dos dados, restringindo o acesso somente por quem, de fato, está autorizado a fazê-lo, como veremos mais adiante.

A segurança da informação pode ser dividida em três camadas para garantir que todos os dados sejam salvos com o máximo de segurança. São elas: física, lógica e humana.

Física

Refere-se ao ambiente em que os *hardwares* (computadores, servidores e meios de comunicação) estão fisicamente instalados.

É necessária estrutura e manutenção que ofereça proteção contra ameaças de diversas naturezas, como incêndios, desabamentos, alagamentos e qualquer desastre que afete o espaço.

Também é preciso pensar em proteção e segurança quanto à entrada de pessoas não autorizadas no local de instalação.

Lógica

É constituída pelo uso de *softwares*. Eles que são os responsáveis pelo funcionamento dos *hardwares* e pela movimentação de dados que acontece.

Desse modo, esses sistemas precisam de cuidados, atualizações e outras ações que falaremos ao longo da nossa cartilha de segurança da informação.

Humana

O ponto mais fraco em muitas arquiteturas de segurança cibernética é o elemento humano. Os erros do usuário podem facilmente expor dados confidenciais, criar pontos de acesso exploráveis para invasores ou interromper sistemas.

É uma das camadas mais complexas de se gerenciar, pois exige mudança de cultura, treinamentos de conscientização e não apenas simples programações.

Por que é importante cuidar da segurança da informação?

A segurança da informação é importante porque protege todas as categorias de dados contra roubo e danos. Isso inclui dados confidenciais, informações de identificação pessoal, informações de saúde, propriedade intelectual, dados e sistemas de informações, tanto corporativas como governamentais.

Com a chegada da Lei Geral de Proteção de Dados, a questão da segurança da informação passa também a ser uma obrigação a ser cumprida pelas empresas, visando oferecer maior controle e transparência para os usuários.

A LGPD além de oferecer maior controle e transparência do tratamento dos dados dos usuários, traz a necessidade de controles de segurança para prevenção e mitigação de riscos

como a análise preventiva e corretiva de vulnerabilidades, proteção de dados armazenados e outros.

Confira 10 importantes dicas de segurança na internet

1. Aprenda sobre o mundo virtual

Informe-se. Não há nada melhor do que saber maneira de se prevenir das ameaças on-line. Procure sempre informações na internet, cursos, palestras e maneiras de se proteger. E caso haja algum problema com seu computador, leve seu equipamento até um especialista em T.I pois esses profissionais são os mais indicados para resolver qualquer problema operacional ou de contaminação que seus aparelhos venham a ter.

2. Não salve suas senhas

Elas são restritas e de uso pessoal. Por isso, não salve suas senhas no computador - nem no seu e muito menos em algum de uso compartilhado. O mundo da internet é muito perigoso e um deslize pode fazer você ter seus dados descobertos. Melhor prevenir que remediar.

3. Altere suas senhas periodicamente

Passar muito tempo com uma única senha é um erro muito cometido. Altere sempre suas senhas, para que seja mais difícil que outras pessoas descubram seus dados confidenciais. Também lembre-se de usar letras, números e símbolos na criação das suas senhas. Não esqueça de evitar usar a mesma palavra-chave para serviços diferentes.

4. Não instale softwares suspeitos

Na dúvida, não instale. Os programas podem estar infectados e conter malwares que podem roubar dados do seu computador. Opte por aqueles softwares de empresas que você já conhece e das renomadas no mercado.

5. Atenção aos downloads

Assim como softwares, outros downloads também podem te levar a problemas com a sua máquina. Jogos, filmes, músicas, caso não bem selecionados, podem ser baixados com algum vírus e causar grandes dores de cabeça. Fique atent@ a isso e não esqueça de fazer o download por meio de sites confiáveis e renomados.

6. Cuidados com os links que você clica

Atenção redobrada nesse caso. Muito cuidado com os links que você clica, principalmente nas redes sociais como Facebook e Twitter. Histórias diferentes, curiosas e engraçadas demais podem ser uma armadilha para sua proteção contra vírus e ataques cibernéticos. Use do bom senso e pesquise sobre o assunto, com o intuito de arranjar uma fonte confiável para o tema.

7. Atualize seu antivírus

Ele é sua defesa contra os malwares da internet. Ter um antivírus atualizado é uma das melhores saídas para obter proteção. Faça as renovações assim que for solicitado - ou em um prazo semanal - e evite passar muito tempo sem utilizá-lo. As versões pagas são mais completas e com mais garantias de segurança.

8. Não acredite em super promoções da internet

A famosa expressão norte-americana “não existe almoço grátis” é verdadeira no mundo capitalista em que vivemos. Propagandas de objetos com descontos astronômicos, em sites que você nunca ouviu falar, e anúncios de que você foi o milionésimo a acessar alguma página na internet são indícios de que há algo errado. Um vírus pode invadir seu computador, caso clique em links encontrados em situações parecidas, e ter acesso aos seus dados pessoais.

9. Fique atentos aos falsos e-mails e anexos

Muitas vezes os e-mails são corrompidos e falsos e-mails caem na sua caixa de entrada. É muito comum se tratarem de assuntos como traição, emprego, dinheiro e rastreamento de encomendas. Não clique em links ou anexos enviados por endereços virtuais desconhecidos.

10. Verifique se o site é seguro

O Google oferece uma certificação de segurança aos sites. Quando o gigante da tecnologia enxerga um endereço virtual como perigoso, o próprio navegador indica isso ao usuário. Em outros casos, até mesmo o antivírus bloqueia o site e alerta perigo.

Ações implementadas pelo setor TI:

- Supervisão e orientação na instalação de qualquer APP, através de permissão de acesso administrativo.
- Bloqueios e restrição de acesso a sites.
- Controle de acesso, tráfego e monitoramento da rede.
- Gerenciamento e controle de acessos de dispositivos (Celulares, Tablets, Notebook e outros) na rede.
- Elaboração e implementação de projetos para reestruturação de rede.
- Sistema de armazenamento de arquivos com Backup na rede.

Referencias Bibliográficas:

- https://blog.ecoit.com.br/cartilha-de-seguranca-da-informacao/
- https://www.uninassau.edu.br/noticias/confira-10-importantes-dicas-de-seguranca-na-internet
- https://triplait.com/entenda-o-que-sao-vulnerabilidades/
- https://www.cisco.com/c/pt_br/products/security/what-is-it-security.html