INSTITUTO FEDERAL DE SANTA CATARINA – IFSC
CAMPUS CANOINHAS
DEPARTAMENTO DE ENSINO, PESQUISA E EXTENSÃO
CURSO TÉCNICO EM MANUTENÇÃO E SUPORTE EM INFORMÁTICA

ERICLES GABRIEL
PEDRO TALLES
SANDERLEI PEREIRA
THIAGO SANDRO

SEGURANÇA DA INFORMAÇÃO

.....

CANOINHAS
2017

Segurança da Informação

.....

INSTITUTO FEDERAL
SANTA CATARINA

Relatório apresentado à Unidade Curricular de Projeto Integrador II do Curso Técnico em Manutenção e Suporte em Informática, como requisito parcial de aprovação.

Prof. Orientador: Luciano Barreto

CANOINHAS
2017

INSTITUTO FEDERAL
SANTA CATARINA

RESUMO

O presente trabalho se trata a respeito da segurança da informação e como ela deve ser aplicada nas organizações ou em nosso dia a dia. Tratando de forma específica das Políticas de Segurança e suas diretrizes.

De modo em que todas as pessoas da organização estejam cientes dos ricos e de que forma isso pode prejudica las.

Sumário

SEGURANÇA DA INFORMAÇÃO •..... 1
1 • INTRODUÇÃO •..... 7
2 OBJETIVOS •..... 8
2.2 OBJETIVOS ESPECÍFICOS..... 8
3 INFORMAÇÃO •..... 8
SEGURANÇA DA INFORMAÇÃO 9
Confidencialidade:..... 9
3.2 MATERIAIS E MÉTODOS..... 9
3.3 Resultados e Discussão..... 9
3.4 Disponibilidade 9
4 Política de segurança da informação 10
Mas como elaborar uma Política de Segurança? 10
E como essa política deve ser implementada? 10
IMPORTÂNCIA DENTRO DE UMA ORGANIZAÇÃO 11
SEGURANÇA FÍSICA 11
Ameaça 11
Vírus 11
Vulnerabilidade 12
5.5 Risco 13
5.6 RISCO = (Ameaça) x (Vulnerabilidade) x (Valor do Risco) 13
As cinco maiores ameaças 13
Kilim 14
Sality 14

INSTITUTO FEDERAL
SANTA CATARINA

6 POLITICAS DE SENHAS • 15
6.1 Oque seria uma boa senha? 16
6.2 Cuidados com sua senha..... 16
Alguns dos mais famosos casos de invasão de informação 16
Vladimir Levin 17
Usuários de Uber, tem seus dados expostos. 17
Ameaças de espionagem em dispositivos móveis 17
7 CONCLUSÃO •..... 17

INSTITUTO FEDERAL
SANTA CATARINA

INFORMAÇÃO

INSTITUTO FEDERAL
SANTA CATARINA

A informação é todo e qualquer tipo de dado processado. Tendo em conta, seu uso racional, pode ser dizer que a informação, é a base do conhecimento, pois com ela se resolve problemas e toma decisões.

Le Coadic, pesquisador da área da Ciência da Informação, destaca que o “valor da informação varia conforme o indivíduo, as necessidades e o contexto em que é produzida e compartilhada”.

Com o avanço da tecnologia e também a concorrências nos mercados de trabalho, a informação acaba sendo essencial dentro de uma empresa, pois contribui diretamente para uma maior competitividade. No entanto, também aumenta os ricos de ameaças e vulnerabilidades.

A informação é todo e qualquer tipo de dado processado. Tendo em conta, seu uso racional, pode ser dizer que a informação, é a base do conhecimento, pois com ela se resolve problemas e toma decisões.

Le Coadic, pesquisador da área da Ciência da Informação, destaca que o “valor da informação varia conforme o indivíduo, as necessidades e o contexto em que é produzida e compartilhada”.

Com o avanço da tecnologia e também a concorrências nos mercados de trabalho, a informação acaba sendo essencial dentro de uma empresa, pois contribui diretamente para uma maior competitividade. No entanto, também aumenta os ricos de ameaças e vulnerabilidades

SEGURANÇA DA INFORMAÇÃO

INSTITUTO FEDERAL
SANTA CATARINA

É um meio de proteger contra ameaças e ataques todo e qualquer dado de uma organização.
Garantindo a segurança do investimento, aplicando os seus princípios básicos, que são a Confidencialidade, Integridade e a Disponibilidade

Confidencialidade

A confidencialidade serve para que pessoas sem autorização não possam acessar dados ou informações privadas, se essa privacidade for rompida causará danos como a conta do e-mail e senha de uma certa pessoa serem roubados ou até mesmo do Facebook.

3.2 MATERIAIS E MÉTODOS

Os materiais que foram utilizados para a elaboração deste trabalho foram os computadores do Instituto.

INSTITUTO FEDERAL
SANTA CATARINA

3.3 Resultados e Discussão

Este trabalho foi realizado durante as aulas de PI, com pesquisas no laboratório do Instituto, utilizando os computadores e foi elaborado com pesquisas em vários sites.

3.4 Disponibilidade

isponibilidade é a garantia de acesso à informação fornecida ou autorizada pelo usuário. Ou então, ter acesso a qualquer tipo de informação, em um banco de dados, sempre que necessário.

4 Política de segurança da informação

INSTITUTO FEDERAL
SANTA CATARINA

É importante a política de segurança da informação para garantir que as informações estarão seguras correndo o mínimo de risco de serem violadas, tem que ser seguida como um documento de alta importância pois se as informações de uma empresa forem violadas acarretaram muitos problemas para a mesma por exemplo a WEG uma das maiores empresas de motores do mundo, se suas informações forem totalmente apagadas desde funcionários, estoque de produtos, matéria prima entre outros, ela teria de armazenadas novamente que causaria um grande tumulto, e ela teria de ficar um tempo sem produção alguma, oque traria um prejuízo milionário para esta grande empresa.

Mas como elaborar uma Política de Segurança?

INSTITUTO FEDERAL
SANTA CATARINA

Primeiro devemos definir as pessoas responsáveis pela elaboração, implantação e manutenção da politica. Definir oque cada equipe será responsável a apresentar e trabalhar junto com pessoas de alta administração da organização para que essa política seja implementada, assim, obtendo a colaboração dos demais.

E como essa política deve ser implementada?

Para implementar essa política, é necessário a colaboração de todos os funcionários.
Todos devem estar cientes dos ricos, vulnerabilidade de segurança e ter maior responsabilidade.
Também contar com o apoio e comprometimento da administração, do contrário, acaba sendo algo impraticável.

IMPORTÂNCIA DENTRO DE UMA ORGANIZAÇÃO

INSTITUTO FEDERAL
SANTA CATARINA

A política de segurança da informação deve ensinar como será entrada ao acesso as informações de todas as formas possíveis, seja ela internamente ou externamente, e quais os tipos de mídias podem transportar e ter acesso a esta informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alocados.

Segurança Física

A segurança física tem como objetivo, prevenir o acesso não autorizado pela empresa. Usando uma segurança reforçada em ambientes onde existam, instalações e informações mais importantes.

Isso pode ser feito, através de portas com cartão de acesso, leitores biométricos, e uma pessoa responsável que controle o acesso de quem entra e sai das instituições.

Backup

INSTITUTO FEDERAL
SANTA CATARINA

É uma cópia de segurança de arquivos considerados importantes para o usuário.
É recomendado que essas cópias sejam feitas em locais ou ambientes diferentes. Pois assim evitam que esses arquivos sejam perdidos, em caso de acidentes, ou algum outro tipo de dano físico.

Ameaça

INSTITUTO FEDERAL
SANTA CATARINA

É um agente externo que pode trazer riscos a e causar danos em seu computador. Consequentemente quebrar os princípios de segurança. Nesse caso é extremamente importante o uso de antivírus e firewalls para proteger seu sistema.

Vírus

INSTITUTO FEDERAL
SANTA CATARINA

São pequenos programas “maliciosos” que se instalados, podem danificar seu computador, deixando lento, muitas vezes fazendo com que o usuário perca a suas informações

Casos mais frequentes, são os usuários do Windows, visto que é o sistema operacional mais utilizado no mundo.

Esses programinhas levam esse nome, devido ao fato de se espalhar rapidamente, lembrando um vírus comum, bem como um vírus biológico que ataca o corpo humano, deixando o indivíduo debilitado.

Isso ocorre por conta de uma falha de segurança e acaba contaminando vários computadores.

Essa contaminação pode ser feita por e mail e até mesmo pela rede.

O Vírus age de forma discreta, muitas vezes o usuário acaba espalhando sem saber.

Segundo Campos (2007), “na gestão do controle de acesso, bloquear entradas de dados (arquivos), mídias, acesso à internet ou e-mails pessoais, no ambiente computacional é uma forma de minimizar as possibilidades de entrada de vírus, entretanto, nem todas as entradas podem ser fechadas, pois, claro, são necessárias para as atividades da empresa.”

Antivírus

INSTITUTO FEDERAL
SANTA CATARINA

Mecanismos de segurança devem ser montados para proteger as entradas que necessitam ficar abertas. Nesse caso, o firewall, bloqueando as portas lógicas de acesso à rede que não são necessárias, e principalmente o antivírus são as melhores opções para exercer essa função de proteção. Os antivírus garantem a integridade dos sistemas basicamente com três funções, no ponto de vista de Campos (2007): a) detecção – identificando a presença do vírus; b) prevenção – impedindo a atuação do vírus; c) reação – removendo o vírus.
Para uma boa atuação do antivírus é essencial que ele esteja sempre atualizado, entretanto, ainda assim não garante a integridade absoluta do sistema já que todos os dias surgem novos vírus e o intervalo entre o surgimento e a atualização abre uma “janela de fragilidade”.

Vulnerabilidade

INSTITUTO FEDERAL
SANTA CATARINA

É quando o ativo se encontra frágil diante das ameaças, podendo acarretar a quebra da segurança da informação.

Isso pode ocorrer por vários motivos, como instalações físicas mal feitas, funcionários despreparados, programas de segurança ultrapassados ou desatualizados ou simplesmente ausentes em seu computador.

“As vulnerabilidades podem advir de vários aspectos: instalações físicas desprotegida contra incêndios, inundações, e desastres naturais; material inadequado empregado nas construções; ausência de política de segurança para RH; funcionários sem treinamento e insatisfatório nos locais de trabalho; ausência de procedimento de controle de acesso e utilização de equipamentos por pessoal contratado; equipamentos obsoletos, sem manutenção e sem restrições para sua utilização; software sem patch de atualização e sem licença de funcionamento, etc”. (DANTAS, 2001, p.25-26)

5.5 Risco

INSTITUTO FEDERAL
SANTA CATARINA

Com relação a segurança, os riscos são condições que permitem acontecer danos e perdas de informações. Para evitar essas possíveis perdas, é necessário a elaboração de uma gestão de riscos, onde os riscos são determinados e classificados, sendo depois especificado um conjunto equilibrado de medidas de segurança que permitirá reduzir ou eliminar os riscos a que a empresa se encontra sujeita.

• 5.6 RISCO = (Ameaça) x (Vulnerabilidade) x (Valor do Risco)

INSTITUTO FEDERAL
SANTA CATARINA

Mesmo em fase inicial, é sempre bom a Organização estar ciente dos riscos que ela pode correr. Ciente disso, a administração deve fazer um investimento adequado, separando valores e riscos

As cinco maiores ameaças

INSTITUTO FEDERAL
SANTA CATARINA

Conficker/Downadup

O vírus chamado Conficker (Downadup) que surgiu no ano de 2008, ele e causa muitos problemas, como bloquear sites de empresas de segurança, impossibilitar a atualizações do sistema e de antivírus, o país mais atacados por esse vírus são é os Emirados Árabes Unidos.

Kilim

O Kilim é um vírus que funciona como uma extensão de navegadores é responsável por fazer posts indesejados e dar em nome de perfis nas redes sociais funcionando como um spam.

Sality

O Sality é um vírus que surgiu no ano de 2007, esse vírus faz com que programas que já vem instalados na máquina sumam, os últimos países que foram infectados por esse vírus foram o Paquistão, o Egito e Tunísia, ele pode detectar o antivírus e fechá-lo antes que aja.

Ramnit

O Ramnit é como o Sality mas a sua principal funcionalidade é de roubar informações, a maior parte das vítimas se encontra na Indonésia, no Paquistão, no Vietnã, na Tunísia e na Malásia.

Autorun

O Autorun é um vírus que infecta principalmente Pen drives e HDs externos, ele pode roubar dados, corrompê-los ou ate mesmo exclui-los, ele se encontra principalmente na Malásia, na Turquia, na Índia, no Brasil e em Taiwan.

Adicionar Os melhores antivírus para Windows

Para combater essas ameaças, listaremos alguns dos melhores antivírus atuais para Windows

Avg Internet Security

Um dos mais antigos e melhores antivírus existentes. A versão atual oferece segurança aos usuários de maneira eficaz, sem consumir recursos do seu computador.
Além de trazer firewal poderoso que avisa o usuário em caso de arquivos ou sites maliciosos.

Avast

O velho conhecido dos usuários, também listas entre os melhores atuais.Assim como o AVG, ele também não consome muitos recursos. Protege suas informações confidenciais. Sua versão gratuita é uma das mais utilizadas, mas a Premier é mais recomendada para quem prefere algo mais barato e seguro

INSTITUTO FEDERAL
SANTA CATARINA

Kaspersky

Apesar de listar entre os melhores, o Kaspersky é visto com um antivírus que consome muitos recursos do sistema, deixando o seu computador lento. A parte boa nisso tudo é que o mesmo tem a capacidade encontrar vulnerabilidades onde os demais não conseguem.

No entanto, tem a capacidade de suprir as necessidades em vários dispositivos para um mesmo usuário

BitDefender

Uma ótima opção para quem prefira algo mais silencioso, o qual não precise fazer verificações a todo momento.

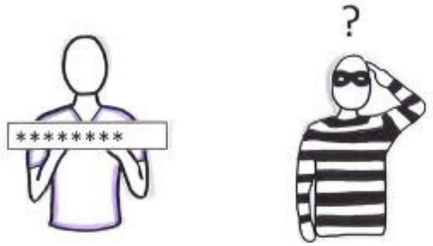
Fácil de ser configurado, oferece proteção contra vírus e ameaças na internet.

Microsoft Security Essentials

Antivírus feito pela própria Microsoft. Integrado nas versões mais recentes do Windows com o nome de Windows Defender.

Perfeito para quem não quer gastar com uma boa proteção

6 Políticas de senhas



INSTITUTO FEDERAL
SANTA CATARINA

É uma forma de identificação de acesso do usuário. Caso mais alguém tenha acesso a sua senha, poderá utiliza la de forma ilegal ou simplesmente se passar por você

Em algumas empresas, existem uma denominada política de senha, que respeitam algumas regras.

Tais como:

Validade da senha, que obriga o usuário a sempre atualizar a sua senha

Letras e números diferentes a cada atualização

Senhas com letras e números. Por exemplo: 4 letras e 4 números

Elaborar uma lista de senhas que não devem ser utilizadas

Ao elaborar uma senha, evitar usar nomes, sobrenomes, registros de documentos, telefones e etc.

Pois são informações importantes que poder ser obtidas com facilidade, até mesmo, servir de alvo p/ descobrir suas senhas.

6.1 Oque seria uma boa senha?

Uma boa senha, deve conter de 8 a 10 caracteres
Alternar entre letras e números, letras maiúsculas e minúsculas
Sempre lembrar da senha
Utilizar senhas diferentes em casa local, site com cadastros e etc.

6.2 Cuidados com sua senha

Verificar se ninguém se está olhando, enquanto você digita sua senha
Jamais fornecer sua senha a outra pessoa.
Evitar o acesso em computadores de terceiros

Alguns dos mais famosos casos de invasão de informação

INSTITUTO FEDERAL
SANTA CATARINA

Adrian "The Homeless Hacker" Lamo

O Hacker “Sem Teto”, ficou famoso após invadir os sistemas do New York Times, Google e Yahooo, foi preso em 2003, mas após um acordo, cumpriu 6 meses e prisão domiciliar. Hoje ele é conhecido como “dedo duro”, entre os hackers, após denunciar o vazamento de informações ao governo americano.

Owen "AKILL" Walker

Aos 17 anos Walker, já liderava uma rede de Hakcers, a qual foi responsável por invadir diversos computadores e roubar 20 milhões de dólares de contas correntes. Walker não participava diretamente da ação, ele apenas escrevia os códigos, arrecadando mais de 36 mil dólares. Hoje, Walker atua como um especialista em segurança de empresas de tecnologia.

Vladimir Levin

INSTITUTO FEDERAL
SANTA CATARINA

Um dos mais famosos e incríveis casos de ataque hacker da história. Visto que Levin, não utilizou a internet, mas sim um sistema de grampos telefônico, que ouvia os dígitos teclados pelos clientes, quando eles ligavam para seus bancos.

Com isso, Levin “arrebatou” mais de 10 milhões de dólares, dos quais, apenas 400 mil, foram recuperados, quando ele foi preso em 1998. Atualmente, ninguém tem informações sobre ele.

Usuários de Uber, tem seus dados expostos.

Mais de 50 milhões de usuários, entre passageiros e motoristas, tiveram seus dados(nome, endereço de e-mail e telefone) expostos, após um ciberataque.

A companhia tentou ocultar o caso, tanto que chegou a oferecer mais de 100 milhões de dólares para que os responsáveis pelo ato, mantivessem tudo no mais absoluto sigilo.

Ameaças de espionagem em dispositivos móveis

INSTITUTO FEDERAL
SANTA CATARINA

Há alguns anos, os celulares tinham como sua única função, receber e realizar chamadas, estando em qualquer lugar, região do país. Com o passar dos anos, as coisas foram se aprimorando, e hoje, com o avanço da tecnologia é possível ter acesso à internet, e-mail, redes sociais e etc.

Com isso, o risco de vazamento de informações e espionagem também aumentou. Segundo uma pesquisa realizada pela Symantec, 57% dos usuários de celulares no Brasil, são vítimas de crimes virtuais.

Os Spywares são considerados os aplicativos que oferecem um maior risco para os dispositivos.

Uma vez instalado, ele permite espionar comunicações e outras atividades no seu dispositivo, roubando informações do celular ou o tablet. Sua funcionalidade acaba atraindo a atenção dos usuários, por isso os Spywares estão sempre presentes no mercado virtual. No entanto, essas pessoas acabam não tendo conhecimento do que esses aplicativos podem ocasionar.

Os riscos são vários, Desde um monitoramento de localização, que em alguns casos, pode ocasionar até um “falso sequestro” até um roubo de informações de acesso a e-mail ou rede social

Mas como evitar esses tipos de ameaças?

INSTITUTO FEDERAL
SANTA CATARINA

Estar a tento as ofertas de aplicativos, que oferecem segurança a seu dispositivo. Verificar sempre se a fonte é de confiança.
Sempre ter seu dispositivo próximo, onde você o possa ver o tempo todo. Pois criminosos virtuais conseguem instalar aplicativos maliciosos em pouquíssimo tempo.
Sempre tenha um backup em seu dispositivo, caso precise restaurá-lo
Somente permita a administração remota se ela for necessária.
Jamais clicar em links “suspeitos” que chegam em seu e-mail ou por SMS.

7 CONCLUSÃO

Com o uso frequente de computadores em nosso dia a dia,é recomendado aos os usuários alguns princípios básicos de segurança da informação.
Tais como, o uso de um bom antivírus, uma limpeza de histórico (considerando principalmente que não esteja em seu computador pessoal),evitar compartilhamento de fotos ou arquivos pessoais em computadores públicos, atos que possam por em risco a sua integridade.