FAC U L DA D E

CERRADO

Ana Carolina Nascimento Alves

André Ferreira Nascimento Arthur

Barbosa Pinheiro

Daniel Cardoso Jersey Dielly

Diniz de Sousa

Emanoela Alves Silva

Gabriel de Sousa Gonçalves

João Victor Nascimento

Mateus Lima Lopes

Rosa Cristina do Nascimento Moreira

SEGURANÇA DE INFORMAÇÃO E SEUS PRINCÍPIOS

Brasília
2021

Ana Carolina Nascimento Alves
André Ferreira Nascimento
Arthur Barbosa Pinheiro
Daniel Cardoso Jersey
Dielly Diniz de Sousa
Emanoela Alves Silva
Gabriel de Sousa Gonçalves João
Victor Nascimento
Matheus Lima Lopes
Rosa Cristina do Nascimento Moreira

SEGURANÇA DA INFORMAÇÃO E SEUS PRINCÍPIOS

Relatório apresentado ao curso ao Curso Superior de Gestão Pública da Faculdade Cerrado, em cumprimento às Exigências legais como requisito parcial à obtenção título de tecnólogo na área de Gestão Pública.

Professor orientador: Wesley Augusto Louzeiro.

Brasília
2021

Dedicamos esse projeto aos nossos familiares que sempre nos apoiou e caminhou junto com a gente, para que pudéssemos sempre enfrentar as adversidades e trabalhos, que aconteceu durante o curso.

AGRADECIMENTOS

Agradecemos aos nossos familiares e colegas que caminharam junto conosco em toda nossa trajetória acadêmica,nossos agradecimentos também a instituição de ensino, que nos proporcionou ao longo do curso, professores que foram essenciais em nossas trajetórias acadêmica.

RESUMO

O trabalho teve como objetivoestudaras práticas, habilidades, recursos e mecanismos que são utilizadas para proteger sistemas de qualquer tipo de ataques, prevenir que usuários tenha perda ou sequestro de dados, hoje a tecnologia estar inserida em nossas vidas, por meio de celulares, tablets, notebooks, câmeras, contas. Apesar de ter pessoas que se relacionam com a tecnologia, sabem manusear o que precisamas mesmo assim ainda é normal ver pessoas leigas quando o assunto é por trás da profundidade que a tecnologia pode nos proporcionar, esse assunto nunca pode ser deixado de lado, principalmente para os gestores quesão ferramentas essenciais para qualquer negócio, para interferir em atividades. Para alcançar resultados e ao mesmo tempo conseguir manter sua boa reputação em uma empresa, e para tudo isso qualquer pessoa deve estar por dentro da segurança da informação.

Palavras Chave: Conhecimento. Compreender. Sucesso.

ABSTRACT

The aim of thisstudywastostudy the practices, skills, resourcesandmechanismsthat are usedtoprotect systems fromanytype of attacks, preventusersfromlosingorhijacking data, today the technologyisinserted in ourlives, throughcellphones, tablets, notebooks, cameras, beads. Despitehavingpeoplewho relate totechnology, theyknowhowtohandlewhattheyneedbutevenso it is still normal toseelaypeoplewhen the subjectisbehind the depththattechnologycanprovideus, thissubjectcanneverbeleftaside, especially for managers, as they are essential tools for any business, to interfere in activities. In ordertoachieveresultsandat the same time managetomaintain its goodreputation in a company, and for allthis, anyoneshouldhavetobeinsideinformationsecurity.

Keywords: Knowledge. Understanding.Success.

SUMÁRIO

1 INTRODUÇÃO

Neste trabalho apresentaremos os conceitos de Segurança da informação. O presente trabalho apresenta que isso nada mais é que vários mecanismos que existem para proteger sistemas de usuários que tendem a estar em perigo. Apresentamos conceitos, noções, gráficos e tabela de pesquisa para melhor entendimento do leitor.

A reflexão do tema traz um novo conhecimento sobre um assunto não comentado muito socialmente. Porém já vemos bastante esse tema nos dias de hoje, como por exemplo, no comércio eletrônico, que por mais que seja um processo perigoso é muito usado por milhões de usuários.

Desejamos com esse trabalho aumentar um pouco o conhecimento do leitor e que isso ajude na sua vida.

2 OBJETIVOS

2.1 Geral

O objetivo deste trabalho é analisar os princípios da segurança da informação e mostrar vários conceitos para a segurança de usuários que estão a todo momento expostos no mundo da tecnologia.

2.2 Objetivo Específico

Com base no objetivo geral, traçamos os seguintes objetivos específicos:

- Mostrar todos os Conceitos para a segurança do usuário;
- Controle de Acesso e segurança; • Apontar várias formas de incidentes computacional;
- Formas de seguranças Admissíveis.

3 DESENVOLVIMENTO

A Sistema de informação são vários mecanismos que existem para proteger sistemas de usuários que tendem a estar em perigo, é muito importante estar presente em empresas, pois as empresas necessitam de sua segurança, claro que nenhuma empresa vai estar 100% segura e estar livre de ameaças por estar em constante inovação com a hardware e software.

"As mudanças na segurança cibernética vão requerer novos tipos de habilidades para fazer frente as ameaças, não é possível controlar tudo igualmente, pois é preciso priorizar o que é mais importante" — Gartner (15 de novembro de 2017)

3.1 0 Conceito e Noções da Segurança dos Sistemas

Atualmente a infraestrutura e suportes sobre a internet se encontra critico, principalmente quando se trata em suportes do governo como, sistema de transportes, coordenações de finanças, esses problemas são só o retrato da má realização nos negócios pois influencia diretamente, como os governos disponibiliza para os cidadãos e com esses suportes na maioria das vezes falho fez com que aumentasse a habilidade de dispositivos e grupos que se conectam e tende a ficar mais expostos cada vez mais e ter um maior número de ameaças.

> O conceito da segurança de informação não se baseia somente em sistemas adaptados, a segurança de sistemas bancários hoje em dia é completamente diferente como antigamente, antes para você roubar de fato um banco, você teria que ir ao banco para conseguir efetuar o furto ou o roubo, hoje com o manuseio de dados pela internet qualquer pessoa do mundo que saiba os procedimentos pode roubar e atacar a segurança dos sistemas bancários. Armários e fechaduras hoje em dia são todas digitais, hoje é muito discutido pontos importantes para a segurança digital.

- Sistema Computacional - conjunto de dispositivos eletrônicos Hardware e

Software

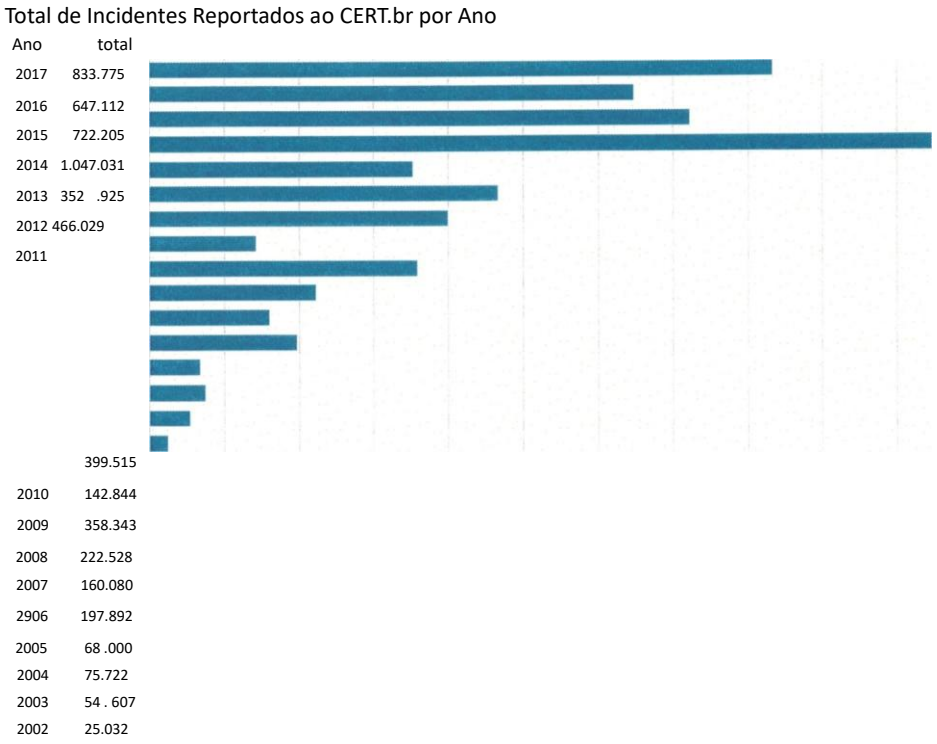
- Segurança de Rede na conexão entre elementos de computação

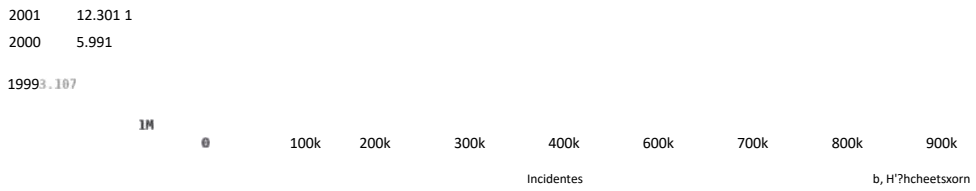
Essa são duas áreas que são muitas importantes no mundo da computação nos dias atuais, todas as áreas se juntam, agora irei citar o que pode fazer com que o sistema computacional sofra, de acordo com a RFC 2828 temos a:

- Ameaça: Uma potência para a violação de segurança quando a pessoa tem condição e a capacidade de quebrar a segurança e causar danos, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade.
- Ataque: O ataque e o conjunto da ameaça os dois estão interligados, é uma tentativa de burlar as regras dos serviços de segurança e de um sistema, usando uma técnica com eficiência.

3.2 Estatísticas e Gráficos sobre Acidentes de Segurança Computacional

O CERT.BR que significa Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil tem de proposito de acompanhar e fazer estatística sobre incidentes de segurança computacional, segundo o gráfico do CERT que foram reportaram incidentes durante o período do ano 2000 até 2017, de 6 mil em no ano 2000 esse número foi triplicado e cresceu para 833 mil o número foi triplicado, como mostra baixo o gráfico feito pelo CERT.



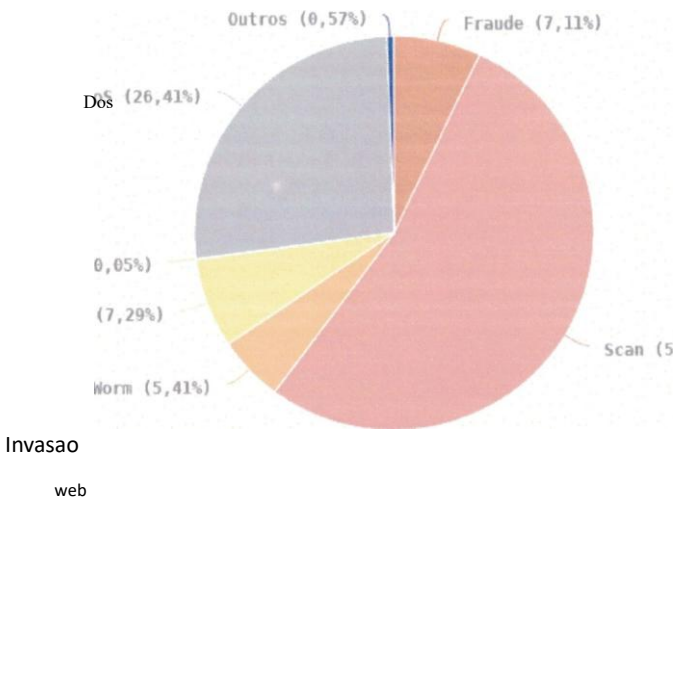


Com outro gráfico disponibilizado pela CERT que reportou incidentes durante todo o ano de 2017, podemos por meio desse gráfico podemos ter uma ideia dos principais tipos de incidentes de segurança computacional que são:

- Invasão é a tentativa de acessar sistemas não autorizado;
- Web é modificando um sistema, sem o ou consentimento do dono do sistema;
- Scan com notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores e quais alvos estão ativos para um possível ataque;
- Fraude segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé.com intuito de lesar ou ludibriar outrem, ou de não cumprir determinadodever; logro". Esta categoria engloba em notificações de tentativas de fraudes, em outras palavras são incidentes que ocorre uma tentativa de obter vantagem. Existe vários tipos de fraude nos dias de hoje como Cavalos de Troia, Páginas Falsas com a tentativa de fins financeiros.

Como diz no gráfico abaixo:

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2017
Tipos de ataque



3.3 Comércio Eletrônico

O comercio eletrônico hoje em dia é um setor que a todo ano cresce, um meio usado por várias pessoas, as transações na maioria das vezes é feita por desktops(computador) mas os crescimento do e-commerce, hoje a metade das buscas por produtos ocorre pelo celular, mas a compra ainda tende a ocorrer pelo computador. Apesar de ser um processo perigoso que tem processos em que devemos informar dados secretos e individuais e que está sujeito a interferências de terceiros não desejado. O portal do comercio eletrônico é enorme com várias empresas que abriram com o intuito só de vendas pela Web mas por trás desse comercio grande existe um transação simples do inicio como a parte em que o navegador/cliente acessa o portal eletrônico e o processo de efetuar e efetivar a compra e operação como, Verificar Negociante, receber pedido, receber pagamento e o processo final que é confirmar o pedido. O pagamento em comércio eletrônico pode ser feito diretamente com asinstituições financeiras através de boleto bancário, cartões de credito, transferências eletrônicas ou através de empresas terceirizadas especializadas em pagamentos, como PayPal,PagSeguro, BCash,

MercadoPago etc.

3.4 Combinações Para Proteger As Empresas

Os gastos que as empresas investem para a segurança da informação superam mais de 80 milhões, tudo isso com o intuito de proteger seus dados, e principalmente proteger seus clientes, empresas que tem um comercio eletrônico é exigido de seus clientes tecnologias mais modernas e com um acesso mais protegido e evitar fraudes indevidas, os principais métodos que as empresas implantam em suas empresas são:

- Proteção contra riscos "humanos", segundo os incidentes computacional a causa mais provável de vazamento interno é o usuário que acessa regularmente os recursos e dados da rede. De acordo com uma pesquisa da IBM em 74% dos incidentes, a falha do usuário que desempenha um papel decisivo para uma possível ataque, ameaça e epidemias de vírus, então as empresas devem ter uma proteção contra ataques de hackers, inspeção de tráfego, análise de registros e outros métodos de combate contra ameaças tecnológicas.

- Aumentando a capacitação de usuários, na maioria das vezes o usuário comete erro por falta de conhecimento e imprudência, então a estabilidade do sistema de proteção da informação para esses usuários, como treinar os funcionários até que decorem o regulamento de trabalhocom informações confidenciais e aprendendo quea gravidade de perdas e em caso de negligência ou não conhecimento, consolide a responsabilidade pessoal e financeira de cada funcionário.
- O Monitoramento dos direitos de acesso.
- A compreensão da hierarquia dos funcionários em relação aos níveis de acesso sempre, em pequenas empresas isso é muito falho, pois a falta de um administrador experiente, no qual as ferramentas padrão não serão suficientes para monitorar privilégios e gerenciar os direitos de acesso a todos os recursos e programas.

- A limitação dos direitos de acesso que é o "corte" de direitos: quanto menos possibilidades de realizar violações intencionais ou acidentais o usuário tiver, maior o nível de proteção da informação. Dois

procedimentos importantes precedem a limitação de direitos primeiro, é necessário fazer uma lista das pessoas com direitos legítimos de posse de informações críticas na empresa. Em segundo lugar regulamentar claramente as obrigações dos funcionários, definir os recursos e os documentos necessários para um processo de trabalho ininterrupto. Por exemplo, se um contador ficar sem acesso ao gerenciamento de tarefas do departamento de desenvolvimento e não tomar conhecimento sobre quais tarefas estão na lista do departamento de suporte técnico, o trabalho do departamento de contabilidade não será paralisado. Da mesma forma, se tirarmos de um engenheiro o acesso ao site corporativo para edição de notícias, o processo de desenvolvimento dos produtos também não será afetado

3.5 Segurança de Rede

Os usuários devem ter bastante medo dos riscos que ocorre no uso da internet, como banda larga seja fixa ou móvel, wi-fi e bluetooth, nos tempos de hoje é comum termos de vários mecanismos para ser oferecido a a Wi-Fi e Bluetooth, como dispositivos moveis, TV, sistema de áudio e eletrodomésticos. Independentemente do tipo da tecnologia explorada, ao se conectar a esses dois tipos e mecanismos a rede, estaremos sujeitos a ameaças, como: Furto de Dados

- Varredura
- Ataque de negação de serviço
- Ataque de força brutal
- Ataque de personaficação — que é quando um atacante introduz um dispositivo de rede, induzindo outros a se conectarem, fazendo assim com que eles tenham acesso a suas senhas e informações que ele pode trafegar tranquilamente.

4 CRONOGRAMA

Quadro 1 - Cronograma

	Junho	Julho	Agosto	Setembro	Outubro	Novembro
Escolha do tema						
Montagem do projeto						
pesquisas						

5 CONCLUSÃO

O sistema de informação não está relacionado apenas a sistemas computacionais,eletrônicos ou de armazenamento, no entanto, o conceito se aplica a proteção de dados e informações. Confidencialidade, disponibilidade e integridade são algumas das características básicas da segurança da informação, e podem ser considerados até mesmo atributos. Nos dias de hoje aprendemos diariamente a nos manter alerta durante o uso da internet para evitar problemas com proteção de dados em redes sociais, sites de compras (ecommerce), entre outros.

Este projeto teve um desenvolvimento que viabilizou para todos um resultado e uma boa reflexão sobre o tema, por meio de pesquisas usamos sempre no máximo analisar os principais aspectos que o tema pode propor, a profundidade do tema nos proporcionou um conhecimento, pois nesse projeto falamos sobre as noções de sistema de segurança da informação e por meio disso nós pudemos tirar uma conclusão significativa sobre o tema

REFERÊNCIA BIBIOGRÁFICA

12 Práticas Para a Segurança da Informação e Citação.Site Positivo. Brasil. 15 nov.2017. Disponível em:<https://www.meupositivo.com.br/panoramapositivo/seguranca-dainformacao>. Acessado 10/11/2018.

Conceitos da Segurança da Informação. Redação Oficina.Brasil, 26nov.2008. Disponível em:https://www.oficinadanet.com.br/artigo/1307/seguranca_da_informacao conceitos_e_mec anismos. Acessado 1 1/11/2018.

Citação do RFC 2828. Rede Grupo de Trabalho R. Shire. Brasil, 31 maio. 2000. Disponível em: <http://www.ietf.org/rfc/rfc2828.txt >. Acessado 15/11/2018.

Estatísticas e Gráficos. CERT.Brasil,20Março. 2017 .Disponível em: < https://www.cert.br/stats/>. Acessado 15/11/2018.

CeoloMairum.- . Fundamentos de Sistemas de Informação: MairumCeolo. Rio de Janeiro: SESES, 2014 . 112 a 120 p.

Comitê Gestor da Internet no Brasil.-. Cartilha de Segurança para Internet: CERT.br. São Paulo, Comitê Gestor da Internet no Brasil, 2012. 101 a 106 p.