FACULDADE IDEAL FACI WYDEN

SILVIO CEZAR DE SOUZA TEIXEIRA

MAINÁ DA SILVA TOMAZ

PROJETO DE PESQUISA

Belém

2022

SILVIO CEZAR DE SOUZA TEIXEIRA

MAINÁ DA SILVA TOMAZ

Vulnerabilidade em sistemas operacionais e dispositivos tecnológicos

Projeto de pesquisa do curso de graduação apresentado à Faculdade Ideal Faci Wyden, como requisito parcial para obtenção de aprovação na disciplina de Desenvolvimento de Software INTEGRADA

Belém

2022

Information security

Information security can be portrayed as a set of actions that ensures the conservation of confidentiality, integrity and availability of information and precious data, because confidential data of companies and people needs to be protected, because if left unprotected, those become the target of hackers and malware aimed at invading systems and retrieving unauthorized data, this document is meant for readers who are not familiar with basic data protection procedures.

SUMÁRIO

1 Introdução

Segurança da informação pode ser entendida como um conjunto de ações que assegura a conservação da confidencialidade, integridade e disponibilidade da informação e às informações por serem dados privilegiados de empresas e pessoas precisa-se ser protegido,pois deixando-os desprotegidos ,se torna alvo de ações maliciosas voltadas à invasão de sistemas. Entretanto algumas empresas contratam Hackers com objetivo de testar e proteger dados da empresa.

1.1 Justificativa

Justifica-se a escolha do tema frente a necessidade de discutir sobre segurança da informação, um tema tão comentado porém pouco pesquisado: é encontrada pouca literatura referente à usuários de sistemas de informação e segurança da informação, com a nova Lei Geral de Proteção de Dados entrando em vigor em 2020, há uma necessidade de alertar às pessoas de que a ética no armazenamento de dados é de grande importância. Outro fator é o crescimento atual do mercado de segurança da informação pois há cada ano é necessário intensificar a segurança seja em dispositivos móveis a mainframes.

1.2 Problemática

Quão prejudicial pode ser deixar seus dados vulnerável às malícias do cibercrime?

1.3 Objetivo Geral

Este projeto tem como objetivo fornecer uma visão geral sobre a segurança da informação dentro das organizações e aos usuários, visando proporcionar uma base

para que qualquer usuário possa iniciar seu processo de segurança ou, caso esse já exista, se possa melhorá-lo com as novas tendências de mercado.

1.4 Objetivo Específico

Conscientização das pessoas e de organizações a investir em metodologias que garantam a proteção, blindando os sistemas e as suas informações, pois, sem políticas adequadas os riscos de acessos indesejados, quebra de sigilo e fraudes serão problemas constantes.

"Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades do negócio" (ABNT NBR ISO/IEC 17799:2005, p. ix).

2 Bibliografia

Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 - Autores : Kees Hintzbergen e Jule Hintzbergen onde no livro é abordado a forma clara de abordagens, ou políticas, de gerenciamento de segurança da informação que muitas organizações podem analisar e implementar nos seus negócios.

Guerra Cibernética : A próxima ameaça a segurança e o que fazer a respeito - Richard A. Clarke e Robert K. Knake (2015) - apresenta um panorama surpreendente — e, ao mesmo tempo, convincente — no qual o uso de armas cibernéticas é uma questão concreta a ser considerada nas ações de Defesa Nacional.

Investigação Digital em Fontes Abertas: Alessandro Gonçalves Barreto (2017)
As atividades de inteligência de segurança pública e de investigação policial têm potencializado a utilização de fontes abertas para produção de conhecimento e/ou provas. Vários são os casos bem-sucedidos de prisão, localização de foragidos, identificação de testemunhas e produção de provas com informações disponíveis livremente na web. A obra auxilia o leitor no processo de qualquer investigação moderna, em especial a criminal. Dentre as novidades, destaca-se a coleta de informações no Facebook e na Deep Web.

Segurança e redes sem fio 4 edição : Nelson Murilo de O. Rufino (2014)
O autor teve a ideia de proporcionar ao leitor tanto uma visão abrangente das características e peculiaridades de redes sem fio (notadamente a tecnologia Wi-Fi e também similares, como a Bluetooth) quanto o entendimento das vulnerabilidades

comuns associadas à tecnologia e aos seus riscos e das possibilidades de uso com maior segurança.

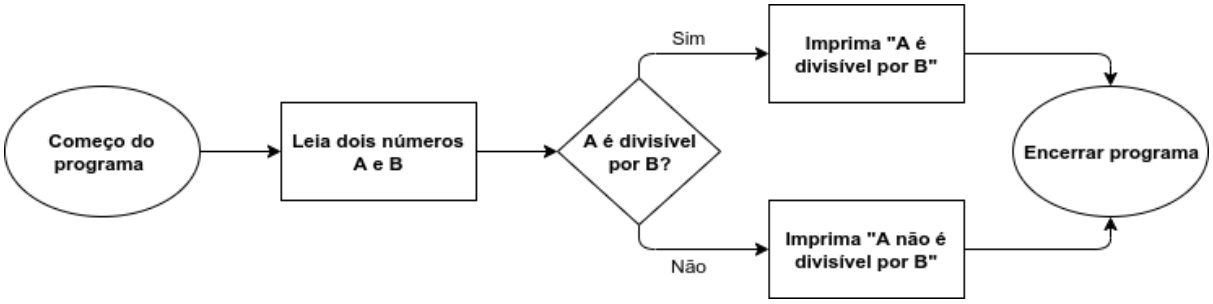
Segurança da informação: Por Edison Luiz Gonçalves Fontes, O livro explica o que é segurança da informação, o porquê de sua existência, e alguns procedimentos básicos e necessários para garanti-la dentro de uma organização. De leitura agradável e fácil compreensão, o livro mostra como a segurança da informação pode naturalmente fazer parte do dia-a-dia da corporação.

Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados - Pelos autores Carlos Cabral e William Okuhara Caprino, onde este livro é composto de uma série de artigos inéditos escritos por profissionais de destaque na área atuando no Brasil e no exterior e que entendem que Segurança da Informação não pode ser um "trilho" de maneira que imobilize a operação das organizações, mas, sim, uma "trilha", na medida em que a proteção é dosada por meio da análise dos riscos no percurso. O leitor poderá usar o conteúdo desta obra de forma não linear, como apoio para decidir qual caminho seguir, aproveitando não somente o conteúdo técnico aqui contido, como também a experiência e as lições aprendidas de cada autor.

3 Programação

Como a maioria das atividades que fazemos no dia a dia, programar também possui modos diferentes de se fazer. Esses modos são chamados de paradigmas de programação e, entre eles, estão a programação orientada a objetos (POO) e a programação estruturada. Quando começamos a utilizar linguagens como Java, C#, Python e outras que possibilitam o paradigma orientado a objetos, é comum errarmos e aplicarmos a programação estruturada achando que estamos usando recursos da orientação a objetos.

- sequências: são os comandos a serem executados
- condições: sequências que só devem ser executadas se uma condição for satisfeita (exemplos: if-else, switch e comandos parecidos)
- repetições: sequências que devem ser executadas repetidamente até uma condição for satisfeita (for, while, do-while etc)



alternativa a essas características da programação estruturada. O intuito da sua criação também foi o de aproximar o manuseio das estruturas de um programa ao manuseio das coisas do mundo real, daí o nome "objeto" como uma algo genérico, que pode representar qualquer coisa tangível.

3.1 O que são classes e objetos?

Imagine que você comprou um carro recentemente e decide modelar esse carro usando programação orientada a objetos. O seu carro tem as características que você estava procurando: um motor 2.0 híbrido, azul escuro, quatro portas, câmbio automático etc.

Exemplo em Python

class Carro:

def __init__(self, modelo):

self.modelo = modelo;

self.velocidade = 0

def acelerar(self):

 # Codigo para acelerar o carro

def frear(self):

 # Codigo para frear o carro

def acenderFarol(self):

 # Codigo para acender o farol do carro

4. Enfim, e a Web?

Usamos as linguagens de programação para nos comunicar com os computadores. Ou seja, da mesma maneira que estudamos o inglês para falar com pessoas de outros países, temos que aprender a língua dos computadores se quisermos que as máquinas respondam aos nossos comandos. E programar é justamente se comunicar nesta outra língua, que o computador consegue interpretar e devolver um resultado ao usuário.

- **HTML:** determina a estrutura dos elementos. Funciona como se fosse o texto da página.
- **CSS:** define a aparência do website, cores, formas, bordas, fontes, etc. É o que dá o estilo, deixando o site mais bonito e atraente.
- **JavaScript:** responsável pelas interações e por como os elementos irão se comportar dentro da página.
-

“Há muitos editores de código no mercado e a escolha depende de cada programadora. Um dos que indicamos é o Atom, pois é gratuito e desenvolvido pela equipe do GitHub, que são ativistas da internet opensource. E nós amamos esse tipo de iniciativa democrática, não é mesmo?”

4.1 Engenheiro de software

Enquanto os engenheiros aprendem sobre os processos envolvidos em desenvolver e manter programas, os cientistas da computação têm estudos mais focados na teoria, ligados à modelos matemáticos, algoritmos e lógica dos processos.

Com cada vez mais empresas automatizando seus serviços e criando suas próprias plataformas digitais, a profissão de engenheiro de software foi considerada a 2ª melhor da área de TI em crescimento e remuneração, segundo o site especializado em carreiras de tecnologia, CareerCast.

O software consiste na “parte lógica” do computador, que inclui sistema operacional e programas. Então, basicamente, estes profissionais projetam e guiam o desenvolvimento de programas, aplicativos e sistemas, de forma que atendam aos requisitos e cumpram as funções determinadas.

Entre as principais atribuições do engenheiro de software, estão:

- Desenvolver softwares e apps
- Gerenciar projetos ligados aos softwares
- Arquitetar o design estrutural dos programas
- Realizar testes nos sistemas

5. Segurança Web

Confidencialidade

A informação só pode ser acessada e utilizada por pessoas autorizadas e devidamente credenciadas.

Confiabilidade

É o caráter de fidedignidade da informação. Deve ser assegurada ao usuário a boa qualidade da informação com a qual ele estará trabalhando.

Integridade

É a garantia de que a informação estará completa, exata e preservada contra alterações indevidas, fraudes ou até mesmo com a sua destruição.

Disponibilidade

É a certeza de que a informação estará acessível e disponível em escala contínua para as pessoas autorizadas.

Autenticidade

É saber, por meio de registro apropriado, quem realizou acessos, atualizações e exclusões de informações, de modo que haja confirmação da sua autoria e originalidade.

Como vimos, todos os aspectos da segurança da informação precisam estar em vista e serem tratados com o máximo de critério e cuidado para que os gestores e colaboradores da empresa sejam beneficiados, assim como os públicos externos — parceiros e clientes — que interagem com ela.

5.1 PRÁTICAS

Detectar vulnerabilidades de hardware e software

A defasagem tecnológica torna vulnerável toda a infraestrutura e a segurança de TI e gera consequências tais como: perda de competitividade, ineficiência operacional, insatisfação de colaboradores e clientes, morosidade e ineficácia do processo decisório.

Os equipamentos estão sujeitos a defeitos de fabricação, instalação ou utilização incorreta, quebra ou queima de componentes e má conservação, o que pode comprometer um ou mais dos princípios da segurança da informação.

- **Cópias de segurança**

  O backup pode ser armazenado em dispositivos físicos — servidores de backup, CD, pen drive, HD externo — ou em nuvem.

- **Redundância de sistemas**

A alta disponibilidade das informações é garantida com a redundância de sistemas, ou seja, quando a empresa dispõe de infraestrutura replicada — física ou virtualizada.

- **Eficácia no controle de acesso**

portas acionadas por senha (misto físico/lógico). Já os principais mecanismos lógicos.

- **Firewall**

Ele trabalha segundo protocolos de segurança (TCP/IP, IPSec, HTTP etc.)

- **Assinatura digital**

É uma forma de identificação do usuário que está acessando aos recursos de TI, ela dá validade legal aos documentos digitais, assegurando a autenticidade do emissor da informação.

- **Biometria**

O acesso às informações somente é liberado para a pessoa autorizada, levando em consideração as suas características físicas (impressão digital, voz ou padrões da íris do olho ou do rosto inteiro.).

População alvo: População de interesse. Exemplo: pessoas residentes

no Brasil no mês de Agosto de 2019.

População referenciada: subconjunto da População alvo para a qual está

disponível um sistema de referência. Exemplo: pessoas residentes no

Brasil no mês de Agosto de 2019 das quais se possui o endereço correto.

População amostrada: subconjunto da População referenciada da qual, efetivamente, é possível retirar uma amostra. Exemplo: pessoas

residentes no Brasil no mês de Agosto de 2019 das quais se possui o

endereço correto e não residem em localidades de difícil acesso.

Sistema de referência: banco de dados contendo informações sobre os elementos da população referenciada (organizado de modo a permitir

implementar o PA).

Unidade elementar: elemento da população portadora das informações de interesse. Exemplo: Eleitor brasileiro.

Unidade amostral: entidade que será selecionada no processo de amostragem. Pode ser formada por uma ou mais de unidades elementares.

Exemplo: Domicílio.

Unidade resposta: entidade que fornece as informações de interesse relacionadas a unidade amostral. Exemplo: Pessoa responsável pelo sustento do domicílio.

1- Segurança de computadores ou *cibersegurança*

É a proteção de sistemas de computador contra roubo ou danos ao hardware, software ou dados eletrônicos, bem como a interrupção ou desorientação dos serviços que fornecem. O campo está crescendo em importância devido à crescente dependência de sistemas de computadores, internet e redes sem fio, como Bluetooth e Wi-Fi, e devido ao crescimento de dispositivos **"inteligentes"**. Devido à sua complexidade, tanto em termos de política quanto de tecnologia, é também um dos maiores desafios do mundo contemporâneo.

Também chamada de segurança cibernética, a cibersegurança é a prática de proteger informações e dados que chegam ao usuário da organização, provenientes de fontes externas e somente por meio de protocolos de internet. Se alguém do outro lado do mundo conseguir invadir a rede de uma empresa e violar seu sistema, essa companhia precisará de uma melhor segurança cibernética.

Desenvolvido no final da década de 60 para os sistemas Unix, o protocolo de comunicação TCP/IP tinha como objetivo facilitar o compartilhamento de informações e não previa uma função comercial. Em virtude destas características, apresenta falhas clássicas de segurança. Sem um modelo formalizado de segurança, as organizações estão sujeitas a perda ou alteração de informações, acessos indevidos e outros problemas. Ao optar pela ampliação do uso comercial da

super estrada, as empresas devem se conscientizar que operações 100% seguras estão fora da realidade, pelo menos por enquanto.

2.0 Backdoor

Uma backdoor em um sistema de computador, *um sistema criptográfico ou um algoritmo*, é qualquer método secreto de contornar a autenticação normal ou os controles de segurança. Eles podem existir por uma série de razões, incluindo pelo design original ou configuração inadequada. Eles podem ter sido adicionados por uma parte autorizada para permitir algum acesso legítimo ou por um invasor por motivos maliciosos; mas, independentemente dos motivos de sua existência, eles criam uma vulnerabilidade. Backdoors podem ser muito difíceis de detectar, e a detecção de backdoors geralmente é feita por alguém que tem acesso ao código-fonte do aplicativo ou conhecimento íntimo do **Sistema Operacional do computador.**

2.1 Ataques de acesso direto

Um usuário não autorizado que obtém acesso físico a um computador provavelmente é capaz de copiar dados diretamente dele. Eles também podem comprometer a segurança fazendo modificações no sistema operacional, instalando software worms, keyloggers, dispositivos de escuta ou usando microfone sem fio. Mesmo quando o sistema está protegido por medidas de segurança padrão, elas podem ser contornadas inicializando outro sistema operacional ou ferramenta de um CD-ROM ou outra

mídia inicializável. Criptografia de disco e o padrão Trusted Platform Module são projetados para evitar esses ataques.

Algumas das coisas que os cibercriminosos tentam fazer pela Internet são:

- Roubar informações
- Corromper informações
- Atacar sistemas ou equipamentos
- Roubar identidade
- Vender dados pessoais
- Roubar dinheiro

2.2 Tipos de hackers

White Hats*:* são conhecidos como *hackers* éticos. É uma categoria que possui pesquisadores e operadores de segurança para rastrear e monitorar ameaças de forma ativa. Quando descobertas, esses *hackers* notificam as empresas sobre vulnerabilidades, mas sem levá-las ao público.

2. **Black Hats***:* essa categoria tem amplo conhecimento sobre como invadir redes de computadores, ignorar protocolos de segurança das empresas e em escrever *malwares*. A principal motivação dos *Black Hats*, ao invadir empresas, é ganho

pessoal ou financeiro, além da espionagem cibernética.

3. **Gray Hats***:* é um *hacker* que explora uma falha de segurança em um sistema de computador ou produto para chamar a atenção da empresa. É uma pessoa que age sem intenção maliciosa, mas com o objetivo de melhorar a segurança do sistema e da rede. Ao contrário do *White Hat*, essa categoria divulga publicamente essas brechas de segurança, o que pode permitir que criminosos explorem isso.

4. **Cracker:** o termo *"cracker"* foi criado pelos próprios *hackers* para diferenciar as atividades exercidas por cada categoria. Um cracker tem muito conhecimento em informática e usa isso para quebrar (daí o termo *crack*) sistemas de segurança (e monetizar em cima disso) e de softwares (fomentando a pirataria).

Script Kiddies*:* são pessoas que rejeitam algumas premissas mantidas por *hackers* profissionais, tais como: busca de conhecimento, educação e promoção de habilidades. Geralmente utilizam programas escritos por outros *hackers* porque eles não têm habilidades para escrever os próprios códigos. Esta categoria foca seus ataques em sistemas e redes de computadores e sites de internet.

3.0 Reduzindo Vulnerabilidades

Embora a verificação formal da correção dos sistemas de computador seja possível, ainda não é comum pois há muitos tipos de hackers que conseguem burlar o sistema e os sistemas operacionais verificados formalmente incluem L4, e SYSGO do PikeOS- mas constituem uma porcentagem muito pequena do mercado.

A autenticação de dois fatores é um método para mitigar o acesso não autorizado a um sistema ou informações confidenciais. Requer uma senha ou PIN e um cartão, Isso aumenta a segurança, pois uma pessoa não autorizada precisa de ambos para obter acesso.
Ataques de engenharia social e acesso direto ao computador (físico) só podem ser evitados por meios que não sejam de computador, o que pode ser difícil de aplicar, em relação à confidencialidade das informações. O treinamento é frequentemente envolvido para ajudar a mitigar esse risco, mas mesmo em ambientes altamente disciplinados (por exemplo, organizações militares), os ataques de engenharia social ainda podem ser difíceis de prever e prevenir.
A inoculação, derivada da teoria da inoculação, visa prevenir a engenharia social e outros truques ou armadilhas fraudulentas, instilando uma resistência às tentativas de persuasão por meio da exposição a tentativas semelhantes ou relacionadas.
É possível reduzir as chances de um invasor mantendo os sistemas atualizados com patches e atualizações de segurança, usando um scanner de segurança Predefinição: Definition needed e / ou contratação de pessoas com experiência em segurança, embora nenhuma delas garanta a prevenção de um ataque. Os efeitos da perda / dano de dados podem ser reduzidos com ***backups e seguros cuidadosos.***

Por que a segurança em computadores é importante?

a segurança em computadores é uma medida que previne contra invasões e ameaças digitais, reduzindo os impactos negativos no negócio.

Sem essa consciência, você deixa vulnerável o trabalho de uma vida toda: seus projetos, suas estratégias, seus diferenciais — sem falar, claro, nas informações pessoais e comunicação de sua equipe.

Em um descuido, você pode ter dados de clientes e fornecedores roubados, trocas de mensagens e outras informações delicadas.
Além de ser péssimo para a imagem da empresa, o gestor vai precisar encarar as consequências da LGPD, a Lei brasileira de Proteção de Dados, com aplicação prevista a partir de 2020.

Projeto na metodologia RUP

RUP (Rational Unified Process), traduzido em Processo Unificado Rational ou comumente falado “Processo Unificado” foi criado pela Rational Software Corporation, mas em 2003 foi adquirida pela IBM.

Metodologias são práticas que oferecem técnicas e rotinas criadas para aumentar a produtividade e dar mais coesão e coerência para o desenvolvimento de software. Continuando com a série de artigos sobre metodologias, essas que nos ajudam a ter mais qualidade e agilidade no desenvolvimento de software, vamos abordar neste artigo a metodologia RUP. Caso você queira ver outras metodologias, já abordamos aqui as metodologias Scrum, Crystal e RAD.

O RUP organiza o desenvolvimento em 4 fases bem direcionadas, contendo em cada uma delas no mínimo uma iteração, ou seja, um ciclo de vida, são nessas iterações que são mostradas ao cliente o andamento da produção para que ele possa validar e assim liberar a continuação do desenvolvimento. São elas:

- Concepção: define o escopo do software. É uma fase preliminar, é nessa etapa que se concentra o levantamento de requisitos, define preços e prazos da entrega do sistema e onde se avalia os possíveis riscos.

- Elaboração: plano do projeto, especificação de características e arquitetura. Aqui todas as análises de riscos são aprofundadas, como também os custos.

- Construção: ocorre a codificação do software.

- Transição: implantação do software, assegurando que ele esteja disponível aos usuários finais. Nesta fase está incluída os testes e o treinamento dos usuários.

Apesar de parecer um modelo em cascata, na verdade cada fase é composta de uma ou mais iterações, o que se assemelha a um modelo em espiral e abordam algumas poucas funções do sistema. Isto reduz o impacto de mudanças, pois quanto menor o tempo, menor a probabilidade de haver uma mudança neste período para as funções em questão.

O objetivo do RUP é atender as necessidades dos usuários garantindo uma produção de software de alta qualidade que cumpra um cronograma e um orçamento previsíveis. Assim, o RUP mostra como o sistema será construído na fase de implementação, gerando o modelo do projeto e, opcionalmente, o modelo de análise que é utilizado para garantir a robustez. O RUP define perfeitamente quem é responsável pelo que, como as coisas deverão ser feitas e quando devem ser realizadas, descrevendo todas as metas de desenvolvimento especificamente para que sejam alcançadas.

Modelagem de negócios: os processos de negócios são modelados com a utilização de casos de uso de negócio;

Requisitos: os casos de usos são criados para modelar os requisitos do software;

Análise e projeto: cria-se um modelo de projeto com base em modelos de arquitetura, de componente, de objeto e de sequência;

Implementação: os componentes do software são implementados;

Teste: o teste é um processo iterativo e é efetuado em conjunto com a implementação do sistema;

Implantação: cria-se uma versão do produto e instala-a no local de trabalho dos usuários;

Gerenciamento de configuração e mudanças: esse workflow serve como apoio à gerência do projeto em relação às mudanças no sistema;

Gerenciamento de projetos: esse workflow de apoio gerencia o processo de desenvolvimento do software;

Ambiente: este workflow relaciona-se à disponibilizado.

Com base nestes recursos a adoção do RUP pode ser feita de mais de uma maneira. Um extremo seria usar o RUP à risca, ou seja, aplicar todos os métodos e processos exatamente como são propostos. A vantagem desta abordagem é que nada deve ser alterado, pois o RUP é bem completo e detalhado. Porém existe um preço a ser pago, pois o RUP na íntegra é complexo. Esta abordagem implicaria em treinamentos, projetos piloto, etc. Propostas de projetos de adoção do RUP são descritos no próprio produto.

O extremo oposto seria adotar outro modelo de processo mais simples ou conhecido (o atual, se existir) e utilizar o material do RUP como fonte de referência complementar para assuntos não abordados em outro modelo como, por exemplo, os modelos de documentos. A primeira abordagem é interessante para empresas que precisam de uma grande formalização do processo de desenvolvimento de software e cujo método atual seja totalmente inadequado ou inexistente. A segunda abordagem seria interessante para quem já tem alguma metodologia que considera adequada, mas que tem deficiência em alguma área como, por exemplo, suporte a UML. Soluções intermediárias também são possíveis.

Vulnerabilidade em sistemas operacionais e dispositivos tecnológicos

Segurança da informação pode ser entendida como um conjunto de ações que assegura a conservação da confidencialidade, integridade e disponibilidade da informação e às informações por serem dados privilegiados de empresas e pessoas precisa-se ser protegido, pois deixando-os desprotegidos, se torna alvo de ações maliciosas voltadas à invasão de sistemas. Entretanto algumas empresas contratam Hackers com objetivo de testar e proteger dados da empresa. 1.1 Justificativa Justifica-se a escolha do tema frente a necessidade de discutir sobre segurança da informação, um tema tão comentado porém pouco pesquisado: é encontrada pouca literatura referente à usuários de sistemas de informação e segurança da informação, com a nova Lei Geral de Proteção de Dados entrando em vigor em 2020, há uma necessidade de alertar às pessoas de que a ética no armazenamento de dados é de grande importância. Outro fator é o crescimento atual do mercado de segurança da informação pois há cada ano é necessário intensificar a segurança seja em dispositivos móveis a mainframes.
1.2 Problemática Quão prejudicial pode ser deixar seus dados vulnerável às malícias do cibercrime?

1.3 Objetivo Geral Este projeto tem como objetivo fornecer uma visão geral sobre a segurança da informação dentro das organizações e aos usuários, visando proporcionar uma base para que qualquer usuário possa iniciar seu processo de segurança ou, caso esse já exista, se possa melhorá-lo com as novas tendências de mercado.
1.4 Objetivo Específico Conscientização das pessoas e de organizações a investir em metodologias que garantam a proteção, blindando os sistemas e as suas informações, pois, sem políticas adequadas os riscos de acessos indesejados, quebra de sigilo e fraudes serão problemas constantes.
“Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades do negócio” (ABNT NBR ISO/IEC 17799:2005, p. ix).
2 Bibliografia
Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 - Autores : Kees Hintzbergen e Jule Hintzbergen onde no livro é abordado a forma clara de abordagens, ou políticas, de gerenciamento de segurança da informação que muitas organizações podem analisar e implementar nos seus negócios. Guerra Cibernética : A próxima ameaça a segurança e o que fazer a respeito - Richard A. Clarke e Robert K. Knake (2015) - apresenta um panorama surpreendente — e, ao mesmo tempo, convincente — no qual o uso de armas cibernéticas é uma questão concreta a ser considerada nas ações de Defesa Nacional. Investigação Digital em Fontes Abertas : Alessandro Gonçalves Barreto (2017) As atividades de inteligência de segurança pública e de investigação policial têm potencializado a utilização de fontes abertas para produção de conhecimento e/ou provas. Vários são os casos bem-sucedidos de prisão, localização de foragidos, identificação de testemunhas e produção de provas com informações disponíveis livremente na web. A obra auxilia o leitor no processo de qualquer investigação moderna, em especial a criminal. Dentre as novidades, destaca-se a coleta de informações no Facebook e na Deep Web.
Segurança e redes sem fio 4 edição : Nelson Murilo de O. Rufino (2014) O autor teve a ideia de proporcionar ao leitor tanto uma visão abrangente das características e peculiaridades de redes sem fio (notadamente a tecnologia Wi-Fi e também similares, como a Bluetooth) quanto o entendimento das vulnerabilidades comuns associadas à tecnologia e aos seus riscos e das possibilidades de uso com maior segurança.
Segurança da informação : Por Edison Luiz Gonçalves Fontes , O livro explica o que é segurança da informação, o porquê de sua existência, e alguns procedimentos básicos e necessários para garanti-la dentro de uma organização. De leitura agradável e fácil compreensão, o livro mostra como a segurança da informação pode naturalmente fazer parte do dia-a-dia da corporação.
Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados - Pelos autores Carlos Cabral e William Okuhara Caprino, onde este livro é composto de uma série de artigos inéditos escritos por profissionais de destaque na área

atuando no Brasil e no exterior e que entendem que Segurança da Informação não pode ser um "trilho" de maneira que imobilize a operação das organizações, mas, sim, uma "trilha", na medida em que a proteção é dosada por meio da análise dos riscos no percurso. O leitor poderá usar o conteúdo desta obra de forma não linear, como apoio para decidir qual caminho seguir, aproveitando não somente o conteúdo técnico aqui contido, como também a experiência e as lições aprendidas de cada autor.

3 Metodologia e Práticas “ A importância da metodologia utilizada em uma pesquisa é justificada devido à necessidade de um embasamento científico adequado, buscando a melhor abordagem para esclarecer as questões da pesquisa “ (MIGUEL, 2010)

Confidencialidade A informação só pode ser acessada e utilizada por pessoas autorizadas e devidamente credenciadas. Confiabilidade É o caráter de fidedignidade da informação. Deve ser assegurada ao usuário a boa qualidade da informação com a qual ele estará trabalhando. Integridade É a garantia de que a informação estará completa, exata e preservada contra alterações indevidas, fraudes ou até mesmo com a sua destruição. Disponibilidade É a certeza de que a informação estará acessível e disponível em escala contínua para as pessoas autorizadas. Autenticidade É saber, por meio de registro apropriado, quem realizou acessos, atualizações e exclusões de informações, de modo que haja confirmação da sua autoria e originalidade. Como vimos, todos os aspectos da segurança da informação precisam estar em vista e serem tratados com o máximo de critério e cuidado para que os gestores e colaboradores da empresa sejam beneficiados, assim como os públicos externos — parceiros e clientes — que interagem com ela.

PRÁTICAS Detectar vulnerabilidades de hardware e software A defasagem tecnológica torna vulnerável toda a infraestrutura e a segurança de TI e gera consequências tais como: perda de competitividade, ineficiência operacional, insatisfação de colaboradores e clientes, morosidade e ineficácia do processo decisório. Os equipamentos estão sujeitos a defeitos de fabricação, instalação ou utilização incorreta, quebra ou queima de componentes e má conservação, o que pode comprometer um ou mais dos princípios da segurança da informação. ➢ Cópias de segurança O backup pode ser armazenado em dispositivos físicos — servidores de backup, CD, pen drive, HD externo — ou em nuvem. ➢ Redundância de sistemas A alta disponibilidade das informações é garantida com a redundância de sistemas, ou seja, quando a empresa dispõe de infraestrutura replicada — física ou virtualizada. ➢ Eficácia no controle de acesso portas acionadas por senha (misto físico/lógico). Já os principais mecanismos lógicos. ➢ Firewall Ele trabalha segundo protocolos de segurança (TCP/IP, IPSec, HTTP etc.) ➢ Assinatura digital É uma forma de identificação do usuário que está acessando aos recursos de TI, ela dá validade legal aos documentos digitais, assegurando a autenticidade do emissor da informação. ➢ Biometria O acesso às informações somente é liberado para a pessoa autorizada, levando em consideração as suas características físicas (impressão digital, voz ou padrões da íris do olho ou do rosto inteiro.).

Amostragem
População alvo: População de interesse. Exemplo: pessoas residentes no Brasil no mês de Agosto de 2019.
População referenciada: subconjunto da População alvo para a qual está disponível um sistema de referência. Exemplo: pessoas residentes no Brasil no mês de Agosto de 2019 das quais se possui o endereço correto.
População amostrada: subconjunto da População referenciada da qual, efetivamente, é possível retirar uma amostra. Exemplo: pessoas residentes no Brasil no mês de Agosto de 2019 das quais se possui o endereço correto e não residem em localidades de difícil acesso.
Sistema de referência: banco de dados contendo informações sobre os elementos da população referenciada (organizado de modo a permitir implementar o PA).
Unidade elementar: elemento da população portadora das informações de interesse. Exemplo: Eleitor brasileiro.
Unidade amostral: entidade que será selecionada no processo de amostragem. Pode ser formada por uma ou mais de unidades elementares.
Exemplo: Domicílio.
Unidade resposta: entidade que fornece as informações de interesse relacionadas a unidade amostral. Exemplo: Pessoa responsável pelo sustento do domicílio.

Conclusão

Após esta intensa pesquisa, foi constatado que há muito com o que se preocupar quanto a segurança dos dados profissionais e pessoais. Esperando que atinja o máximo de pessoas possíveis para que possam armazenar seus dados com a devida segurança, como foi visto, a segurança da informação depende de tecnologias, mas também de pessoal preparado. A segurança em computadores é uma área da Tecnologia que, assim como aumentam os dispositivos e formas de conexão, aumentam as ameaças e vulnerabilidades digitais.
Dessa forma, a empresa deve tomar medidas necessárias para evitar ter suas informações e arquivos estratégicos expostos a invasores e programas maliciosos. Uma gestão de ativos eficaz é um primeiro passo para esse controle. Conte com um sistema que automatiza e facilita a rotina de sua TI, deixando os profissionais focados nas atividades que têm mais valor para sua empresa, como a segurança em computadores.

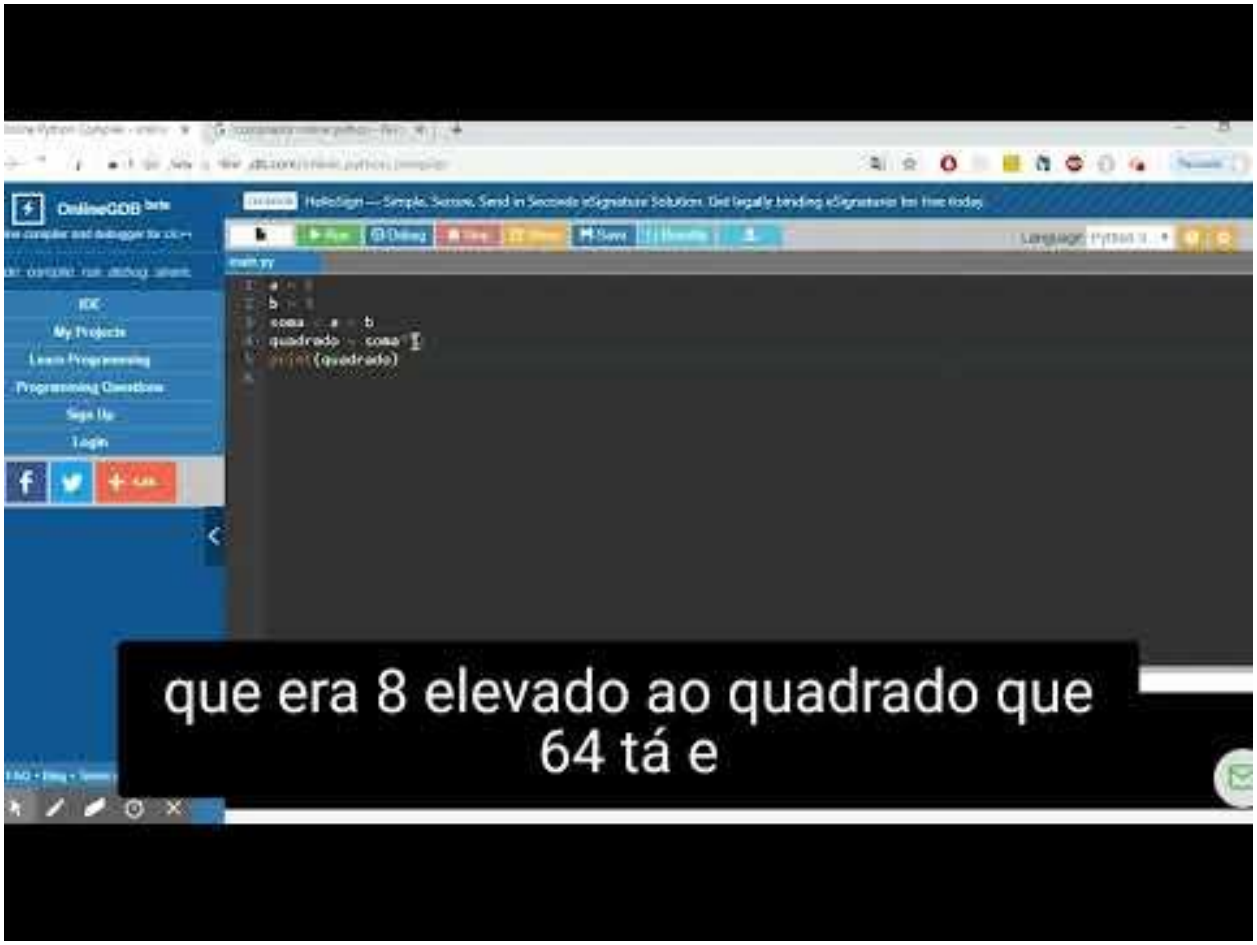
Afinal a Internet trabalha enviando informações de computador para computador até que as informações cheguem ao seu destino. Quando os dados são enviados do ponto A para o ponto B, todo computador entre eles tem oportunidade de observar o que está sendo enviado.
Em primeiro lugar, a empresa faz o levantamento e análise de riscos, estabelece uma política adequada à sua necessidade e começa o trabalho de peregrinação junto aos seus colaboradores. Depois, parte para a implementação. E as etapas seguintes estão relacionadas à monitoração e administração do plano.

A monitoração é fundamental para identificar comportamentos suspeitos e prevenir invasões. A política é voltada ao negócio e não à informática, plataformas ou ambientes de desenvolvimento. Isso requer que você digite informações em um formulário de pedidos, onde você deverá informar o número de seu cartão de crédito. Você sabe que a empresa de confecções em questão é reputável, portanto, você digita o seu número de cartão de crédito e outras informações e, em seguida, envia o formulário preenchido. Suas informações passam de computador para computador no seu caminho para a empresa de confecções. Infelizmente, um dos computadores entre eles foi infiltrado por criminosos que observam a passagem dos dados por esse computador, até que vejam algo interessante, como o número de seu cartão de crédito.

Necessita de planejamento, mas também de ações efetivas. Exige que se conheça as ameaças e os riscos, mas também a própria organização e acima de tudo o negócio, pois a segurança da informação existe em função do negócio e das suas coisas pessoais.

VIDEO USANDO E EXPLICANDO PYTHON

CASO APAREÇA ALGUNS ERROS DE ORTOGRÁFIA NA LEGENDA, SENTIMOS MUITO POIS ESTAVAMOS USANDO UM PROGRAMA ON-LINE.



Referências (obrigatório)

https://www.totvs.com/blog/seguranca-da-informacao/
https://ecoit.com.br/seguranca-da-informacao/
https://www.portalgsti.com.br/seguranca-da-informacao/sobre/